Answers

Chapter Review

This chapter examined the attack methods used by hackers. Seven major categories of attack were covered: malware, password attacks, physical attacks, adversarial artificial intelligence, supply-chain attacks, cloud-based vs. onpremises attacks, and cryptographic attacks. Each of these sections details several specific attacks.

The malware section examined ransomware, trojans, worms, potentially unwanted programs (PUPs), fileless virus attacks, command and control, bots, crypto-malware, logic bombs, spyware, keyloggers, remote-access trojans (RAT), rootkits, and backdoors. The password attack section covered passwordspraying attacks, dictionary and brute force attacks, offline and online attacks, rainbow tables, and attacks against plaintext/unencrypted passwords. The section on physical attacks examined attacks using physical manipulation, including malicious USB cables, malicious USB devices, card cloning, and skimming attacks. The section on the adversarial use of artificial intelligence covered the concept of tainting a machine learning system through contaminating the training data. This section also covered the importance of security for machine learning algorithms and parameters.

The chapter concluded with sections on supply-chain attacks and cloud-based vs. on-premise attacks. The last section covered cryptographic attacks, including birthday attacks, collision attacks, and downgrade attacks. What is important to remember is that this material is designed to assist you in understanding CompTIA Security+ exam objective 1.2: Given a scenario, analyze potential indicators to determine the type of attack. You need to be prepared to differentiate between the types of attacks.

Questions

1. A disgruntled administrator is fired for negligence at your organization.Thirty days later, your organization’s internal file server and backup server crash at exactly the same time. Examining the servers, you determine that critical operating system files were deleted from both systems. If the disgruntled administrator was responsible for administering those servers during her employment, this is most likely an example of what kind of malware?

A. Crypto-malware

B. Trojan

C. Worm

D. Logic bomb

2. A colleague has been urging you to download a new animated screensaver he has been using for several weeks. While he is showing you the program, the cursor on his screen moves on its own and a command prompt window opens and quickly closes. You can’t tell what if anything was displayed in that command prompt window. Your colleague says, “It’s been doing that for a while, but it’s no big deal.” Based on what you’ve seen, you suspect the animated screensaver is really what type of malware?

A. A worm

B. A trojan

C. Ransomware

D. Spyware

3. Several desktops in your organization are displaying a red screen with themessage “Your files have been encrypted. Pay 1 bitcoin to recover them.” These desktops have most likely been affected by what type of malware?

A. Spyware

B. Spraying

C. Ransomware

D. Crypto-malware

4. While port-scanning your network for unauthorized systems, you notice oneof your file servers has TCP port 31337 open. When you connect to the port with the security tool netcat, you see a prompt that reads, “Enter password for access:”. Your server may be infected with what type of malware?

A. PUP

B. Fileless virus

C. Backdoor

D. Man in the middle attack

5. While port-scanning your network for unauthorized systems, you notice oneof your file servers has TCP port 61337 open. When you use Wireshark and examine the packets, you see encrypted traffic, in single packets, going back and forth every five minutes. The external connection is a server outside of your organization. What is this connection?

A. Command and control

B. Backdoor

C. External backup location

D. Remote login

6. A user in your organization is having issues with her laptop. Every time sheopens a web browser, she sees different pop-up ads every few minutes. It doesn’t seem to matter which websites are being visited—the pop-ups still appear. What type of attack does this sound like?

A. A potentially unwanted program (PUP)

B. Ransomware

C. Worm

D. Virus

7. Users at your organization are complaining about slow systems. Examiningseveral of them, you see that CPU utilization is extremely high and a process called “btmine” is running on each of the affected systems. You also notice each of the affected systems is communicating with an IP address outside your country on UDP port 43232. If you disconnect the network connections on the affected systems, the CPU utilization drops significantly. Based on what you’ve observed, you suspect these systems are infected with what type of malware?

A. Rainbow tables

B. Crypto-malware

C. Dictionary

D. Hybrid attack

8. A piece of malware is infecting the desktops in your organization. Everyhour, more systems are infected. The infections are happening in different departments and in cases where the users don’t share any files, programs, or even e-mails. What type of malware can cause this type of infection?

A. Virus

B. Trojan

C. RAT

D. Worm

9. Which of the following are characteristics of remote-access trojans?A. They can be deployed through malware such as worms.

B. They allow attacks to connect to the system remotely.

C. They give attackers the ability to modify files and change settings.

D. All of the above.

10. To test your systems against weak passwords, you as an admin (with properpermissions) test all the accounts using the top 100 commonly used passwords. What is this test an example of?

A. Dictionary

B. Password spraying

C. Rainbow tables

D. Online

Answers

1. D. Because both servers crashed at exactly the same time, this is most likely a logic bomb. A logic bomb is a piece of code that sits dormant for a period of time until some event or date invokes its malicious payload—in this case, 30 days after the disgruntled employee was fired.

2. B. The animated screensaver is most likely a trojan. The software appears to do one thing, but contains hidden, additional functionality. Your colleague brought the trojan “inside the walls” when he downloaded and installed the software on his desktop.

3. C. This is quite clearly ransomware. The malware has encrypted files on the affected systems and is demanding payment for recovery of the files.

4. C. This prompt most likely belongs to a backdoor—an alternate way of accessing the system. The TCP service is listening for incoming connections and prompts for a password when connections are established. Providing the correct password would grant command-line access to the system.

5. A. Periodic traffic that looks like a heartbeat on high ports to an unknown server outside the network is suspicious, and this is what many commandand-control signals look like.

6. A. This behavior is often seen in a potentially unwanted program—a type of application that has been bundled with others and is performing tasks that are undesired.

7. B. These systems are most likely infected with crypto-malware and are now part of a botnet that’s mining cryptocurrency. The systems are running an unknown/unauthorized process, communicating with an external IP address, and using significant resources. These are all classic signs of cryptomalware.

8. D. This is most likely a worm attack. Attacks that move across the network, seemingly without user intervention, are commonly worms.

9. D. All of these are characteristics of remote-access trojans (RATs). RATs are often deployed through other malware, allow remote access to the affected system, and give the attacker the ability to manipulate and modify the affected system.

B. Using preset passwords against all accounts is an example of password spraying.

Questions

1. When an attacker captures network traffic and retransmits it at a later time,what type of attack are they attempting?

A. Denial-of-service attack

B. Replay attack

C. Bluejacking attack

D. Man in the middle attack

2. What type of attack involves an attacker putting a layer of code between anoriginal device driver and the operating system?

A. Refactoring

B. Trojan horse

C. Shimming

D. Pass the hash

3. You’re reviewing a custom web application and accidentally type a numberin a text field. The application returns an error message containing variable names, filenames, and the full path of the application. This is an example of which of the following?

A. Resource exhaustion

B. Improper error handling

C. Generic error message

D. Common misconfiguration

4. You’re working with a group testing a new application. You’ve noticed thatwhen three or more of you click Submit on a specific form at the same time, the application crashes every time. This is most likely an example of which of the following?

A. A race condition

B. A nondeterministic error

C. An undocumented feature

D. A DLL injection

5. An externally facing web server in your organization keeps crashing.Looking at the server after a reboot, you notice CPU usage is pegged and memory usage is rapidly climbing. The traffic logs show a massive amount of incoming HTTP and HTTPS requests to the server. Which type of attack is this web server experiencing?

A. Input validation

B. Distributed error handling

C. Resource exhaustion

D. Race condition

6. Your organization is considering using a new ticket identifier with yourcurrent help desk system. The new identifier would be a 16-digit integer created by combining the date, time, and operator ID. Unfortunately, when you’ve tried using the new identifier in the “ticket number” field on your current system, the application crashes every time. The old method of using a five-digit integer works just fine. This is most likely an example of which of the following?

A. Common misconfiguration

B. Zero-day vulnerability

C. Memory leak

D. Integer overflow

7. While examining a laptop infected with malware, you notice the malwareloads on startup and also loads a file called netutilities.dll each time

Microsoft Word is opened. This is an example of which of the following?

A. Race condition

B. DLL injection

C. System infection

D. Memory overflow

8. A web application you are reviewing has an input field for username and indicates the username should be between 6 and 12 characters. You’ve discovered that if you input a username that’s 150 characters or more in length, the application crashes. What is this is an example of?

A. Memory leak

B. Buffer overflow

C. Directory traversal

D. Integer overflow

9. Your organization is having issues with a custom web application. Theapplication seems to run fine for a while but starts to lock up or crash after seven to ten days of continuous use. Examining the server, you notice that memory usage seems to climb every day until the server runs out of memory. The application is most likely suffering from which of the following?

A. Memory leak

B. Overflow leak

C. Zero-day exploit

D. Pointer dereference

10. Your database server is returning a large dataset to an online user, saturatingthe network. The normal return of records would be a couple at most. This is an example of what form of attack?

A. Memory leak

B. LDAP injection

C. Man in the middle

D. SQL injection

Answers

1. B. A replay attack occurs when the attacker captures a portion of the communication between two parties and retransmits it at a later time. For example, an attacker might replay a series of commands and codes used in a financial transaction to cause the transaction to be conducted multiple times. Generally, replay attacks are associated with attempts to circumvent authentication mechanisms, such as the capturing and reuse of a certificate or ticket.

2. C. Shimming is the process of putting a layer of code between the device driver and the operating system.

3. B. When an application fails to properly trap an error and generates error messages containing potentially sensitive information, this is known as improper error handling.

4. A. This is most likely an example of a race condition. A race condition is an error condition that occurs when the output of a function is dependent on the sequence or timing of the inputs. In this case, the application crashes when multiple inputs are submitted at the same time because the application is not receiving the inputs or handling the inputs in the expected order.

5. C. Resource exhaustion is the state where a system does not have all of the resources it needs to continue to function. In this case, the server does not have the memory or CPU capacity to handle the massive volume of incoming HTTP/HTTPS requests.

6. D. An integer overflow is a programming error condition that occurs when a program attempts to store a numeric value, an integer, in a variable that is too small to hold it. In this case, the 16-digit integer is too large for the field, which is working just fine with the five-digit integer.

7. B. This is an example of DLL injection, which is the process of adding to a program, at runtime, a DLL that has a specific function vulnerability that can be capitalized upon by an attacker.

8. B. This is a fairly classic example of a buffer overflow. The input routine

does not validate the provided input to ensure a maximum of 12 characters is received and processed. In this case, the application tries to store all 150 (or more) characters of the username, resulting in areas of memory being overwritten and causing the application to crash.

9. A. Memory leaks are programming errors caused when a computer program does not properly handle memory resources. Over time, while a program runs, if it does not clean up memory resources as they are no longer needed, chunks of dead memory can become scattered across the program’s footprint in memory. If a program executes for a long time, these dead memory areas can grow in size and consume resources, causing the system to crash.

D. Excessive records being returned from a SQL query is a sign of SQL injection.

Questions

To help you prepare further for the CompTIA Security+ exam, and to test your level of preparedness, answer the following questions and then check your answers against the correct answers at the end of the chapter.

1. A user reports “odd” certificate warnings on her web browser this morningwhenever she visits Google. Looking at her browser, you see these certificate warnings. Looking at the network traffic, you notice that all HTTP and HTTPS requests from that system are being routed to the same

IP regardless of destination. Which of the following attack types are you

seeing in this case?

A. Evil twin

B. Man in the middle

C. Disassociation

D. MAC cloning

2. Users are reporting that the wireless network on one side of the building isbroken. They can connect but can’t seem to get to the Internet. While investigating, you notice all of the affected users are connecting to an access point you don’t recognize. These users have fallen victim to what type of attack?

