Appendix eK

Answers To Review Questions/Exercises, Hands-On Projects, Case Projects And Optional Team Case Project By Chapter

John Vacca

CHAPTER 1: BUILDING A SECURE ORGANIZATION

Review Questions/Exercises

True/False

1. True
2. False
3. True
4. False
5. True

Multiple Choice

1. E
2. D
3. A
4. D
5. A

Exercise

Solution

The following is a partial exercise solution. The students should be able to expand on the following:

The SAT should examine: Access control policy; procedures addressing access enforcement and dual authorization; security plan; information system design documentation; information system configuration settings and associated documentation; list of privileged commands requiring dual authorization; list of approved authorizations (user privileges); and, other relevant documents or records.

Hands-on Project

Solution

The following is a partial project solution. The students should be able to expand on the following:

The SAT should examine: Access control policy; procedures addressing information flow enforcement; information system design documentation; information system configuration settings and associated documentation; information system baseline configuration; list of information flow authorizations; information system audit records; and, other relevant documents or records

Case Projects

Solution

The following is a partial project solution. The students should be able to expand on the following through extensive research:

The SAT should examine: Security assessment and authorization policies and procedures; and, other relevant documents or records. They should also interview organizational personnel with security assessment and authorization responsibilities.

Optional Team Case Project

Solution

The following is a partial project solution. The students should be able to expand on the following through extensive research:

The SAT should examine: Contingency planning policy; procedures addressing contingency operations for the information system; contingency plan; security plan; and, other relevant documents or records. They should also interview organizational personnel with contingency planning and plan implementation responsibilities.

CHAPTER 2: A CRYPTOGRAPHY PRIMER

Review Questions/Exercises

True/False

1. False
2. False
3. False
4. True
5. True

Multiple Choice

1. A, C
2. E
3. B
4. E
5. B

Exercise

Solution

The following is a partial exercise solution. The students should be able to expand on the following:

The risk manager should do the following to fix the problem:

1. Listen for signs of complexity.
2. Know which areas of crypto are very hard, and which are simple.
3. If your team has to do something tricky (and you know that randomness is very tricky) then encourage them to do it clearly and openly.
4. If you are dealing in high-security areas, remember that only application security is good enough.
5. Do not distribute your own fixes to someone else's.
6. A good high-security design always considers what happens when each component fails in its promise.
7. Teach your team to work on the problem, not the people.
8. Do not believe in your own superiority.
9. If you've made a mistake, own it.

Hands-on Project

Solution

The following is a partial project solution. The students should be able to expand on the following:

Random bit strings required for the generation of cryptographic keys should be obtained from an approved Random Bit Generator (RBG). The RBG should either provide full entropy output or have been instantiated at a security strength that meets or exceeds the security strength required to protect the data that will be protected by the key.

The output of the approved RBG should be used to either generate the key directly or used as a seed to generate the key according to approved criteria. An example of a key that can be directly generated is an AES or DSA private key; an example of a key that is generated from a seed is an RSA key, whereby the seed is used as a starting point to find a prime number that meets approved criteria. Thus, key generation is performed within a key-generating module (a cryptographic module in which keys are generated).

Case Projects

Solution

The following is a partial project solution. The students should be able to expand on the following through extensive research:

Asymmetric algorithms, also known as public key algorithms, require the use of asymmetric key-pairs, consisting of a private key and a corresponding public key. The key to be used for each operation depends on the cryptographic process being performed (digital signature generation or key establishment). Each public/private key pair is associated with only one entity; this entity is known as the key pair owner. The public key may be known by anyone, whereas the private key must be known and used only by the key pair owner. Key pairs should be generated by:

- The key-pair owner
- A trusted party that provides the key pair to the owner in a secure manner. The trusted party must be trusted by all parties that use the public key.

Optional Team Case Project

Solution

The following is a partial project solution. The students should be able to expand on the following through extensive research:

Symmetric key algorithms use a single key to apply cryptographic protection to information (transform plaintext data into ciphertext data using an encryption operation) and to remove or verify the protection. Keys used with symmetric key algorithms must be known by only the entities authorized to apply, remove or verify the protection, and are commonly known as secret keys. A secret key is often known by multiple entities that are said to share or own the secret key, although it is not uncommon for a key to be generated, owned and used by a single entity (for secure storage). A secret key should be generated by:

- One or more of the entities that will share the key.
- A trusted party that provides the key to the intended sharing entities in a secure manner. The trusted party must be trusted by all entities that will share the key.

CHAPTER 3: DETECTING SYSTEM INTRUSIONS

Review Questions/Exercises

True/False

1. True
2. True
3. True
4. False
5. False

Multiple Choice

1. B
2. A
3. C
4. A
5. C

Exercise

Solution

The following is a partial exercise solution. The students should be able to expand on the following:

Under normal conditions, the TCP sequence number changes whenever a host sends a packet to a new system. In the exhibit, us.us.us.44 and us.us.us.50 are targeted using the same TCP sequence number of 2410044679.

Hands-on Project

Solution

The following is a partial project solution. The students should be able to expand on the following:

The HEAD request is used obtain meta information about the requested resource without actually receiving the body of the file. Alternatively, the GET request actually retrieves the desired resource if it is found on the Web server. HEAD requests speed up the scan because the attacker's client application does not need to wait for the file to be retrieved when it is found on the targeted server.

Case Projects

Solution

The following is a partial project solution. Students should be able to expand on the project analysis through extensive research.

Logging in via telnet; as well as, accessing a CGI program via HTTP, requires the TCP connection to be fully established, which is difficult to accomplish if the attacker uses a spoofed source address. ICMP-based ping packets, however, are stateless, and are often spoofed, especially when targeting a network broadcast address in a Smurf-like attack.

Optional Team Case Project

Solution

The following is a partial solution to aid students in coming up with their own solution to solve this case:

If multiple systems on a LAN get assigned the same IP address, they will each try convincing their neighbors that their MAC address is the correct address for communicating with the IP address in conflict.

CHAPTER 4: PREVENTING SYSTEM INTRUSIONS

Review Questions/Exercises

True/False

1. False
2. True
3. False
4. False
5. False

Multiple Choice

1. A
2. E
3. A, B, D
4. D
5. B

Exercise

Solution

The following is a partial exercise solution. The students should be able to expand on the following:

You will need to examine the system and information integrity policy; procedures addressing information system monitoring tools and techniques; information system design documentation; information system monitoring tools and techniques documentation; information system configuration settings and associated documentation; information system protocols; and, other relevant documents or records. You will also need to examine the information system-wide intrusion detection and prevention capability.

Hands-on Project

Solution

The following is a partial project solution. The students should be able to expand on the following:

The company implemented a wide range of intrusion prevention capabilities/services to provide 24/7 monitoring, instant alerts and in-depth threat analysis. The company's intrusion prevention capabilities/services should put it on track to achieving ISO 27001 accreditation. The company also benefited by gaining 24/7 responsiveness and in-depth threat analysis; the IT team saved the expense of adding additional members to its staff; compliance with diverse local legislation secured customer confidence and drove the business; and, it's multinational parent company approved the security infrastructure.

Case Projects

Solution

The following is a partial project solution. The students should be able to expand on the following through extensive research:

To safeguard its network and the patients it serves, the medical center found a powerful IPS security solution that could continuously protect its high-throughput network without compromising network performance. The medical center's Intrusion Prevention System (IPS) provided the pervasive and proactive protection against malicious attacks by indicating where on the network a threat originated; thus, making it less difficult and time consuming for its IT staff to identify and cleanse infected departments before worms and viruses spread further. The IPS that was implemented was cost-effective and interoperated transparently with the medical center's multivendor infrastructure. More importantly, though, this IPS security solution did deliver pervasive protection in advance of threats; thus, leaving the medical center less vulnerable to evolving cyber attacks.

Optional Team Case Project

Solution

The following is a partial project solution. The students should be able to expand on the following through extensive research. The following is a list of the basic IPS questions that a company might ask their vendors:

1. Can your IPS security vendor refer you to customers who are running in-band devices with a high percentage of blocking filters turned on?
2. Does your IPS security solution block bad traffic without blocking good traffic?
3. Does your IPS security solution protect not just your network perimeter, but also key points within the core of your network?
4. Does your IPS security solution provide attack coverage that is broad and deep?
5. Does your IPS security solution provide the performance needed to deeply inspect traffic without slowing down the network or business applications?
6. Does your IPS solution support maximum network and application availability?
7. How accurate is your IPS security solution attack coverage?
8. How timely and up to date is the attack coverage?
9. Is your IPS security solution in-band?

CHAPTER 5: GUARDING AGAINST NETWORK INTRUSIONS

Review Questions/Exercises

True/False

1. False
2. False
3. True
4. True
5. False

Multiple Choice

1. B
2. A
3. C
4. E
5. C

Exercise

Solution

The following is a partial exercise solution. The students should be able to expand on the following:

The company focused on a high availability network security solution. For the size of their network, a firewall was the right solution for the job. They installed two of them, working in a secondary failover mode.

The installation itself was a breeze, because the security company was able to pre-build the configuration at their offices. They also used their standard, rule-of-thumb security set, based on their past work with the vendor sales engineers. In addition, the security company spent no more than 30 minutes customizing the security policies for the various proxy agents that were needed. In the end, they were able to create a very secure network environment pretty much out of the box.

Hands-on Project

Solution

The following is a partial project solution. The students should be able to expand on the following:

The solution services company provided firewalls at each school district location, for a total of 245 security appliances. This gave the school district full proxy firewall capabilities at each school and facility, providing protection against intrusions, viruses, worms, and spyware, from both external and internal sources.

Two of the company's highest-end firewalls were placed at the school district's data center in the central office. These appliances are specifically designed for complex networks and data centers, and provided multigigabit performance and Ethernet interfaces with fiber interface support. They also provided stateful packet and application-based proxy inspection, branch office and mobile user VPN capabilities, and zero day attack prevention to deliver a much higher level of security than systems that rely solely on signature analysis for protection.

Case Projects

Solution

The following is a partial project solution. Students should be able to expand on the project analysis through extensive research.

As a first step, the town purchased a software solution, which logged all attacks and alerted network administrators to their source IP addresses. The town then sought an enterprise-class network security solution that would proactively shield servers, desktops, and data automatically and minimize the need for manual intervention by its IT staff. After surveying the marketplace, the town selected an Intrusion Prevention System (IPS) to protect its network.

Protected by IPS, the town can now fulfill the country's initiative with complete protection against cyber threats. By examining every incoming packet at Gigabit speed and near-zero latency, the IPS maintains the integrity of the town's network; thus, allowing town employees to sustain their productivity and constituent service to effectively satisfy taxpayers' needs.

Optional Team Case Project

Solution

The following is a partial solution to aid students in coming up with their own solution to solve this case:

The following are the basic benefits of IDS and IPS systems:

- Normal and intrusive malicious activities detected
- Proactive protection of network security infrastructure
- Operational efficiencies to a reduced need to react to event logs for protection
- Increased coverage against packet attacks and zeroday attacks

CHAPTER 6: SECURING CLOUD COMPUTING SYSTEMS

Review Questions/Exercises

True/False

1. True
2. True
3. False
4. False
5. True

Multiple Choice

1. B
2. B
3. D
4. D
5. E

Exercise

Solution

The following is a partial exercise solution. The students should be able to expand on the following:

To determine this, you should review and compare available solutions, including firewalls, patch management procedures, security monitoring and response methods, and other relevant data security measures.

Hands-on Project

Solution

The following is a partial project solution. The students should be able to expand on the following:

You should consider that cloud services are an increasingly attractive target for hackers. Some clouds have experienced direct malicious attacks, potentially exposing any information stored there. In other instances, the clouds have been the targets of denial of service attacks.

Case Projects

Solution

The following is a partial project solution. Students should be able to expand on the project analysis through extensive research.

1. Create a VPC.
2. Create and attach an Amazon VPC Internet gateway.
3. Create an Amazon VPC subnet.
4. Set up routing in the VPC to enable traffic to flow between the subnet and the Internet.
5. Set up a security group.
6. Launch a Linux instance in the subnet.
7. Assign an Elastic IP address to the instance. A Elastic IP address is a static, public address that you can assign to any instance in your VPC.
8. After you complete the tasks, you will have a VPC with a running instance in it. You can connect to the instance from your network using SSH.
9. Add Amazon S3 resources for storage.
10. Deploy a basic e-commerce web application.

Optional Team Case Project

Solution

The following is a partial solution to aid students in coming up with their own solution to solve this case:

You should evaluate your existing incident response capabilities and determine if changes are needed before deciding whether to move to the cloud. Organizational policies and procedures may need to be updated to accommodate anticipated changes introduced by the addition of a cloud—based system. Any such changes should be made well in advance of the implementation and updated regularly.

CHAPTER 7: FAULT TOLERANCE AND RESILIENCE IN CLOUD COMPUTING ENVIRONMENTS

Review Questions/Exercises

True/False

1. False
2. False
3. False
4. False
5. False

Multiple Choice

1. C
2. C
3. E
4. E
5. A

Exercise

Solution

The following is a partial exercise solution. The students should be able to expand on the following:

AppSpace leverages on the Amazon EC2 (Elastic Compute Cloud) service and inherits the security features of Amazon Web Services. Security within Amazon EC2 is provided on multiple levels: The operating system (OS) of the host system, the virtual instance operating system or guest OS, a stateful firewall and signed API calls. Each of these items builds on the capabilities of the others. The goal is to ensure that data contained within Amazon EC2 cannot be intercepted by non-authorized systems or users and that Amazon EC2 instances themselves are as secure as possible without sacrificing the flexibility in configuration that customers demand.

Hands-on Project

Solution

The following is a partial project solution. The students should be able to expand on the following:

Cloud computing architecture typically involves multiple cloud components communicating with each other over application programming interfaces, usually in the form of web services. This architecture works by having multiple programs each doing one thing well and working together over universal interfaces. Complexity is controlled and the resulting systems are more manageable than their monolithic counterparts. The two most significant components of cloud computing architecture are known as the front end and the back end. The front end is the part seen by the client (the computer user). This includes the client's network (or computer) and the applications used to access the cloud via a user interface such as a web browser. The back end of the cloud computing architecture is the 'cloud' itself, comprising various computers, servers and data storage devices.

Case Projects

Solution

The following is a partial project solution. Students should be able to expand on the project analysis through extensive research.

Scalability within a Cloud architecture is via dynamic (on-demand) provisioning of resources on a fine-grained, self-service basis near real-time, without users having to engineer for peak loads. Performance is monitored, and consistent and loosely coupled architectures are constructed using web services as the system interface. This makes for an extremely organic structure and is capable of overcoming performance bottlenecks through distributed and parallel computing grids.

Optional Team Case Project

Solution

The following is a partial solution to aid students in coming up with their own solution to solve this case:

By using a combination of Elastic Load Balancing, Auto Scaling Groups and CloudWatch, you can create a very fault tolerant environment with very little effort. Amazons Elastic Load Balancer is defiantly is a very fault tolerant product, load balanced instances can be spread across regions, which means you can have up to 5–6 instances each behind a separate set of hardware. If somehow Amazon experiences an outage in one of the regions, you still have your application online. The Elastic Load Balancer will also monitor a port on each of the instances to check the health of the application running on the instance. In addition to health checks on the application, Amazon also does a health check of the hardware and will replace your instance on failure.

CHAPTER 8: SECURING WEB APPLICATIONS, SERVICES AND SERVERS

True/False

1. True
2. True
3. True
4. True
5. True

Multiple Choice

1. C
2. B
3. D
4. B, E
5. A, D

Exercise

Solution

The following is a partial exercise solution. The students should be able to expand on the following:

There are two different types of mechanisms for coordinating Web services: Web services orchestration and Web services choreography. Web services orchestration is performed within an organization's SOA and concerns the use of existing Web services to create another Web service. Web services choreography is performed among multiple organizations' SOAs and describes relationships between Web services so that Web services understand how to interact with one another to perform a process. When invoking a Web service orchestration, the encapsulating Web service uses an orchestration engine to define which Web services will be invoked. In contrast, when invoking a Web service choreography, the sequence of Web services is more dynamic, and the decisions are made by the relationships defined between individual Web services rather than by a unifying orchestration engine.

Hands-on Project

Solution

The following is a partial project solution. The students should be able to expand on the following:

Web services security is based on several important concepts, including:

- **Identification and Authentication**: Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.

- **Authorization**. The permission to use a computer resource, granted, directly or indirectly, by an application or system owner.
- **Integrity**. The property that data has not been altered in an unauthorized manner while in storage, during processing, or in transit.
- **Non-repudiation**. Assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the information.
- **Confidentiality**. Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information
- **Privacy**. Restricting access to subscriber or relying party information in accordance with Federal law and organization policy

Case Projects

Solution

The following is a partial project solution. Students should be able to expand on the project analysis through extensive research.

There are several options available for securing Web service messages:

- **HTTP over SSL/TLS (HTTPS)**. Because SOAP messages are transmitted using HTTP, it is trivial to modify a Web service to support HTTPS.
- **XML Encryption and XML Signature**. These XML security standards developed by W3C allow XML content to be signed and encrypted. Because all SOAP messages are written in XML, Web service developers can sign or encrypt any portion of the SOAP message using these standards, but there is no standard mechanism for informing recipients how these standards were applied to the message.
- **WS-Security**. WS-Security was developed to provide SOAP extensions that define mechanisms for using XML Encryption and XML Signature to secure SOAP messages.

Each secure messaging option has its own strengths and weaknesses.

Optional Team Case Project

Solution

The following is a partial solution to aid students in coming up with their own solution to solve this case:

The top threats facing Web services today are:

- **Message alteration**. An attacker inserts, removes or modifies information within a message to deceive the receiver
- **Loss of confidentiality**. Information within a message is disclosed to an unauthorized individual
- **Falsified messages**. Fictitious messages that an attacker intends the receiver to believe are sent from a valid sender
- **Man in the middle**. A third party sits between the sender and provider and forwards messages such that the two participants are unaware, allowing the attacker to view and modify all messages
- **Principal spoofing**. An attacker constructs and sends a message with credentials such that it appears to be from a different, authorized principal
- **Forged claims**. An attacker constructs a message with false credentials that appear valid to the receiver
- **Replay of message**. An attacker resends a previously sent message
- **Replay of message parts**. An attacker includes portions of one or more previously sent messages in a new message
- **Denial of service**. An attacker causes the system to expend resources disproportionately such that valid requests cannot be met.

The importance of the preceding threats may vary depending on an organization's needs and purpose. In some instances, messages need not be kept confidential, so loss of confidentiality is not a concern. Similarly, organizations may offer a Web service to the public. For example, a Web service that provides information about the current weather forecast need not be concerned if a request is from a falsified sender. Regardless, it is important to understand these threats and what technologies are available.

CHAPTER 9: UNIX AND LINUX SECURITY

Review Questions/Exercises

True/False

1. False
2. True
3. True
4. False
5. True

Multiple Choice

1. D
2. C
3. C
4. B
5. C

Exercise

Solution

The following is a partial exercise solution. The students should be able to expand on the following:

At that point, the company's incident response plan was triggered into action. Since the FTP server was not of a critical business value, it was decided to complete the investigation before redeploying the server and to utilize other channels for software distribution temporarily. The primary purpose of the investigation was to learn about the attack in order to secure the server against recurrence. The secondary focus was to trace the actions of the attacker.

Hands-on Project

Solution

The following is a partial project solution. The students should be able to expand on the following:

Security administrators need to pay greater attention to locking down operating systems. Even with a security enhanced Linux (SELinux), you have to turn on the SE features. And, you have to know where they are to activate them.

Another major area of vulnerability is server passwords, which are administered manually. Security administrators need an automated scanning tool that searches all servers for conformity to commercial and military guidelines; and, identifies vulnerabilities. The operating system is a traditionally overlooked piece of Linux security. With the proper tools, this can be done easily and result in a far more secure operation.

Case Projects

Solution

The following is a partial project solution. The students should be able to expand on the following through extensive research:

The following are some of rlogin's possible security problems:

- All information, including passwords, is transmitted unencrypted (making it vulnerable to interception).
- The common practice of mounting users' home directories via NFS exposes rlogin to attack by means of fake .rhosts files.
- The protocol partly relies on the remote party's rlogin client providing information honestly (including source port and source host name).
- The .rlogin (or .rhosts) file is easy to misuse (potentially allowing *anyone* to login without a password).

Optional Team Case Project

Solution

The following is a partial project solution. The students should be able to expand on the following through extensive research:

Security-conscious administrators should use SSH or another encrypted protocol as their method of interactive remote access. If the version of SSH is current and it is fully patched, the service is generally assumed to be safe. However, regardless of whether it is up to date and patched SSH can still be compromised via brute-force password-guessing attacks. Use public key authentication mechanism for SSH to thwart such attacks. For the other interactive services, audit passwords to ensure they are of sufficient complexity to resist a brute-force attack.

Minimizing the number of running services on a host will also make it more secure. Many services have been used to further exploits and some combinations of services (such as web servers and FTP servers that share published directories) are particularly prone to exploits.

CHAPTER 10: ELIMINATING THE SECURITY WEAKNESS OF LINUX AND UNIX OPERATING SYSTEMS

Review Questions/Exercises

True/False

1. True
2. False
3. False
4. True
5. False

Multiple Choice

1. E
2. D
3. D
4. C
5. D

Exercise

Solution

The following is a partial exercise solution. The students should be able to expand on the following:

For you to determine whether you think Linux is a secure operating system, there are a few pieces of information you should be aware of before making your decision:

- Linux, as well as other popular freely available operating systems, have thousands of people scrutinizing each line of code, not only for possible exploits, but also to further audit its level of security. Closed operating systems have only a small staff of people to determine its level of security.

- UNIX, and UNIX-like operating systems such as Linux, have an established background to work from, and despite Linux's relative youth, it is still older than many commercial operating systems.

Hands-on Project

Solution

The following is a partial project solution. The students should be able to expand on the following:

Some people think it is better to disable the ability to load device drivers using modules, because an intruder could load a Trojan module or himself load a module that could affect system security. However, in order to load modules, you must be root. The module object files are also only writable by root. This means the intruder would need root access to insert a module. If the intruder gains root access, there are more serious things to worry about than whether he/she will load a module. Modules are for dynamically loading support for a particular device that may be infrequently used. On server machines, or firewalls for instance, this is very unlikely to happen. For this reason, it would make more sense to compile support directly into the kernel for machines acting as a server. Modules are also slower than support compiled directly in the kernel.

Case Projects

Solution

The following is a partial project solution. Students should be able to expand on the project analysis through extensive research.

This is done intentionally to prevent remote users from attempting to connect via telnet to your machine as root, which is a serious security vulnerability, because then the root password would be transmitted in cleartext, across the network. Don't forget: potential intruders have time on their side, and can run automated programs to find your password.

Optional Team Case Project

Solution

The following is a partial solution to aid students in coming up with their own solution to solve this case:

To enable shadow passwords, run pwconv as root, and /etc/shadow should now exist, and be used by applications. If you are using RH 4.2 or above, the PAM modules will automatically adapt to the change from using normal /etc/passwd to shadow passwords without any other change. The shadow passwords are a mechanism for storing your password in a file other than the normal /etc/passwd file. This has several advantages. The first one is that the shadow file, /etc/shadow, is only readable by root, unlike /etc/passwd, which must remain readable by everyone. The other advantage is that as the administrator, you can enable or disable accounts without everyone knowing the status of other users' accounts. The /etc/passwd file is then used to store user and group names, used by programs like /bin/ls to map the user ID to the proper username in a directory listing. The /etc/shadow file then only contains the username and his/her password, and perhaps accounting information, like when the account expires, etc. To enable shadow passwords, run pwconv as root, and /etc/shadow should now exist, and be used by applications. Since you are using RH 4.2 or above, the PAM modules will automatically adapt to the change from using normal /etc/passwd to shadow passwords without any other change. Finally, since you're interested in securing your passwords, perhaps you would also be interested in generating good passwords to begin with. For this, you can use the pam_cracklib module, which is part of PAM. It runs your password against the Crack libraries to help you decide if it is too-easily guessable by password-cracking programs.

CHAPTER 11: INTERNET SECURITY

Review Questions/Exercises

True/False

1. True
2. True
3. True
4. False
5. False

Multiple Choice

1. C
2. B
3. D
4. A
5. D

Exercise

Solution

The following is a partial exercise solution. The students should be able to expand on the following:

An organization should decide their authentication strategy by basing it on their user credential store location and the location of their clients on the Internet or an intranet.

Hands-on Project

Solution

The following is a partial project solution. The students should be able to expand on the following:

Know your authorization options and choose the most appropriate one for your scenario. First decide if you want to use resource-based or role-based authorization. Resource-based authorization uses access control lists (ACLs) on the resource to authorize the original caller. Role-based authorization allows you to authorize access to service operations or resources based on the group a user is in.

Case Projects

Solution

The following is a partial project solution. The students should be able to expand on the following through extensive research:

Message security encrypts each individual message to protect sensitive data. Transport security secures the end-to-end network connection to protect the network traffic. So, with the preceding in mind, use the following criteria to decide whether to use transport security:

- Point-to-point.
- Streaming.
- Binding limitations.
- Authentication limitations.
- Performance.

Now, use the following criteria to decide whether to use message security:

- Intermediaries.
- Encryption flexibility.
- Binding limitations.
- Secure conversations.
- Authentication limitations.

Optional Team Case Project

Solution

The following is a partial project solution. The students should be able to expand on the following through extensive research:

If your users are in Active Directory, consider using Windows, username, or Basic authentication. All of the following authentication schemes can be mapped to users in Active Directory:

- Windows authentication.
- Basic authentication.
- Username authentication.

CHAPTER 12: THE BOTNET PROBLEM

Review Questions/Exercises

True/False

1. False
2. True
3. False
4. True
5. False

Multiple Choice

1. D
2. C
3. E
4. C
5. E

Exercise

Solution

The following is a partial exercise solution. The botnet incident response team should be able to expand on the following questions and provide solutions:

1. How would the botnet incident response team identify all infected hosts?
2. How would the organization attempt to prevent the worm from entering the organization before antivirus signatures were released?
3. How would the organization attempt to prevent the worm from being spread by infected hosts before antivirus signatures were released?
4. Would the organization attempt to patch all vulnerable machines? If so, how would this be done?

5. How would the handling of this botnet incident change if infected hosts that had received the DDoS agent had been configured to attack another organization's Web site the next morning?
6. How would the botnet incident response team keep the organization's users informed about the status of the incident? What if e-mail services were overloaded or unavailable due to the worm?
7. What additional measures, if any, would the botnet incident response team use to take care of hosts that were not currently connected to the network (staff members on vacation, offsite employees who dial in occasionally)?

Hands-on Project

Solution

The following is a partial exercise solution. The botnet incident response team should be able to expand on the following questions and provide solutions:

1. How would the botnet incident response team determine which hosts within the organization were producing the traffic? Which other teams might assist the botnet incident response team?
2. After identifying a server that was producing the traffic, how would the botnet incident response team determine whether the server was infected with botnets?

Case Projects

Solution

The following is a partial exercise solution. The botnet incident response team should be able to expand on the following questions and provide solutions:

1. How would the botnet incident response team determine what vulnerability or configuration settings permitted the malicious mobile code to infect the systems?
2. How would the botnet incident response team determine what Web site or sites sent the malicious mobile code to the users' systems?

Optional Team Case Project

Solution

The following is a partial exercise solution. The botnet incident response team should be able to expand on the following questions and provide solutions:

1. Since the botnet is most likely a blended attack, how would the response differ from that for a worm?
2. Which attack vector would the organization focus its containment measures on first, and why?

CHAPTER 13: INTRANET SECURITY

Review Questions/Exercises

True/False

1. True
2. True
3. True
4. True
5. False

Multiple Choice

1. A
2. B
3. C
4. D
5. E

Exercise

Solution

The following is a partial exercise solution. The students should be able to expand on the following:

There are times when an intranet will encounter suspicious traffic, such as spam, phishing, spyware, adware and malware; so, deploying an effective email filter (and firewall) can help block the suspicious traffic from entering the network.

Hands-on Project

Solution

The following is a partial project solution. The students should be able to expand on the following:

There have been several cases reported of an intranet being attacked. A network-based intrusion prevention system (IPS) or an intrusion detection prevention system (IDPS) can offer great protection. They also can be deployed for monitoring network traffic and detecting and preventing well-known threats and attacks.

Case Projects

Solution

The following is a partial project solution. The students should be able to expand on the following through extensive research:

Unauthorized access happens much too often when an internal or external user (not authorized) gains access to data and corporate information stored on an intranet. It may be wise to use some type of authentication like passwords, smart cards, or biometrics; in addition, to deploying a bastion host before a user has access to the intranet.

Optional Team Case Project

Solution

The following is a partial project solution. The students should be able to expand on the following through extensive research:

Too often are users gaining unauthorized access to systems from the Intranet. Businesses may want to use some type of intranet monitoring software to see what their employees are doing on the intranet or on their own PCs.

Network administrators want to know what happens on their network. This is both from a machine and sftware perspective; as well as, from a user perspective. This is monitoring the network. The idea is to watch what happens so that the network can keep functioning during business or critical times.

Intranet software sits on a server. It monitors all data traffic between the Internet and the intranet. Moreover, it can monitor all traffic on the intranet itself. It works by examining every Internet Protocol (IP) packet moving in and moving out of the intranet. It examines both the IP header and the data itself. The IP header keeps track of the address, source, and destination. The data can be documents, spreadsheets, e-mail, and so on.

So, with the preceding in mind, what should monitoring software provide the network administrator? It should provide information about who is logged on, who is sending e-mail, and who is signing in late or signing out early. It should record key strokes if necessary.

CHAPTER 14: LOCAL AREA NETWORK SECURITY

Review Questions/Exercises

True/False

1. False
2. False
3. False
4. False
5. True

Multiple Choice

1. B
2. C
3. D
4. E
5. A

Exercise

Solution

The following is a partial exercise solution. The students should be able to expand on the following:

You need to meet the following minimum requirements to connect to a local area network (LAN):

- A wireless capable computer or wireless card (802.11 a/g/n with WPA2-Enterprise encryption compatibility).
- A supported operating system is also needed: The operating system is the software that “runs” your computer and allows other software to be installed and used.

Hands-on Project

Solution

The following is a partial project solution. The students should be able to expand on the following:

In a traditional network, the company will need to consider Routers, Firewalls and SPAM filtering requirements for each site. The number of Routers, Firewalls and SPAM filtering devices will depend on how each site is connected to each other (dedicated lines, VPN or other). In addition, there will probably be a need for a requirement for a DMZ on some of the sites.

Case Projects

Solution

The following is a partial project solution. The students should be able to expand on the following through extensive research:

A mapping entry in the application config file is one possible solution. It could help the organization do what it needed to do without any kind of reconfiguring of the network connections.

Optional Team Case Project

Solution

The following is a partial project solution. The students should be able to expand on the following through extensive research:

The company needs to gather more information, such as:

1. What model of Cisco Router they are using?

2. What type of WAN connectivity do they have?
3. How is their router connected to their LAN and WAN devices?

A basic topology with the specific devices and how they are interconnected, would be the most helpful way for the company to solve this problem.

CHAPTER 15: WIRELESS NETWORK SECURITY

Review Questions/Exercises

True/False

1. True
2. True
3. True
4. True
5. False

Multiple Choice

1. C
2. D
3. E
4. A
5. B

Exercise

Solution

The following is a partial exercise solution. The students should be able to expand on the following:

Short for Wired Equivalent Privacy, WEP is a security protocol for wireless local area networks (WLAN), as defined in the 802.11b standard. WEP is designed to provide the same level of security as that of a wired LAN. LANs are inherently more secure than WLANs, because LANs are somewhat protected by the physical nature of their structure, having some or all part of the network inside a building that can be protected from unauthorized access. WLANs, which use radio waves, do not have the same physical structure and therefore are more vulnerable to tampering. WEP provides some security by encrypting data being transmitted over radio waves so that it is protected as it is transmitted from one end point to another. However, it has been found that WEP is not as secure as once believed. WEP alone is not sufficient security.

Hands-on Project

Solution

The following is a partial project solution. The students should be able to expand on the following:

A WEP key is basically an encryption password that is shared by an access point and a wireless client, allowing basic encryption and decryption of information between the access point and the client device. A WEP key will need to be added to your wireless client on your PC to access wireless resources. The WEP key for an organization can be obtained from an IT person responsible for your area or by contacting a Help Desk.

Case Projects

Solution

The following is a partial project solution. Students should be able to expand on the project analysis through extensive research.

Using the risk assessment as its basis, the computer security department should concentrate on four areas for risk mitigation: physical security, access point (AP) location, AP configuration, and security policy. Analysis of physical security reveals that nonemployees are able to gain access to the building after checking in at the main desk. To ensure that only authorized employees and guests may access the building, the security department should recommend that Organization A adopt the use of photo identification, card badges, or biometric devices. The security team should physically secure the APs by installing them within the secured building facility, which requires users to have proper identification to enter.

The computer security department should minimize the possibility that unauthorized users will access the WLAN from outside the building. The security department should also evaluate each AP to determine the network vulnerabilities, such as eavesdropping. Network engineers should conduct a site survey to determine the best physical location for the APs, to reduce the threat of eavesdropping. This involves physically mapping where users have wireless access to the network. The security department realizes that with a high-gain antenna, attackers will still be able to eavesdrop on wireless network traffic. To offset this risk, the department proposes placing the WLAN outside the firewall and passing traffic through a VPN that supports high-level encryption. This configuration will greatly reduce the risks associated with eavesdropping.

Next, the computer security department should focus on vulnerabilities related to AP configuration. Because many APs retain the original default factory password setting, the computer security department should choose a robust password to ensure a higher level of assurance. In conjunction with management and network administrators, the security department should develop a security policy that requires passwords to be regularly updated and have a minimum length of eight alphanumeric characters. The policy should include the provision to change the encryption setting from "no encryption" to 128-bit encryption. The policy should further deal with the Medium Access Control (MAC) and Access Control List (ACL) usage.

To provide an additional level of access security, the department should allow the use of MAC ACLs whenever possible. The policy should also addresses the use of SNMP. The computer security department decides to disable remote SNMP, because of the related threat and only allows it from internal hosts. Finally, since many vendors use default shared authentication keys, unauthorized devices can gain access to the network if they know the default key. Consequently, the security department should stipulate the use of a username and password as supplemental authentication to APs.

The security department should add additional policies to address software upgrades and use of the network. The policy should require system administrators to test and update security patches and upgrades; as soon as, the vendor makes them available. Frequent patches and upgrades will help reduce the possibility of attack on the older, faulty version of the software. Check for a comprehensive list of known vulnerabilities in major software packages and hardware products. The policy should also strongly discourage users from processing proprietary or employee personal data when connected from their laptops to the WLAN, thus helping to reduce the risk of personnel data exploitation. Additionally, the policy should state that if a laptop is lost or stolen, the employee to whom the laptop belongs to will promptly notify the security department. This will ensure that the security department can quickly identify the IP address assigned to the laptop and prevent that IP address from accessing the network.

As an additional security measure, the security department should recommend that Organization A incorporate the use of an IDS. The IDS will help determine whether unauthorized users are attempting to access, have already accessed, or have compromised the network. The department should view an IDS as a useful tool in protecting Organization A's network and, more importantly, the data that traverses it.

Finally, the security department should present the manager with a risk assessment, which includes the countermeasures described in the preceding. The risk assessment also should include an update of the residual risk with the proposed measures in place. Realizing that the benefits of system operation now outweigh the residual risks, the manager should agree to implement the WLAN. However, the security department should warn that although the risk assessment is thorough, WLAN technology is continually changing along with the security vulnerabilities that malicious users expose.

The security department should also offer encryption algorithms as an example. As encryption-breaking programs become more sophisticated, malicious users may expose more software flaws in vendor programs or weaknesses in encryption algorithms. It should be pointed out that users always represent the weakest link in a security chain. The organization must continue to educate the user community about the risks that wireless technologies pose, reiterating, for example, how important it is not to give others their usernames and passwords and not to execute programs that come from unknown sources. In conclusion, the security department should convey that the strategy is one of defense-in-depth. For example, the WEP encryption should be enabled with random keys; use of MAC ACLs, and a IPsec-based VPN overlay should be deployed. The security department should also monitor the appropriate standards organizations and the availability of products, such that the optimal security solution (most secure and cost-effective) for the enterprise can be determined.

Optional Team Case Project

Solution

The following is a partial solution to aid students in coming up with their own solution to solve this case:

A canvas of user attitudes reveals that most of the organization's users do not appreciate the implications of losing a mobile device and the loss of sensitive organizational data. The network administrators should test the devices and set up a one-hour training course for the employees that will be using the mobile devices. During the training course, the users are given the security policy and documentation explaining the security risks associated with the devices. The security team also recommends instituting security policies that address the appropriate uses of mobile devices, the use of random inventory and security audits, and the users' responsibilities and liabilities. The security policy should specify the type of information users can store on the mobile device, proper handling of mobile devices, password requirements (frequency of change, minimum character length), procedures for reporting a lost or stolen mobile device, and any disciplinary actions that may result from misuse.

The security department completes its risk assessment and cautions that even though it has done a thorough analysis of the mobile devices, there are still risks given the fast pace with which mobile devices are evolving and the likelihood that malicious users will try to exploit any new or existing vulnerability. Organization C determines that the operational benefits outweigh the residual risks of the mobile devices and moves forward with the purchase.

Organization C considers the protection of sales-leads information paramount. Encryption software is used to encrypt database files stored on the PC and the mobile device. Users are encouraged to synchronize their handheld devices every other day; consequently, Organization C does not purchase backup storage modules. The security department realizes that infrared (IR) beaming has important benefits and decides not to prohibit IR beaming completely. However, it does recommend that users keep IR ports closed during periods of nonuse. The sales force also needs to update the corporate sales tracking database, view inventory information, and access corporate e-mail. It is decided that access to corporate resources will be through a VPN.

Before issuing the mobile devices to its sales force, the department ensures that the default settings of the Bluetooth cards are changed to comply with the organization's security policy. The security team upgrades its existing antivirus software to allow it to screen data being transferred to the PC during synchronization. The security team also installs software that automatically prompts the users to enter a password to access the device after 15 minutes of inactivity on all the mobile devices. The security team labels the devices and issues the devices to users with the proper security settings. The security team performs regular audits and follows vendor sites and security mailing lists for security news about handheld devices and applications.

CHAPTER 16: WIRELESS SENSOR NETWORK SECURITY

Review Questions/Exercises

True/False

1. False
2. True
3. False
4. False
5. False

Multiple Choice

1. C
2. C
3. B
4. E
5. B

Exercise

Solution

The following is a partial exercise solution. The students should be able to expand on the following:

Wireless sensor network data acquisition is an extension of PC-based data acquisition to measurement applications where cables are inconvenient or impractical. NI CompactDAQ combines IEEE 802.11 wireless technology and support for over 50 measurement modules with the flexibility of NI LabVIEW software for remote monitoring and control of electrical, physical, mechanical, and acoustic signals. The NI cDAQ-9191 chassis houses a single C Series module and delivers IEEE 802.11b/g *and* Ethernet connectivity back to a host PC, while the NI cDAQ-9181 provides Ethernet connectivity only. C Series modules offer direct network sensor connections and built-in signal conditioning for a variety of measurements, including temperature, strain, high-voltage digital I/O, acceleration, current, and voltage. You can use C Series modules interchangeably for a variety of measurement and control applications across several platforms, including both NI CompactDAQ and CompactRIO.

Hands-on Project

Solution

The following is a partial project solution. The students should be able to expand on the following:

Unlike most wireless sensors or wireless sensor networks, wireless data acquisition devices are meant to stream data continuously back to a host PC or laptop. A wireless sensor node is typically a low-power, autonomous battery-operated device intended for long-term deployment in applications where measurements are needed only every few minutes, hours, or even days. Wi-Fi data acquisition devices, on the other hand, behave in much the same way as a USB data acquisition device a host PC collects data continuously (in real time) as the device acquires it. The data acquisition device may be battery-operated, but the focus is on the measurement versus the battery life. Also, Wi-Fi Wi-Fi NI CompactDAQ chassis use the near-ubiquitous wireless networking standard, IEEE 802.11, instead of ZigBee or other IEEE 802.15.4 variants because of its higher bandwidth and broader applicability. Finally, because the NI CompactDAQ chassis uses the same NI-DAQmx driver software as other NI data acquisition devices, you can develop your applications using NI LabVIEW; LabWindows/CVI; ANSI C/C++; or Microsoft C#, Visual Basic, or Visual Basic .NET.

Case Projects

Solution

The following is a partial project solution. Students should be able to expand on the project analysis through extensive research.

Sensors enable a security system to monitor entryways such as doors and windows. A wireless security sensor can be added to an existing security system that uses wiring to connect sensors to the control panel. This eliminates safety concerns that otherwise would occur if wires had to be strung for great distances, such as from a backyard shed's door. A wireless security sensor kit can be acquired from select hardware and home and garden shops. Adding wireless security sensors requires the use of a few common household tools and does not negatively affect the wired security system in any way.

Optional Team Case Project

Solution

The following is a partial solution to aid students in coming up with their own solution to solve this case:

A window sensor is designed to register a disturbance when its companion sensor plate is no longer making contact. You can install window sensors to use with a wireless burglar alarm without the need for any extra wires or special tools. A tool common to most homes is all that is needed, along with the wood screws that come with the window sensor when it is purchased from a hardware store or security store supplier.

CHAPTER 17: CELLULAR NETWORK SECURITY

Review Questions/Exercises

True/False

1. True
2. True
3. False
4. True
5. True

Multiple Choice

1. D
2. D
3. C
4. A
5. C

Exercise

Solution

The following is a partial exercise solution. The students should be able to expand on the following:

Compared to Wired Networks, Wireless Cellular Network security has a lot of limitations.

1. Open Wireless Access Medium: Since the communication is on the wireless channel, there is no physical barrier that can separate an attacker from the network.
2. Limited Bandwidth: Although wireless bandwidth is increasing continuously, because of channel contention everyone has to share the medium.
3. System Complexity: Wireless systems are more complex due to the need to support mobility and making use of the channel effectively. By adding more complexity to systems, potentially new security vulnerabilities can be introduced.
4. Limited Power: Wireless Systems consume a lot of power and therefore have a limited time battery life.
5. Limited Processing Power: The processors installed on the wireless devices are increasing in power, but still they are not powerful enough to carry out intensive processing.
6. Relatively Unreliable Network Connection: The wireless medium is an unreliable medium with a high rate of errors compared to a wired network.

Hands-on Project

Solution

The following is a partial project solution. The students should be able to expand on the following:

There are several security issues that have to be taken into consideration when deploying a cellular infrastructure. The importance of which has increased with the advent of advanced networks like 3G and 4G.

1. Authentication: Cellular networks have a large number of subscribers, and each has to be authenticated to ensure the right people are using the network. Since the purpose of 3G and 4G is to enable people to communicate from anywhere in the world, the issue of cross region and cross provider authentication becomes an issue.
2. Integrity: With services such as SMS, chat and file transfer it is important that the data arrives without any modifications.
3. Confidentiality: With the increased use of cellular phones in sensitive communication, there is a need for a secure channel in order to transmit information.
4. Access Control: The Cellular device may have files that need to have restricted access to them. The device might access a database where some sort of role based access control is necessary.
5. Operating Systems In Mobile Devices: Cellular Phones have evolved from low processing power, adhoc supervisors to high power processors and full fledged operating systems. Some phones may use a Java Based system, others use Microsoft Windows CE and have the same capabilities as a desktop

computer. Issues may arise in the OS which might open security holes that can be exploited.

6. Web Services: A Web Service is a component that provides functionality accessible through the web using the standard HTTP Protocol. This opens the cellular device to variety of security issues such as viruses, buffer overflows, denial of service attacks etc.
7. Location Detection: The actual location of a cellular device needs to be kept hidden for reasons of privacy of the user. With the move to IP based networks, the issue arises that a user may be associated with an access point and therefore their location might be compromised.
8. Viruses And Malware: With increased functionality provided in cellular systems, problems prevalent in larger systems such as viruses and malware arise. The first virus that appeared on cellular devices was Liberty. An affected device can also be used to attack the cellular network infrastructure by becoming part of a large scale denial of service attack.
9. Downloaded Contents: Spyware or Adware might be downloaded causing security issues. Another problem is that of digital rights management. Users might download unauthorized copies of music, videos, wallpapers and games.
10. Device Security: If a device is lost or stolen, it needs to be protected from unauthorized use so that potential sensitive information such as emails, documents, phone numbers etc. cannot be accessed.

Case Projects

Solution

The following is a partial project solution. The students should be able to expand on the following through extensive research:

Due to the massive architecture of a cellular network, there are a variety of attacks that the infrastructure is open to.

1. Denial Of Service (DOS): This is probably the most potent attack that can bring down the entire network infrastructure. This is caused by sending excessive data to the network, more than the network can handle, resulting in users being unable to access network resources.
2. Distributed Denial Of Service (DDOS): It might be difficult to launch a large scale DOS attack from a single host. A number of hosts can be used to launch an attack.
3. Channel Jamming: Channel jamming is a technique used by attackers to jam the wireless channel; and, therefore deny access to any legitimate users in the network.
4. Unauthorized Access: If a proper method of authentication is not deployed then an attacker can gain free access to a network and then can use it for services that he might not be authorized for.
5. Eavesdropping: If the traffic on the wireless link is not encrypted then an attacker can eavesdrop and intercept sensitive communication such as confidential calls, sensitive documents etc.
6. Message Forgery: If the communication channel is not secure, then an attacker can intercept messages in both directions and change the content without the users ever knowing.
7. Message Replay: Even if communication channel is secure, an attacker can intercept an encrypted message and then replay it back at a later time and the user might not know that the packet received is not the right one.
8. Man In The Middle Attack: An attacker can sit in between a cell phone and an access station and intercept messages in between them and change them.
9. Session Hijacking: A malicious user can highjack an already established session, and can act as a legitimate base station.

Optional Team Case Project

Solution

The following is a partial project solution. The students should be able to expand on the following through extensive research:

While there are several security mechanisms available in wireless cellular networks, continued research is going on to provide new and even more secure mechanisms for cellular security. For example:

1. New Authentication Scheme with Anonymity For Wireless Networks:

   When a mobile user is roaming, it is necessary to provide anonymity to the users so that malicious parties are unable to associate the user with a particular session. The most basic method to provide anonymity is to have a temporary identity (TID) instead of the real id of the user. There are several issues to consider when designing a security protocol for cellular networks. One, they have low computational power which means that algorithms that require high processing power are not suitable. Second, the error rate of messages increase on wireless networks as compared to cellular networks. Therefore, any mechanism that is designed should minimize message sizes and the number of messages in order to reduce the error rate.

2. Manual Authentication For Wireless Devices:
   This is a technique used by devices to authenticate one another by manually transferring data between the devices. This means that the users will enter some information using some form of input (keypad). Underneath they employ MAC algorithms for authentication. Although the scheme that is proposed is secure, it usability depends upon how many numbers (or alphabets) the users have to input.
3. Elliptic Curve Cryptography For Wireless Security:
   Elliptic Curve Cryptography (ECC) is a mechanism which uses points on an elliptic curve to encrypt/decrypt data. It has an advantage over the popular RSA algorithm in that it is much faster. 163 - bit ECC provides the same security as a 1024 bit RSA algorithm, and can be anywhere from 5 to 15 times faster depending on the platform. For example, in order to secure a 128 bit AES shared key and 521 - bit ECC provides the same level of security as an 15,360 bit RSA while being about 400 times faster.
4. Channel Surfing And Spatial Retreats:
   Defense against Wireless Denial Of Service DOS attacks are one of the most dangerous attacks because they can bring down an entire network. An adversary can either trying to fill the buffer in a network device, or can by pass the MAC layer and try to jam the channel. Channel Surfing is a technique where the transmission frequency is changed to one where there is no interference. Spatial Retreats is a technique where the wireless users move to a location where there is no interference.