A. Rogue AP

B. WPS

C. Bluejacking

D. Disassociation

3. You’re sitting at the airport when your friend gets a message on her phone.In the text is a picture of a duck with the word “Pwnd” as the caption. Your friend doesn’t know who sent the message. Your friend is a victim of what type of attack?

A. Snarfing

B. Bluejacking

C. Quacking

D. Collision

4. All of the wireless users on the third floor of your building are reportingissues with the network. Every 15 minutes, their devices disconnect from the network. Within a minute or so they are able to reconnect. What type of attack is most likely underway in this situation?

A. Evil twin

B. Jamming

C. Domain hijacking

D. Disassociation

5. Your e-commerce site is crashing under an extremely high traffic volume. Looking at the traffic logs, you see tens of thousands of requests for the same URL coming from hundreds of different IP addresses around the

world. What type of attack are you facing?

A. Domain hijacking

B. DDoS

C. DNS poisoning

D. URL redirection

6. A user wants to know if the network is down because she is unable toconnect to anything. While troubleshooting, you notice the MAC address for her default gateway setting doesn’t match the MAC address of your organization’s router. What type of attack has been used against this user?

A. MAC cloning

B. ARP poisoning

C. Disassociation

D. Rogue access point

7. You have a helpdesk ticket for a system that is acting strangely. Looking atthe system remotely, you see the following in the browser cache: www.micros0ft.com/office. What type of attack are you seeing?

A. PowerShell

B. Domain hijacking

C. URL redirection

D. Disassociation

8. You are seeing a bunch of PDFs flood people’s inboxes with titles such as“New Tax Rates for 2021.” What attack vector is most likely in use?

A. Python

B. Macro

C. Man in the middle

D. DDoS

9. When you update your browser, you get a warning about a plugin not beingcompatible with the new version. You do not recognize the plugin, and you aren’t sure what it does. Why is it important to understand plugins? What attack vector can be involved in plugins?

A. Man in the middle attack

B. Domain hijacking attack

C. Man in the browser attack

D. URL redirection attack

10. Your network scan is showing a large number of address changes to the MAC tables and lots of ARP and RARP messages. What is happening?

A. MAC flooding attack

B. Disassociation attack

C. Jamming attack

D. DNS poisoning

Answers

1. B. This is most likely some type of man in the middle attack. This attack method is usually done by routing all of the victim’s traffic to the attacker’s host, where the attacker can view it, modify it, or block it. The attacker inserts himself into the middle of his victim’s network communications.

2. A. This is a rogue AP attack. Attackers set up their own access points in an attempt to get wireless devices to connect to the rogue APs instead of the authorized access points.

3. B. This is most likely a bluejacking attack. If a victim’s phone has Bluetooth enabled and is in discoverable mode, it may be possible for an attacker to send unwanted texts, images, or audio to the victim’s phone.

4. D. Disassociation attacks against a wireless system are attacks designed to disassociate a host from the wireless access point and from the wireless network. If the attacker has a list of MAC addresses for the wireless devices, they can spoof de-authentication frames, causing the wireless devices to disconnect from the network.

5. B. This is a DDoS attack. DDoS (or distributed denial-of-service) attacks attempt to overwhelm their targets with traffic from many different sources. Botnets are quite commonly used to launch DDoS attacks.

6. B. ARP poisoning is an attack that involves sending spoofed ARP or RARP replies to a victim in an attempt to alter the ARP table on the victim’s system. If successful, an ARP poisoning attack will replace one of more MAC addresses in the victim’s ARP table with the MAC address the attacker supplies in their spoofed responses.

7. C. This is a URL redirection, as the name Microsoft has a zero in place of the o character.

8. B. PDFs have macro capability and can execute a variety of code bases if allowed.

9. C. Man in the browser attacks are frequently carried out via browser extensions or plugins.

A. This is a MAC flooding attack—an attempt to overflow the MAC tables in the switches.

Questions

1. Your senior financial people have been attacked with a piece of malwaretargeting financial records. Based on talking to one of the executives, you now know this is a spear phishing attack. Which of the following is the

most likely vector used?

A. Cloud

B. Wireless

C. Direct access

D. Removeable media

2. You are new to your job, new to the industry, and new to the city. Which ofthe following sources would be the best to connect with your peers on threat intelligence information?

A. Vendors

B. Social media

C. Local industry groups

D. Vulnerability or threat feeds

3. Your company has had bad press concerning its support (or lack of support)for a local social issue. Which type of hacker would be the most likely threat to attack or deface your website with respect to this issue?

A. State actor

B. Hacktivist

C. Black hat

D. Competitor

4. Proper use of separation of duties with respect to privileged users on yoursystems is a defense against which type of hacker?

A. Nation-state actor

B. Insider

C. Criminal syndicate

D. All of the above

5. You have read about a new threat against software that is vulnerable tohacking. The vulnerability is in a Python library, and your firm uses Python for the development of many in-house projects. Where is the best source of information with respect to this threat?

A. File/code repositories

B. Vulnerability databases

C. Open source intelligence

D. Indicators of compromise

6. Your threat intelligence vendor is sending out urgent messages concerning anew form of memory-resident malware. What is the likely item they are sharing with you?

A. Vulnerability database

B. Indicator of compromise

C. Dark web

D. Trusted Automated Exchange of Intelligence Information (TAXII)

7. You use a “golden disk” to provision new machines from your vendors. Aspart of the incident response, you have discovered that the source of the malware you are seeing comes from this golden disk. This is an example of what vector?

A. Insider

B. Direct access

C. Removeable media

D. Supply chain

8. Understanding how an attacker operates so that you can develop adefensive posture is done through the use of which of the following?

A. Predictive analysis

B. TTPs

C. Threat maps

D. Automated Indicator Sharing

9. Which of the following items do you as a defender have control over withrespect to using threat intelligence to defend your systems?

A. Vectors

B. Actors

C. Threat intelligence sources

D. Attributes of actors

10. You want to get specific information on a specific threat that you have readabout in your online newsfeed on your phone. Which of the following is the best source for detailed information?

A. Vulnerability database

B. Open source intelligence

C. Dark web

D. Predictive analysis

Answers

1. D. Removeable media is commonly linked to social engineering attacks such as spear phishing.

2. C. Networking between peers is a useful attribute of local industry groups.

3. B. Hacktivists are hackers that are pursuing a mission associated with a cause.

4. D. Separation of duties is designed to provide defenses against malicious insiders. But nation-state actors and criminal organizations have the resources and abilities to hack accounts and gain insider access. There are no external accounts, so once a well-resourced hacker is in, they will have permissions associated with an insider.

5. A. File/code repositories is the correct answer because the code you are concerned about was developed in-house; hence, it will not show up in commercial databases or other sources.

6. B. An indicator of compromise (IoC) provides the details associated with how one can find active malware on a system.

7. D. This is a supply chain vector. Although the work was done in-house, the supply chain stretches from each part to functioning system, and you added the final software to create the functioning system, so your own team is part of the supply chain.

8. B. Adversary tactics, techniques, and procedures (TTPs) provide details on how an adversary operates.

9. A. Vectors is the correct answer because this is the only item you have any direct control over. The other items are real issues, just not ones you have any measure of direct control over.

B. Open source intelligence is the best answer. Because you are looking for threat information, this eliminates vulnerability information as an answer. The dark web may or may not have information, and you would have to find it, and predictive analysis needs the information you seek in order to function.

Questions

To help you prepare further for the CompTIA Security+ exam, and to test your level of preparedness, answer the following questions and then check your answers against the correct answers at the end of the chapter.

1. Direct third-party risks include which of the following? (Choose all thatapply.)

A. System integration

B. Supply chain

C. Financial management

D. Vendor management

2. Common sources of vulnerability issues for systems include which of thefollowing? (Choose all that apply.)

A. Weak patch management

B. Data loss

C. Identity theft

D. Weak configurations

3. Weak configurations can include which of the following? (Choose all thatapply.)

A. Open ports

B. Lack of vendor support

C. Firmware

D. Use of unsecure protocols

4. A patch management process should include which of the following?

(Choose all that apply.)

A. Automated management of software assets

B. Automated verification of current patch levels

C. A specified period by which systems should be patched

D. Connection of the patch management process to the change controlprocess

5. Financial risks associated with vulnerabilities can include which of thefollowing? (Choose all that apply.)

A. Regulatory fines and penalties

B. Business reputation loss

C. Loss of revenue due to downtime

D. Loss of data

6. What type of threat exploits system and application vulnerabilities that are unknown to software developers and even anti-malware manufacturers?

A. An on-premises attack

B. A zero-day attack

C. A cloud-based attack

D. A legacy platform attack

7. As a security professional, what should you do to address weakconfigurations that pose security risks to your organization? (Choose all that apply.)

A. Change default usernames and passwords.

B. Remove unnecessary apps.

C. Disable unnecessary services.

D. Open all ports so that everything can be scanned.

8. Which statement is false regarding cryptographic practices and weakencryption?

A. Developing your own cryptographic algorithm is considered aninsecure practice.

B. Cryptographic algorithms become trusted only after years of scrutinyand repelling attacks.

C. The ability to use ever-faster hardware has enabled attackers to defeatsome cryptographic methods.

D. Because TLS is deprecated, SSL should be used instead.

9. Who assumes the risk associated with a system or product after it hasentered EOL status?

A. The original manufacturer

B. The vendor

C. The organization

D. The supply chain manager

10. Which of the following best describes the exporting of stolen data from anenterprise?

A. Data loss

B. Data breach

C. Data exfiltration

D. Identity theft

Answers

1. A, B, and D. System integration, supply chain, and vendor management are sources of third-party risk. Financial management is related to impacts, not mainly third-party risks.

2. A and D. Improper or weak patch management and weak configurations are defined as common sources for vulnerabilities.

3. A and D. Having open ports and using unsecure protocols can both provide openings for attackers to get into a system. Lack of vendor support is a third-party risk, and firmware has a fixed configuration.

4. A, B, C, and D. A good patch management process should include automated management of software assets, automated verification of current patch levels, a specified period by which systems should be patched, and connection of the patch management process to the change control process.

5. A and C. Regulatory fines and penalties as well as lost income because of downtime are direct financial impacts of cybersecurity problems. Business reputation may lead to a loss of customers, but this is not a direct connection. Loss of data may or may not have a financial impact depending upon the data and its connection to revenue.

6. B. A zero-day attack exploits system and application vulnerabilities that are unknown to others except the person who found it. The other answer options are not attack types. Vulnerabilities can exist on premises or be cloud based, and legacy platforms is the term used to describe systems that are no longer being marketed or supported.

7. A, B, and C. Every effort should be made to remove unnecessary apps, disable any unnecessary services, and change default account usernames and passwords. Opening all ports is a recipe for disaster. Unnecessary or unused ports should be closed or secured.

8. D. All versions of SSL are now considered deprecated and should not be used. Everyone should switch their systems to TLS-based solutions. All other statements are true.

9. C. An organization that continues to use a system or product assumes all of the risk associated with issues uncovered after the product has entered endof-life (EOL) status. The manufacturer is in fact most often the vendor, and from their standpoint, the product reaches EOL when they stop supporting it. The supply chain manager is a distractor answer choice.

10. C. Data exfiltration is the exporting of stolen data from an enterprise. Data loss is when an organization actually loses information. Data breaches are the release of data to unauthorized parties. Identity theft is a crime where someone uses information on another party to impersonate them.

Questions

To help you prepare further for the CompTIA Security+ exam, and to test your level of preparedness, answer the following questions and then check your answers against the correct answers at the end of the chapter.