CHAPTER 18: RFID SECURITY

Review Questions/Exercises

True/False

1. True
2. False
3. True
4. True
5. True

Multiple Choice

1. A
2. E
3. C
4. B
5. D

Exercise

Solution

The following is a partial exercise solution. The students should be able to expand on the following:

Comprehensive automatic test methods ensure that no code exists in duplicate in any of the transponder types, and that the codes are programmed correctly in a readable manner. In each transponder, 39 bits of memory are reserved for the code. That translates into 239 (or about 550 billion) possible unique codes. If one were to assign all 550 billion codes to transponder with the smallest dimensions known today, specifically the ID-100 Microtransponders with their length of 12 mm, and then line these transponders up end to end, the resulting string would measure 6.5 million kilometers in length, which is about 160 times the circumference of the earth.

Hands-on Project

Solution

The following is a partial project solution. The students should be able to expand on the following:

Unattended data capture is one of the stronger business benefits to RFID. And this leads to the question: How do you know that the data is secure and accurate? Work continues to develop new security protocols between the tag and reader, but the fact that the range of the technology is limited really does significantly minimize the risk. More important is the need for a robust wired and wireless network security methodology to ensure that as the RFID data moves around a corporation, and possibly over large geographic areas, it remains secure.

Case Projects

Solution

The following is a partial project solution. The students should be able to expand on the following through extensive research:

The first step in the case project is to conduct a risk assessment to help shape the final scope of the project and identify the most appropriate uses of the RFID technology, as well as potential controls to mitigate the accompanying risk. Some risks identified during the assessment are as follows:

- RFID systems could open a “backdoor” to the FSRC computer network, which could result in the compromise of mission-critical systems and research archives.
- Anyone eavesdropping on RFID transactions could compromise the privacy of patient medical records.

- The FSRC could be held liable for violations of the privacy provisions of Health Insurance Portability and Accountability Act (HIPAA).
- The radio frequencies used by the RFID system could interfere with wireless patient sensors and medical telemetry devices, which could impact quality of care and research results.
- Dermal contact with RFID tags might be a potential vector for the transmission of some highly contagious diseases.

The risk assessment also concluded that some RFID risks were minimal or nonexistent in the FSRC environment. The worst case for expected patient and staff exposure to RF radiation was forecasted to be significantly below any level that might adversely affect their health. FSC already had a well-enforced policy that prohibits the storage of fuel or ordnance at the facility, and the use of potentially explosive material such as ether and oxygen tanks was tightly controlled. The likelihood that an adversary would attempt to use the FSRC RFID system to gather intelligence or target personnel was deemed negligible.

As a result of the risk assessment, the FSRC enhanced its network security policy to require that the RFID system be separated from other network systems using a firewall that permits only required data and management traffic to traverse the network boundary. The network security policy also was amended to require user authentication to all non-stationary RFID readers and encryption of wireless traffic between mobile readers and access points. Existing policy regarding secure server configurations and least privilege data access would extend to the RFID systems without requiring any modifications. The FSRC also decided that it would not institute a new requirement for wireless intrusion detection, but it would revisit this decision during the following fiscal year.

The FSRC also conducted a privacy assessment based on information collected during the risk assessment. As a result, the FSRC privacy policy was revised to account for the introduction of RFID technology. The revision noted that any patient data collected by the RFID system would be subject to the FSRC's internal procedures implementing HIPAA regulations. A final determination was made to update patient release forms to include a statement that inherent risks exist with wireless communications and that network security controls were implemented to help mitigate these risks. Based on the project charter and the updated security and privacy policies, the CIO led an interdisciplinary team of medical practitioners and information technology professionals to develop the business and functional requirements for the RFID system.

Optional Team Case Project

Solution

The following is a partial project solution. The students should be able to expand on the following through extensive research:

The project team began with a risk assessment, which identified a number of concerns, the most significant of which were as follows:

- An adversary could identify and target a vehicle containing RAD-regulated material.
- An adversary could eavesdrop on tag transactions to learn the characteristics of the material, which could help determine whether it is worth stealing.
- An adversary could damage or disable a tag, making it easier to steal material without detection.
- An adversary could alter sensor or manifest data stored on the tag in an effort to undermine the business processes for which the material is being used.
- The radiation from readers could accidentally cause combustion of collocated volatile materials when several of them are operating concurrently in close proximity.

To help address the risks, RAD established a policy that required that tagged items only be identifiable during embarkation, debarkation, and storage, but not during transport. The policy further stated that tag-reader communication should be authenticated whenever technically feasible with commercial-off-the-shelf systems. RAD also conducted a privacy assessment that identified that the system would handle Personally Identifiable Information (PII) due to the need to associate materials with particular individuals, although most such information was already contained in existing logs. Furthermore, RAD updated its privacy disclosure statement for employees and contractors to account for the new technology. Finally, it required that all personnel involved in handling of the tagged materials be provided RFID security and privacy awareness training. In addition, RAD already had a Hazards of Electromagnetic Radiation to Fuel (HERF) policy, but everyone agreed the introduction of the RFID system would require the agency to revisit the efficacy of these HERF-related controls.

CHAPTER 19: OPTICAL NETWORK SECURITY

Review Questions/Exercises

True/False

1. False
2. True

3. False
4. False
5. True

Multiple Choice

1. B
2. A
3. D
4. C
5. A

Exercise

Solution

The following is a partial exercise solution. The students should be able to expand on the following:

Yes. Optical network security is one of the most robust features of a NAS optical storage server. A NAS optical storage server has a unified optical network security model enabled throughout all of the client protocols. Concepts such as Local Users, Local Groups, Share Level Passwords, User Level security, NT Domain Users, and NDS Users are usually supported.

Hands-on Project

Solution

The following is a partial project solution. The students should be able to expand on the following:

Seamlessly. The optical network security model of a NAS optical storage server functions independently of any protocol that is accessing it. If a NetWare user logs in as Supervisor, for example, and sets privileges to a given directory to only NDS users named “Nate”, then all other clients are denied access to this directory. If the administrator then adds a local user “Steve” to this same directory then a user from a Macintosh, Unix system, Microsoft or Novell Bindery client can access the directory as “Steve;” as well as, the NDS user “Nate.” In this example all other users (regardless of protocol) are locked out of this directory.

Case Projects

Solution

The following is a partial project solution. The students should be able to expand on the following through extensive research:

Yes. Unlike other NAS servers, which only allow optical network security to be configured at the volume level, a NAS optical storage server allows security to be configured down to the directory level.

Optional Team Case Project

Solution

The following is a partial project solution. The students should be able to expand on the following through extensive research:

Yes. All of the methods of setting optical network security on physical volumes or directories are available for virtual volumes.

CHAPTER 20: OPTICAL WIRELESS SECURITY

Review Questions/Exercises

True/False

1. True
2. False
3. False
4. False
5. True

Multiple Choice

1. B
2. C
3. A
4. D
5. E

Exercise

Solution

The following is a partial exercise solution. The students should be able to expand on the following:

The truth is that wireless fiber cabling is just as vulnerable to hackers as wired networks using easily obtained commercial hardware and software.

Hands-on Project

Solution

The following is a partial project solution. The students should be able to expand on the following:

Setting up a fiber tap is no more difficult than setting up equipment for any other type of hack, wired or wireless. Optical wireless network exploits are accomplished by extracting light from the ultra-thin glass fibers. The first, and often easiest, step is to gain access to the targeted fiber optic cable. Hundreds of millions of miles of fiber cable stretch across the globe; there are more than 190 million miles in the United States alone. Although most of this cabling is difficult to access: It’s underground, undersea, encased in concrete, and run through walls and elevator shafts; plenty of cables are readily accessible for those willing to look. Some cities, for example, have detailed maps of their wireless fiber-optic infrastructure posted online in an effort to lure local organizations to hook into the network.

Case Projects

Solution

The following is a partial project solution. The students should be able to expand on the following through extensive research:

Bending light is the easiest method. It is also the most undetectable, since there is no interruption to the light signal. Commercially available clip-on couplers cost less than a thousand dollars; these devices place a micro-bend in the cable, leaking a small amount of light through the polymer cladding. Once the light signal has been accessed, the data is captured using a photo detectora transducer capable of translating an optical signal into an electrical signal.

Optional Team Case Project

Solution

The following is a partial project solution. The students should be able to expand on the following through extensive research:

At this point, the only measure to prevent information from being pilfered off of optical wireless networks is the encryption of transmitted data. Many organizations make the mistake of encrypting the data and the transmission, which is redundant. If the data is encrypted, there is no need to spend extra money to send it through a secured tunnel. The trend is leaning toward encryption at the data layer, which reduces the latency and overhead associated with transport.

Unfortunately, optical hacks render most traditional security methodologies ineffective. Financial, health care, insurance and publicly traded companies saddled with regulatory compliance rarely consider that private and sensitive data delivered over fiber optic wireless communication systems is vulnerable to being captured through virtually undetectable hacks. Your data transmissions may have already been compromised without your being aware of it. Securing a fiber optic wireless transmission can be costly and difficult, and the bad guys, as usual, have a head start.

CHAPTER 21: INFORMATION SECURITY ESSENTIALS FOR IT MANAGERS: PROTECTING MISSION-CRITICAL SYSTEMS

Review Questions/Exercises

True/False

1. False
2. True
3. True
4. False
5. True

Multiple Choice

1. C
2. D
3. A
4. B
5. B

Exercise

Solution

The following is a partial exercise solution. The students should be able to expand on the following:

Continuous monitoring determines if the complete set of planned, required, and deployed security controls within an information system or inherited by the system continue to be effective over time in light of the inevitable changes that occur. Continuous monitoring is an important activity in assessing the security impacts on an information system resulting from planned and unplanned changes to the hardware, software, firmware, or environment of operation (including threat space). IT managers' risk based decisions (security authorization decisions) should consider how continuous monitoring will be implemented organization wide as one of the components of the security life cycle.

Hands-on Project

Solution

The following is a partial project solution. The students should be able to expand on the following:

No. Security authorization, requires the explicit review and acceptance of risk by an IT manager on an ongoing basis. These risk based decisions are based on security control assessments and continuous monitoring activities. Continuous monitoring does not replace the security authorization requirement. Rather, continuous monitoring is implemented as part of a holistic, risk management and (defense-in-depth) information security strategy that is integrated into enterprise architectures and system development life cycles. The continuous monitoring program, developed and implemented by an organization as a component in the security life cycle based approach, becomes a consideration in the risk based decisions (security authorization decisions) rendered by IT managers. Continuous monitoring also supports the requirement for conducting assessments of security controls with a frequency depending on risk, but no less than annually.

Case Projects

Solution

The following is a partial project solution. The students should be able to expand on the following through extensive research:

Continuous monitoring in and of itself, does not provide a comprehensive, enterprise-wide risk management approach. Rather, it is a key component in the risk management process. The fundamental tenet of a unified information security framework is an enterprisewide risk management approach to information security that is life cycle-based and implemented across three hierarchical tiers within an organization (governance, mission/business process, and information system). The ongoing determination and acceptance of information system security-related risks remains the primary responsibility of IT managers' and for which they are held accountable. Continuous monitoring activities contribute to helping IT managers' make better risk-based decisions, but do not replace the security authorization process.

Optional Team Case Project

Solution

The following is a partial project solution. The students should be able to expand on the following through extensive research:

Front-end security, exemplified by security categorization, security control selection, and implementation, focuses on building security into information technology products and systems early in the system development life cycle. The initial steps are also linked to the organization's enterprise architecture and information security architecture. Better front-end security results in fewer weaknesses and deficiencies in information systems, directly translating to a lesser number of vulnerabilities that can be exploited by threat sources. Back-end security, exemplified by security control assessment, information system authorization, and continuous monitoring, focuses on the effectiveness of the implemented security controls, the determination and acceptance of risk, and the ongoing monitoring of the security state of the information system.

CHAPTER 22: SECURITY MANAGEMENT SYSTEMS

Review Questions/Exercises

True/False

1. True
2. True
3. False
4. True
5. False

Multiple Choice

1. C
2. D
3. E
4. A
5. C

Exercise

Solution

The following is a partial exercise solution. The students should be able to expand on the following:

Certification of a security management system (SMS) brings several advantages. It gives an independent assessment of your organization's conformity to an international standard that contains best practices from experts for SMS. A certified SMS does not guarantee compliance with legislative and local policies, but provides a systematic platform to build on.

Hands-on Project

Solution

The following is a partial project solution. The students should be able to expand on the following:

ISO/IEC 27001 (BS 7799-2) is aligned with both the ISO 9001 (quality management systems) and ISO 14001 (environmental management systems) standards. The three standards share system elements and principles, including adopting the PLAN, DO, CHECK, ACT cyclic process. This approach makes it possible to integrate the systems to the extent it makes sense.

Case Projects

Solution

The following is a partial project solution. The students should be able to expand on the following through extensive research:

If information assets are important to an organization's business, it should consider implementing an SMS in order to protect those assets within a sustainable framework. If an organization implements an SMS, it should consider going through the process to be certified against the ISO/IEC 27001 standard. ISO/IEC 27001 and BS 7799 continues to build a reputation for helping to model business practices that enhance an organization's ability to protect its information assets. A growing number of organizations around the world have already gone through the certification process.

Optional Team Case Project

Solution

The following is a partial project solution. The students should be able to expand on the following through extensive research:

Selecting the right set of controls requires the use of a risk assessment-based approach. This approach is a mandatory part of the PLAN (identify, analyze and evaluate the risks), DO (select, implement, and use controls to manage the risks to acceptable levels), CHECK, and ACT cyclic process defined in BS 7799-2 for the establishment, implementation, and maintenance of an SMS.

CHAPTER 23: POLICY-DRIVEN SYSTEM MANAGEMENT

Review Questions/Exercises

True/False

1. False
2. False
3. True
4. True
5. False

Multiple Choice

1. B
2. C
3. C
4. A
5. D

Exercise

Solution

The following is a partial exercise solution. The students should be able to expand on the following:

The speed of implementation is driven by

1. The client's commitment and available resources.
2. The size and complexity of the organisation.
3. The policies and procedures already in place.

Many certification/**accreditation** bodies require at least 3 months of the management system running, in order to have enough genuine records to audit. The date of the final certification audit can depend on the availability of the external auditors, so it is an advantage to start talking to the certification body in advance.

Hands-on Project

Solution

The following is a partial project solution. The students should be able to expand on the following:

The certification body will agree a "certification cycle". This involves a re-certification and interim surveillance audits. For example, an ISO 27001 Information Security Management system is usually re-certified every 3 years, with interim surveillance audits every 6 months from certification.

Case Projects

Solution

The following is a partial project solution. The students should be able to expand on the following through extensive research:

Risk can not be eliminated, only reduced and an audit is a sampling process. Auditors understand this and if they do come across an inconsistency, they may extend their sampling to establish if it is a "major break down of the management system" or a rare occurrence. Don't forget, auditors will be watching what is happening in your organization while they are there, so it's important that you deal with any day to day issues appropriately.

Optional Team Case Project

Solution

The following is a partial project solution. The students should be able to expand on the following through extensive research:

Auditors can raise non-conformances against the standard or the process/procedures of your organization. A minor non-conformance will be noted if a deficiency has been found, providing it hasn't shown a serious break down in the system. The auditor will set a deadline for any minor non-conformances to be corrected and may require some evidence of this before awarding a certificate. A major non-conformance is more serious and will lead to the application for certification to be refused. These usually occur when an aspect required by the standard has not been implemented, or it has been implemented to the extent it does not meet it's objective.

CHAPTER 24: INFORMATION TECHNOLOGY SECURITY MANAGEMENT

Review Questions/Exercises

True/False

1. False
2. False
3. True
4. False
5. True

Multiple Choice

1. B
2. C
3. C
4. D
5. A

Exercise

Solution

The following is a partial exercise solution. The students should be able to expand on the following:

Business continuity planning provides a quick and smooth restoration of operations after a disruptive event. Business continuity planning is a major component of risk management and includes business impact analysis, business continuity plan (BCP) development, testing, awareness, training, and maintenance.

Hands-on Project

Solution

The following is a partial project solution. The students should be able to expand on the following:

Legal and regulatory requirements say at least annually. However, all organizationsshould closely monitor their critical business environments for changes and issue updates as needed.

Case Projects

Solution

The following is a partial project solution. The students should be able to expand on the following through extensive research:

Functions should be considered critical if any of the following apply:

- Support primary mission statement
- Support other organizations' mission critical function
- Must be recovered quickly
- Have a high dollar value
- Have a high business impact
- Have political ramifications or implications
- Have legal requirements or liabilities

Optional Team Case Project

Solution

The following is a partial project solution. The students should be able to expand on the following through extensive research:

Certification of an IT security management system (ITSMS) brings several advantages. It gives an independent assessment of your organization's conformity to an international standard that contains best practices from experts for ITSMS. A certified ITSMS does not guarantee compliance with legislative and local policies, but provides a systematic platform to build on.

CHAPTER 25: ONLINE IDENTITY AND USER MANAGEMENT SERVICES

Review Questions/Exercises

True/False

1. False
2. True
3. True
4. False
5. False

Multiple Choice

1. E
2. A
3. B
4. C
5. D

Exercise

Solution

The following is a partial exercise solution. The students should be able to expand on the following:

The term digital identity is used to describe the combination of validating your identity through prescribed vetting and proofing procedures and once completed, issue a digital certificate to be used as a representation of your identity in the digital world. Digital certificates give individuals, corporations and governments the ability to prove that they are who they say they are in an electronic environment. Digital certificates will give individuals acting on behalf of a corporation or government the ability to:

- Authenticate themselves – proving in a binding, nonrepudiable fashion that they are who they say they are.
- Protect information – allowing them to lock down documents or material being sent electronically so that it cannot be tampered with or viewed without their permission
- Digitally sign – allowing them to replace ink signatures with an electronic signature that is the legal equivalent and that is accepted around the globe

Hands-on Project

Solution

The following is a partial project solution. The students should be able to expand on the following:

In terms of managing identities, whether digital or physical, banks are uniquely positioned as providers. The reasons:

- Banks have always played the role of trusted intermediaries for financial transactions, whether on a consumer or corporate level In terms of managing identities, whether digital or physical, banks are uniquely positioned as providers
- Banks are regulated, operating under independent oversight where failure to comply leads to serious financial implications and thus creating a strong incentive to behave properly
- Banks exist everywhere, with a broad reach into even the smallest town or location, and are subject to global requirements that ensure consistency across multiple legal or regulatory jurisdictions
- Banks have experience in dealing with information that needs to be managed carefully
- Some banks have a global scale and a scalable information systems infrastructure to support large volumes of transactions
- Banks have experience in dealing with risk management and mitigation - they are fundamentally in the business of transferring and managing risk, which makes them uniquely positioned to price and manage the risk elements of identity

Case Projects

Solution

The following is a partial project solution. The students should be able to expand on the following through extensive research:

The digital identity does not capture the physical signature of the signer but instead imprints an electronic identifier, known as a private key, unique to the individual signing the transaction. Moreover, thanks to the legal and operational framework surrounding the issuance and management of the digital identities, digital signatures are legally binding, just like wet ink signatures.

Optional Team Case Project

Solution

The following is a partial project solution. The students should be able to expand on the following through extensive research:

In your organization, you may have many types of digital credentials. A digital credential is a proof of qualification, competence, or clearance that is attached to a person and can encompass many forms of authentication (username/password, one-time passwords, smart cards or internally-issued digital certificates) into enterprise systems, such as business applications, online portals, Network Operating Systems, etc. The levels of identity assurance and federation that these internally issued digital credentials can convey, starts to become in question in the context of B2B transactions, particularly those of high sensitive natures (such as financial transactions). In such cases, an interoperable, bank-issued digital identity is an ideal solution to enable the B2B electronic workflow.

CHAPTER 26: INTRUSION DETECTION AND PREVENTION SYSTEMS

Review Questions/Exercises

True/False

1. False
2. True
3. True
4. True
5. True

Multiple Choice

1. B
2. C
3. D
4. A
5. E

Exercise

Solution

The following is a partial exercise solution. The students should be able to expand on the following:

Intrusion detection systems are made up of three functional components, information sources, analysis, and response. The system obtains event information from one or more information sources, performs a pre-configured analysis of the event data, and then generates specified responses, ranging from reports to active intervention when intrusions are detected.

Hands-on Project

Solution

The following is a partial project solution. The students should be able to expand on the following:

Each security protection serves to address a particular security threat to a system. Furthermore, each security protection has weak and strong points. Only by combining them (this combination is sometimes called *security in depth*) do organizations protect from a realistic range of security attacks. Firewalls serve as barrier mechanisms, barring entry to some kinds of network traffic and allowing others, based on a firewall policy. IDSs serve as monitoring mechanisms, watching activities, and making decisions about whether the observed events are suspicious. They can spot attackers circumventing firewalls and report them to system administrators, who can take steps to prevent damage.

Case Projects

Solution

The following is a partial project solution. The students should be able to expand on the following through extensive research:

There are many ways of describing IDSs. The primary descriptors are the system monitoring approaches, the analysis strategy and the timing of information sources and analysis. The system monitoring approaches are network-based, host-based, and applications-based. The analysis strategies are misuse detection and anomaly detection. The timing categories are interval-based (or batch mode) and real-time. The most common commercial IDSs are real-time network-based systems.

Optional Team Case Project

Solution

The following is a partial project solution. The students should be able to expand on the following through extensive research:

The best IDS for your organization is the IDS that best satisfies the security goals and objectives of your organization, given the constraints of the organization. Governing factors are usually defined as the following:

- System environment, in terms of hardware and software architectures.
- Security environment, in terms of policy, existing security mechanisms, and constraints.
- Organizational goals, in terms of functional goals of the enterprise (for instance, e-commerce organizations might have different goals and constraints from manufacturing organizations).
- Resource constraints, in terms of acquisition, staffing, and infrastructure.

CHAPTER 27: TCP/IP PACKET ANALYSIS

Review Questions/Exercises

True/False

1. True
2. False
3. True
4. False
5. True

Multiple Choice

1. C
2. C
3. C
4. C
5. E

Exercise

Solution

The following is a partial exercise solution. The students should be able to expand on the following:

Detecting crashed systems over TCP/IP is difficult. TCP doesn't require any transmission over a connection if the application isn't sending anything, and many of the media over which TCP/IP is used (Ethernet) don't provide a reliable way to determine whether a particular host is up. If a server doesn't hear from a client, it could be because it has nothing to say, some network between the server and client may be down, the server or client's network interface may be disconnected, or the client may have crashed. Network failures are often temporary (a thin Ethernet will appear down while someone is adding a link to the daisy chain, and it often takes a few minutes for new routes to stabilize when a router goes down) and TCP connections shouldn't be dropped as a result.

Hands-on Project

Solution

The following is a partial project solution. The students should be able to expand on the following:
The OSI - Open System Interconnection and the TCP/IP - Transmission Control Protocol/ Internet Protocol.

Case Projects

Solution

The following is a partial project solution. The students should be able to expand on the following through extensive research:

Each application running over TCP or UDP distinguishes itself from other applications using the service by reserving and using a 16-bit port number. Destination and source port numbers are placed in the UDP and TCP headers by the originator of the packet before it is given to IP, and the destination port number allows the packet to be delivered to the intended recipient at the destination system.