1. If a system sends an alert that a user account is being hacked because of toomany password failures, but analysis shows that the person’s device had cached an old password, triggering the failures, what is this an example of?

A. False negative

B. False positive

C. Measurement error

D. Analysis failure

2. Anti-malware software fails to detect a ransomware attack that is supposed to be within its capabilities of detecting. What is this an example of?

A. False negative

B. False positive

C. Measurement error

D. Analysis failure

3. What is the primary limitation of a credentialed scan on a network?

A. Speed

B. Examining too deeply into individual boxes

C. The inability to scale across multiple systems

D. Slowing down your network with ancillary traffic

4. You desire to prove a vulnerability can be a problem. The best methodwould be to use a(n) \_\_\_\_\_\_\_\_\_\_\_\_\_ scan?

A. credentialed

B. non-intrusive

C. non-credentialed

D. intrusive

5. Which of the following best describes what CVE is?

A. A place to report errors and vulnerabilities

B. A measure of the severity of a vulnerability

C. A list of known vulnerabilities

D. A list of systems that have vulnerabilities

6. Which of the following is not associated typically with SIEM processes?

A. Applications

B. Syslog

C. Log capture

D. Log aggregation

7. Which of the following is not part of SIEM processes?

A. Data collection

B. Event correlation

C. Alerting/reporting

D. Incident investigation

8. Threat hunting involves which of the following? (Choose all that apply.)

A. Analysis of adversarial actions

B. Interpretation of threats to other companies

C. Compliance reporting

D. Understanding how data flows in an enterprise

9. Which process allows log files to be enriched with additional data toprovide context?

A. Log aggregation

B. Log collectors

C. Log reviews

D. Syslog

10. Which of the following are not typically scanned during a vulnerabilityscan?

A. End users

B. Network

C. Applications

D. Web applications

Answers

1. B. This is a false positive, as the report was positive that something had happened, when in fact it had not.

2. A. Failing to report on a known reportable event is a false negative.

3. C. Because a credentialed scan requires credentials for each system it is examining, and these credentials will change across a network, this type of scan is less scalable with automation.

4. D. An intrusive scan attempts to exercise a vulnerability. This presents risk in that it might upset the system, but if it works, it is clear proof of the risk associated with a vulnerability.

5. C. Common Vulnerabilities and Exposures is an enumeration or list of known vulnerabilities.

6. A. Applications may be all over the network and may provide data to a SIEM, but they are not typically part of the SIEM process.

7. D. Incident investigations occur after and as a result of SIEM processes but are not typically part of them.

8. A, B, and D. Threat hunting involves analyzing adversarial actions, interpreting the threats to other companies, and understanding how data flows in an enterprise so adversaries can be caught maneuvering.

9. A. During the process of aggregation, the log entries can be parsed, modified, and have key fields extracted or modified based on lookups or rules.

10. A. End users are not part of a vulnerability scan; they are air gapped from the system and are not part of the elements that are searched for vulnerabilities.

Questions

To help you prepare further for the CompTIA Security+ exam, and to test your level of preparedness, answer the following questions and then check your answers against the correct answers at the end of the chapter.

1. Which of the following teams is commonly used for active pen testing?

A. Red team

B. Black team

C. White team

D. Green team

2. War flying is a term to describe which of the following?

A. Pen testing networks on commercial planes

B. The use of aerial platforms to gain access to wireless networks

C. Driving around and sampling open Wi-Fi networks

D. The use of pen testing techniques against the Defense Department

3. When an attacker moves to a new machine and rescans the network to lookfor machines not previously visible, what is this technique called?

A. Lateral movement

B. Privilege escalation

C. Persistence

D. Pivoting

4. What is the most important first step in a penetration test?

A. OSINT

B. Rules of engagement

C. Reconnaissance

D. Privilege escalation

5. Covering one’s tracks to prevent discovery is also known as what?

A. Lateral movement

B. OSINT

C. Cleanup

D. Pivoting

6. When a pen tester uses OSINT to gain information on a system, the type ofenvironment can be changed from \_\_\_\_\_\_ to \_\_\_\_\_\_\_.

A. closed, open

B. unknown, known

C. secure, vulnerable

D. unknown, partially known

7. Which team involves members who emulate both attackers and defenders?

A. Purple team

B. Gold team

C. Blue team

D. White team

8. OSINT involves which of the following?

A. Passive reconnaissance

B. Active reconnaissance

C. Port scanning

D. Persistence

9. Which of the following is a formal approach to identifying system ornetwork weaknesses and is open to the public?

A. Active reconnaissance

B. Passive reconnaissance

C. OSINT

D. Bug bounty

10. What is the purpose of a white team?

A. To represent senior management

B. To provide judges to score or rule on a test

C. To represent parties that are targets in a pen test

D. To provide a set of team members with offense and defensive skills (allstars)

Answers

1. A. The red team is a team of offense actors used in penetration testing.

2. B. War flying is the use of drones, airplanes, and other flying means of gaining access to wireless networks that are otherwise inaccessible.

3. D. The key part of the question is the rescanning. Pivoting involves the rescanning of network connections to find unknown or previously unseen connections.

4. B. The rules of engagement describe the scope of an engagement and provide important information regarding contacts and permissions.

Obtaining these rules is essential before any pen test work begins.

5. C. Cleanup involves the steps of clearing logs and other evidence to prevent one from being easily discovered.

6. D. OSINT provides information about systems and their addresses and connections, including applications. This takes the status of a system from a completely unknown environment to a partially known environment.

7. A. Purple teams have both offensive (red) and defensive (blue) personnel to provide a balanced response.

8. A. OSINT is a passive activity, so passive reconnaissance is the correct answer. All of the other answers involve active measures.

9. D. Bug bounty programs can open up vulnerability discovery to the public with a set of rules that manages the disclosure process and the engaging of the systems.

10. B. When an exercise involves scoring and/or a competition perspective, the team of judges is called the white team. If the exercise is such that it requires an outside set of coordinators to manage it, independent of the defending team, they are also called a white team. White team members are there to ensure that the actual exercise stays on track and involves the desired elements of a system.

Questions

To help you prepare further for the CompTIA Security+ exam, and to test your level of preparedness, answer the following questions and then check your answers against the correct answers at the end of the chapter.

1. Which of the following is not a state of data in the enterprise?

A. At rest

B. In storage

C. In processing

D. In transit/motion

2. Creating fake network traffic to deceive attackers in segments of thenetwork designed to deceive them is called what?

A. DNS sinkhole

B. Honeytraffic

C. Fake telemetry

D. Masking

3. If end-to-end encryption is used, which of the following technologiesfacilitates security monitoring of encrypted communication channels?

A. Fake telemetry

B. Tokenization

C. Hashing

TLS inspections

4. Enterprises can employ \_\_\_\_\_\_\_\_\_\_\_ to block malicious command-and-control traffic from malware.

A. encryption

B. honeyfiles

C. DNS sinkholes

D. honeynets

5. Which of the following can provide complete traceability to an originaltransaction without revealing any personal information if disclosed to an outside party?

A. Tokenization

B. Data sovereignty

C. Rights management

D. Baseline configuration

6. A system that is ready for immediate use in the event of an outage is calledwhat?

A. Standby system

B. Disaster recovery site

C. Backup site

D. Hot site

7. Data protection includes all of the following topics except which ones?

(Choose all that apply.)

A. Honeypots

B. Masking

C. Tokenization

D. DNS sinkholes

8. Which of the following is important to consider when specificallyexamining configuration management?

A. Data loss prevention

B. Standard naming conventions

C. Rights management

Hashing

9. What is masking?

A. The use of stand-in data to replace real-time data

B. The marking of regions where data is not allowed by policy

C. The use of backups to preserve data during disruptive events

D. Redacting portions of data using a covering symbol such as \* or x

10. What is the purpose of deception in an enterprise? (Choose all that apply.)

A. To trick attackers into stealing fake data

B. To identify misconfigured systems

C. To permit easy identification of unauthorized actors

D. To provide a place to test new systems without impacting regularoperations

Answers

1. B. In storage is not a correct term used in describing the states of data. The correct states are at rest, in transit/motion, and in processing.

2. C. Fake telemetry is the name for fake network traffic in a deception-based environment.

3. D. TLS inspection systems allow TLS channels to be broken and reestablished, permitting monitoring of secure traffic.

4. C. DNS sinkholes can prevent communications on command-and-control systems associated with malware and botnets by blocking the destination address through the intentional misrouting of traffic to a dead end.

5. A. Tokenization is the use of a random value to take the place of a data element that has traceable meaning. This provides complete traceability to the original transaction, and yet if disclosed to an outside party, it reveals nothing. Data sovereignty relates to a country’s specific laws regarding the storage and transmission of personal data. Rights management is the systematic establishment of rules and order to the various rights that users can invoke over digital objects. A baseline configuration is originally created at system creation and is a representation of how the system is supposed to be configured.

6. A hot site is one that is ready for immediate use in the event of a failure.

All of the other options are names created using distractor words.

7. A and D. Honeypots and DNS sinkholes are part of deception and disruption activities, not data protection.

8. B. Standard naming conventions improve the communication of critical elements, thus enabling better configuration management activities.

9. D. Masking is the marking over of portions of information to prevent disclosure (for example, using x’s for all but the last four numbers of a credit card).

10. A, B, and C. Deception techniques such as honeynets and honeypots can trick attackers into stealing fake data and make them easier to find in the network. These techniques can also help in determining systems that are misconfigured.

Questions

To help you prepare further for the CompTIA Security+ exam, and to test your level of preparedness, answer the following questions and then check your answers against the list of correct answers at the end of the chapter.

1. How does a hypervisor enable multiple guest operating systems to runconcurrently on a host computer?

A. Via a specialized driver package

B. By abstracting the hardware from the guest operating system

C. By providing specific virtual hardware to each guest OS

D. By hiding the underlying Linux operating system

2. You have deployed a network of Internet-connected sensors across a wide geographic area. These sensors are small, low-power IoT devices, and you need to perform temperature conversions and collect the data into a database. The calculations would be best managed by which architecture?

A. Fog computing

B. Edge computing

C. Thin client

D. Decentralized database in the cloud

3. Your new application has multiple small processes that provide services tothe network. You want to make this application run more efficiently by virtualizing it. What is the best approach for virtualization of this application?

A. Type II hypervisor

B. Linux KVM

C. Containerization

D. Type I hypervisor

4. Why is VM sprawl an issue?

A. VM sprawl uses too many resources on parallel functions.

B. The more virtual machines in use, the harder it is to migrate a VM to alive server.

C. Virtual machines are so easy to create, you end up with hundreds ofsmall servers only performing a single function.

D. When servers are no longer physical, it can be difficult to locate aspecific machine.

5. When doing incident response for your company, you review the forensicsof several virtual servers and you see the attacker on the web server injecting code into uninitialized memory blocks. What attack is the attacker likely attempting?

A. Denial-of-service attack on the hypervisor

B. VM escape

C. Containerization attack

D. Crashing the CASB

6. You are planning to move some applications to the cloud, including yourorganization’s accounting application, which is highly customized and does not scale well. Which cloud deployment model is best for this application?

A. SaaS

B. PaaS

C. IaaS

D. None of the above

7. You need to move to the cloud a specific customer service module that has a web front end. This application is highly scalable and can be provided on demand. Which cloud deployment model is best for this application?

A. SaaS

B. PaaS

C. IaaS

D. None of the above

8. One of the primary resources in use at your organization is a standarddatabase that many applications tie into. Which cloud deployment model is best for this kind of application?