Optional Team Case Project

Solution

The following is a partial project solution. The students should be able to expand on the following through extensive research:

TCP/IP is a protocol stack used for data transmission from source to destination. In the physical layer, all the physical connections like LAN cards, cables etc., will be there; which will send data in the form of bits. Layer 2, operates with frames where the switches come into picture in the network layer, which operates on packets. The routing then takes place; and, routers are the devices used for this. The transport layer is above the network layer and it uses mainly TCP/ UDP for transport of data. The application layers is on top of this layer.

CHAPTER 28: THE ENEMY (THE INTRUDER'S GENESIS)

Review Questions/Exercises

True/False

1. True
2. False
3. False
4. False
5. False

Multiple Choice

1. D
2. D
3. A
4. A
5. B

Exercise

Solution

The following is a partial exercise solution. The students should be able to expand on the following:

Download IP-Tools and install it:

The purpose of this exercise is to let the student down load the freely available software IP-Tools. This software is very easy to use and explore the concepts presented in this chapter.

Hands-on Project

Solution

The following is a partial project solution. The students should be able to expand on the following:

Download LANguard N.S.S. (Commercial grade Network Security Scanner, N.S.S.):

The purpose of this project is to have the student download a commercial scanner with lots of options. The network should be connected to the Internet so that the students can use the Whois option and discover the name servers for a given Internet domain. This step amounts to network mapping.

Case Projects

Solution

The following is a partial project solution. The students should be able to expand on the following through extensive research:

Using LANguard software to Enumerate the computers in your Windows domain:

In this project students will learn about enumeration, and what information does it provide to a would be hacker. A screen-shot is displayed in the file ch04_artmsprj_au1st as Enumerate Computers.

Optional Team Case Project

Solution

The following is a partial project solution. The students should be able to expand on the following through extensive research:
Using any of the search engines on the Internet, search for the keyword as "Packet Crafting" for Windows based software, and Packet Generation under Linux.

CHAPTER 29: FIREWALLS

Review Questions/Exercises

True/False

1. True
2. False
3. False
4. False
5. False

Multiple Choice

1. D
2. D
3. A
4. A
5. B

Exercise

Solution

The following is a partial exercise solution. The students should be able to expand on the following:

A firewall policy defines how an organization's firewalls should handle inbound and outbound network traffic for specific IP addresses and address ranges, protocols, applications, and content types based on the organization's information security policies. Organizations should conduct risk analysis to develop a list of the types of traffic needed by the organization and how they must be secured—including which types of traffic can traverse a firewall under what circumstances. Examples of policy requirements include permitting only necessary Internet Protocol (IP) protocols to pass, appropriate source and destination IP addresses to be used, particular Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) ports to be accessed, and certain Internet Control Message Protocol (ICMP) types and codes to be used. Generally, all inbound and outbound traffic not expressly permitted by the firewall policy should be blocked because such traffic is not needed by the organization. This practice reduces the risk of attack and can also decrease the volume of traffic carried on the organization's networks.

Hands-on Project

Solution

The following is a partial project solution. The students should be able to expand on the following:

There are many considerations that organizations should include in their firewall selection and planning processes. Organizations need to determine which network areas need to be protected, and which types of firewall technologies will be most effective for the types of traffic that require protection. Several important performance considerations also exist, as well as concerns regarding the integration of the firewall into existing network and security infrastructures. Additionally, firewall solution design involves requirements relating to physical environment and personnel as well as consideration of possible future needs, such as plans to adopt new IPv6 technologies or virtual private networks (VPN).

Case Projects

Solution

The following is a partial project solution. The students should be able to expand on the following through extensive research:

Firewall rulesets should be as specific as possible with regards to the network traffic they control. To create a ruleset involves determining what types of traffic are required, including protocols the firewall may need to use for management purposes. The details of creating rulesets vary widely by type of firewall and specific products, but many firewalls can have their performance improved by optimizing firewall rulesets. For example, some firewalls check traffic against rules in a sequential manner until a match is found; for these firewalls, rules that have the highest chance of matching traffic patterns should be placed at the top of the list wherever possible.

Optional Team Case Project

Solution

The following is a partial project solution. The students should be able to expand on the following through extensive research:

There are many aspects to firewall management. For example, choosing the type or types of firewalls to deploy and their positions within the network can significantly affect the security policies that the firewalls can enforce. Policy rules may need to be updated as the organization's requirements change, such as when new applications or hosts are implemented within the network. Firewall component performance also needs to be monitored to enable potential resource issues to be identified and addressed before components become overwhelmed. Logs and alerts should also be continuously monitored to identify threats—both successful and unsuccessful. Firewall rulesets and policies should be managed by a formal change management control process because of their potential to impact security and business operations, with ruleset reviews or tests performed periodically to ensure continued compliance with the organization's policies. Firewall software should be patched as vendors provide updates to address vulnerabilities.

CHAPTER 30: PENETRATION TESTING

Review Questions/Exercises

True/False

1. False
2. True
3. True
4. True
5. True

Multiple Choice

1. E
2. C
3. C
4. B
5. D

Exercise

Solution

The following is a partial exercise solution. The students should be able to expand on the following:

- How well the system tolerates real world-style attack patterns.
- The likely level of sophistication an attacker needs to successfully compromise the system.
- Additional countermeasures that could mitigate threats against the system.
- Defenders' ability to detect attacks and respond appropriately.

Hands-on Project

Solution

The following is a partial project solution. The students should be able to expand on the following:

- **Host name and IP address information** can be gathered through many methods, including DNS interrogation, InterNIC (WHOIS) queries, and network sniffing (generally only during internal tests)
- **Employee names and contact information** can be obtained by searching the organization's Web servers or directory servers
- **System information, such as names and shares** can be found through methods such as NetBIOS enumeration (generally only during internal tests) and Network Information System (NIS) (generally only during internal tests)
- **Application and service information**, such as version numbers, can be recorded through banner grabbing.

In some cases, techniques such as dumpster diving and physical walkthroughs of facilities may be used to collect additional information on the targeted network, and may also uncover additional information to be used during the penetration tests, such as passwords written on paper.

Case Projects

Solution

The following is a partial project solution. The students should be able to expand on the following through extensive research:

- **Misconfigurations**. Misconfigured security settings, particularly insecure default settings, are usually easily exploitable.
- **Kernel Flaws**. Kernel code is the core of an OS, and enforces the overall security model for the system—so any security flaw in the kernel puts the entire system in danger.
- **Buffer Overflows**. A buffer overflow occurs when programs do not adequately check input for appropriate length. When this occurs, arbitrary code can be introduced into the system and executed with the privileges—often at the administrative level—of the running program.
- **Insufficient Input Validation**. Many applications fail to fully validate the input they receive from users. An example is a Web application that embeds a value from a user in a database query. If the user enters SQL commands instead of or in addition to the requested value, and the Web application does not

filter the SQL commands, the query may be run with malicious changes that the user requested—causing what is known as a SQL injection attack.

- **Symbolic Links**. A symbolic link (symlink) is a file that points to another file. Operating systems include programs that can change the permissions granted to a file. If these programs run with privileged permissions, a user could strategically create symlinks to trick these programs into modifying or listing critical system files.
- **File Descriptor Attacks**. File descriptors are numbers used by the system to keep track of files in lieu of filenames. Specific types of file descriptors have implied uses. When a privileged program assigns an inappropriate file descriptor, it exposes that file to compromise.
- **Race Conditions**. Race conditions can occur during the time a program or process has entered into a privileged mode. A user can time an attack to take advantage of elevated privileges while the program or process is still in the privileged mode.
- **Incorrect File and Directory Permissions**. File and directory permissions control the access assigned to users and processes. Poor permissions could allow many types of attacks, including the reading or writing of password files or additions to the list of trusted remote hosts.

Optional Team Case Project

Solution

The following is a partial project solution. The students should be able to expand on the following through extensive research:

Penetration test scenarios should focus on locating and targeting exploitable defects in the design and implementation of an application, system, or network. Tests should reproduce both the most likely and most damaging attack patterns—including worst-case scenarios such as malicious actions by administrators. Since a penetration test scenario can be designed to simulate an inside attack, an outside attack, or both, external and internal security testing methods are considered. If both internal and external testing is to be performed, the external testing usually occurs first.

Outsider scenarios simulate the outsider-attacker who has little or no specific knowledge of the target and who works entirely from assumptions. To simulate an external attack, testers are provided with no real information about the target environment other than targeted IP addresses or address ranges, and perform open source research by collecting information on the targets from public Web pages, newsgroups, and similar sites. Port scanners and vulnerability scanners are then used to identify target hosts. Since the testers' traffic usually goes through a firewall, the amount of information obtained from scanning is far less than if the test were undertaken from an insider perspective. After identifying hosts on the network that can be reached from outside, testers attempt to compromise one of the hosts. If successful, this access may then be used to compromise other hosts that are not generally accessible from outside the network. Penetration testing is an iterative process that leverages minimal access to gain greater access.

Insider scenarios simulate the actions of a malicious insider. An internal penetration test is similar to an external test, except that the testers are on the internal network (behind the firewall) and have been granted some level of access to the network or specific network systems. Using this access, the penetration testers try to gain a greater level of access to the network and its systems through privilege escalation. Testers are provided with network information that someone with their level of access would normally have—generally as a standard employee, although depending on the goals of the test it could instead be information that a system or network administrator might possess.

Penetration testing is important for determining the vulnerability of an organization's network and the level of damage that can occur if the network is compromised. It is important to be aware that depending on an organization's policies, testers may be prohibited from using particular tools or techniques or may be limited to using them only during certain times of the day or days of the week. Penetration testing also poses a high risk to the organization's networks and systems because it uses real exploits and attacks against production systems and data. Because of its high cost and potential impact, penetration testing of an organization's network and systems on an annual basis may be sufficient. Also, penetration testing can be designed to stop when the tester reaches a point when an additional action will cause damage. The results of penetration testing should be taken seriously, and any vulnerabilities discovered should be mitigated. Results, when available, should be presented to the organization's managers. Organizations should consider conducting less labor-intensive testing activities on a regular basis to ensure that they are maintaining their required security posture. A well-designed program of regularly scheduled network and vulnerability scanning, interspersed with periodic penetration testing, can help prevent many types of attacks and reduce the potential impact of successful ones.

CHAPTER 31: BUILDING A SECURE ORGANIZATION

Review Questions/Exercises

True/False

1. True
2. True

3. False
4. False
5. True

Multiple Choice

1. A
2. A
3. D
4. C
5. A

Exercise

Solution

The following is a partial exercise solution. The students should be able to expand on the following:

When a vulnerability is exploited the impact will be a security violation. Denial of Service (DoS) and Privilege escalation are two dangerous impacts. Vulnerabilities are exploited by Malware such as viruses, trojan horses, worms, spyware and so on. Malicious hackers compromise the systems through vulnerability exploitation

Hands-on Project

Solution

The following is a partial project solution. The students should be able to expand on the following:

The default scanning process will not have any impact on your server resources. However, when a scanning is performed with custom options such as scanning all the ports or scanning by connecting to the ports, there will be very low impact on performance. You can assigh a custom scan timings such as out-of-office hours to perform such resource intensive scans.

Case Projects

Solution

The following is a partial project solution. The students should be able to expand on the following through extensive research:

Open Vulnerability and Assessment Language (OVAL®) is an international, information security, community standard to promote open and publicly available security content, and to standardize the transfer of this information across the entire spectrum of security tools and services. OVAL includes a language used to encode system details, and an assortment of content repositories held throughout the community. The language standardizes the three main steps of the assessment process: representing configuration information of systems for testing; analyzing the system for the presence of the specified machine state (vulnerability, configuration, patch state, etc.); and reporting the results of this assessment. The repositories are collections of publicly available and open content that utilize the language.

Optional Team Case Project

Solution

The following is a partial project solution. The students should be able to expand on the following through extensive research:

OVAL itself is not a vulnerability scanner. Rather, it is an open language to express checks for determining whether software vulnerabilities—and configuration issues, programs, and patches—exist on a system. OVAL allows the sharing of technical details regarding how to identify the presence or absence of vulnerabilities on a computer system. The public nature of OVAL provides computer security researchers, software vendors, and system administrators with the means to collaborate to develop OVAL definitions. The end user of an OVAL-compliant tool benefits from this collaboration because of increased quality from the number of experts participating in the development of definitions, and now has the option of personally reviewing the individual definitions to see exactly how the vulnerability determination was made. This is in direct contrast to closed, proprietary methods of vulnerability assessment.

CHAPTER 32: SECURITY METRICS: AN INTRODUCTION AND LITERATURE REVIEW

Review Questions/Exercises

True/False

1. False
2. False
3. True
4. False
5. True

Multiple Choice

1. C
2. D

3. A
4. D
5. E

Exercise

Solution

The following is a partial exercise solution. The students should be able to expand on the following:

There are *loads* of sources of inspiration if you are hunting for security metrics. For now, here is a shortlist: Consider existing security metrics, or indeed other kinds of metrics already used by your organization. Use standards such as ISO/IEC 27004 (not the best example, admittedly!) Take advice from professional bodies such as ISACA and the Information Security Forum. Use your social networks: ask professional colleagues and peers, raise metrics at the next ISSA meeting or security conference, or discuss it online! Finding possible metrics (information-security-related things that could be measured) is very much the easy part. Deciding which of the thousands of candidate security metrics are actually worth measuring, reporting and using is a different matter entirely.

Hands-on Project

Solution

The following is a partial project solution. The students should be able to expand on the following:

Reporting security metrics often implies a rather tedious written management report stuffed with graphs and tables, but there are sound reasons for being far more creative in your approach. For a start, think about who you are reporting *to*. What do *they* want from you? What type or types of communication do *they* prefer - written reports with all the gory details, short executive summaries, web pages, presentations, rough notes discussed over coffee or something else?

Often it is better to discuss security metrics with the recipients rather than simply submitting a report. Discussion gives everyone the chance to explain things, ask questions, provide feedback, and generally mull over the information. Given that the prime purpose of metrics is for decision support, discussion and persuasion seems far more likely to facilitate sensible decisions than passively providing written information in a report, although it makes sense to provide the figures, graphs *etc.* on paper or on screen as well as discussing them - the best of both worlds.

A bonus to presenting and discussing security metrics is the opportunity to get instant feedback on the metrics themselves, and to make sure that everyone understands exactly what is being measured, why and how if necessary. Simple security metrics are generally self-evident but more complicated or convoluted ones deserve and may in fact *require* explanation.

Case Projects

Solution

The following is a partial project solution. The students should be able to expand on the following through extensive research:

Metrics that are *inherently* bad (in the sense of having low scores, low utility, low value) should not be used. If however the measurements themselves - the *numbers* - are bad, that is a different matter entirely.

Good metrics sometimes do show bad numbers for two reasons: either the subjects of measurement have turned bad in some measurable way (for example, the actual rate and/or severity of security incidents has markedly increased) or the measurement process has gone wrong (for example, security incidents are occurring at about the same rate as ever but the *reporting* of incidents has dramatically improved, or new sources of information such as additional classes of incident reports have been incorporated into the metric). Either way, that is potentially useful information provided it can be explained and understood - and to do that will probably require additional analysis and information. This is where the ability to dig deeper, going beneath the headline figures to identify the specific factors involved, pays off. Interpreting security metrics combines science with art!

Reporting really bad numbers may not seem a sensible move - indeed, in extreme cases, it could be career-limiting. On the other hand, *not* reporting those numbers could have severe if the information in question, or the fact that it was withheld, eventually comes out. On top of that, the recipients of metrics may well smell a fish if a regular report is late or doesn't show up, or the figures appear suspiciously good, or the written analysis and/or verbal description paint a rosier picture than the numbers (discordant reporting). It takes guts to report really bad numbers.

Just remember that bad numbers focus attention on issues and present improvement opportunities. Good numbers tend to just wash over us, having little impact and hence limited information value. In fact, the most useful metrics tend to highlight and provide some explanation for *changes* in values rather than absolute numbers. If the numbers are consistently good, why bother reporting them when there are doubtless other issues that deserve attention? [This is a common complaint about those voluminous Service Level Accounting reports often delivered by service providers to their customers. Is the real reason why so many numbers are presented simply to hide or divert attention from the few bad ones?]

Optional Team Case Project

Solution

The following is a partial project solution. The students should be able to expand on the following through extensive research:

While decisions *can* be made on a whim, many business decisions have serious consequences, hence the risk of making wrong decisions, or indeed not making necessary decisions in time, can be substantial. Gathering and assessing information that is relevant and timely for a decision could therefore be deemed a risk management activity, and naturally metrics are a key source of relevant information.

Consider for example the use of Ishikawa (fishbone) diagrams in quality assurance and process engineering to assess the factors that contribute to or cause some effect on a process. While approaches vary, a popular method involves analyzing the possible causes of a problems on a process along six lines radiating out from the backbone, each covering one of the **M**s:

- **Manpower**: the people performing activities - are they suitably trained and competent? Are they over- or under-worked? Are they well motivated and energetic?
- **Machines**: including machine tools, computer systems *etc*. - are they working efficiently and effectively? Are they functional and reliable?
- **Materials**: raw materials, supplies and other process inputs - are they of suitable quantity, quality and reliability? Do they always arrive in time or sometimes cause delays? Are they within specifications?
- **Methods**: how people use the machines to perform activities on the materials- are they doing the right things, and doing things right? Are the procedures suitable and efficient, or are there better ways?
- **Mother Nature** (the **Mvironment**): the surroundings in which activities are performed - are they conducive to good work? Is the workplace comfortable and safe, or is it an impediment?
- **Metrics**: measures relating to the process - do we know what is going on and what might be going wrong? Do we have the information necessary to plan, direct, control and improve the process?

Security metrics, then, provide information about the people, the machinery, the inputs, the processes, and the environment, both statically (in planning/designing the process, or reviewing the start-of-day situation in a morning quality meeting) and dynamically (monitoring and where necessary adjusting the process during the course of the day according to events and feedback). Security metrics don't replace the other **M**s - they complement and support them, enabling management to get more out of the available resources and cope with perturbations. Just as importantly, security metrics don't exist in isolation. They have negligible inherent value (information that is just nice-to-know) but immense value for managing business (or indeed other) activities. They have a purpose in life.

CHAPTER 33: CYBER FORENSICS

Review Questions/Exercises

True/False

1. True
2. False
3. True
4. False
5. True

Multiple Choice

1. D
2. D
3. C
4. C
5. E

Exercise

Solution

The following is a partial exercise solution. The students should be able to expand on the following:

The vast majority of documents now exist in electronic form. No investigation involving the review of documents, either in a criminal or corporate setting, is complete without including properly handled computer evidence. Cyber forensics ensures the preservation and authentication of cyber data, which is fragile by its nature and can be easily altered, erased, or subject to claims of tampering without proper handling. Additionally, cyber forensics greatly facilitates the recovery and analysis of deleted files and many other forms of compelling information normally invisible to the user.

Hands-on Project

Solution

The following is a partial project solution. The students should be able to expand on the following:

Most recoveries will be completed in 1–4 days. If you need e*xpedited data recovery*, you'll need a dedicated technician assigned to your drive within 3 hours of the time that you send in your hard disk. This process will normally cut your turnaround time in half. However, if you need e*mergency data recovery*, you will need to make arrangements for a technician to be available who will be assigned to work on your recovery until complete. The goal here is to return your data to you within two to four working days. However, because of the complexity of data recovery, there will be times when it will take longer.

Case Projects

Solution

The following is a partial project solution. The students should be able to expand on the following through extensive research:

There are instances where the damage to the hard drive is so severe that data recovery is not possible. This usually occurs when the read/write heads actually "crash" and gouge the magnetic storage media to the point where the data is destroyed.

However, in a number of cases, data recovery was possible at the time the damage first occurred, but the data became nonrecoverable through the use of commercial-recovery software. This software is designed to recover data from working drives. If your drive has experienced a mechanical or electrical failure, the use of recovery software can cause permanent loss of your data.

Optional Team Case Project

Solution

The following is a partial project solution. The students should be able to expand on the following through extensive research:

Avoid Heat and Vibration

All drive components, both electronic and mechanical, are sensitive to heat and vibration. Keep your computer in a dry, controlled environment that is clean and dust-free. Set up your computer in an area with little traffic to ensure that it does not get bumped. Heat and/or vibration are two of the leading causes of hard drive failure. Also, beware of static.

Back-Up Your Data

The surest way to avoid data loss, even if your hard drive fails, is to back-up your data. If you don't have a tape back-up device or network drive at your fingertips, back-up your most important files at least once a week.

To Avoid Premature Drive Failure,Run Scandisk

Scandisk examines your hard disk for logical inconsistencies and damaged surfaces. Run it every two or three weeks just to be safe. It is important to save any changes until you are sure that the changes you are about to make will not adversely affect your hard drive.

Run Defrag Frequently

Files will most likely not be stored in adjacent clusters. Defrag rearranges the data on your hard disk so that each file is stored in a set of contiguous clusters. This is essential for data recovery because success is more likely when the damaged file's clusters are adjacent to each other.

Antivirus Software

Use antivirus software and update it at least four times a year. Also, use an uninterrupted power supply (UPS).

In the event of a surge of electricity, black out, brown out, or lightning strike, a UPS can protect your system from electrical damage. A UPS is also a back-up power source that keeps your computer running for a short period of time, giving you the opportunity to properly save your work and shut down, avoiding a potential data loss.

Be Cautious When Using Recovery Utilities

Use diagnostic and repair utilities with caution. Verify that your utility software is compatible with your operating software. Never use file-recovery software if you suspect an electrical or mechanical drive failure. Always make an undo disk when you allow a utility to make changes to your hard drive.

CHAPTER 34: CYBER FORENSICS AND INCIDENT RESPONSE

Review Questions/Exercises

True/False

1. True
2. True
3. False
4. True
5. False

Multiple Choice

1. C
2. E
3. D
4. D
5. A

Exercise

Solution

The following is a partial exercise solution. The students should be able to expand on the following:

It is extremely important that your hard drive is packaged carefully—to avoid any additional damage during shipment. Only your drive is required for data recovery.

Packaging the Hard Drive
Wrap the hard drive in an antistatic material. If an antistatic bag is not available, a freezer bag will suffice. It is recommended that you ship the drive in its original manufacturer's packaging. If this is not possible, pack the hard drive in a sturdy corrugated cardboard box twice the size of the drive, with heavy foam padding, bubble wrap, or other antivibration materials. Do not use Styrofoam peanuts as they attract static electricity. Be sure the padding material is at least two inches thick around the drive.

Water-Damaged Hard Drives
If your drive has suffered water damage, please do not dry it. Enclose the drive along with a damp sponge in a sealed plastic bag to prevent it from drying out.

Controller Boards
When recovering from older models, you may need to send the controller along with the drive. Please remove the controller carefully, enclose in antistatic material, and ship it along with the drive.

Other
Please package all other types of media, following the guidelines in the preceding for a typical hard drive.

Locations

Ship the drive directly to the recovery facility nearest you: It is recommended that you ship via UPS or Federal Express domestically and internationally, using next-day service. If you elect to use another carrier, it is suggested that you use an overnight service. Also, if you have any special shipping considerations, questions, or concerns, please contact your overnight carrier

Hands-on Project

Solution

The following is a partial project solution. The students should be able to expand on the following:
If your drive is repairable, the repair will be completed and your data returned to you on your original drive. When your data is recovered and your drive is not repairable, there are many different ways to return your data.

Case Projects

Solution

The following is a partial project solution. The students should be able to expand on the following through extensive research:
There are no answers for this case project. It's just an exercise that students will go through to gain experience.

Optional Team Case Project

Solution

The following is a partial project solution. The students should be able to expand on the following through extensive research:

As soon as possible. While CSI and other forensic television shows primarily provide entertainment, they also accurately emphasize that time is critical for an investigation. The longer a computer or digital device is used or awaits inspection, the higher the probability that the digital evidence will be tainted. Even for computers in storage awaiting discovery for trial, the sooner a computer forensic examiner can preserve the valuable data, the greater the chance of recovering important and relevant evidence.