A. SaaS

B. PaaS

C. IaaS

D. None of the above

9. Which cloud deployment model has the fewest security controls?

A. PrivateB. Public

C. Hybrid

D. Community

10. What is the primary downside of a private cloud model?

A. Restrictive access rules

B. Cost

C. Scalability

D. Lack of vendor support

Answers

1. B. The hypervisor abstracts the hardware from the guest operating system to enable multiple guest operating systems to run concurrently on a host computer.

2. B. Edge computing on the way to the cloud would be the best fit given the lightweight processing capability of the IoT devices.

3. C. Containerization runs small applications on a host OS with virtually no overhead.

4. D. VM sprawl is an issue because when virtual machines proliferate, they can be easily moved and potentially easily copied to random locations. This can make finding a specific machine difficult without a carefully constructed and consistently managed organizational structure.

5. B. Although all hypervisors actively try to prevent it, any flaw in memory handling could allow code that is maliciously placed in a block to be read by the hypervisor or another machine. This is known as VM escape. The scenario states virtual server, eliminating answers C and D, and operational code blocks in uninitialized memory would not cause a denial of service, eliminating answer A.

6. C. Infrastructure as a Service is appropriate for highly customized, poorly scaling solutions that require specific resources to run.

7. A. Software as a Service is suitable for delivering highly scalable, ondemand applications without installing endpoint software.

8. B. Platform as a Service is suitable for standard resources in use by many other applications.

9. B. The shared environment of a public cloud has the least amount of security controls.

10. B. A private cloud model is considerably more expensive, as it is a dedicated resource, negating some of the advantages of outsourcing the infrastructure in the first place.

Questions

1. To develop secure software that prevents attackers from directly injectingattacks into computer memory and manipulating the application’s process, one should employ which method?

A. Elasticity

B. Dead code

C. Normalization

D. Software diversity

2. Problems in which phase will specifically stop continuous deployment butnot necessarily continuous delivery?

A. Continuous integration

B. Continuous monitoring

C. Continuous validation

D. Continuous development

3. Why is memory management important in software development?A. A program can grow and consume other program spaces.

B. Memory is expensive.

C. Memory can be a speed issue.

D. None of the above.

4. When a program is installed and needs permissions, what is this called?

A. Staging

B. Provisioning

C. Continuous integration

D. Version control

5. Which of the following statements concerning elasticity and scalability are true?

A. Scalability requires elasticity.

B. Elasticity involves enabling software to use more processors to domore work.

C. Elasticity means being prepared to take advantage of scalability.

D. All of the above.

6. To protect software from reverse engineering by attackers, developers canuse which of the following?

A. Dead code

B. Obfuscation

C. Binary diversity

D. Stored procedures

7. To manage various releases of software over time, the organization useswhich of the following?

A. Staging environment

B. Provisioning and deprovisioning steps

C. Version control

D. Continuous integration

8. Which of the following environments is used to test compatibility againstmultiple target environments?

A. Production

B. Test

C. Quality assurance

D. Staging

9. The fact that there are multiple methods of representing an object in acomputer system can lead to issues when logical comparisons are needed. What can be used to ensure accuracy of comparison elements?

A. Normalization

B. Stored procedures

C. Third-party libraries

D. Third-party software development kits

10. What is the only sure method of ensuring input is valid before use on aserver?

A. Use of third-party libraries and software development kits

B. Server-side validation

C. Stored procedures

D. Client-side validation

Answers

1. D. Software diversity in the form of diverse binaries will prevent direct memory attacks against known software structures.

2. C. Continuous validation is required to ensure error-free software, and errors will stop continuous deployment.

3. A. Memory management failures can lead to a program growing in size when executing. This can result in either its own failure or the diminishing of memory resources for other programs.

4. B. Provisioning is the assignment of permissions or authorities to objects.

5. D. All of the above is the correct answer. Scalability requires elasticity to scale, elasticity involves enabling software to use more processors to do more work, and elasticity means developing software that is prepared to take advantage of scalability.

6. B. Obfuscation is the technique of hiding properties to prevent examination. Making code hard to decompile and not storing any specific clues in the source code can make reverse engineering a challenge.

7. C. Version control comprises the processes and procedures employed to manage different releases of software over time.

8. D. The staging environment can be used to manage software releases against different targets to ensure compatibility.

9. A. Normalization is the process of reducing items to a canonical form before comparisons to ensure appropriate logical matching.

B. Server-side validation is the only sure validation method for inputs to the application.

Questions

To help you prepare further for the CompTIA Security+ exam, and to test your level of preparedness, answer the following questions and then check your answers against the correct answers at the end of the chapter.

1. During a visit to a hosting center where your organization keeps someoffsite servers, you see a door with an odd-looking panel next to it. You see people approaching the panel and placing their eyes into a hooded viewer. A few seconds after they’ve done this, the door unlocks. What type of biometric scanner might this be?

A. Voice recognition scanner

B. Retinal scanner

C. Fingerprint scanner

D. Facial recognition scanner

2. You’ve spent the last week tweaking a fingerprint-scanning solution foryour organization. Despite your best efforts, roughly 1 in 50 attempts will fail, even if the user is using the correct finger and their fingerprint is in the system. Your supervisor says 1 in 50 is “good enough” and tells you to move on to the next project. Your supervisor just defined which of the following for your fingerprint scanning system?

A. False rejection rate

B. False acceptance rate

C. Critical threshold

D. Failure acceptance criteria

3. Which of the following algorithms uses a secret key with a currenttimestamp to generate a one-time password?

A. Hash-based Message Authentication Code

B. Date-Hashed Message Authorization Password

C. Time-based One-Time Password

D. Single sign-on

4. With regard to authentication, an access token falls into which factorcategory?

A. Something you are

B. Something you have

C. Something you know

D. Something you see

5. Which of the following is not a common form of hardware token?

A. Proximity card

B. Common access card

C. USB token

D. Iris scan

6. While depositing cash from a charity fundraiser at a local bank, you noticebank employees are holding up cards next to a panel near a door. A light on the panel turns green and the employees are able to open the door. The light on the panel is normally red. What type of electronic door control is this bank using?

A. Iris scanner

B. Hardware token

C. Proximity card

D. Symmetric key token

7. Your colleague is telling you a story she heard about a way to trick fingerprint scanners using gummy bears. She heard that if you press a gummy bear against an authorized user’s finger, you can then use that gummy bear as their fingerprint to fool a fingerprint scanner. If this works, the result is an example of which of the following?

A. False negative

B. False positive

C. Crossover positive

D. Crossover negative

8. To ensure customers entering credentials in your website are valid and notsomeone with stolen credentials, your team is tasked with designing multifactor authentication. Which of the following would not be a good choice?

A. Static code

B. Phone call

C. Authentication application

D. Short Message Service

9. When you’re designing and tweaking biometric systems, the point whereboth the accept and reject error rates are equal is known as which of the following?

A. Crossover acceptance rate

B. Accept-reject overlap rate

C. Crossover error rate

D. Overlap acceptance rate

10. Which of the following is not a term used in multifactor authentication?

A. Someone you know

B. Somewhere you are

C. Something you have

D. Something you see

Answers

1. B. This is most likely a retinal scanner. Retinal scanners examine blood vessel patterns in the back of the eye. Retinal scanning must be done at short distances; the user has to be right at the device for it to work.

2. A. Your supervisor just defined the false rejection rate (FRR) for your system. The FRR is the level of false negatives, or rejections, that are going to be allowed in the system. In this case, your supervisor is willing to accept one false rejection for every 50 attempts.

3. C. The Time-based One-Time Password (TOTP) algorithm is a specific implementation of an HOTP that uses a secret key with a current timestamp to generate a one-time password. Note that timestamp is the key clue in the question.

4. B. An access token is a physical object that identifies specific access rights, and in authentication it falls into the “something you have” factor category.

5. D. An iris scan would be considered a biometric technique and is not a hardware token. A hardware token is a physical item the user must be in possession of to access their account or certain resources.

6. C. The bank employees are using proximity cards, which are contactless access cards that provide information to the electronic door control system. Proximity cards just need to be close enough to the scanner to work—they do not need to actually touch the scanner.

7. B. This is an example of a false positive. A false positive occurs when a biometric is scanned and allows access to someone who is not authorized.

8. A. Static codes can be captured and replayed and are not well suited for systems with active users.

9. C. The crossover error rate (CER) is the rate where both accept and reject error rates are equal. This is the desired state for the most efficient operation of a biometric system, and it can be managed by manipulating the threshold value used for matching.

10. D. Something you see is neither a factor (something you know, something you have, or something you are) nor an attribute (somewhere you are, something you can do, something you exhibit, or someone you know).

Questions

To help you prepare further for the exam, and to test your level of preparedness, answer the following questions and then check your answers against the correct answers at the end of the chapter.

1. Which backup strategy includes only the files and software that havechanged since the last full backup?

A. Incremental

B. Full

C. Snapshot

D. Differential

2. Which backup strategy focuses on copies of virtual machines?

A. Incremental

B. Full

C. Snapshot

D. Differential

3. When discussing location for storage of backups, which of the followingstatements are true? (Choose all that apply.)

A. The most recent copy should be stored offsite, as it is the one that ismost current and is thus the most valuable.

B. Offsite storage is generally not necessary, except in cases where thepossibility of a break-in at the main facility is high.

C. Offsite storage is a good idea so that you don’t lose your backup to thesame event that caused you to lose your operational data and thus need the backup.

D. The most recent copy can be stored locally, as it is the most likely to beneeded, while other copies can be kept at other locations.

4. To deal with nonpersistence in a system, which of the following items offer risk mitigation? (Choose all that apply.)

A. Image backups

B. Cloud

C. Last known-good configuration

D. Revert to a known state

5. To have easily available quick backup of critical user documents, which ofthe following is recommended for backing these items up?

A. Differential

B. Snapshot

C. Copy

D. NAS

6. You have offices in six locations across town and wish to utilize a commonbackup restore methodology. Which would be the most efficient solution for your small offices?

A. SAN

B. NAS

C. Cloud

D. Offline

7. Which of the following statements is true about redundancy?A. It prevents failures.

B. It is complicated and expensive to do.

C. It applies only to hardware.

D. It can be done across many systems.

8. What distinguishes high availability systems?

A. The ability to change with respect to usage conditions

B. The ability to process, even in times of disruption

C. Automated backups and recovery functions

D. The use of diversity to mitigate single threats

9. The continual changing of information in a system is referred to as what?

A. Nonpersistence

B. Snapshots

C. Differentials

D. Images

10. A PDU provides management of what in an enterprise?

A. Redundant backup processing

B. Power distribution to servers

C. Improved network connection to data storage

D. Load balancing

Answers

1. D. In a differential backup, only the files and software that have changed since the last full backup was completed are backed up. The incremental backup is a variation on a differential backup, with the difference being that instead of copying all files that have changed since the last full backup, the incremental backup backs up only files that have changed since the last full or incremental backup occurred, thus requiring fewer files to be backed up.

In a full backup, all files and software are copied onto the storage media. Snapshots refer to copies of virtual machines.

2. C. Snapshots refer to copies of virtual machines. The incremental backup is a variation on a differential backup, with the difference being that instead of copying all files that have changed since the last full backup, the incremental backup backs up only files that have changed since the last full or incremental backup occurred, thus requiring fewer files to be backed up. In a full backup, all files and software are copied onto the storage media. In a differential backup, only the files and software that have changed since the last full backup was completed are backed up.

3. C and D. Offsite storage is a good idea so that you don’t lose your backup

to the same event that caused you to lose your operational data and thus need the backup. Additionally, the most recent copy can be stored locally, as it is the most likely to be needed, while other copies can be kept at other locations.