CHAPTER 35: SECURE E-DISCOVERY

Review Questions/Exercises

True/False

1. False
2. False
3. True
4. True
5. False

Multiple Choice

1. D
2. D
3. C
4. A
5. D

Exercise

Solution

The following is a partial exercise solution. The students should be able to expand on the following:

Although internal IT staff are often highly knowledgeable regarding their working environment and the technology employed within, computer forensic investigations are best performed by outside experts. Specifically, the nature of the forensic analysis process coupled with the requirements by law enforcement agencies and the court system necessitates that computer forensic investigations are performed by external entities equipped with authorized forensic technology and trained to observe forensic protocols. Forensic specialists:

- Employ the proper hardware and software to identify, isolate, and preserve electronic information in a court admissible manner
- Possess the expertise and experience vital to efficiently analyze electronic information and uncover electronic evidence
- Rely upon essential training and experience to ensure the court admissibility of electronic evidence
- Offer truly objective expert testimony that only a third-party computer forensic investigator can
- Expose flaws in opposing counsel's interpretation of electronic evidence and results from their forensic analysis efforts

Hands-on Project

Solution

The following is a partial project solution. The students should be able to expand on the following:

A common misconception is that when information or a specific file is deleted, it is permanently erased from the hard drive. In reality, the act of deleting a file does not actively delete any information. What occurs is a small portion of information that points to the location of the file on the hard drive is erased.

This pointer is used by the operating system to compile the directory tree structure and by removing this pointer file, the actual file becomes invisible to the operating system. Overtime, the location of the unwanted file will be overwritten by new information. Forensic technology exists to locate, reconstruct, and recover information and files that were deleted, however, still exist in total or have been partially overwritten by new data.

Case Projects

Solution

The following is a partial project solution. The students should be able to expand on the following through extensive research:

The fragile and volatile nature of electronic information requires orchestrated efforts to ensure electronic evidence is protected and maintained to facilitate its thorough analysis by a computer forensic specialist and its introduction into an active litigation. Internal technology relevant to an investigation or litigation should be immediately removed from operation and isolated from unauthorized use with a clearly documented chain of custody agreement to ensure electronic evidence is not unintentionally corrupted or overwritten.

If relevant technology is under the management of opposing counsel, a notification of the duty to preserve electronic evidence should be transmitted. This letter should detail the information to be preserved, potential locations of suspect information, listing of people that may have access to the technology, and all potential storage media where the information may reside, such as hard drives, CD-ROMs, and backup tapes. If necessary, an injunction or preservation order forbidding the deletion or manipulation of electronic information can be obtained.

Optional Team Case Project

Solution

The following is a partial project solution. The students should be able to expand on the following through extensive research:

Spoliation is the intentional or negligent destruction or alteration of evidence when there is current litigation or an investigation or there is reasonable anticipation that either may occur in the near future. Some jurisdictions also define it as a failure to preserve information that may become evidence. To address spoliation and minimize threats to the forensic integrity of electronic evidence and its admissibility in a litigation, technology potentially containing electronic evidence must be handled methodically and in response to the fragile and volatile nature of electronic information.

When litigation arises, corporate counsel needs to think both offensively and defensively about managing electronic evidence. Preservation memos should be sent to all employees who have potentially relevant data, specifically identifying each type of system records that may have relevance to the case. Monitoring preservation compliance is extremely important to avoid spoliation sanctions. Technology relevant to an investigation or litigation should be immediately removed from operation and isolated from unauthorized use with a clearly documented chain of custody agreement to ensure electronic evidence is not unintentionally corrupted or overwritten. Furthermore, the nature of the forensic analysis process coupled with the requirements by law enforcement agencies and the court system necessitates that computer forensic investigations are performed by certified experts equipped with authorized forensic technology and trained to observe forensic protocols to greatly reduce the risk of error, omission, or direct damage to the forensic integrity of electronic evidence.

CHAPTER 36: NETWORK FORENSICS

Review Questions/Exercises

True/False

1. False
2. False
3. True
4. False
5. True

Multiple Choice

1. A
2. A
3. C
4. D
5. A

Exercise

Solution

The following is a partial exercise solution. The students should be able to expand on the following:

With a network forensics analysis, data is always available for reconstruction, with an easy analysis of intermittent issues, cyber attacks, and network security or data breaches. All pertinent network traffic is collected in a single location, rather than scattered across the network. Data is captured in a common data format and does not need to be transferred or translated in any way for analysis.

Using network forensics data mining tools, network engineers have the data they need to identify and fix problems users are complaining about that only occur intermittently, and security teams can reconstruct the sequence of events that occur at the time of a network breach or cyber attack and get the complete picture. Network forensics data mining tools, will enable you to analyze data at the point of capture, and eliminate the need for large data transfers that consume time and bandwidth.

Hands-on Project

Solution

The following is a partial project solution. The students should be able to expand on the following:

24 × 7 access to all network data and network forensics mining tools lets an organization do the following:

- Ensure network and security data are captured 24 × 7 and not sacrificed when SPAN ports are needed for other applications
- Reduce Mean-Time-To-Resolution (MTTR) by eliminating the time consuming step of having to reproduce problems before they can be analyzed and responding to issues in real-time, often solving issues before mission critical applications are impacted
- Understand service-level compliance within your organization
- Comply with government regulations and Human Resources policies by auditing and tracking all network activity

Case Projects

Solution

The following is a partial project solution. The students should be able to expand on the following through extensive research:

A network forensics analysis solution offers the following capabilities:

- **Comprehensive data collection:** Hours or even days of network traffic —anything that crosses the network, whether email, IM, VoIP, FTP, HTML, or some other application or protocol — collected by a single system and stored in a common, searchable format. Terabytes of data are available through a single interface.
- **Flexible data collection:** Collects all data on a network segment for future inspection or focus on a specific user or server.
- **High-level analysis:** Eliminates the need for brute-force analysis across disparate data sources.

Optional Team Case Project

Solution

The following is a partial project solution. The students should be able to expand on the following through extensive research:

- Network performance benchmarking for detailed reporting on network performance, bottlenecks, activates, etc.
- Network troubleshooting for handling any type of network problem, especially those that happen intermittently.
- Transactional analysis for providing the “ultimate audit trail” for any transactions where server logs and other server-based evidence doesn’t provide a thorough picture of a transaction. Remember, packets don’t lie!

- Security attack analysis for enabling security officers and IT staff to characterize and mitigate an attack that slipped past network defense such as a zero day attack.

Intermittent Issues

- Capture and analyze intermittent network problems
- Troubleshoot problems that occurred hours or days ago
- Find the patterns that ad hoc, reactive troubleshooting will miss

Security Cyber Attack Analysis

- Detect and characterize attacks—whether they've just begun or occurred days ago
- Apply filters to isolate malicious behavior
- Equip your network IT team with a powerful incident response tool

Transaction Analysis

- Create the ultimate audit trail for business transactions—not just server activity but the business transactions enacted by clients and servers
- Troubleshoot the transaction problems that server logs miss

CHAPTER 37: DATA ENCRYPTION

Review Questions/Exercises

True/False

1. False
2. False
3. True
4. False
5. False

Multiple Choice

1. A
2. A
3. AB
4. C
5. D

Exercise

Solution

The following is a partial exercise solution. The students should be able to expand on the following:

Subsequent processing of the protected data (decryption) is accomplished using the same key as was used to protect the data. Each 64-bit key shall contain 56 bits that are randomly generated and used directly by the algorithm as key bits. The other eight bits, which are not used by the algorithm, may be used for error detection. The eight error-detecting bits are set to make the parity of each 8-bit byte of the key odd. That is, there is an odd number of "1"s in each 8-bit byte.

Hands-on Project

Solution

The following is a partial project solution. The students should be able to expand on the following:

A TDEA key consists of three keys for the cryptographic engine (***Key*1**, ***Key*2** and ***Key*3**); the three keys are also referred to as a key bundle (***KEY***). Two options for the selection of the keys in a key bundle are **approved**. Option 1, the preferred option, employs three unique keys (***Key*1**, ***Key*2** and ***Key*3**, where ***Key*1≠*Key*2**, ***Key*2≠*Key*3**, and ***Key*3≠*Key*1**). Option 2 employs two unique keys and a third key that is the same as the first key (***Key*1**, ***Key*2** and ***Key*3**, where ***Key*1≠*Key*2** and ***Key*3 = *Key*1**). A key bundle **shall not** consist of three identical keys.

Case Projects

Solution

The following is a partial project solution. The students should be able to expand on the following through extensive research:

- Be kept secret.
- Be generated using an approved method that is based on the output of an approved random bit generator.
- Be independent of other key bundles.
- Have integrity whereby each key in the bundle has not been altered in an unauthorized manner since the time it was generated, transmitted, or stored by an authorized entity.
- Be used in the appropriate order as specified by the particular mode.
- Be considered a fixed quantity in which an individual key cannot be manipulated while leaving the other two keys unchanged; and cannot be unbundled except for its designated purpose.

Optional Team Case Project

Solution

The following is a partial project solution. The students should be able to expand on the following through extensive research:

- 01010101 01010101
- FEFEFEFE FEFEFEFE

- E0E0E0E0 F1F1F1F1
- 1F1F1F1F 0E0E0E0E

CHAPTER 38: SATELLITE ENCRYPTION

Review Questions/Exercises

True/False

1. True
2. False
3. True
4. True
5. True

Multiple Choice

1. A, B
2. B
3. A
4. D
5. A

Exercise

Solution

The following is a partial exercise solution. The students should be able to expand on the following:

An encryption security team simply used generally-available phone equipment, found the crypto key and managed to break it fairly easily by analyzing the software running on the satphones.

Hands-on Project

Solution

The following is a partial project solution. The students should be able to expand on the following:

The bank opted first for a hardware solution, but quickly realized that a software solution delivered greater long-term flexibility. Like many financial companies that take their responsibilities for data security very seriously, bank decided to encrypt their satellite data backups to protect sensitive customer and bank data. Initially, the hardware approach was attractive as it was faster, fully integrated, easy to implement and appeared to manage every part of the satellite data encryption process. However, soon after installation, the bank began to realize the disadvantages of relying primarily on a hardware solution.

As the bank began to explore satellite encryption software options, they decided to demo and compare trial versions from the market's two primary leaders. The selected solutions were roughly comparable in terms of price (which was much less than a hardware device) and functionality. They both were easy to install, configure and use. The software documentation was more detailed regarding the required steps and configuration options to implement satellite encryption into their backup routine.

Case Projects

Solution

The following is a partial project solution. Students should be able to expand on the project analysis through extensive research.

The solution is to develop an entirely new hardware platform and incorporate control software and encryption into it. The new platform should be of the kind that is widely used in commercial grade receivers in the industry.

Optional Team Case Project

Solution

The following is a partial solution to aid students in coming up with their own solution to solve this case:

The company redesigned their commercial grade satellite receiver, while incorporating their encryption system at a reduced cost. They delivered over 200,000 satellite receivers and met all delivery schedules.

CHAPTER 39: PUBLIC KEY INFRASTRUCTURE

Review Questions/Exercises

True/False

1. False
2. False
3. True
4. True
5. True

Multiple Choice

1. B
2. B
3. D
4. A
5. E

Exercise

Solution

The following is a partial exercise solution. The students should be able to expand on the following:

Public-key cryptography is becoming a vital business tool for any organisation that seeks to protect its information assets in potentially untrusted network environments. The use of public-key cryptography makes it possible to:

- Encrypt communications (when sending confidential e-mail over an untrusted network)
- Detect unauthorised changes to data transmitted over networks
- Positively identify and authenticate remote users over networks (when required to provide access to sensitive systems)
- Digitally sign information (when authorising services electronically and where evidential value is important)
- Ensure users cannot repudiate their actions at a later date (when required to confirm the identity of the specific user who sent a particular message or instruction over an untrusted network).

Hands-on Project

Solution

The following is a partial project solution. The students should be able to expand on the following:

There are some practical problems associated with the use of public-key cryptography that, unless properly addressed, serve to undermine the above capabilities and cast doubt on the trustworthiness of any system that employs it. Foremost amongst these is the management of cryptographic keys where a lack of control could lead to the:

- Inability to update or renew keys
- Inability to recover data encrypted with an old key
- Continued use of a compromised or lapsed key.

Other considerations that arise as a consequence of using public-key cryptography include:

- Protecting public keys from impersonation and forgery
- Making public-key cryptography available to a wide number of users in a manner that is consistent and reliable
- Making public-key cryptography transparent to end-users.

Case Projects

Solution

The following is a partial project solution. Students should be able to expand on the project analysis through extensive research.

A PKI addresses these issues by:

- Managing keys throughout their life cycle
- Using digital certificates to protect and assure the authenticity of public keys
- Providing a consistent, dependable and scalable infrastructure for the use of public-key cryptography.

By providing an environment for the reliable use of authentication, confidentiality, integrity and non-repudiation services, a PKI can help to provide the trust that is necessary to conduct business in insecure networked environments.

Optional Team Case Project

Solution

The following is a partial solution to aid students in coming up with their own solution to solve this case:

A typical PKI consists of seven core components. These are briefly described below:

1. Digital certificates (public-key certificates, X.509 certificates): A digital certificate is a signed data structure that binds one or more attributes of an entity with its corresponding public key. By being signed by a recognised and trusted authority (the Certification Authority) a digital certificate provides assurances that a particular public key belongs to a specific entity (and that the entity possesses the corresponding private key).
2. Certification Authority (CA): Certification Authorities are the people, processes and tools that are responsible for the creation, issue and management of public-key certificates that are used within a PKI.
3. Registration Authority (RA) : Registration Authorities are the people, processes and tools that are responsible for authenticating the identity of new entities (users or computing devices) that require certificates from CAs. RAs additionally maintain local registration data and initiate renewal or revocation processes for old or redundant certificates. They act as agents of CAs (and

in that regard can carry out some of the functions of a CA if required).

4. Certificate repository: A database, or other store, which is accessible to all users of a PKI, within which public-key certificates, certificate revocation information and policy information can be held.
5. PKI client software: Client-side software is required to ensure PKI-entities are able to make use of the key and digital certificate management services of a PKI (key creation, automatic key update and refreshment).
6. PKI-enabled applications: Software applications must be PKI-enabled before they can be used within a PKI. Typically this involves modifying an application so that it can understand and make use of digital certificates (to authenticate a remote user and authenticate itself to a remote user).
7. Policy (Certificate Policy and Certification Practice Statement): Certificate Policies and Certification Practice Statements are policy documents that define the procedures and practices to be employed in the use, administration and management of certificates within a PKI.

Under certain circumstances other PKI components may also be required, including:

- A trusted time-stamping service (where it is important to keep an accurate record of the precise timing of events).
- A Validation Authority (where automatic, real-time validation of certificates is required, for example in highly critical systems).
- A notary service (where it is important to ensure accurate records of all transactions are lodged and maintained in a secure manner, for example where the implications of a PKI user repudiating their actions would be damaging or costly).

In addition to the above components a PKI must operate within an IT infrastructure (a network with servers and client computers). This infrastructure must be able to support the processing, resilience and performance demands of a PKI.

CHAPTER 40: PASSWORD-BASED AUTHENTICATED KEY ESTABLISHMENT PROTOCOLS

Review Questions/Exercises

True/False

1. False
2. True
3. True
4. True
5. False

Multiple Choice

1. D
2. C
3. C
4. B
5. D

Exercise

Solution

The following is a partial exercise solution. The students should be able to expand on the following:

This implies that no mechanism can be in place to directly ensure at either end of the protocol that the correct password is being used by the other party. For instance, the password cannot satisfy any kind of efficiently verifiable equation, which happens to be the flaw of the dummy protocol. In contrast, this is exactly how a digital signature scheme functions, the key difference again being that the long-term secret is cryptographically strong. This is the method behind STS.

Hands-on Project

Solution

The following is a partial project solution. The students should be able to expand on the following:

In this work, the protocol and several of its variants have been *proven secure*(a very precise mathematical proof of security was given assuming that the encryption function satisfies some idealized properties). This is methodologically important and theoretically interesting; however, such proofs do not necessarily immediately translate into real-world security guarantees.

Case Projects

Solution

The following is a partial project solution. Students should be able to expand on the project analysis through extensive research.

As with EKE, the prime p has to be at least 1024 bits in length, so as to be sure the computing discrete logarithms will be difficult. Thus, also as in EKE, the random numbers chosen by the parties are quite large: at least 1023 bits in this case.

Optional Team Case Project

Solution

The following is a partial solution to aid students in coming up with their own solution to solve this case:

The purpose of the protocol is for P to convince V that a certain statement is true without revealing any more information on that statement. For this to be of any use to V, it should be infeasible for a cheating P to trick V into believing a false statement.

CHAPTER 41: INSTANT-MESSAGING SECURITY

Review Questions/Exercises

True/False

1. True
2. False
3. True
4. False
5. True

Multiple Choice

1. C
2. D
3. C
4. C
5. E

Exercise

Solution

The following is a partial exercise solution. The students should be able to expand on the following:

Fundamentally, the difference between IM and email is the notion of presence. This means that users of the IM system are aware that other users have logged in and are willing to accept messages. Unlike email, IM content can only be sent to users who are logged in to the system and accepting messages. If users are not logged in, others do not have the ability to send them messages. Because IM is not predicated upon an open standard, there is no uniformity regarding message transmission and structure.

Hands-on Project

Solution

The following is a partial project solution. The students should be able to expand on the following:

Organizations developing a comprehensive policy need to ensure that IM content is managed consistently across the organization in its component offices. An effective policy addresses the authorized use of the IM technology and provides guidelines for the management of the records generated during an IM session. This is especially important because IM content may be subject to various types of access requests, including under the Freedom of Information Act (FOIA) or as part of a discovery process in a litigation context.

IM content that is a record must be managed as such. Here are two ways:

- Provide policies that inform users what steps to undertake to manage the content; or,
- Configure the IM client or server to capture IM without user intervention.

Case Projects

Solution

The following is a partial project solution. Students should be able to expand on the project analysis through extensive research.

Nearly all IM client software has the ability to capture the content as either a plain text file or in a format native to that client. Generally, the location and maximum size of that file is determined by a configuration setting in the client. Such formats include those files produced by the various IM clients.

In addition, various IM management products have the ability to address the monitoring and management of IM content, either from those clients that are part of the agency's enterprise or the various public clients. Generally, these products operate at the server level and should be able to capture IM sessions regardless of the configuration of the individual client. Determining which solution is appropriate for your organization involves collaboration among the program staff, the information technology (IT) staff and the records management staff.

Optional Team Case Project

Solution

The following is a partial solution to aid students in coming up with their own solution to solve this case:

If an organization determines IM content to be a record, the record must have an approved disposition authority. Do not identify IM content as a single series of records with a universal disposition. Instead, evaluate IM content within the context of the overall records of the program to which the IM relates and the business rules that may apply. Disposition instructions for IM should be consistent with similar organization records. Schedule in accordance with the organization 's established records management policy. IM records may already be scheduled as part of other series, such as records typically found in a case file or a correspondence system.

CHAPTER 42: PRIVACY ON THE INTERNET

Review Questions/Exercises

True/False

1. True
2. False
3. False
4. False
5. False

Multiple Choice

1. C
2. D
3. A
4. A
5. B

Exercise

Solution

The following is a partial exercise solution. The students should be able to expand on the following:

Many websites that collect personal information also publish privacy policies or privacy statements that describe how the site will use your information. Before entering any personal information into a website, you should read the privacy statement carefully, especially if you are unfamiliar with the site. Look for conditions that you do not agree with, such as allowing the website to share your information with others or the requirement that you will accept e-mail or advertising. Remember that even though the website might have a privacy statement, it doesn't mean that the website will not misuse your information. You should not give personal information to a website you do not trust.

Hands-on Project

Solution

The following is a partial project solution. The students should be able to expand on the following:

Most online merchants use secure connections to provide an encrypted connection between Internet Explorer and the website. Encrypted connections make it difficult for a hacker to intercept your personal or financial information as it is being sent to the website. This encryption is provided by a security certificate, which is an electronic document that identifies the website. Although encryption can help protect your information as it travels over the Internet, it doesn't guarantee that the website is reputable or that they protect your information once they receive it.

Case Projects

Solution

The following is a partial project solution. Students should be able to expand on the project analysis through extensive research.

Filtering can help you control whether information about the websites you visit is shared with other content providers. When you visit a website that displays content from another content provider, that content provider automatically receives some information about your visit. If you visit additional websites that have content from the same provider, that content provider can build a profile of your browsing habits. This information can be sold to other websites, or used for things such as targeted advertising.

Optional Team Case Project

Solution

The following is a partial solution to aid students in coming up with their own solution to solve this case:

Browsing can help you browse the web without leaving a trail on your computer while you're using the web. This can be helpful when using a public kiosk or if you don't want others who use your computer to see where you've been.

CHAPTER 43: PHYSICAL SECURITY ESSENTIALS

Review Questions/Exercises

True/False

1. True
2. False
3. False
4. False
5. True

Multiple Choice

1. E
2. D
3. A
4. A
5. B

Exercise

Solution

The following is a partial exercise solution. The students should be able to expand on the following:

Cyber crime is growing and has become more organized and sophisticated. As we increasingly perform high-value transactions online such as mortgage applications, buying stocks, or reviewing health care information, our vulnerability to theft, fraud, and privacy violations increases proportionately.

Sixty years ago, before the invention of the credit card, people simply accepted the danger inherent in carrying cash with them to make a large payment. Today we accept the dangers of using easy-to-break passwords and providing personal information to dozens of different Web sites as the cost of doing business on the Internet. But we don't have to.

Privacy enhanced technologies exist now to make online transactions more secure, private, and more convenient. NSTIC offers a vision of the future where the private sector, civil societies, and the public sector collaborate to create the standards and policies needed for interoperable trusted credentials that would dramatically reduce ID theft and fraud online. In addition, by acting now and creating a more trusted environment for online transactions, we will ensure that the Internet continues to support innovation and the creation of new jobs.

Hands-on Project

Solution

The following is a partial project solution. The students should be able to expand on the following:

No. Like the bank card and PIN you use to obtain money from an ATM, having a password and a credential in physical form such as a cell phone, token, or smart card is much more secure than passwords alone. In addition, you may choose to have multiple credentials from different identity providers. However, even a single Identity Ecosystem credential is privacy-enhancing, because it can send different types of information to different service providers. For example, you could use your credential to log in to your online magazine subscription as "John568," because the magazine doesn't need to know your real name. But if you want to access your medical records, the same credential could prove that you are truly "John Smith."

Past experience has shown that "multi-factor authentication" is much more secure than passwords alone. For example, a bank could issue you both a physical device, such as a key fob (something you have), combined with a short PIN number (something you know) to access your accounts. This two-factor method would make it much more difficult for thieves to break into your accounts. Your cell phone could also carry a digital certificate (something you have) that requires a password (something you know).

The key is that you can have multiple trusted identity credentials, and even if you lose the physical device, a cyber criminal still can't assume your identity without your PIN or password. Having even a few PIN numbers or passwords - should you choose to use multiple credentials - would be much more convenient than the dozens of passwords most people are forced to remember now. Also, should a credential be lost, you can more easily notify all necessary parties to secure accounts through the credential provider, rather than having to notify each individually. The ID provider would then discontinue that credential and issue you a new one, helping to minimize the likelihood of unauthorized activity.

No solution, of course, is a magic fix for all possible cybersecurity risks, and NSTIC does not claim to have answers to all threats associated with online transactions. It is, however, a major step forward in making the growing number of online transactions more convenient, more secure and more private.

Case Projects

Solution

The following is a partial project solution. Students should be able to expand on the project analysis through extensive research.

One of the first actions for the National Program Office once it is established will be to convene a workshop for companies, privacy advocates, and other stakeholders to develop a steering group for the Identity Ecosystem. This group would administer the process for developing the technical standards and policies needed for the Identity Ecosystem. A community of members with similar goals and perspectives (known as a trust framework) can hold its members accountable to follow specific standards and policies. An accreditation authority would assure that individual service providers adhered to accepted Identity Ecosystem practices. Those who violate the rules would lose their trustmark status. Furthermore, the role of the government in the Identity Ecosystem is to ensure that individuals are protected from serious harm.