4. A, C, and D. Image backups capture the nonpersistence of the OS. Also, reverting to a known state and using the last known-good configuration both can resolve nonpersistence issues. Cloud (answer B) is not a direct answer, as by itself, the cloud does not offer persistence to a nonpersistent system. An image backup has everything, so restoring from it can resolve a persistence problem. For the cloud to be involved, it would be as a secondary item (that is, a place to store an image backup), but then it is not actually directly involved.

5. C. User-managed copies on external media of critical documents can make it very easy for the end user to manage recovery in a quick manner.

6. C. Cloud backup solutions can be ideal for small offices, and with the different offices, centralized administration can be added.

7. D. A wide range of options are associated with creating redundant systems —some as simple as configuration elements and system choices.

8. B. High availability systems continue to process data even when disrupting events occur.

9. A. Nonpersistence refers to system items such as memory and registry elements that are not permanent and can change over time, even while running.

10. B. Power distribution units provide a centralized means of managing and monitoring the power delivered to servers in a rack.

Questions

To help you prepare further for the exam, and to test your level of preparedness, answer the following questions and then check your answers against the correct answers at the end of the chapter.

1. Which of the following statements is not true?

A. Embedded systems are designed with a single control purpose in mindand typically have no additional functionality.

B. Embedded systems are free of risk and security concerns.

C. Embedded is the name given to a computer that is included as an integral part of a larger system.

D. Embedded systems can be as complex as the dozens of interconnectedembedded systems in a modern automobile.

2. Which of the following statements is true regarding the risk of next-generation vehicles?

A. There are minimal risks when next-generation automobiles shareinformation.

B. Passing traffic and other information between vehicles does notincrease security risks.

C. The sharing of navigation and other inputs between vehicles presents apotential security issue.

D. Time-to-market and cost minimization have minimal impact onpotential risks being exploited.

3. Which of the following properly defines supervisory control and dataacquisition (SCADA)?

A. A scaled-down version of Linux designed for use in an embeddedsystem

B. The standard used for communicating between intelligent car systems

C. The risk created by connecting control systems in buildings

D. A system designed to control automated systems in cyber-physicalenvironments

4. Which of the following statements is true about smart devices and the Internet of Things (IoT)?

A. The use of a Linux-type kernel as the core engine makes programmingmore complex.

B. Mass production introduces significant security risks.

C. The scaling of the software development over large numbers of unitsmakes costs scalable, and functionality is paramount.

D. Security or anything that might impact new expanded functionality isconsidered early and gets the focus and resources necessary.

5. Which of the following statements is true about HVAC and buildingautomation systems?

A. They have not been exploited to any significant degree yet.

B. Interconnecting these systems and using Internet-based central controlmechanisms increases the risk profile from outside attacks.

C. Having a “smart building” that reduces the use of building resources inaccordance with the number and distribution of people inside has not increased efficiency or reduced costs.

D. The rise of hyper-connectivity has introduced no additional securityconcerns.

6. Which of the following statements is not true about system on a chip?

A. It provides the full functionality of a computing platform on a singlechip.

B. It typically has low power consumption and efficient design.

C. Programming of SoC systems can occur at several different levels, andthus potential risks are easily mitigated.

D. Because SoC represents computing platforms with billions of devicesworldwide, it has become a significant force in the marketplace.

7. What distinguishes real-time operating systems (RTOSs) from general-purpose operating systems?

A. Unlike RTOSs, most general-purpose operating systems handleinterrupts within defined time constraints.

B. Unlike general-purpose OSs, most RTOSs are capable of multitaskingby design.

C. Unlike RTOSs, most general-purpose operating systems aremultitasking by design.

D. Unlike general-purpose OSs, RTOSs are designed to handle multiplethreads.

8. Which of the following statements is true about printers and multifunction devices?

A. They rely on the computer to manage the printing and scanningprocesses.

B. Because of their long history and widespread use, security is designedinto these products.

C. These devices communicate in a bidirectional fashion, accepting printjobs and sending back job status, printer status, and so forth.

D. So far, they have not been shown to be hackable or capable of passingmalware to the computer.

9. Which of the following is a very important aspect to always rememberwhen dealing with security of medical devices? A. They are still relatively new in their usage.

B. They can directly affect human life.

C. Security is not related to safety.

D. They are almost exclusively stand-alone devices, without Internetconnectivity.

10. Which of the following poses a significant potential risk of unmanned aerialvehicles?

A. They have sophisticated autopilot functions.

B. They have cameras, sensors, and payloads.

C. Some models have a low price.

D. Because they are pilotless, their remote-control systems may benetworked and therefore vulnerable to potential risks.

Answers

1. B. Embedded systems are not free of risk or security concerns, as hackers have demonstrated.

2. C. The sharing of navigation and other inputs presents a potential security issue for next-generation vehicles. False information, when shared, can cause problems.

3. D. SCADA is a system designed to control automated systems in cyberphysical environments.

4. C. The scaling of the software development over large numbers of units makes costs scalable, and functionality is paramount in smart devices and IoT.

5. B. Interconnecting HVAC and building automation systems and using Internet-based central control mechanisms to manage them increases the risk profile from outside attacks.

6. C. Programming of SoC systems can occur at several different levels, and thus potential risks are difficult to mitigate.

7. C. One thing that distinguishes real-time operating systems (RTOSs) from general-purpose operating systems is that most general-purpose operating systems are designed for multitasking.

8. C. Printers and multifunction devices communicate in a bidirectional fashion, accepting print jobs and sending back job status, printer status, and so forth.

9. B. A very important aspect to always remember when dealing with security of medical devices is that they can directly affect human life.

10. D. A significant potential risk of unmanned aerial vehicles is that, because they are pilotless, their remote-control systems may be networked and therefore vulnerable to potential risks.

Questions

To help you prepare further for the CompTIA Security+ exam, and to test your level of preparedness, answer the following questions and then check your answers against the correct answers at the end of the chapter.

1. Why is physical security important to protecting data?

A. Physical access to data will negate the security advantages of thecloud.

B. Information resides on physical assets, linking physical andinformation security.

C. Social engineering can negate any information security controls.

D. None of the above.

2. Why is proper interior and exterior lighting important?

A. It can detect people who are where they don’t belong.

B. It shows who is in a restricted space.

C. It allows more people and activities to be observed.

D. It is needed for the use of closed-circuit television cameras.

3. Your organization has experienced multiple incidents of graffiti tagging andpeople loitering in the parking lot despite the chain-link fence surrounding it. What is the best solution to the issue?

A. “No Trespassing” signage

B. More guard stations

C. Additional external lighting

D. Changing the chain-link fencing to anti-scale fencing

4. After a physical security incident, what critical data can security guardscommonly provide?

A. Employee ID information

B. Access logs of who has entered and exited the building

C. Alarm codes

D. Blueprints showing unmonitored areas of the building

5. Alarms are effective only if which of the following is true? A. They alert on abnormal conditions.

B. Every entrance is monitored with a sensor.

C. They are not tied to the information systems.

D. They are tuned to provide accurate and useful alerts.

6. You are implementing a test lab at your organization for early alphasoftware development. To prevent any of the development code from inadvertently getting put on production computers, what should you implement?

A. Air gap

B. Strict firewalls

C. Protected distribution

D. Patch management

7. What is the security benefit of a Faraday cage?

A. Prevents attack by EMP

B. Prevents accessing a device using a wireless network or cell connection

C. Works better than anti-scale fencing

D. Prevents stack overflows by EMI

8. What is an example of a human-based screened subnet (DMZ)?

A. A visitor’s lobby that is separated from a company office by areceptionist

B. Hallways between the company lobby and offices

C. A server room with a locked door

D. The networking cabinets in the facility

9. What is a primary problem with biometrics?

A. Technically, biometrics are difficult to implement.

B. The human body changes over time.

C. Biometrics are easily faked.

D. Biometrics can’t be loaned or delegated.

10. What should you do to protect your IP-based CCTV system from a DDoSattack?

A. Reconfigure your firewalls.

B. Connect it to an intrusion detection system.

C. Require multifactor authentication to access the CCTV system.

D. Place all CCTV components on a separate network.

Answers

1. B. Information resides on physical assets, linking physical security with the security of information.

2. C. Proper lighting allows more people and activities to be observed.

3. D. A change from chain-link fencing to anti-scale fencing to prevent intruders from climbing the fence is the best solution.

4. B. Guards commonly have logs of who has entered and exited a building.

5. D. Alarms are effective only if they are tuned to provide accurate and useful alerting information.

6. A. A lab environment can be air gapped from the rest of the network to prevent software from being accidentally copied to production machines.

7. B. A Faraday cage can prevent accessing a device via radio frequency waves, either from a wireless network or cell radio.

8. B. The lobby is part of the outside environment, so the hallways are the

better choice. Server rooms and networking rooms are the more secured spaces.

9. B. Some biometric features can change over time, or medical conditions can make them less reliable, thus forcing a re-identification phase to resync a user and their biometric.

10. D. The CCTV system should be on a completely separate network, air gapped if possible, with only security personnel having access.

Questions

To help you prepare further for the CompTIA Security+ exam, and to test your level of preparedness, answer the following questions and then check your answers against the correct answers at the end of the chapter.

1. If you need to perform operations such as addition on encrypted elements,what type of encryption scheme would you use?

A. Asymmetric

B. Homomorphic

C. Stream

D. Lightweight

2. Which of the following is not a limitation associated with cryptographic solutions?

A. Speed

B. Computational overhead

C. Longevity

D. Entropy

3. What set of algorithms is designed for low-power devices such as theInternet of Things and embedded systems?

A. Lightweight

B. Hashing

C. Stream

D. Blockchain

4. How do you make a short secret, such as a password, become long enoughfor use?

A. Salting

B. Key elongation

C. Key stretching

D. Ephemeral operations

5. What is the best way to get the plaintext from a hash value?A. Use linear cryptanalysis.

B. Use a reverse hash function.

C. You cannot get the plaintext out of a hash value.

D. Use an ephemeral key.

6. What does a salt provide?

A. It tells the algorithm how many digits of primes to use.

B. It primes the algorithm by giving it initial noncritical data.

C. It adds additional rounds to the cipher.

D. It provides additional entropy.

7. What makes a digitally signed message different from an encryptedmessage?

A. The digitally signed message has encryption protections for integrityand nonrepudiation.

B. The digitally signed message uses much stronger encryption and isharder to break.

C. The encrypted message only uses symmetric encryption.

D. There is no difference.

8. Steganography is commonly accomplished using which method?

A. Encryption

B. Initialization vectors (IVs)

C. LSB encoding

D. Entropy substitution

9. To prevent the loss of a single message due to accidental decryption fromaffecting other encrypted messages, which of the following properties is needed?

A. Stream encryption

B. Perfect forward secrecy

C. Entropy

D. Obfuscation

10. Given a large quantity of data in the form of a streaming video file, what isthe best type of encryption method to protect the content from unauthorized live viewing?

A. Symmetric block

B. Hashing algorithmC. Stream cipher

D. Asymmetric block

Answers

1. B. Homomorphic schemes allow computations on encrypted elements.

2. D. Entropy is a measure of randomness, not a limitation of a cryptographic solution.

3. A. Lightweight encryption algorithms are designed for resource-constrained systems.

4. C. Key stretching is a mechanism that takes what would be weak keys and “stretches” them to make the system more secure.

5. C. Hash ciphers are designed to reduce the plaintext to a small value and are built to not allow extraction of the plaintext. This is why they are commonly called “one-way” functions.

6. D. The salt adds additional entropy, or randomness, to the encryption key, specifically providing separation between equal inputs such as identical passwords on different accounts.