Optional Team Case Project

Solution

The following is a partial solution to aid students in coming up with their own solution to solve this case:

New ways of conducting business in the marketplace sometimes create uncertainty. If the marketplace does not respond in a timely way to that ncertainty with ways to ensure that privacy is protected and limits on liability are described then changes to current federal laws may be necessary.

CHAPTER 44: PERSONAL PRIVACY POLICIES

Review Questions/Exercises

True/False

1. False
2. True
3. True
4. True
5. True

Multiple Choice

1. D
2. C
3. C
4. B
5. D

Exercise

Solution

The following is a partial exercise solution. The students should be able to expand on the following:

When providing copies of information for others, do employees make sure that nonessential information is removed and that personally identifiable information that has no relevance to the transaction is either removed or masked?

Are employees trained never to leave computer terminals unattended when personally identifiable information is on the screen?

Do you use password-activated screen-saver programs?

Are all employees who handle personal information—including temporary, back-up and contract staff—trained to detect when they are being "pumped" for personal information by unauthorized and unscrupulous persons? "Pretext" interviews are more common than might be expected and are the stock in trade of persons bent on finding out confidential personal information to which they are not entitled.

Do you perform background checks on prospective employees who will have access to personal information of customers, clients, or employees?

Have employees been instructed on what might constitute inappropriate use of social networking sites? Employees must be made aware of the privacy pitfalls inherent in social media. "Twittering" or "Facebooking" about sensitive work issues can have adverse consequences far beyond a simple conversation.

Have you inventoried the various types of data being stored and classified it according to how important it is and how costly it would be to the organization if it were lost or stolen?

Hands-on Project

Solution

The following is a partial project solution. The students should be able to expand on the following:

Does your organization have a records retention/disposal schedule for personally identifiable information, whether stored in paper, micrographic or electronic (computer) media? Customer records stored electronically or in paper files are a company asset, just like the furniture or the computers. Not only that, but customers' personal information, unlike the furniture, is subject to a myriad of laws that dictate privacy protections, safeguarding measures, and proper disposal. Even in hard times, when a company has to close its doors, customer data should never be abandoned or left at the curb for the trash collector. Such actions could subject owners, even of a defunct business, to unwanted lawsuits by customers and government regulators.

When disposing of computers, diskettes, magnetic tapes, CD-ROMs, hard drives, memory sticks, mother boards, and any other electronic media which contain personally identifiable information, are all data rendered unrecoverable by either physically destroying the device or by over-writing the data sufficiently to ensure destruction?

If you use third-party services for computer recycling or destruction, have you selected a service that provides a certificate of destruction? Does it dispose of toxic materials properly?

As an asset, customer data may be up for sale in the case of bankruptcy. However, all parties to a bankruptcy should be familiar with the Federal Trade Commission's lawsuit brought against ToySmart under Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45(a), for disclosing, selling or offering for sale personal customer information, contrary to the terms of the company's privacy policy that personal information would never be disclosed to third parties.

When disposing of waste and recycling paper, are all documents that contain personally identifiable information placed in secure padlocked containers or shredded?

(Shredding should be cross-cut, diamond-cut, or confetti-cut shredding, not simply continuous [single-strip] shredding, which can be reconstructed.) Does your recycling company certify its disposal/destruction methods? Is it bonded?

When engaging an external business to destroy records or electronic media, do you check references? Do you insist on a signed contract spelling out the terms of the relationship? Do you visit the destruction site and require that a certificate of destruction be issued upon completion?

When dealing with another company or government agency, do you ask about its security protocol regarding personal information? Do you inquire whether it shares that information with anyone? Do you find out if it does background checks on employees with access to your personal information. Contracts with outside service providers as well as employee agreements should specify that customer data is the company's exclusive property and should only be used as necessary to carry out contractor or employment duties. Such contracts and agreements should also incorporate the company's privacy and data security policies. Contracts should also delineate the service provider's specific obligations, rather than simply stating that the contractor will comply with all applicable laws.

Case Projects

Solution

The following is a partial project solution. Students should be able to expand on the project analysis through extensive research.

Is the fax machine in a supervised area, off-limits to unauthorized persons? Is use restricted to authorized personnel only?

Is the fax machine used exclusively for sending non-confidential materials?

When sending documents, do all users complete a cover sheet that indicates the sender's and receiver's names, addresses and telephone numbers?

When confidential materials are sent, is notice of their confidential nature indicated on the cover sheet?

Do users always check the receiver's telephone number before transmitting documents? Do they compare the number displayed with number being called to check for errors? Do they check the transmission report after the fax has been sent?

When transmitting confidential materials, is the recipient notified in advance that the document is being sent? Does the sender check with the receiver to make sure the document has been received?

Optional Team Case Project

Solution

The following is a partial solution to aid students in coming up with their own solution to solve this case:

These machines are capable of storing an image of every document that has been copied, scanned, printed, emailed, or faxed. Although it may be stored in a proprietary language or encrypted, a hacker can easily gain access to years of sensitive data. Some machines don't even require hacking because they may allow jobs to be reprinted from a printed job list. Sophisticated copiers may contain a list of user's email addresses, outgoing fax numbers, and contact names. All of this information can easily be transferred from the copier to a hacker's laptop. Accordingly, simply disposing of this equipment presents a significant opportunity for a security breach.

While much of the hard drive space in many machines is used for processing, the drive may also store thousands of pages of information. Once the hard drive memory has been exceeded, files are automatically overwritten. "Cap points" limit the number of pages stored to hard drives, and the cap limitation will vary in each make and model. Depending on the type of machine, information from small print jobs may be stored in random access memory (RAM) only, and the files may be overwritten with each new print request, or lost when the machine is powered off.

Most major manufacturers now offer security or encryption packages to help protect against this problem. However, many businesses fail to pay for this protection. If your equipment does not have this protection, you should erase or remove the copier's hard drive, clear its memory, and change the copier's passcodes.

Does your organization have security procedures in place for deleting digital data from copiers, printers and fax/multifunction machines?

Does your organization recycle or resell copiers, printers or fax/multifunction machines to wholesalers or refurbishers? If so, does your organization take steps been taken to remove any data history?

CHAPTER 45: DETECTION OF CONFLICTS IN SECURITY POLICIES

Review Questions/Exercises

True/False

1. True
2. True
3. False
4. False
5. True

Multiple Choice

1. D
2. A
3. D
4. C
5. A

Exercise

Solution

The following is a partial exercise solution. The students should be able to expand on the following:

Technical feasibility refers only to engineering possibility and is expected to be a "can/cannot" determination in every circumstance. It is also intended to be determined in light of the equipment and facilities already owned by a responsible entity. The responsible entity is not required to replace any equipment in order to achieve compliance with the cyber security standards. When existing equipment is replaced, however, the responsible entity is expected to use reasonable business judgment to evaluate the need to upgrade the equipment, so that the new equipment can perform a particular specified technical function in order to meet the requirements of these standards.

Although some standards do not require documentation and compensating measures when a determination of technical infeasibility has been made, responsible entities are free to do so in every such circumstance. Some standards do require such documentation and compensating measures because of the criticality of the specific requirement.

Hands-on Project

Solution

The following is a partial project solution. The students should be able to expand on the following:

The phrase "reasonable business judgment" has an almost 200-year history in the business and corporation laws of America, Canada, and other Common Law nations. The phrase is meant to inform (any regulatory body or ultimate judicial arbiter of disputes regarding interpretation of these Standards) responsible entities that they have a significant degree of flexibility in implementing cyber security policy standards. Courts generally hold that the phrase indicates reviewing tribunals should not substitute their own judgment for that of the entity under review other than in extreme circumstances. A common formulation indicates that the business judgment of an entity (even if incorrect in hindsight) should not be overturned as long as it was made (1) in good faith (not an abuse or indiscretion), (2) without improper favor or bias, (3) using reasonably complete (if imperfect) information as available at the time of the decision, and (4) based on a rational belief that the decision is in the entity's business interest. This principle, however, does not protect an entity from simply failing to make a decision.

Case Projects

Solution

The following is a partial project solution. Students should be able to expand on the project analysis through extensive research.

As used in these cyber security policy standards, these five terms are intended to be understood generally as follows (although these informal definitions do indicate some degree of overlap, depending upon the context in which the terms are used):

1. DATA: information in a "raw" form; facts which may be represented or symbolized in records.
2. RECORDS: Records typically provide evidence of data, such as a "snapshot" in time of actions and events. A record may be in paper or "electronic" format (either analog or digital, such as "on" videotape or DVD, or "on" or "in" a hard-drive). Typically, official records (such as "business records") can only be modified or revised in compliance with proper and auditable trails, and thus can serve as objective, reliable evidence to demonstrate that a fact, situation or activity has occurred (thereby being usable, for instance, to demonstrate compliance with a requirement of these cyber security policy standards).
3. LOGS: Generally, a log is a specific type or collection of recorded data (generally, as pertaining to a series of similar or related actions or events) that may be generated automatically or manually. At a minimum, logs identify the event, who or what caused the event, and when the event occurred (a "time-stamp"). A log, as a type of record, can be in paper or electronic format. A log may also, in some contexts, be referred to as a type of document, and several similar (or a "set" of) logs may be referred to as a type of documentation.
4. DOCUMENTS: A document is a record that generally is used to represent or demonstrate what an organization has done or expects to do (such as a "business record" in the legal sense). Documents may include but are not limited to policies, processes and procedures, specifications, drawings, maps, etc. As a type of record, a document can be in paper or electronic format.
5. DOCUMENTATION: A series or collection of related documents generally pertaining to a particular issue. Documentation can be records that demonstrate what

an organization does, should do, or plans to do, including instructions to employees on how they should perform certain tasks. Documentation may also be records that represent, or can be used to demonstrate, what an organization has done or expects to do (such as a set of "business records"). Thus, the term "documentation" may be used to refer to any collection of documents (or "documentary" material) such as "business records," a plan or set of plans, a policy with associated procedures, or "the log" or "all the logs" generated by a specific system or device over a specified period.

Optional Team Case Project

Solution

The following is a partial solution to aid students in coming up with their own solution to solve this case:

- Basic "port scans" to identify open/available services.
- File integrity checking to identify change in size of certain files.
- Review of active user accounts subsequent to changes to the system.
- Validate security-related functions: access controls, audit functions, file protection.
- Test for malicious logic in source code.
- Review technical documentation to determine security features.
- Review source code if available for application security.

CHAPTER 46: SUPPORTING USER PRIVACY PREFERENCES IN DIGITAL INTERACTIONS

Review Questions/Exercises

True/False

1. True
2. False
3. True
4. True
5. True

Multiple Choice

1. C
2. D
3. C
4. B
5. E

Exercise

Solution

The following is a partial exercise solution. The students should be able to expand on the following:

No. An organization is free to filter out requests before or after **a distributed access control system** is invoked on a web service request.

A distributed access control system can control access to a program that has its own authentication or authorization methods, because **the distributed access control system** does its work before the program runs. For example, the **distributed access control system** can be used to filter requests to a database application. The application does not need to be changed in any way and is unaware that the **distributed access control system** is even being used. Requests that are denied by a **distributed access control system** never reach the application, because the application is not executed. Requests that are granted by a **distributed access control system** allow the application to run and it may perform its usual authentication or authorization procedures.

Hands-on Project

Solution

The following is a partial project solution. The students should be able to expand on the following:

Organizations will typically (but are not required to) trust each other's authentication services. Each organization is completely autonomous with respect to granting and denying access to its own information resources.

Case Projects

Solution

The following is a partial project solution. Students should be able to expand on the project analysis through extensive research.

To be authenticated by a **distributed access control system** at a particular organization, a user must already be known to that organization; that is, the organization must have previously established some way of confirming the user's identity, such as by providing the user with a username, secret password, and the name of the organization.

Optional Team Case Project

Solution

The following is a partial solution to aid students in coming up with their own solution to solve this case:

No. And unless their organization requires it, users do not have to have client certificates.

If an organization chooses to authenticate a user using an X.509 certificate, it must merely be able to validate a client certificate passed to it by a **distributed access control system** and map the certificate to a **distributed access control system** username. In cases where the web server is configured to do this validation itself, a **distributed access control system** may not need to repeat this validation. If the organization is already using this certificate to authenticate its owner for other purposes (web access), it must also already have the necessary means of validating the certificate.

A **distributed access control system** obtains the X.509 certificate through its SSL connection with the user. It is possible to use self-signed certificates if an organization (or the federation) chooses to operate its own certificate authority. And, unless their organization requires it, users do not have to have client certificates. It is possible to use self-signed certificates if an organization chooses to operate its own certificate authority.

CHAPTER 47: PHYSICAL SECURITY ESSENTIALS

Review Questions/Exercises

True/False

1. True
2. False
3. True
4. False
5. True

Multiple Choice

1. C
2. D
3. C
4. C
5. B

Exercise

Solution

The following is a partial exercise solution. The students should be able to expand on the following:

The data gathered by the stationary monitors and the deployable monitors are different. The stationary monitors send beta gross count rate and gamma gross count rate ranges. The beta gross count rate measures the radiation from all radionuclides that emit beta particles, which is indicated by the term gross or total. The term count rate tells us how quickly beta particles are being detected, which indicates how much radioactivity the monitor is seeing.

The gamma data measures radiation from all radionuclides that emit gamma raysand splits them into ranges of energy. The word gross, or total, indicates that the measurement is from all gamma emitting radionuclides. Not all gamma rays have the same amount of energy. Breaking the data into discrete energy ranges helps scientists to determine which radionuclides may be present.

The deployable monitors show external exposure rate. A graph would show the external exposure rate data, which is the dose, or amount of radiation, you would receive on the outside of your body if you were standing in that particular location. Background, or normal, radiation levels depend on factors including altitude and the amount of naturally occurring radioactive elements in the soil. Background external exposure rates typically range between 0.005 and 0.020 millirem per hour (mR/hr).

Both sets of data provide us with information on the type and amount of radioactive material in the air, and both serve the same purpose: to notify scientists, in near real time, of elevated levels of radiation so they can determine whether protective action is required. Following the Japanese nuclear incident, all of our near real time data showed background radiation levels.

Hands-on Project

Solution

The following is a partial project solution. The students should be able to expand on the following:

EPA's nationwide radiation monitoring system, RadNet, continuously monitors the nation's air and regularly monitors drinking water, milk and precipitation for environmental radiation. The network contains more than 100 air monitors across the United States and 40 deployable air monitors that can be sent to take readings anywhere in the country.

The near-real-time air monitoring data is continually reviewed by computer, and if the results show a significant increase in radiation levels, EPA laboratory staff is alerted immediately and further reviews the data to ensure accuracy. The system has been used to track radioactive material associated with foreign atmospheric nuclear weapons testing as well as for monitoring foreign nuclear accidents such as Chernobyl. EPA maintains additional monitoring capabilities that can be deployed to any location in the United States or its territories.

Case Projects

Solution

The following is a partial project solution. Students should be able to expand on the project analysis through extensive research.

During the last five years, EPA has been upgrading the nationwide RadNet system by installing new near-real-time radiation air monitors across the country. Currently the RadNet system contains more than 100 real-time radiation air monitors in 48 states. EPA also has 40 deployable monitors that can be sent to supplement the system.

Optional Team Case Project

Solution

The following is a partial solution to aid students in coming up with their own solution to solve this case:

EPA has 40 deployable radiation air monitors that can be sent anywhere in the United States to gather data. The RadNet deployable monitors have built in weather stations and measure gamma radiation. Like all RadNet radiation air monitors, the RadNet deployable monitors send both weather and gamma radiation readings hourly to EPA's National Air and Radiation Environmental Laboratory.

CHAPTER 48: VIRTUAL PRIVATE NETWORKS

Review Questions/Exercises

True/False

1. False
2. True
3. False
4. False
5. False

Multiple Choice

1. C
2. C
3. B
4. A, E
5. B

Exercise

Solution

The following is a partial exercise solution. The students should be able to expand on the following:

The organization first identified its needs based on its current operations and its stated future goals for secure remote access. In designing the proposed solution, the organization followed the typical steps of creating both an access control and an endpoint security policy: laying out its methods for authentication of users; designing an overall architecture for the expected remote access solution; selecting the hardware needed to meet its goals; specifying where in its current network the hardware will go; determining whether or not it needs a high availability solution; creating a management policy for the system and users; selecting the client software; designing the portal that the users will see when they connect to the system; and, developing an encryption policy.

After this design was completed, the organization implemented a prototype of the system before deploying it fully. The test plan for this prototype involved creating a sample configuration for the network access, the list of users for the system, definitions of the types of access that will be given to the users, and a specific policy plan linking the users to the types of access; as well as, other policy restrictions on the users.

Hands-on Project

Solution

The following is a partial project solution. The students should be able to expand on the following:

The company calculated the network capacity required and determined the most cost effective access technologies for each site. They then quickly set up the IP VPN to connect five main sites with different bandwidth allocations, according to the specific requirements of each office. To solve its data center relocation dilemma, the company decided to take advantage of a co-location service and outsource the hosting of its core application and data servers. It leased more than adequate capacity for the company's data center with room to expand in the future.

Case Projects

Solution

The following is a partial project solution. Students should be able to expand on the project analysis through extensive research.

The company subscribed to a Virtual Private Network (VPN) service to meet all its telecommunications requirements. Its main offices are permanently linked via Multi-Protocol Label Switching (MPLS) technology with a capacity of 100 Mbps. Other remote sites are connected to this central VPN at any one time by using Asymmetric Digital Subscriber Line (ADSL) technology.

Optional Team Case Project

Solution

The following is a partial solution to aid students in coming up with their own solution to solve this case:

The company initially developed the solution to securely connect its users spread throughout its global network of offices and data centers. The company anticipates this solution will save billions of dollars over dedicated point-to-point data circuits. This will provide comprehensive network security, reduced bandwidth costs, better user responsiveness and the ability for local offices to easily publish content for access by customers. In addition, the company supplied remote access for multiple service types (e-mail, file and print sharing, internet/intranet access, antivirus, remote support options, security, etc. . . .) to the staff across the world with minimal capital outlay with the shortest lead time; provided a secure transport method for internal information transfer; and, designed a transportable/scaleable/reproducible methodology that can be implemented in new offices with minimum capital cost and shortened time frames.

CHAPTER 49: IDENTITY THEFT

Review Questions/Exercises

True/False

1. True
2. True
3. False
4. True
5. True

Multiple Choice

1. C
2. E
3. D
4. D
5. C

Exercise

Solution

The following is a partial exercise solution. The students should be able to expand on the following:

- Requires you to supply personal information.
- Threatens to close or suspend your account if you do not take immediate action and provide personal information.
- Solicits your participation in a survey where you are asked to enter personal information.
- States that your account has been compromised or that there has been third-party activity on your account and requests you to enter or confirm your account information.
- States that there are unauthorized charges on your account and requests your account information.
- Asks you to enter your User ID, password or account numbers, PIN numbers or card expiration dates into an e-mail, non-secure webpage or text message.
- Asks you to confirm, verify, or refresh your account, credit card, or billing information.

Hands-on Project

Solution

The following is a partial project solution. The students should be able to expand on the following:

You can enhance security and help control risks when using your PC in a number of ways. Tips concerning PC access controls, virus management and software upgrades and maintenance follows:

Online Security Guidance PC Security

- Control physical access to your personal computer (PC); that is, do what you can to prevent unauthorized persons from using your PC.
- If you are using your PC and need to walk away from it for any reason, log off or lock your workstation.
- Select passwords that would be difficult for others to guess and change them frequently.
- Do not give your passwords to anyone. Do not save passwords on your website or leave written notes with your password near your PC
- Report suspicious activity you notice relating to your PC or use of your PC to the appropriate parties and do so as quickly as possible. If you notice suspicious activity relating to accounts at your bank that you access online, promptly report that activity to your bank account officer.

Virus Management

- Install virus management software on your PC and use it regularly.
- Keep it up to date (latest signature files, product upgrades).
- Be cautious when downloading and running programs or Java or ActiveX applets as they may contain unsecure data which cannot be filtered, for example, using firewall or anti-virus software.
- Use extreme caution when opening Email received from unknown sources and pay special attention to any attachments. Do not launch or open an attachment from an unknown source. When in doubt ... delete it without opening it.

If you suspect your computer has a virus, here are some tips you may want to consider:

1. Make sure your anti-virus software has the most recent updates. If you aren't sure, please contact the software maker.
2. Run a complete scan using your updated anti-virus software.
3. Remove any dangerous or harmful files from your PC.
4. Change your e-mail password.
5. Contact your bank so that they can walk you through changing your User ID and Password.
6. Contact any other financial companies that you do business with online.

PC Software

- Understand and use the security features provided by your PC software, such as those included in many operating systems, browsers and word processing systems.
- Ensure that your browser uses the strongest encryption available and be aware of the level of encryption used when you connect to various sites and applications. Use only software from reliable vendors.
- Stay abreast of the latest release and patch levels of the PC software you use.

Encryption/Browser Check

Encryption is the scrambling of data into a code that is unreadable to anyone who does not have the key that deciphers it. Only you and your bank have the key to unlock your code. All your account information should be protected by at least 128-bit encryption to maintain the privacy and confidentiality of your data. To take advantage of strong encryption technology, you will need to obtain a secure browser, one that supports 128-bit encryption.

E-mail Tips

Do not provide your e-mail address to third party websites without reading the privacy and security policies and terms and conditions of these sites to ensure you understand the circumstances in which your e-mail address will be used.

If you suspect suspicious or fraudulent activity related to your bank account(s), please let us know right away. You should also contact your Internet Service Provider so they may block suspect companies from your e-mail inbox. To learn more about how to control and manage your incoming e-mails, please refer to your Internet Service Provider's online resources.

Case Projects

Solution

The following is a partial project solution. Students should be able to expand on the project analysis through extensive research.

Identity theft and related account fraud happen when someone steals personal information such as your bank account number or Social Security number and poses as you, withdrawing money from your account and/or running up debt in your name.

Optional Team Case Project

Solution

The following is a partial solution to aid students in coming up with their own solution to solve this case:

If you are a victim of Identity Theft or account fraud, you should call your bank customer service representative immediately. They will work with you to correct all unauthorized transactions in your bank accounts, and correct any inaccurate Credit Bureau reports. They will also provide you with additional information and direct you to other sources of assistance.

CHAPTER 50: PHYSICAL SECURITY ESSENTIALS

Review Questions/Exercises

True/False

1. False
2. False
3. True
4. True
5. False

Multiple Choice

1. D
2. D

3. C
4. A
5. D

Exercise

Solution

The following is a partial exercise solution. The students should be able to expand on the following:

a. Startup cost – Although VOIP can be expected to save money in the long run, the initial installation can be complex and expensive. In addition, a single standard has not yet emerged for many aspects of VOIP, so an organization must plan to support more than one standard, or expect to make relatively frequent changes as the VOIP field develops.
b. Security – The flexibility of VOIP comes at a price: added complexity in securing voice and data. Because VOIP systems are connected to the data network, and share many of the same hardware and software components, there are more ways for intruders to attack a VOIP system than a conventional voice telephone system or PBX.

Hands-on Project

Solution

The following is a partial project solution. The students should be able to expand on the following:

No, except possibly for home use. VOIP demands high performance because voice communications must be in real time. A few seconds delay in data transmission is accepted and common, but a similar delay in a telephone conversation would make the system unacceptable to users. VOIP network equipment uses special protocols to over come the performance problems involved in transmitting voice over the Internet. Existing local area network cabling can be used.

Case Projects

Solution

The following is a partial project solution. Students should be able to expand on the project analysis through extensive research.

The term softphone refers to a telephone capability implemented on an ordinary PC, using only special software and a microphone/headset that plugs into the PC's audio ports. As noted in the body of this publication, though, softphones should not be used where security or privacy are a concern because of the ease with which they can be attacked. These systems are also more vulnerable to denial of service attacks from worms and viruses.

Optional Team Case Project

Solution

The following is a partial solution to aid students in coming up with their own solution to solve this case:
If all components have an uninterruptible power supply, the system should continue to function as long as the UPS batteries last. However, if the VOIP system is implemented on a cable modem, phone service will not be available during a cable outage. Similarly, if DSL is used, an outage of the DSL line will interrupt phone service. A conventional phone connection or mobile phones can serve as a backup.

CHAPTER 51: SAN SECURITY

Review Questions/Exercises

True/False

1. False
2. False
3. True
4. False
5. True

Multiple Choice

1. A
2. A
3. C
4. D
5. C

Exercise

Solution

The following is a partial exercise solution. The students should be able to expand on the following:

SAN zoning is a method of arranging Fibre Channel devices into logical groups over the physical configuration of the fabric. SAN zoning may be utilized to implement compartmentalization of data for security purposes. Each device in a SAN may be placed into multiple zones.

Hands-on Project

Solution

The following is a partial project solution. The students should be able to expand on the following:

1. Snooping: Mallory reads data Alice sent to Bob in private Allows access to data
2. Spoofing: Mallory fools Alice into thinking that he is Bob Allows access to or destruction of data
3. Denial of Service: Mallory crashes or floods Bob or Alice Reduces availability.

Case Projects

Solution

The following is a partial project solution. Students should be able to expand on the project analysis through extensive research.

- Node Name/Port Name spoofing at Port Login time
- Source Port ID spoofing on dataless FCP commands
- Snooping and spoofing on FC-AL
- Snooping and Spoofing after Fabric reconfiguration
- Denial of Service attacks can be made in User mode

Optional Team Case Project

Solution

The following is a partial solution to aid students in coming up with their own solution to solve this case:

- Fibre Channel - Security Protocol (FC-SP) is a security protocol for Fibre Channel Protocol (FCP) and fiber connectivity (Ficon).
- FC-SP is a project of the Technical Committee T11 of the InterNational Committee for Information Technology Standards (INCITS) [http://www.t11.org/t11/stat.nsf/7db1e1431d9d045f852566dc004cc14d/43b527df16f4b28d85256b9a00653843?OpenDocument].
- FC-SP is a security framework which includes protocols to enhance Fibre Channel security in several areas, including authentication of Fibre Channel devices, cryptographically secure key exchange, and cryptographically secure communication between Fibre Channel devices.
- FC-SP is focused on protecting data in transit throughout the Fibre Channel network. FC-SP does not address the security of data which is stored on the Fibre Channel network.

CHAPTER 52: STORAGE AREA NETWORKING SECURITY DEVICES

Review Questions/Exercises

True/False

1. False
2. False
3. True
4. False
5. False

Multiple Choice

1. A
2. A
3. B
4. C
5. B

Exercise

Solution

The following is a partial exercise solution. The students should be able to expand on the following:

When a computer interacts with a storage device, disk, tape, optical or RAID, this interaction occurs at the block level. Data is transferred in blocks rather than by the file. Block level transfer is considerably faster and easier to manage than file level transfer.

Hands-on Project

Solution

The following is a partial project solution. The students should be able to expand on the following:

A group of disk drives that collectively acts as a single storage system. Two types of storage arrays are available: RAID (Redundant Array of Independent Disks) and JBOD (Just a Bunch Of Disks). A RAID system provides fault tolerance by storing the same data redundantly on multiple disks, but appears as a single disk. A JBOD is, typically, a group of individual disks cabled together in a chassis with redundant power.

Case Projects

Solution

The following is a partial project solution. Students should be able to expand on the project analysis through extensive research.

A SAN solution should be used for applications that require large amounts of storage capacity and need block level access to the storage infrastructure. Additionally if you are looking to deploy a clustering solution such as Microsoft's Clustering technology a SAN must be used. Examples of SAN solutions include the Microsoft Exchange System and Oracle Databases.

Optional Team Case Project

Solution

The following is a partial solution to aid students in coming up with their own solution to solve this case:

No, as long as the server is within the accepted standards and ratings for Fibre Channel over fiber optic cable. These distances are 175 meters (574.1 feet) over Multimode 62.5 micron cable, 500 meters (1640 feet) over a multimode 50 micron cable and 10 kilometers (6.214 miles) over 9 micron single mode cable.

CHAPTER 53: RISK MANAGEMENT

Review Questions/Exercises

True/False

1. False
2. True
3. True
4. True
5. True

Multiple Choice

1. B
2. B
3. D
4. A
5. E

Exercise

Solution

The following is a partial exercise solution. The students should be able to expand on the following:

Continuous monitoring is one of six steps in the Risk Management Framework (RMF). The objective of a continuous monitoring program is to determine if the complete set of planned, required, and deployed security controls within an information system or inherited by the system continue to be effective over time in light of the inevitable changes that occur. Continuous monitoring is an important activity in assessing the security impacts on an information system resulting from planned and unplanned changes to the hardware, software, firmware, or environment of operation (including threat space). An organization's riskbased decisions (security authorization decisions) should consider how continuous monitoring will be implemented organization-wide as one of the components of the security life cycle represented by the RMF.

Hands-on Project

Solution

The following is a partial project solution. The students should be able to expand on the following:

No. Security authorization, requires the explicit review and acceptance of risk by an authorizing official on an ongoing basis. These risk-based decisions are based on security control assessments and continuous monitoring activities. Continuous monitoring does *not* replace the security authorization requirement for information systems. Rather, continuous monitoring is implemented as part of a holistic, risk management and (defense-in-depth) information security strategy that is integrated into enterprise architectures and system development life cycles. The continuous monitoring program, developed and implemented by an organization as a component in the RMF security life cycle-based approach, becomes a consideration in the risk-based decisions (security authorization decisions) rendered by authorizing officials.

Case Projects

Solution

The following is a partial project solution. Students should be able to expand on the project analysis through extensive research.

Continuous monitoring in and of itself, does not provide a comprehensive, enterprise-wide risk management approach. Rather, it is a key component in the risk management process. The fundamental tenet of the unified information security framework is an enterprisewide risk management approach to information security that is life cycle-based and implemented across three hierarchical tiers within an organization (governance, mission/business process, and information system). The RMF, employs a security life cycle approach when considering information system security. The six-step RMF fundamentally transformed the previous certification and accreditation (C&A) process to provide emphasis on "front-end" and "back-end" security. The ongoing determination and acceptance of information system security-related risks remains the primary responsibility of authorizing officials and for which they are held accountable. Continuous monitoring activities contribute to helping authorizing officials make better risk-based decisions, but do not replace the security authorization process.

Optional Team Case Project

Solution

The following is a partial solution to aid students in coming up with their own solution to solve this case:

Front-end security, exemplified by the first three steps in the RMF (security categorization, security control selection, and implementation), focuses on building security into information technology products and systems early in the system development life cycle. The initial steps are also linked to the organization's enterprise architecture and information security architecture. Better front-end security results in fewer weaknesses and deficiencies in information systems, directly translating to a lesser number of vulnerabilities that can be exploited by threat sources. Back-end security, exemplified by the last three steps in the RMF (security control assessment, information system authorization, and continuous monitoring), focuses on the effectiveness of the implemented security controls, the determination and acceptance of risk, and the ongoing monitoring of the security state of the information system. The RMF overall provides a disciplined and structured process that integrates information security and risk management activities into the system development life cycle.

CHAPTER 54: PHYSICAL SECURITY ESSENTIALS

Review Questions/Exercises

True/False

1. False
2. True
3. False
4. True
5. False

Multiple Choice

1. A, B, D
2. A
3. A, C, E
4. D
5. E

Exercise

Solution

The following is a partial exercise solution. The students should be able to expand on the following:

The company focused on identifying vulnerabilities in existing pedestrian and vehicle access controls and the overall security posture of the center. The company also provided specific security measure recommendations, priorities and cost-benefits, determined an action plan, including milestones, and provided a detailed description of the benefits and risks of the various approaches.

Hands-on Project

Solution

The following is a partial project solution. The students should be able to expand on the following:

Structured interviews should be conducted with security managers, internal customers and other corporate functions to provide an overall perspective and identify issues for an external benchmark study. The study should be designed to identify similarities and differences between the physical security solution and its industry peers; as well as, other companies renowned to have superior physical security practices. This should provide a framework for choosing between alternatives for physical security investment and resourcing strategies. A detailed questionnaire should focus on the key topics identified. The data generated should identify potential areas for improvement and provide a baseline to document relative positioning within its industry.

Case Projects

Solution

The following is a partial project solution. Students should be able to expand on the project analysis through extensive research.

If the virtual fences are breached, or if specific behaviors are identified, visual and audible alarms are triggered. Additionally, a full range of intrusion detection sensors for facilities and barriers are available to enhance the intrusion detection system and protect high security facilities; these options include seizure vaults, safes, and other secure storage sites.

Optional Team Case Project

Solution

The following is a partial solution to aid students in coming up with their own solution to solve this case:

The company developed a remote port entry system (a sub-system of the access control system, or ACS) that provides off-hours remote secure identification and US access to people and vehicles through select land ports of entry (LPOEs). The system uses video surveillance for visual identification of people and/or vehicles and integrates proximity-based ID cards, biometric identification and verification, radio frequency identification (RFID), voice-over internet protocol (VoIP), and remotely operated gates under the control of a command center (information and date are transmitted over a secure WAN). RFID tags are used on vehicles to ensure the identification of both people and their assigned vehicles. The company also uses a wide range of current and proven ACS technologies to control access of personnel, vehicles, and equipment through manned and unmanned perimeter check points, facilities, and secure areas.

CHAPTER 55: DISASTER RECOVERY

Review Questions/Exercises

True/False

1. True
2. False
3. True
4. False
5. True

Multiple Choice

1. C
2. D
3. C
4. C
5. E

Exercise

Solution

The following is a partial exercise solution. The students should be able to expand on the following:

Organizations require a suite of plans to prepare themselves for response, continuity, recovery, and resumption of mission/business processes and information systems in the event of a disruption. Each plan has a specific purpose and scope; however, because of the lack of standard definitions for these types of plans, in some cases, the scope of actual plans developed by organizations may vary from the following basic descriptions.

A **COOP** is required by Homeland Security Presidential Directive (HSPD) - 20/National Security Presidential Directive (NSPD) - 51, *National Continuity Policy* and Federal Continuity Directive (FCD) - 1, *Federal Executive Branch National Continuity Program and Requirements* for sustaining an organization's (usually a headquarters element) *mission essential functions* (MEF) at an alternate site and performing those functions for up to 30 days before returning to normal operations. A **BCP** addresses sustaining mission/business processes and the information systems that support those mission/business processes during and after a significant disruption. BCPs are often developed at the organization's field level or for mission/business processes that are not prioritized as mission essential. A **CIP** plan is a set of policies and procedures that serve to protect and recover those components of the national infrastructure that are deemed so vital that their loss would have a debilitating effect of the safety, security, economy, and/or health of the United States. A **DRP** refers to an information system-focused plan designed to restore operability of one or more information systems at an alternate site after a major disruption usually causing physical damage to the original data center. An **ISCP** provides recovery and resumption procedures for a single information system resulting from disruptions that do not necessarily require relocation to an alternate site. A **Cyber Incident Response Plan** establishes procedures to enable security personnel to identify, mitigate, and recover from cyber attacks against an organization's information system(s). An **OEP** provides directions for facility occupants to follow in the event of an emergency situation that threatens the health and safety of personnel, the environment, or property.

Careful coordination must be maintained between plan developers to ensure that their respective policies and procedures complement one another. Any changes in one plan, system, or process must be communicated to plan developers of associated systems and functions.

Hands-on Project

Solution

The following is a partial project solution. The students should be able to expand on the following:

The type of alternate site should be determined through the BIA with consideration of the FIPS 199 impact level. The alternate site choice must be cost-effective and match the availability needs of the organization's information systems. Thus, if a system requires near 100 percent availability, then a mirrored or hot site might be the right choice. However, if the system can allow for several days of downtime, then a cold site might be a better option.

Case Projects

Solution

The following is a partial project solution. Students should be able to expand on the project analysis through extensive research.

Notification procedures must be outlined in the ISCP. The ISCP Coordinator should determine who should be notified if a disruption occurs to the information system and in what sequence they should be contacted. Parties notified typically include the system owners, users, and interconnected information system points of contact. External entities that might be interconnected to the information system should also be included in the notification procedures. Design of a call tree will assist the sequence and responsibilities of executing notifications to appropriate contacts.

Optional Team Case Project

Solution

The following is a partial solution to aid students in coming up with their own solution to solve this case:

In addition to integrating contingency planning into the SDLC, information system contingency planning should be coordinated with network security policies. System security controls can help to protect against malicious code or attacks that could compromise system availability and are closely coordinated with the incident response procedures. The ISCP should be closely coordinated with all other emergency preparedness plans related to the information system or interconnected systems and mission/business processes.

CHAPTER 56: BIOMETRICS

Review Questions/Exercises

True/False

1. True
2. False
3. False
4. False
5. False

Multiple Choice

1. C
2. D
3. A
4. A
5. B

Exercise

Solution

The following is a partial exercise solution. The students should be able to expand on the following:

Biometrics are typically collected using a device called a sensor. These sensors are used to acquire the data needed for recognition and to convert the data to a digital form. The quality of the sensor used has a significant impact on the recognition results. Example “sensors” could be digital cameras (for face recognition) or a telephone (for voice recognition).

Hands-on Project

Solution

The following is a partial project solution. The students should be able to expand on the following:

A biometric template is a digital representation of an individual’s distinct characteristics, representing information extracted from a biometric sample. Biometric templates are what are actually compared in a biometric recognition system. Templates can vary between biometric modalities as well as vendors. Not all biometric devices are template based. For example, voice recognition is based on “models.”

Case Projects

Solution

The following is a partial project solution. Students should be able to expand on the project analysis through extensive research.

This depends on the specific modality being used. For example, with today’s current technology, an individual would be required to touch a fingerprint sensor for the system to obtain the biometric sample, whereas face imaging for face recognition and iris imaging for iris recognition are contactless and would not require the user to touch the system.

Optional Team Case Project

Solution

The following is a partial solution to aid students in coming up with their own solution to solve this case:

Different applications and environments have different constraints. For instance, adequate fingerprint samples require user cooperation, whereas, a face image can be captured by a surveillance camera. Furthermore, fingerprints are not available for many of the suspects on watch lists. There are also multiple biometric modalities for technical and financial reasons. Many scientists become interested in developing a system based on their own research. Upon a successful implementation, venture capitalist, interested in the implementation of such a system, commercialize a product. Therefore, wide varieties of modalities are being researched and are available on the market.

CHAPTER 57: HOMELAND SECURITY

Review Questions/Exercises

True/False

1. True
2. False
3. False
4. False
5. True

Multiple Choice

1. E
2. D
3. A
4. A
5. B

Exercise

Solution

The following is a partial exercise solution. The students should be able to expand on the following:

When there is credible information about a threat, an NTAS Alert will be shared with the American public. It may include specific information, if available, about the nature of the threat, including the geographic region, mode of transportation, or critical infrastructure potentially affected by the threat, as well as steps that individuals and communities can take to protect themselves and help prevent, mitigate or respond to the threat. The advisory will clearly indicate whether the threat is **Elevated**, if we have no specific information about the timing or location, or **Imminent**, if we believe the threat is impending or very soon.

Hands-on Project

Solution

The following is a partial project solution. The students should be able to expand on the following:

The Secretary of Homeland Security will announce the alerts publically. Alerts will simultaneously be posted at DHS.gov/alerts and released to the news media for distribution. The Department of Homeland Security will also distribute alerts across its social media channels, including the Department's blog, Twitter stream, Facebook page, and RSS feed.

Case Projects

Solution

The following is a partial project solution. Students should be able to expand on the project analysis through extensive research.

The NTAS Alert informs the American public about credible terrorism threats, and encourages citizens to report suspicious activity. Where possible and applicable, NTAS Alerts will include steps that individuals and communities can take to protect themselves to help prevent, mitigate or respond to the threat. Individuals should review the information contained in the alert, and based upon the circumstances, take the recommended precautionary or preparedness measures for themselves and their families.

Optional Team Case Project

Solution

The following is a partial solution to aid students in coming up with their own solution to solve this case:

Citizens should report suspicious activity to their local law enforcement authorities. The "If You See Something, Say Something" campaign across the United States encourages all citizens to be vigilant for indicators of potential terrorist activity, and to follows NTAS Alert for information about threats in specific places or for individuals exhibiting certain types of suspicious activity.

CHAPTER 58: CYBER WAREFARE

Review Questions/Exercises

True/False

1. False
2. True
3. True
4. True
5. False

Multiple Choice

1. D
2. C

3. C
4. B
5. D

Exercise

Solution

The following is a partial exercise solution. The students should be able to expand on the following:

To address the advanced persistent cyber threat requires a multi-pronged effort by organizations. First, it requires a major change in strategic thinking to understand that this class of threat cannot always be kept outside of the defensive perimeter of an organization. Rather, this is a threat that in all likelihood, has achieved a foothold within the organization. This situation requires that organizations employ methods to constrain such threats in order to ensure the resiliency of organizational missions and business processes.

Second, it requires the development and deployment of security controls that are intended to address the new tactics, techniques and procedures (TTPs) employed by adversaries (supply chain attacks, attacks by insiders, attacks targeting critical personnel). Finally, to enable cyber preparedness against the advanced persistent cyber threat, organizations must enhance risk management and information security governance in several areas. These include, but are not limited to: (i) development of an organizational risk management and information security strategy; (ii) integration of information security requirements into the organization's core missions and business processes, enterprise architecture, and system development life cycle processes; (iii) allocation of management, operational, and technical security controls to organizational information systems and environments of operation based on an enterprise security architecture; (iv) implementation of a robust continuous monitoring program to understand the ongoing security state of organizational information systems; and (v) development of a strategy and capability for the organization to operate while under attack, conducting critical missions and operations, if necessary, in a degraded or limited mode.

Hands-on Project

Solution

The following is a partial project solution. The students should be able to expand on the following:

There are 3 basic parts to a cyber-attack:

1. *Access*: a method to get inside or gain access to a network or system
2. *Vulnerability*: some part of the system that the attacker can take advantage of or manipulate
3. *Payload*: the purpose of the attack, namely, what exactly is the target and how significant will the damage be

A safe cracker, for instance, must know where the safe is and how to get into it. The vulnerability would require knowledge of the safe, its locking mechanism and what aspects may be exploited. The payload, in this case, would be a bag full of money. Given these three aspects, prior intelligence is needed to understand what access is available and what vulnerability can be exploited in order to attack precise targets.

A standard computer virus, probably the most common form of a cyber-attack, may gain initial access to a computer or system in two ways: remotely or proximately. Some viruses, such as Conficker, spread through a network of computers (remote access) by exploiting holes in the network security or by attaching an infected USB drive to a computer. Such a virus is not only capable of ruining services on the computer itself, but also of blocking certain websites that might enable the user to eliminate the virus. A virus, Trojan, worm, etc. is primarily the means of carrying out a cyber-attack, while the real attack is the virus' payload.

There are many other forms cyber-attacks may take. A denial of service attack occurs when "an attacker attempts to prevent legitimate users from accessing information or services." This is typically accomplished when the attacker overloads a system with requests to view information. This would be an example of a remote attack. By extension, a distributed denial of service (DDoS) occurs when multiple computers are involved in a denial of service attack causing an even larger amount of traffic on the target website. This is the same concept as we've all experienced with cell phone disruption due to high usage.

Spearphishing is another simple method by which an attack may gain access to a computer system or network. Once some information about a target is acquired, an email is sent purporting to be from a legitimate company asking for information such as usernames and passwords to banking websites or network logins.

Backdoors, or hooks, are placed inside a computer or network in order to create a vulnerability that can be exploited later on. If direct access is possible, tampering with basic electronics is a simple type of cyber-attack. It is also possible that such software or even hardware could be installed into electronics by the original manufacturer. Some fear that this is what is being done in Chinese-produced microchips for various American computer companies.

Case Projects

Solution

The following is a partial project solution. Students should be able to expand on the project analysis through extensive research.

As cyber-attacks encompass a wide range of methods, they are also capable of affecting a very wide range of targets. Cyber-attacks can affect anything that is connected to a computer or a computer network. This would include not only single computers and network-connected computers but also USB storage devices and even machinery controlled by computer or network equipment. Due to the great diversity of possible targets for cyber-attacks, the next few sections will present several examples of cyber-attacks that have happened in the past. Despite fear over cyber-attacks on airline services or nuclear facilities, the most common and arguably the most dangerous are attacks on critical infrastructure.

Optional Team Case Project

Solution

The following is a partial solution to aid students in coming up with their own solution to solve this case:

In the case of both cyber- and conventional espionage, plans can be discovered, strategies compromised and secrets stolen. During hostile attacks, systems can be shut down, communications cut off and infrastructure destroyed.

CHAPTER 59: SYSTEMS SECURITY

Review Questions/Exercises

True/False

1. True
2. True
3. False
4. False
5. True

Multiple Choice

1. D
2. A
3. D
4. C
5. A

Exercise

Solution

The following is a partial exercise solution. The students should be able to expand on the following:

A well-designed and well-managed continuous monitoring program can effectively transform an otherwise static and occasional security control assessment and risk determination process into a dynamic process that provides essential, near real-time security status-related information to senior leaders. Senior leaders can use this information to take appropriate risk mitigation actions and make cost-effective, risk-based decisions regarding the operation of their information systems. A continuous monitoring program allows an organization to track the security state of an information system on an ongoing basis and maintain the security authorization for the system over time. Understanding the security state of information systems is essential in highly dynamic environments of operation with changing threats, vulnerabilities, technologies, and missions/business processes.

Hands-on Project

Solution

The following is a partial project solution. The students should be able to expand on the following:

Organizations are required to develop a continuous monitoring strategy for their information systems and environments in which those systems operate. A robust continuous monitoring program that derives from that strategy requires the active involvement of information system owners and common control providers, mission and business owners, chief information officers, senior information security officers, and authorizing officials.

Case Projects

Solution

The following is a partial project solution. Students should be able to expand on the project analysis through extensive research.

Automation, including the use of automated support tools (vulnerability scanning tools, network scanning devices), can make the process of continuous monitoring more cost-effective, consistent, and efficient. Real-time monitoring of implemented technical controls using automated tools can provide an organization with a much more dynamic view of the security state of those selected controls. It is also important to recognize that with any comprehensive information security program, all implemented security controls, including management and operational controls, must be regularly assessed for effectiveness, even if the monitoring of them is not easily automated. Sophisticated adversaries have been exploiting and continue to exploit the weakest controls, and true security for an information system or an organization is dependent on all controls remaining effective over time.

Optional Team Case Project

Solution

The following is a partial solution to aid students in coming up with their own solution to solve this case:

Organizations develop security plans containing the required security controls for their information systems and environments of operation based on mission and operational requirements. All security controls deployed within or inherited by organizational information systems are subject to continuous monitoring. This security control facilitates a defense-in-depth protection capability that includes people, processes, and technologies—a mutually reinforcing set of safeguards and countermeasures to address threats from cyber attacks, human error, and natural disasters.

CHAPTER 60: SECURING THE INFRASTRUCTURE

Review Questions/Exercises

True/False

1. True
2. False
3. True
4. False
5. False

Multiple Choice

1. C
2. D
3. C
4. B
5. E

Exercise

Solution

The following is a partial exercise solution. The students should be able to expand on the following:

It's appropriate to enable 802.1*x* authentication on any and all Ethernet ports on which you do not explicitly trust the device connected to the port. Be aware that to really trust the device, you need to have a high level of confidence in the physical security of the Ethernet switch, the device connecting to it, and the Ethernet cable path connecting them. It's generally assumed that wireless connections are not secure in real-world deployments. People widely recognize the need for security such as 802.1*x* on wireless links. Wired Ethernet does not enjoy the same widespread recognition of the need for extra security measures, so the requirements are explicitly identified here. Typically, the only places where you can be lax in deploying 802.1*x* are within data centers or wiring closets. For example, the connections from your servers, gateways, or other infrastructure devices such as routers and switches are not as susceptible to hackers unplugging the devices and trying to connect rogue devices. That being said, if you have a large organization in which numerous vendors come in and out of data centers with little accountability for who is doing what, you might consider deploying 802.1*x* even in these areas.