7. A. The digital signature includes a hash of the message to supply message integrity and uses asymmetric encryption to demonstrate nonrepudiation (the fact that the sender’s private key was used to sign the message).

8. C. LSB, or least significant bit, is designed to place the encoding into the image in the least significant way to avoid altering the image.

9. B. Perfect forward secrecy (PFS) is a property of a public key system in which a key derived from another key is not compromised even if the originating key is compromised in the future.

10. C. Stream ciphers work best when the data is in very small chunks to be processed rapidly, such as live streaming video. Block ciphers are better when it comes to large chunks of data.

Questions

To help you prepare further for the CompTIA Security+ exam, and to test your level of preparedness, answer the following questions and then check your answers against the correct answers at the end of the chapter.

1. A user reports to the help desk that he is getting “cannot resolve address”error messages from his browser. Which port is likely a problem on his firewall?

A. 22

B. 53

C. 161

D. 162

2. What is a weakness of the DNS protocol?

A. Requests and replies are sent in plaintext.

B. It doesn’t provide billing standardization in cloud infrastructures.

C. TCP can be used for large transfers such as zone transfers.

D. Its encryption capabilities are slow.

3. Which of the following is a benefit of DNSSEC?

A. Scalability

B. Lower expenditures from operations capital (OpsCap) expenditures

C. Enables origin authentication, authenticated denial of existence, and

data integrity

D. Availability and confidentiality

4. What is the Secure Shell (SSH) protocol?

A. It is an encrypted remote terminal connection program used for remoteconnections to a server.

B. It provides dynamic network address translation.

C. It provides Software as a Service (SaaS).

D. It provides snapshots of physical machines at a point in time.

5. What is the purpose of the Secure/Multipurpose Internet Mail Extensions(S/MIME) protocol?

A. It is used in audio encryption.

B. It optimizes the use of ports 80 and 443.

C. It encrypts HTTP traffic.

D. It provides cryptographic protections to e-mails.

6. What is the purpose of Lightweight Directory Access Protocol Secure(LDAPS)?

A. It leverages encryption protections of SSH to secure FTP transfers.

B. It uses an SSL/TLS tunnel to connect LDAP services.

C. It digitally signs DNS records.

D. It provides both symmetric and asymmetric encryption.

7. Which port does FTPS use?

A. 53

B. 83

C. 990

D. 991

8. You are a security admin for XYZ company. You suspect that company e-mails using the default POP and IMAP e-mail protocols and ports are getting intercepted while in transit. Which of the following ports should you consider using?

A. Ports 995 and 993

B. Ports 53 and 22

C. Ports 110 and 143

D. Ports 161 and 16240

9. What is the purpose of the Simple Network Management Protocol version 3(SNMPv3)?

A. It provides asymmetric encryption values.

B. It achieves specific communication goals.

C. It provides a common language for developers.

D. It is used to securely manage devices on IP-based networks.

10. What is the purpose of HTTPS?

A. To allow enumeration and monitoring of network resources

B. To use SSL or TLS to encrypt a channel over which HTTP traffic istransmitted

C. To implement Single Sign-On

D. To enhance communication protocols

Answers

1. B. Domain Name System (DNS) uses TCP and UDP port 53 for standard queries and responses. This port should be open on the firewall in this scenario. Secure Shell (SSH) uses TCP port 22 as its default port. All versions of SNMP require ports 161 and 162 to be open on a firewall.

2. A. A major weakness of the DNS protocol is that requests and replies are sent in plaintext.

3. C. A major benefit of DNSSEC is that it enables origin authentication, authenticated denial of existence, and data integrity.

4. A. The SSH protocol is an encrypted remote terminal connection program used for remote connections to a server.

5. D. The purpose of the S/MIME protocol is to provide cryptographic protections to e-mail and attachments.

6. B. LDAPS uses an SSL/TLS tunnel to connect LDAP services.

7. C. FTPS uses port 990.

8. A. The default POP3 and IMAP4 ports are 110 and 143, respectively. These are not secure. As a security admin, you should consider using secure POP using port 995 and secure IMAP using port 993.

9. D. The purpose of SNMPv3 is to securely manage devices on IP-based networks.

10. B. HTTPS uses SSL or TLS to encrypt a channel over which HTTP traffic is transmitted.

Questions

To help you prepare further for the CompTIA Security+ exam, and to test your level of preparedness, answer the following questions and then check your answers against the correct answers at the end of the chapter.

1. Fuzz testing works best in which of the following testing environments?

A. Known environment testing

B. Partially known environment testing

C. Unknown environment testing

D. Fuzz testing works equally well in all of the above.

2. Which code analysis method is performed while the software is executed,either on a target system or an emulated system?

A. Static analysis

B. Runtime analysis

C. Sandbox analysis

D. Dynamic analysis

3. Which of the following are associated with endpoint protection? (Chooseall that apply.)

A. EDR

B. TPM

C. DLP

D. HTTP headers

4. You have a series of web servers that you wish to harden. Which of thefollowing is the best solution for this case?

A. A block list/deny list

B. An allow list

C. Secure cookies

D. Code signing

5. You are examining the server infrastructure and wish to harden the machines in your server farm. Which is the first task you should perform across all of your servers?

A. Apply a block list/deny list.

B. Apply an allow list.

C. Block open ports and disable unused services.

D. Employ disk encryption.

6. Databases can use which of the following for security? (Choose all thatapply.)

A. Tokenization

B. Salting

C. Code signing

D. Secure cookies

7. When you’re creating a website, which of the following will provideprotection against user attacks against your site? (Choose all that apply.)

A. Tokenization

B. HTTP headers

C. Code signing

D. Fuzzing

8. Your firm has 200 desktops in three sites, split among a dozen businessdepartments. Which of the following would be the first that you should ensure is working correctly to reduce risk?

A. Application security

B. Secure Boot

C. Patch management

D. Secure cookies

9. You have a database full of very sensitive data. Salespeople need to accesssome of this sensitive data when onsite with a customer. The best method to prevent leakage of critical data during these access sessions would be to employ which of the following?

A. Salting

B. Hashing

C. Block list

D. Tokenization

10. Which of the following elements is not part of the Root of Trust?

A. Registry

B. UEFI

C. TPM PCR

D. Digital signatures

Answers

1. D. Fuzz testing works well in known environment, unknown environment, and partially known environment testing, as it can be performed without knowledge of the specifics of the application under test.

2. D. Dynamic analysis is performed while the software is executed, either on a target system or an emulated system. Static analysis is when the code is examined without being executed. Sandboxing refers to the execution of computer code in an environment designed to isolate the code from direct contact with the target system. Runtime analysis is descriptive of the type of analysis but is not the term used in the industry.

3. A and C. Endpoint detection and response (EDR) is the combination of several individual endpoint protection mechanisms into a common management framework. Data loss prevention (DLP) is the checking for sensitive data before exfiltration. Both of these are associated with endpoint security. The Trusted Platform Module (TPM), while involved in many security technologies, does not play a direct role in endpoint protection. Nor do HTTP headers, which are associated with the server serving up the web content.

4. B. Allow lists are ideally suited for single-purpose servers, as the applications that are to be allowed to execute are known in advance.

5. C. Because the server farm may have multiple different types of systems, elements such as allow lists become more complicated, as the results do not scale across different server types. All machines benefit from blocking of unused ports and disabling of unused services.

6. A and B. Databases can use tokens to represent unique sensitive data, allowing joins between tables and records without exposing the data. Salting can be used to ensure that hashed values of identical input fields will not reveal the fact that two records share the same data.

7. B and D. HTTP headers prevent browsers from performing some activities that are allowed (by protocol) but not advised by site rules. Fuzzing will provide input as to input validation errors.

8. C. Patch management reduces the attack surface on the operating systems and application components. Automating this process is an important early step in the security journey because of the number of items it addresses.

9. D. The use of tokens to join records while hiding sensitive fields is common practice for views on database tables.

10. A. The Windows Registry is where configuration parameters for the OS and applications are stored. It is not associated with the Root of Trust, as it is not even accessible during the establishment of this trust chain.

Questions

To help you prepare further for the CompTIA Security+ exam, and to test your level of preparedness, answer the following questions and then check your answers against the correct answers at the end of the chapter.

1. A network-based intrusion prevention system (NIPS) relies on what othertechnology at its core?

A. VPN

B. IDS

C. NAT

D. ACL

2. You have been asked to prepare a report on network-based intrusiondetection systems that compares the NIDS solutions from two potential vendors your company is considering. One solution is signature based and one is behavior based. Which of the following lists what your report will identify as the key advantage of each?

A. Behavioral: low false-negative rate; Signature: ability to detect zero-day attacks

B. Behavioral: ability to detect zero-day attacks; Signature: low false-positive rates

C. Behavioral: high false-positive rate; Signature: high speed of detection

D. Behavioral: low false-positive rate; Signature: high false-positive rate

3. How can proxy servers improve security?

A. They use TLS-based encryption to access all sites.

B. They can control which sites and content employees access, lesseningthe chance of malware exposure.

C. They enforce appropriate use of company resources.

D. They prevent access to phishing sites.

4. What technology can check the client’s health before allowing access to thenetwork?

A. DLP

B. Reverse proxy

C. NIDS/NIPS

D. NAC

5. What kind of device provides tamper protection for encryption keys?

A. HSM

B. IPSec

C. Jump server

D. HTML5

6. What is the purpose of the DNS protocol?

A. It provides a function for charging SaaS on a per-use basis.

B. It supports the networking infrastructure.

C. It translates names into IP addresses.

D. It defines tenants in a public cloud.

7. A user reports to the help desk that he is getting “cannot resolve address”error messages from his browser. Which port is likely a problem on his firewall?

A. 22

B. 553

C. 440

D. 53

8. What is the primary purpose of a screened subnet?

A. To prevent direct access to secure servers from the Internet

B. To provide a place for corporate servers to reside so they can access theInternet

C. To create a safe computing environment next to the Internet

D. To slow down traffic coming and going to the network

9. What is the best tool to ensure network traffic priorities for videoconferencing are maintained?

A. QoS

B. VLAN

C. Network segmentation

D. Next-generation firewall

10. If you wish to monitor 100 percent of the transmissions from your customerservice representatives to the Internet and other internal services, which is the best tool to use?

A. SPAN port

B. TAP

C. Mirror port

D. Aggregator switches

Answers

1. B. A NIPS relies on the technology of an intrusion detection system (IDS) at its core to detect potential attacks.

2. B. The key advantage of a behavior-based NIDS is its ability to detect zeroday attacks, whereas the key advantage of a signature-based NIDS is low false-positive rates.

3. B. Proxy servers can improve security by limiting the sites and content accessed by employees, thus limiting the potential access to malware.

4. D. NAC, or network access control, is a technology that can enforce the security health of a client machine before allowing it access to the network.

5. A. A hardware security module (HSM) has tamper protections to prevent the encryption keys it manages from being altered.

6. C. The Domain Name System (DNS) translates names into IP addresses.

7. D. The Domain Name System (DNS) uses TCP and UDP port 53 for standard queries and responses.

8. A. The primary purpose of a screened subnet is to provide separation between the untrusted zone of the Internet and the trusted zone of enterprise systems. It does so by preventing direct access to secure servers from the Internet.

9. A. Quality of Service (QoS) solutions can manage traffic flows by type to provide guaranteed access and priority for specific traffic flows.

10. B. A test access point (TAP) is required to monitor 100 percent of the transmissions from your customer service representatives to the Internet and other internal services.

Questions

To help you prepare further for the CompTIA Security+ exam, and to test your level of preparedness, answer the following questions and then check your answers against the correct answers at the end of the chapter.