Hands-on Project

Solution

The following is a partial project solution. The students should be able to expand on the following:

Although the common name for Ethernet port authentication is 802.1*x*, it might as well be called Extensible Authentication Protocol (EAP) for Ethernet ports. That's because the real authentication session is directly between the endpoints being authenticated and an access control server. This EAP exchange is carried over 802.1*x* Ethernet frames between the supplicant and the authenticating switch and over RADIUS between the switch and the authentication server.

As you might guess, EAP supports a variety of authentication mechanisms, and more methods can be added to this framework. The most common authentication choices include EAP-MD5 and EAP-TLS. The EAP-MD5 variant is similar to Challenge Handshake Authentication Protocol (CHAP), which traditionally has been used for dialup modem or ISDN remote access. This mechanism relies on a username/password combination for the authentication credentials. The EAP-TLS variant is more closely related to e-commerce applications, in which an X.509v3 certificate represents the server's identity and the client's identity is provided through another X.509v3 client-side certificate or username/password combination.

In addition to the authentication protocol in use, you need to understand whether a user of a device or a device itself is being authenticated. This distinction is important because user and device authentication solve different problems. For example, at a conceptual level, a multiaccess IP phone might have a single credential that proves to the network that it's not a rogue piece of hardware touching the network. In this case, the individual user logins to the phone might trigger a user-based 802.1*x* authentication that lets a different set of QoS and security policies be applied to the switch port based on the individual user permissions.

Case Projects

Solution

The following is a partial project solution. Students should be able to expand on the project analysis through extensive research.

Before you embark on a plan to configure 802.1*x* support on your Ethernet switches, you need to make sure that you coordinate with the desktop PC administrators so that they are ready to enable 802.1*x* in the client machines. As long as you need clients on your network that do not support 802.l*x*, you cannot widely implement 802.l*x*. You might be able to start a pilot project that applies to a limited set of Ethernet jacks in your campus, but note that these jacks do not permit clients lacking 802.1*x* support to connect. Don't forget to consider workgroup printers and other Ethernet devices along with desktop PCs.

Optional Team Case Project

Solution

The following is a partial solution to aid students in coming up with their own solution to solve this case:

Reaping the full security benefits of an 802.1*x* deployment involves important design considerations. Imagine that your network resources are a reservoir of water held back by a dam, and that dam is the security policy as implemented by access lists that filter traffic and authentication at the network's ingress points. Just as a dam must be watertight, all ports in an 802.1*x* deployment for ingress authentication must be part of the deployment. If you have any devices or users who cannot authenticate via 802.1*x*, or if you have Ethernet jacks with 802.1*x* not enabled, you have holes that need to be plugged. To gain access to the LAN segments that 802.1*x* is designed to protect, a hacker can simply use an Ethernet jack on which 802.1*x* is not enabled or masquerade as a user or device that does not support 802.1*x*.

Taking a more pragmatic approach, you can also prioritize the areas of physical access sensitivity. You should first roll out 802.1*x* support to the areas that are least regulated, such as lobbies and cafeterias with limited security checks. Next in order would be break rooms, temporary worker areas, or other areas with minimal restrictions. Finally, you can focus on the common office or cubicle areas. In general, work your way through from the least physically secure areas to the most physically secure.

CHAPTER 61: ACCESS CONTROLS

Review Questions/Exercises

True/False

1. False
2. False
3. True
4. False
5. False

Multiple Choice

1. D
2. D
3. C
4. C
5. E

Exercise

Solution

The following is a partial exercise solution. The students should be able to expand on the following:

There are four basic ways of authenticating users: asking for something only the authorized user knows (such as a password), test for the presence of something only the authorized user has (like a smart card), obtain some non-forgeable biological or behavioral measurement of the user (like a fingerprint) or determine that the user is located at a place where only the authorized user can enter. The best (and most effective) solutions require a combination of two or more authentication methods.

Hands-on Project

Solution

The following is a partial project solution. The students should be able to expand on the following:

The solution must be compatible with current operating systems and applications. Compatibility is a particularly big concern with biometric systems, since existing hardware and applications often must be adapted and/or reprogrammed to work with these tools.

Case Projects

Solution

The following is a partial project solution. Students should be able to expand on the project analysis through extensive research.

Organizations must balance the value of the information being protected with the authentication and access control software's ease-of-use. Solutions that are difficult to use may protect systems, but only at the expense of user convenience and productivity.

Optional Team Case Project

Solution

The following is a partial solution to aid students in coming up with their own solution to solve this case:

You'll want a product that you can use for many years. Over that time span, it will need to be upgraded to accommodate new security practices and technologies.

CHAPTER 62: ASSESSMENTS AND AUDITS

Review Questions/Exercises

True/False

1. True
2. True
3. False
4. True
5. True

Multiple Choice

1. C
2. E
3. D
4. D
5. C

Exercise

Solution

The following is a partial exercise solution. The students should be able to expand on the following:

In the real world, the cost of protecting information must be balanced against the potential cost of security breaches. A company must fully understand the security risks it faces in order to determine the appropriate management action and to implement controls selected to protect against these risks.

Hands-on Project

Solution

The following is a partial project solution. The students should be able to expand on the following:

Selecting the right set of controls requires the use of a risk assessment-based approach. This approach is a mandatory part of the PLAN (identify, analyze and evaluate the risks), DO (select, implement, and use controls to manage the risks to acceptable levels), CHECK, and ACT cyclic process defined in BS 7799-2 for the establishment, implementation, and maintenance of an ISMS.

Case Projects

Solution

The following is a partial project solution. Students should be able to expand on the project analysis through extensive research.

The standard specifies only that the organization should use a systematic approach to risk assessment (method of risk assessment, legal requirements, policy and objectives for reducing the risks to an acceptable level).

Optional Team Case Project

Solution

The following is a partial solution to aid students in coming up with their own solution to solve this case:

An organization that manages change effectively has a better chance of survival. The PDCA process model provides a means of assessing the risks an organization is challenged with as a result of changes in the business environment.

CHAPTER 63: FUNDAMENTALS OF CRYPTOGRAPHY

Review Questions/Exercises

True/False

1. False
2. False
3. True
4. True
5. False

Multiple Choice

1. D
2. D

3. C
4. A
5. D

Exercise

Solution

The following is a partial exercise solution. The students should be able to expand on the following:

A cryptographic module is the set of hardware, software, and/or firmware that implements approved security functions (including cryptographic algorithms and key generation) and is contained within the cryptographic boundary. Another type, hybrid, is a software module that also contains an underlying unique hardware component. There are three distinct physical embodiments: single-chip modules, multiple-chip embedded modules, and multiple-chip standalone modules.

Hands-on Project

Solution

The following is a partial project solution. The students should be able to expand on the following:

Cryptographic key management encompasses the entire lifecycle of the cryptographic keys used by a cryptographic module. This includes random number generation, key generation, key establishment (including key transport), key entry/output, key storage, and key zeroization. The requirements are applicable to modules that implement secret key and/or public key algorithms. Secret and private keys must be protected from unauthorized disclosure, modification and substitution. Public keys must be protected against unauthorized modification and substitution.

Case Projects

Solution

The following is a partial project solution. Students should be able to expand on the project analysis through extensive research.

The test types that must be performed are:

a. Power Up tests
b. Cryptographic algorithm test
c. Software/firmware Integrity test
d. Critical functions test
e. Conditional tests
f. Pairwise consistency test
g. Software/firmware load test
h. Manual key entry test
i. Continuous Random Number Generator test
j. Bypass test

Optional Team Case Project

Solution

The following is a partial solution to aid students in coming up with their own solution to solve this case:

A cryptographic module security policy consists of:

- A specification of the security rules, under which a cryptographic module shall operate, including the security rules derived from the requirements of the standard and the additional security rules imposed by the vendor.

The specification shall be sufficiently detailed to answer the following questions:

- What access does operator *X*, performing service *Y* while in role *Z*, have to security-relevant data item *W* for every role, service, and security-relevant data item contained in the cryptographic module?
- What physical security mechanisms are implemented to protect a cryptographic module and what actions are required to ensure that the physical security of a module is maintained?
- What security mechanisms are implemented in a cryptographic module to mitigate against attacks for which testable requirements are not defined in the standard?

When presenting information in the non-proprietary security policy regarding the cryptographic services that are included in the module validation, the security policy must include, at a minimum, the following information for each service:

- The service name
- A concise description of the service purpose and/or use (the service name alone may, in some instances, provide this information)
- A list of Approved security functions (algorithm(s), key management technique(s) or authentication technique) used by, or implemented through, the invocation of the service.
- A list of the cryptographic keys and/or CSPs associated with the service or with the Approved security function(s) it uses.
- For each operator role authorized to use the service:
  - Information describing the individual access rights to all keys and/or CSPs

- Information describing the method used to authenticate each role.

CHAPTER 64: SECURITY THROUGH DIVERSITY

Review Questions/Exercises

True/False

1. False
2. False
3. True
4. False
5. True

Multiple Choice

1. A
2. A
3. C
4. D
5. C

Exercise

Solution

The following is a partial exercise solution. The students should be able to expand on the following:

Natural disasters cover only one threat vector to sustainability and operational readiness. The information age must balance uniformity and ubiquity in the face of threats though adaptation and vigilances.

Hands-on Project

Solution

The following is a partial project solution. The students should be able to expand on the following:

If you operate in a service industry that is Internet based, this question is perhaps what keeps you up at night—an attack against all your systems and services, from which you might not recover. Denial of Service (DoS) is a simple and straightforward attack that involves an attacker making enough requests to saturate your network or service to the point at which legitimate business and communications fails. The distributed denial-of-service (DDoS) attack is the same type of attack against a uniform presence in the Internet space but with many attacking hosts operating in unison against a site or service.

Case Projects

Solution

The following is a partial project solution. Students should be able to expand on the project analysis through extensive research.

It is possible but highly unlikely. Most browsers are not monolithic; adding code to view pages and perform animation are common practices. Browser extensibility allows anyone to integrate software components. Serious vulnerabilities and poor implementation in some of these extensions has led to exploitable code but usually demands a visit from a vulnerable browser. Since many of us don't use the same software package added to our browsers, this sort of threat, though risky to any enterprise from the standpoint of information disclosure, does not represent the sort of survivability issues security diversity seeks to remedy.

Optional Team Case Project

Solution

The following is a partial solution to aid students in coming up with their own solution to solve this case:

It might not be possible to quantify the advantage of selecting diversity over ubiquity other than the cost in procurement, training, and interoperability. It is quite possible that an investment in "bucking the system" and using uncommon systems and services won't just cause issues; it would drive your competitive advantage into oblivion. This is the single biggest reason to avoid security through diversity, and it will be pointed out repeatedly. Security through diversity starts early and is embraced as a matter of survival. Military and financial institutions abide by the diversity principals in investments and decision-making. Though a threat is not always understood, the institutionalizing lessons learned tend to live on, forcing change and adaptation that require diversity as a fundamental principal of survival.

CHAPTER 65: ONLINE E-REPUTATION MANAGEMENT SERVICES

Review Questions/Exercises

True/False

1. False
2. False
3. True
4. False
5. False

Multiple Choice

1. A
2. A
3. B
4. C
5. B

Exercise

Solution

The following is a partial exercise solution. The students should be able to expand on the following:

Absolutely not! You should never fall for this kind of fake promises, because there are a lot of fraudulent marketers. Online e-reputation management services is a complex area of online marketing; and, as you all know; just like traditional marketing, online e-reputation management services could never provide overnight effective solutions. The clients should understand that the major search engines are quite Daedalian structures and that it requires time, effort, great search engine optimization and communication skills. Expect your optimization results to improve gradually over time. Moreover, it takes time also to determine your stakeholders to participate, to be involved in the development of your Internet reputation and help shape it! No one is going to tell you that it will happen overnight; you can expect to see results in as little as 60 days. Depending on the complexity of the project, the duration is ranked between 3 months, 6 months or 1 year + .

The reasons why online e-reputation management services takes time: starting and running an Internet reputation campaign involves a lot of tasks. To begin with, online e-reputation management services will perform an Internet reputation audit in order to understand who the direct and indirect influencers of your reputation are. Research should be done to analyze one's personal or professional, business, industry or corporate reputation as represented by the content across various types of online media. The GAP analysis will help determine "Where are you?" and "Where do you want to be?" The reasons for any "reputation gap" will be assessed. Furthermore, an online reputation management specialist will establish and implement an online e-reputation management services plan and strategy. Finally, the online e-reputation management services success will be measured and delivered in form of reports to the client. One of the last steps of a successful online e-reputation management services process is the online reputation maintenance. You must keep your organic SEO natural to avoid penalties. All must happen gradually and not overnight. New websites, profiles etc don't rank immediately.

Hands-on Project

Solution

The following is a partial project solution. The students should be able to expand on the following:

You may be able to have the material removed, under particular legal circumstances, otherwise there is no guarantee and online e-reputation management services is dedicated to using only White-Hat-Techniques. Moreover, most of the online pages are archived at the Internet Archive. Furthermore, online e-reputation management services respects each constitution of each country, its privacy, the laws of the press and of the freedom of speech, so content that is protected by the law will not be removed. It is important to generate and promote new positive content.

Case Projects

Solution

The following is a partial project solution. Students should be able to expand on the project analysis through extensive research.

Online e-reputation management services is capable of detecting and blocking web-based security risks, including phishing attacks. You have the option to configure the internal and external user policies.

Optional Team Case Project

Solution

The following is a partial solution to aid students in coming up with their own solution to solve this case:

Here are the levels that one can configure in a management console:

- High: Blocks URLs that are unrated, a Web threat, very likely to be a Web threat, or likely to be a Web threat.
- Medium: Blocks URLs that are unrated, a Web threat, or very likely to be a Web threat.
- Medium-Low: Blocks URLs that are a Web threat or very likely to be a Web threat.
- Low: Blocks only URLs that are a Web threat.

CHAPTER 66: CONTENT FILTERING

Review Questions/Exercises

True/False

1. False
2. True
3. False

4. True
5. False

Multiple Choice

1. B, E
2. B
3. D
4. A
5. E

Exercise

Solution

The following is a partial exercise solution. The students should be able to expand on the following:

- Content filtering can be implemented to prevent under age users from accessing inappropriate material on the Internet while allowing access to educational material.
- Content filtering can be used to prevent access to material that is illegal such as child pornography.
- Content filtering can be an effective means of limiting the liability that institutions face by providing Internet access.
- Content filtering can be used to increase employee productivity by restricting access to inappropriate or non-work related sites.
- Content filtering can conserve bandwidth, freeing existing bandwidth for mission-critical needs and decreasing the need to purchase additional bandwidth.

Hands-on Project

Solution

The following is a partial project solution. The students should be able to expand on the following:

Content filtering will introduce a few milliseconds to the transaction time for each site accessed. This additional time will not be perceptible to users. Some institutions may actually experience faster download times in situations where a significant amount of inappropriate traffic is removed by content filtering.

Case Projects

Solution

The following is a partial project solution. Students should be able to expand on the project analysis through extensive research.

No, only constituents who subscribe to content filtering will have their Internet traffic directed to the content filtering equipment on the backbone. Other constituents will be completely unaffected.

Optional Team Case Project

Solution

The following is a partial solution to aid students in coming up with their own solution to solve this case:

When a user attempts to access a blocked site, the software will redirect the user to a web page indicating that the content filter has blocked access to that site.

CHAPTER 67: DATA LOSS PROTECTION

Review Questions/Exercises

True/False

1. True
2. False
3. True
4. False
5. False

Multiple Choice

1. C
2. D
3. C
4. C
5. E

Exercise

Solution

The following is a partial exercise solution. The students should be able to expand on the following:

- Content filtering can be implemented to prevent under age users from accessing inappropriate material on the Internet while allowing access to educational material.
- Content filtering can be used to prevent access to material that is illegal such as child pornography.
- Content filtering can be an effective means of limiting the liability that institutions face by providing Internet access.
- Content filtering can be used to increase employee productivity by restricting access to inappropriate or non-work related sites.
- Content filtering can conserve bandwidth, freeing existing bandwidth for mission-critical needs and decreasing the need to purchase additional bandwidth.

Hands-on Project

Solution

The following is a partial project solution. The students should be able to expand on the following:

Content filtering will introduce a few milliseconds to the transaction time for each site accessed. This additional time will not be perceptible to users. Some institutions may actually experience faster download times in situations where a significant amount of inappropriate traffic is removed by content filtering.

Case Projects

Solution

The following is a partial project solution. Students should be able to expand on the project analysis through extensive research.

No, only constituents who subscribe to content filtering will have their Internet traffic directed to the content filtering equipment on the backbone. Other constituents will be completely unaffected.

Optional Team Case Project

Solution

The following is a partial solution to aid students in coming up with their own solution to solve this case:

When a user attempts to access a blocked site, the software will redirect the user to a web page indicating that the content filter has blocked access to that site.

CHAPTER 68: SATELLITE CYBER ATTACK SEARCH AND DESTROY

Review Questions/Exercises

True/False

1. True
2. False
3. False
4. False
5. False

Multiple Choice

1. C
2. D
3. A
4. A
5. B

Exercise

Solution

The following is a partial exercise solution. The students should be able to expand on the following:

1. Ground-based threats;
2. Space-based threats;
3. Interference oriented threats.

Hands-on Project

Solution

The following is a partial project solution. The students should be able to expand on the following:

Basic Interoperable Scrambling System, usually known as BISS, is a satellite signal scrambling system developed by the European Broadcasting Union and a consortium of hardware manufacturers. Prior to its development, “ad-hoc” or “Occasional Use” satellite news feeds were transmitted either using proprietary encryption methods (PowerVu), or without any encryption. Unencrypted satellite feeds allowed anyone with the correct equipment to view the program material.

Case Projects

Solution

The following is a partial project solution. Students should be able to expand on the project analysis through extensive research.

PowerVu is a conditional access system for digital television developed by Scientific Atlanta. It is used for professional broadcasting, notably by Retevision, Bloomberg Television, Discovery Channel, AFRTS and American Forces Network. PowerVu is also used by cable companies to prevent viewing by unauthorized viewers. PowerVu has decoders that decode signals from certain satellites for cable distribution services. These decoders can also be used just like the FTA (Free-To-Air) satellite receivers if properly configured. PowerVu was considered highly secure since it uses a complicated system to authorize each PowerVu receiver and trace its history of ownership and usage. Most PowerVu users are professional cable or satellite companies, using the service and equipment for signal redistribution, because regular users cannot afford it. On March 10, 2010, the hacker called “Colibri” published after previous work done in 2005 a cryptanalysis of a PowerVU system implementation, describing a flawed design that can be used to gain access to the encryption keys and ultimately decryption of the transmitted content.

Optional Team Case Project

Solution

The following is a partial solution to aid students in coming up with their own solution to solve this case:

DigiCipher 2, or simply DCII, is a proprietary standard format of digital signal transmission and encryption with MPEG-2 signal video compression used on many communications satellite television and audio signals. The DCII standard was originally developed in 1997 by General Instrument, which is now the Home and Network Mobility division of Motorola. The original attempt for a North American digital signal. encryption and compression standard was DigiCipher 1, which was used most notably in the now-defunct PrimeStar medium-power direct broadcast satellite (DBS) system during the early 1990s. The DCII standard predates wide acceptance of DVB-based digital terrestrial television compression (although not cable or satellite DVB) and therefore, is incompatible with the DVB standard. The primary difference between DigiCipher 2 and DVB lies in how each standard handles SI, or System Information. DigiCipher 2 also relies on the fact that its signals must be understood in terms of a virtual channel number in addition to the DCII signal's downlink frequency, whereas DVB signals have no virtual channel number. Approximately 70% of newer first-generation digital cable networks in North America use the 4DTV/DigiCipher 2 format. The use of DCII is most prevalent in North American digital cable television set top boxes. DCII is also used on Motorola's 4DTV digital satellite television tuner and Shaw Direct's DBS receiver.

CHAPTER 69: VERIFIABLE VOTING SYSTEMS

Review Questions/Exercises

True/False

1. True
2. True
3. False
4. False
5. True

Multiple Choice

1. D
2. A
3. D
4. C
5. A

Exercise

Solution

The following is a partial exercise solution. The students should be able to expand on the following:

Their difference is that in secret sharing, there needs to be a trusted authority to distribute the secret information among all the parties. But in threshold techniques, no trusted authority is needed, and all parties can work together to generate the secret information and distribute it among themselves. Here, we review some basic secret sharing techniques and the threshold ElGamal. Note that the threshold RSA and threshold Paillier are also feasible, but they are more complex.

Hands-on Project

Solution

The following is a partial project solution. The students should be able to expand on the following:

Zero-knowledge: There exists an expected polynomial-time algorithm which can produce, upon input of the assertion to be proven but without interacting with the real prover, transcripts indistinguishable from those resulting from interaction with the real prover.

Case Projects

Solution

The following is a partial project solution. Students should be able to expand on the project analysis through extensive research.

It can be used to prove that a party knows the solution of *k* out of *n* problems without revealing which problems she/he can solve. This protocol is normally used in verifiable voting schemes to prove that a ciphertext is an encryption of one value within a subset of different values.

Optional Team Case Project

Solution

The following is a partial solution to aid students in coming up with their own solution to solve this case:

It takes a list of encrypted values as input, and outputs a list of values (encrypted or decrypted depending on the type of mixnet) corresponding to the input list, but permuted so the links between individual inputs and outputs are hidden. When the mixnet receives a number of encrypted values as inputs, each mix server will either partially decrypt (in a decryption mix) or re-encrypt (in a re-encryption mix) each of the encrypted values and output the results to the next mix server in a permuted order. Therefore, if there exists at least one honest mix server, the relationships between the mixnet inputs and outputs will be kept private. However, the main challenge is how to efficiently prove that the mixnet has generated the correct outputs without revealing the inputs and outputs relationships.

CHAPTER 70: ADVANCED DATA ENCRYPTION

Review Questions/Exercises

True/False

1. True
2. False
3. False
4. False
5. True

Multiple Choice

1. E
2. D
3. A
4. A
5. B

Exercise

Solution

The following is a partial exercise solution. The students should be able to expand on the following:

Advanced data encryption is done either by computer programs or by specially designed computer hardware devices. These programs or devices apply a mathematical algorithm (a recipe for producing encrypted data) to the information. The output is a scrambled form of the original data. When a legitimate user needs to access the data, the scrambling process is reversed and the data is restored to its original form. Only those who are in possession of the "key" can unscramble ("decrypt") the data.

Hands-on Project

Solution

The following is a partial project solution. The students should be able to expand on the following:

A key is a piece of data that an advanced data encryption algorithm uses to determine exactly how to unscramble the protected information. It is called a key because it "unlocks" the encryption formula to unscramble the encrypted data.

Case Projects

Solution

The following is a partial project solution. Students should be able to expand on the project analysis through extensive research.

Actually, there are three types of keys: "secret," "public" and "private." Different advanced data encryption algorithms use different types of keys. The more traditional advanced data encryption algorithm schemes use secret keys to both encrypt and decrypt data. Newer methods of advanced data encryption algorithm, known as "public-key" algorithms, use a public key to encrypt a piece of information and its corresponding private key to decrypt the information.

Optional Team Case Project

Solution

The following is a partial solution to aid students in coming up with their own solution to solve this case:

Any kind of data can be encrypted. You can encrypt plaintext files. PDF documents, spreadsheets, images and any other form of information in your computer. You can even encrypt database information and information on back-up media.