1. The use of an eight-digit PIN to set up a wireless connection is part ofwhich of the following?

A. WPA

B. SAE

C. WPA3

D. WPS

2. What is the role of EAP in wireless connections?

A. It is a framework for establishing connectivity.

B. It is a framework for passing authentication information.

C. It is a framework to secure the authentication process.

D. It is an actual encryption method used during authentication.

3. What is the primary difference between WPA2-Personal and WPA2-Enterprise?

A. The use of a pre-shared secret

B. The number of concurrent supported users

C. Licensing costs on a per-user basis

D. The use of SAE for connections

4. You are setting up a Wi-Fi hotspot for guest visitors. What is the best method of establishing connections?

A. Open access

B. A posted password visually available on site

C. Use of a PSK solution

D. Captive portal

5. What is the most secure means of establishing connectivity to a Wi-Fiaccess point?

A. CCMP

B. SAE protocolC. WPA2

D. IEEE 802.1X

6. A site survey will reveal all of the following except which one?

A. Optimal access point placement

B. Captive portal location

C. Channel allocations

D. Link speeds across the site

7. Forward secrecy exists for which of the following protocols?

A. WPS

B. WPA2

C. WPA3

D. All of the above

8. Your boss has asked you to set up wireless connectivity at a new companylocation. However, she is concerned about planning, coverage, and security regarding AP placement. She wants you to ensure coverage and address security concerns. Which of the following should you consider using while setting up this new location? (Select three.)

A. RADIUS federation

B. Site survey

C. Wi-Fi analyzer

D. Heat map

9. You are using EAP-TTLS, which includes what unique aspect?A. It cannot be used in WPA3.

B. It requires client-side certificates.

C. It cannot be used with CHAP.

D. It is easier to set up than other EAP schemes.

10. Which protocol allows the passing of legacy authentication protocols such as PAP, CHAP, and MS-CHAP?

A. EAP-TTLS

B. EAP-TLS

B. SAE

B. CCMP

Answers

1. D. Wi-Fi Protected Setup (WPS) uses an eight-digit PIN to establish a connection between devices.

2. C. EAP is only a framework to secure the authentication process, not an actual encryption method.

3. A. WPA2-Personal uses a PSK, whereas WPA2-Enterprise does not.

4. D. A captive portal is a method of having users log on to your system. These are common in coffee shops, airports, hotels, and stores.

5. B. The use of SAE, part of WPA3, is currently the most secure way to establish a connection via wireless.

6. B. Captive portals are software-driven locations a user is pointed to, not part of the physical Wi-Fi configuration.

7. C. Forward secrecy is only available via WPA3. This is because the method of establishing the connection is not observable.

8. B, C, and D. Professional site surveys, Wi-Fi analyzers, and heat maps for wireless network installations and proper access point (AP) placement are used to ensure coverage area and security concerns. Answers A is incorrect because RADIUS federation allows users to use their normal credentials across trusted networks.

9. D. EAP-TTLS is easier to set up than other EAP networks because of its ability to operate without client-side certificates.

10. A. The EAP-TTLS protocol tunnels the client side of the authentication, allowing the use of legacy authentication protocols such as Password Authentication Protocol (PAP), Challenge-Handshake Authentication Protocol (CHAP), MS-CHAP, and MS-CHAP-V2.

Questions

1. Which of the following is a weakness of cellular technology?

A. Multiple vendors in a nationwide network

B. Less availability in rural areas

C. Multiple cell towers in close proximity in urban areas

D. Strong signals in areas of reasonable population

2. What frequency spectrum does Bluetooth use?

A. 1.7 GHz

B. 2.4 GHz

C. 5 GHz

D. 6.4 GHz

3. You need to use cryptographic keys between several devices. Which of thefollowing can manage this task?

A. MAM solutions

B. Firmware OTA updates

C. USB OTG

D. MicroSD HSM

4. Which of the following are the three modes supported by Bluetooth 4.0?

A. Classic, Low Speed, High Energy

B. Enhanced Data Rate, Backward Compatible, High Energy

C. Classic, High Speed, Low Energy

D. Synchronous, High Speed, Low Energy

5. What is the primary use of near field communication (NFC)?A. Establishing radio communications over a short proximity

B. Communication in sparsely populated areas

C. Long-distance connectivity

D. Communication in noisy industrial environments

6. You need to manage a whole host of different endpoints in the enterprise,including mobile devices, iPads, printers, PCs and phones. Which of the following is the most comprehensive solution?

A. COPE-based solutions

B. MAM solutions

C. MDM solutions

D. UEM solutions

7. What is a disadvantage of infrared (IR) technology?A. It has a high data rate.

B. It cannot penetrate solid objects.

C. It can penetrate walls.

D. It uses a slow encryption technology.

8. What is the main security concern with Universal Serial Bus (USB) technology?

A. It connects to cell phones for easy charging.

B. It uses proprietary encryption.

C. It automounts and acts like a hard drive attached to the computer.

D. It uses older encryption technology.

9. Why is it important to establish policies governing remote wiping of mobiledevices?

A. Mobile devices typically do not mix personal and business data.

B. Mobile devices are more easily secured.

C. Thieves cannot decrypt mobile devices.

D. They are more susceptible to loss than other devices.

10. What is the purpose of geofencing?

A. It can be used to remotely wipe a lost device.

B. It makes securing the mobile device simpler.

C. It enables devices to be recognized by location and have actions taken.

D. It can enforce device locking with a strong password.

Answers

1. B. A weakness of cellular technology is that it is less available in rural areas.

2. B. Bluetooth uses the 2.4-GHz frequency spectrum.

3. D. MicroSD HSM facilitates HSM functionality via a MicroSD connection. It can be connected via an adapter to any USB device.

4. C. The three modes supported by Bluetooth 4.0 are Classic, High Speed, and Low Energy.

5. A. The primary use of NFC is to establish radio communications over a short proximity.

6. D. UEM (unified endpoint management) solutions can address a wider range of devices in a more comprehensive manner than MDM and MAM solutions.

7. B. A disadvantage of IR technology is that it cannot penetrate solid objects.

8. C. The main security concern with USB technology is that it automounts

and acts like a hard drive attached to the computer.

9. D. It is important to establish policies governing the remote wiping of mobile devices because they are more susceptible to loss than other devices.

10. C. The purpose of geofencing is to enable devices to be recognized by location and have actions taken.

Questions

1. The policies and procedures employed to connect the IAM systems of theenterprise and the cloud to enable communication with the data are referred to as what?

A. API inspection and integration

B. Secrets management

C. Dynamic resource allocation

D. Container security

2. Which of the following terms is not related to storage security in the cloud?

A. Permissions

B. High availability

C. Segmentation

D. Encryption

3. Resource policies involve all of the following except?

A. Permissions

B. IAM

C. Cost

D. Access

4. Virtual networking in a cloud environment can include all of the followingexcept?

A. VPC endpoint

B. Public subnets

C. Private subnets

D. Network function virtualization

5. What structure is used to manage users in cloud environments?

A. Permissions

B. Incident awareness

C. Dynamic resource allocations

D. Security groups

6. Which of the following is a security policy enforcement point placedbetween cloud service consumers and cloud service providers to manage enterprise security policies as cloud-based resources are accessed?

A. SWG

B. VPC endpoint

C. CASB

D. Resource policies

7. Secure web gateways operate by inspecting at what point in the communication channel?

A. Security group membership

B. Application layer

C. Instance awareness

D. API inspection

8. Which of the following are critical in cloud security? (Choose all thatapply.)

A. Firewalls

B. Integration and auditing

C. Secrets management

D. Encryption

9. High availability is dependent on which of the following?

A. Secrets management

B. Dynamic resource allocation

C. Container security

D. CASB

10. Which is the most critical element in understanding your current cloudsecurity posture?

A. Cloud service agreement

B. Networking security controls

C. Encryption

D. Application security

Answers

1. B. Secrets management is the name used to denote the policies and procedures employed to connect the IAM systems of the enterprise and the cloud to enable communication with the data.

2. C. Segmentation is a network issue, separate from storage.

3. C. Cost is not part of the resource policies. Resource policies describe how the elements of IAM, both in the enterprise and in the cloud, work together to provision resources.

4. A. VPC endpoints are not part of the virtual network; although they are virtual applications, they are not part of the network per se.

5. D. Security groups are used to manage users in the cloud environment.

6. C. The definition of a cloud access security broker (CASB) is a security policy enforcement point that is placed between cloud service consumers and cloud service providers to manage enterprise security policies as cloudbased resources are accessed.

7. B. SWGs operate at the application layer, making application layer determinations of suitability.

8. A, B, C, and D. All of these play important roles in securing cloud environments.

9. B. High availability depends on the ability of the cloud to reallocate resources in the event of a failure; this is one of the functions of dynamic resource allocation.

10. A. While many things are involved in cloud security, they all start on the foundation of the cloud services agreement, which describes all of the terms of service.

Questions

1. A friend of yours who works in the IT department of a bank tells you thattellers are allowed to log in to their terminals only from 9 A.M. to 5 P.M., Monday through Saturday. What is this restriction an example of?

A. User auditing

B. Least privilege

C. Time-of-day restrictions

D. Account verification

2. Your organization is revamping its account management policies andyou’ve been asked to clarify the difference between account disablement and account lockout. Which of the following statements best describes that difference?

A. Account disablement removes the user and all their data files; accountlockout does not.

B. Account lockout typically only affects the ability to log in; accountdisablement removes all privileges.

C. Account lockout is permanent; account disablement is easilyreversible.

D. Account disablement requires administrative privileges to execute;account lockout can be performed by any user.

3. Password policies are needed for all of the following except?

A. Password complexity

B. Password history

C. Password reuse

D. Password language

4. Which of the following is used to identify when a device is within aspecified distance of a location?

A. Geofencing

B. Geoproximity

C. Geodistance

D. Geotagging

5. Account audits are used for all of the following except?

A. Testing password strength

B. Verification of user training

C. Verification of user employment/authorization

D. Testing for password policy enforcement

6. Which of the following represents the greatest risk when used?

A. Service accounts

B. User accounts

C. Guest accounts

D. Shared accounts

7. When a new login request comes from a geographically distant location, fora user with a history of recent local logins, what policy can best help address legitimacy?

A. Impossible travel time

B. Geolocation

C. Network location

D. Time-of-day restrictions

8. You wish to tokenize account credentials so people can carry theirpasswords with them and not have to remember or type in long passwords. The best solution would involve which of the following?

A. Identity providers (IdPs)

B. SSH keys

C. Smart card

D. Password managers

9. On a web-facing interface, where your employees can gain access to thenetwork, you wish to employ security against brute force attacks. One of the most cost-effective tools is to enforce which of the following?

A. Geofencing policy

B. Password complexity policy

C. Account lockout policy

D. Certificates

10. Which type of policy sets the direction for the security team to manage who can access what resources in a system?

A. Account permissions policy

B. Time-based login policies

C. Password policies

D. Time-of-day restriction policies

Answers

1. C. Time-of-day restrictions are often used to limit the hours during which a user is allowed to log in to or access a system. This helps prevent unauthorized access outside that user’s normal working hours.

2. B. Account disablement is a step down from removing an account completely. While the account (and associated data files) still exist on the system, the account itself is disabled and has no privileges to access the system. Account lockout typically only affects logon privileges. Performing a temporary account lockout is a common approach to thwarting brute force password-guessing attacks.

3. D. The language used in the creation of passwords is not an issue, especially given that most passwords are ideally strings of random characters.

4. A. Geofencing is an electronic distance-based perimeter used to detect specific devices when they cross within a certain geographic area.

5. B. User training would not be examined during an account audit. Account audits are focused on the authentication system policies and implementations.

6. D. Shared accounts are the greatest risk because you don’t know who is using them.

7. A. When a subsequent account access request is received and there is not adequate time for the user to physically move to the new location, it is likely a fraudulent attempt.

8. C. Smart cards enable employees to easily carry cryptographic keys.

9. C. Account lockout is a temporary measure to slow down brute force attempts at cracking a password.

10. A. Developing a policy for account permissions provides guidance to those who are implementing the access control schemes.

Questions

To help you prepare further for the CompTIA Security+ exam, and to test your level of preparedness, answer the following questions and then check your answers against the correct answers at the end of the chapter.

1. Your organization needs a system for restricting access to files based on thesensitivity of the information in those files. You might suggest which of the following access control systems?

A. Discretionary access control

B. Mandatory access control

C. Confidential access control

D. File-based access control

2. Which of the following describes a major difference between NTFS andFAT32 file systems?

A. NTFS supports user-level access differentiation.

B. FAT32 supports group-level access differentiation.

C. FAT32 natively encrypts files and directories.

D. NTFS logs all file access using secure tokens.

3. Your organization has grown too large to support assigning permissions tousers individually. Within your organization, you have large groups of users who perform the same duties and need the same type and level of access to the same files. Rather than assigning individual permissions, your organization may wish to consider using which of the following access control methods?

A. Group-based access control

B. Shift-based access control

C. Role-based access control

D. File-based access control

4. A ticket-granting server is an important element in which of the followingauthentication models?

A. 802.1X

B. RADIUS

C. TACACS+

D. Kerberos

5. Which of the following is an open standard that uses security tokens andassertions and allows you to access multiple websites with one set of credentials?

A. PAP

B. CHAP

C. SSO

D. SAML

6. What protocol is used for RADIUS?

A. UDP

B. NetBIOS

C. TCP

D. Proprietary

7. What are accounts with greater than “normal” user access called?

A. Privileged accounts

B. System accounts

C. Superuser accounts

D. Audit accounts

8. You have to implement an OpenID solution. What is the typical relationshipwith existing systems?

A. OpenID is used for authentication, OAuth is used for authorization.

B. OpenID is used for authorization, OAuth is used for authentication.

C. OpenID is not compatible with OAuth.

D. OpenID only works with Kerberos.

9. You wish to create an access control scheme that enables the CFO to accessfinancial data from his machine, but not from the machine in the reception area of the lobby. Which access control model is best suited for this?

A. Role-based access control

B. Conditional access control

C. Mandatory access control

D. Discretionary access control

10. You need to design an authentication system where users who have neverconnected to the system can be identified and authenticated in a single process. Which is the best solution?

A. RADIUS

B. Password vault-based authentication

C. TPM-based authentication

D. Knowledge-based authentication

Answers

1. B. Mandatory access control (MAC) is a system used in environments with different levels of security classifications. Access to objects (like files) is based on the sensitivity of the information contained in those objects and the authorization of the user to access information with that level of sensitivity.

2. A. NTFS supports user-level access differentiation and allows you to assign user permissions to files and folders.

3. C. Your organization could consider role-based access control. In rolebased access control, instead of each user being assigned specific access permissions for the objects associated with the computer system or network, each user is assigned a set of roles that he or she may perform. The roles are in turn assigned the access permissions necessary to perform the tasks associated with the roles. Users will thus be granted permissions to objects in terms of the specific duties they must perform—not according to a security classification associated with individual objects.

4. D. Kerberos uses ticket-granting servers to manage the issuance of tickets granting various permissions on the system.

5. D. SAML is an XML-based protocol that uses security tokens and assertions to pass information about a “principal” (typically an end user) to a SAML authority (an “identity provider” or IdP) and the service provider (SP). In simpler terms, by allowing identity providers to pass on credentials to service providers, SAML allows you can log in to many different websites using one set of credentials.

6. A. RADIUS has been officially assigned UDP port 1812 for RADIUS authentication and port 1813 for RADIUS accounting by the Internet Assigned Numbers Authority (IANA). However, previously, ports 1645 (authentication) and 1646 (accounting) were used unofficially and became the default ports assigned by many RADIUS client/server implementations of the time. The tradition of using 1645 and 1646 for backward compatibility continues to this day. For this reason, many RADIUS server implementations monitor both sets of UDP ports for RADIUS requests. Microsoft RADIUS servers default to 1812 and 1813, but Cisco devices default to the traditional 1645 and 1646 ports.

7. A. Privileged accounts are any accounts with greater-than-normal user access. Privileged accounts are typically root- or admin-level accounts and represent risk in that they are unlimited in their powers.

8. A. Typically OpenID is used for authentication, and OAuth is used for authorization.

9. B. Conditional access control models allow differing access control schemes based on specific conditions beyond just user account.

10. D. Knowledge-based authentication schemes allow the authentication of users who have not previously established their identity via a combined identification and authentication methodology.

Questions

To help you prepare further for the CompTIA Security+ exam, and to test your level of preparedness, answer the following questions and then check your answers against the correct answers at the end of the chapter.

1. You are asked by the senior system administrator to refresh the SSLcertificates on the web servers. The process is to generate a certificate signing request (CSR), send it to a third party to be signed, and then apply the return information to the CSR. What is this an example of?

A. Pinning

B. Borrowed authority

C. Third-party trust model

D. Stapling

2. A certificate authority consists of which of the following?

A. Hardware and software

B. Policies and procedures

C. People who manage certificates

D. All of the above

3. Your manager wants you to review the company’s internal PKI system’sCPS for applicability and verification and to ensure that it meets current needs. What are you most likely to focus on?

A. Revocations

B. Trust level provided to users

C. Key entropy

D. How the keys are stored

4. You are preparing an e-mail to send to a colleague at work, and because themessage information is sensitive, you decide you should encrypt it. When you attempt to apply the certificate that you have for the colleague, the encryption fails. The certificate was listed as still valid for another year, and the certificate authority is still trusted and working. What happened to this user’s key?

A. It was using the wrong algorithm.

B. You are querying the incorrect certificate authority.

C. It was revoked.

D. The third-party trust model failed.

5. Which of the following is a requirement for a CRL?

A. It must have the e-mail addresses of all the certificate owners.

B. It must contain a list of all expired certificates.

C. It must contain information about all the subdomains covered by the

CA.

D. It must be posted to a public directory.

6. What does OCSP do?

A. It reviews the CRL for the client and provides a status about thecertificate being validated.

B. It outlines the details of a certificate authority, including how identitiesare verified, the steps the CA follows to generate certificates, and why the CA can be trusted.

C. It provides for a set of values to be attached to the certificate.

D. It provides encryption for digital signatures.

7. The X.509 standard applies to which of the following?

A. SSL providers

B. Digital certificates

C. Certificate revocation lists

D. Public key infrastructure

8. You are browsing a website when your browser provides you with thefollowing warning message: “There is a problem with this website’s security certificate.” When you examine the certificate, it indicates that the root CA is not trusted. What most likely happened to cause this error? A. The certificate was revoked.

B. The certificate does not have enough bit length for the TLS protocol.

C. The server’s CSR was not signed by a trusted CA.

D. The certificate has expired.

9. You are issued a certificate from a CA, delivered by e-mail, but the file doesnot have an extension. The e-mail notes that the root CA, the intermediate CAs, and your certificate are all attached in the file. What format is your certificate likely in?

A. DER

B. CER

C. PEM

D. PFX

10. Why is pinning more important on mobile devices? A. It uses elliptic curve cryptography.

B. It uses less power for pinned certificate requests.

C. It reduces network bandwidth usage by combining multiple CArequests into one.

D. It allows caching of a known good certificate when roaming to low-trust networks.

Answers

1. C. This is an example of the third-party trust model. Although you are generating the encryption keys on the local server, you are getting these keys signed by a third-party authority so that you can present the third party as the trusted agent for users to trust your keys.

2. D. A certificate authority (CA) is the hardware and software that manage the actual certificate bits, the policies and procedures that determine when certificates are properly issued, and the people who make and monitor the policies for compliance.

3. B. You are most likely to focus on the level of trust provided by the CA to users of the system, as providing trust is the primary purpose of the CA.

4. C. The certificate has likely been revoked, or removed from that user’s identity and no longer marked valid by the certificate authority.

5. D. Certificate revocation lists (CRLs) must be posted to a public directory so that all users of the system can query it.

6. A. Online Certificate Status Protocol (OCSP) is an online protocol that will look for a certificate’s serial number on CRLs and provide a status message about the certificate to the client.

7. B. The X.509 standard is used to define the properties of digital certificates.

8. C. In this case, the server’s certificate signing request (CSR) was not signed by a CA that is trusted by the endpoint computer, so no third-party trust can be established. This could be an indication of an attack, so the certificate should be manually verified before data is provided to the web server.

9. C. Because the certificate includes the entire certificate chain, it is most likely delivered to you in Privacy-Enhanced Mail (PEM) format.

10. D. Pinning is important on mobile devices because they are much more likely to be used on various networks, many of which have much lower trust than their home network.

Questions

To help you prepare further for the CompTIA Security+ exam, and to test your level of preparedness, answer the following questions and then check your answers against the correct answers at the end of the chapter.

1. To secure communications during remote access of a system, one can usewhich of the following tools?

A. OpenSSL

B. SSH

C. dd

D. tcpdump

2. Which of the following is not a packet capture/analysis tool?

A. Wireshark

B. tcpreplay

C. tcpdump

D. dd

3. To capture an image of the memory in a running system, one can use whichof the following?

A. grep

B. dumpmem

C. memdump

D. logger

4. Which tools are used in IP address investigations? (Choose all that apply.)

A. tracert

B. theHarvester

C. dnsenum

D. chmod

5. To search through a system to find files containing a phrase, what would thebest tool be?

A. curl

B. logger

C. chmod

D. grep

6. What does chmod do?A. Sets permission on a file

B. Initiates a change modification entry in a log file

C. Cryptographically hashes a file

D. Lists the files in a working directory

7. You need to analyze previously collected packet data on a network,including editing some of the data. Which is the best tool to use?

A. tcpreplay

B. tcpdump

C. netstat

D. Wireshark

8. Which of these tools is used in penetration testing? (Choose all that apply.)

A. nmap

B. Nessus

C. scanless

D. theHarvester

9. To automate system administration across an enterprise Windows network,including using Windows objects, the best choice would be which of the following?

A. Bash scripting

B. Python

C. Wireshark

D. PowerShell

10. You think a file is malware. What is the first tool you should invoke?

A. Cuckoo

B. WinHex

C. OpenSSL

D. Autopsy

Answers

1. B. SSH encrypts the communication channel across the path its packets take.

2. D. The dd utility captures files from file systems, not packets on a network.

3. C. Memdump is a program used to copy what is currently in memory.

4. A and C. Tracert gives the IP addresses of a communication channel, and dnsenum gets information from a DNS server.

5. D. Grep is the pattern-matching tool that can be used to match patterns and search for matches.

6. A. Chmod is used to set/manage file permissions in a Linux environment.

7. A. Tcpreplay is the best tool to use in this case because the question requested packet editing.

8. A, B, C, and D. All of these tools are used in penetration testing. Nmap finds systems, Nessus scans for vulnerabilities, scanless hides the IP of the machine scanning, and theHarvester collects information on potential targets.

9. D. PowerShell is the best tool to use in this case. The key is the inclusion of Windows objects.

10. A. Cuckoo is a sandbox program designed to analyze malicious software, separating the software from direct connection to the OS.