Chp 10 NS

Candidate: Dunkan Gibson (dunkan.gibson)
Date: 4/6/2022 7:43:35 pm • Time spent: 08:55

Score: 98% Passing Score: 80%

Question 1: ✔ Correct

You have been offered a position as a security analyst for Acme, Inc. The position will be remote. Acme Inc. has sent you your employment contract using a system that only allows you to open and digitally sign the contract.

Which rights management method is being used?

- DRM
- Dynamic
- Static
- IRM

EXPLANATION

Information Rights Management (IRM) focuses on business-to-business transfers for files such as documents, emails, spreadsheets, and financial data. Information rights management utilizes encryption and permissions to create rules for the files. These rules could allow or deny copying and pasting, editing, forwarding, and printing.

Digital Rights Management (DRM) is file-level management applied to rich media like music, videos, and software.

Dynamic data masking replaces original information with a mask that mimics the original in form and function, making it useful for data that is in use or processing.

Static data masking is helpful for data at rest in a database. This type of masking can be specified by field or column.

REFERENCES

10.2.2 DLP Facts

q_dlp_irm_secp7.question.fex

Question 2: ✔ Correct

Which TCP/IP protocol is a secure form of HTTP that uses SSL as a sub-layer for security?

- SSH
- DNS
- SMTP
- HTTPS

EXPLANATION

HTTPS is a secure form of HTTP that uses SSL as a sub-layer for security.

SMTP is used to route electronic mail through the internetwork.

SSH allows secure interactive control of remote systems.

DNS is a system that is distributed throughout the internetwork to provide address/name resolution.

REFERENCES

10.1.3 Secure Protocol Facts

q_sec_prot_https_02_secp7.question.fex

Question 3: ✔ Correct

Which type of attack is the act of exploiting a software program's free acceptance of input in order to execute arbitrary code on a target?

- Data diddling
- Covert channel exploitation
- TOCTOU
- ➡ Buffer overflow attack

EXPLANATION

The act of exploiting a software program's free acceptance of input in order to execute arbitrary code on a target is called a buffer overflow.

Data diddling is the change or corruption of data. TOC/TOU is a logon session replay attack. Covert channel exploitation is the use of timing or storage mechanisms to bypass security controls in order to leak information out of a secured environment.

REFERENCES

10.3.14 Web Application Attack Facts

q_webattk_buffer_04_secp7.question.fex

Question 4: ✔ Correct

IPsec is implemented through two separate protocols. What are these protocols called? (Select two.)

- [ ] L2TP
- [ ] SSL
- [x] AH
- [x] ESP
- [ ] EPS

EXPLANATION

IPsec is implemented through two separate protocols, which are IP Authentication Header and IPsec Encapsulating Security Payload. IPsec AH provides authentication and non-repudiation services to verify that the sender is genuine and data has not been modified in transit. IPsec ESP provides data encryption services for the data within the packet.

IPsec SSL and IPsec EPS are not protocols associated with IPsec.

REFERENCES

10.1.7 IPsec Facts

q_ipsec_ah_esp_01_secp7.question.fex

Question 5: ✔ Correct

While using a web-based order form, an attacker enters an unusually large value in the Quantity field.

The value he or she entered is so large that it exceeds the maximum value supported by the variable type used to store the quantity in the web application. This causes the value of the quantity variable to wrap around to the minimum possible value, which is a negative number.

As a result, the web application processes the order as a return instead of a purchase, and the attacker's account is credited with a large sum of money.

Which practices would have prevented this exploit? (Select two.)

- [x] Implementing server-side validation
- [ ] Installing the latest operating system updates
- [x] Implementing client-side validation
- [ ] Installing antivirus, anti-spyware, pop-up blockers, and firewall software
- [ ] Using the latest browser version and patch level

EXPLANATION

Client-side validation and server-side validation should have been used to identify input errors in the order form. In this example, if the user entered an invalid quantity in an order form field, client-side validation would have detected and blocked the error before the data was submitted to the server. Server-side validation should have also been used after the data was sent to the server to detect errors. Experienced attackers can circumvent client-side validation techniques by sending data to the server from outside the application's standard user interface, bypassing any input validation measures that may have been implemented on the client.

Using the latest browser version and patch level, installing the latest operating system updates, and using a script blocker are valuable security measures, but they would not have prevented the exploit in this scenario.

REFERENCES

10.3.14 Web Application Attack Facts

q_webattk_web_02_secp7.question.fex

Question 6: ✔ Correct

What is the primary function of the IKE Protocol used with IPsec?

- Provide authentication services.
- Encrypt packet contents.
- Ensure dynamic key rotation and select initialization vectors (IVs).
- Provide both authentication and encryption.
- ➡ Create a security association between communicating partners.

EXPLANATION

Internet Key Exchange (IKE) Protocol is used with IPsec to create a security association between communicating partners. It controls the negotiation of encryption methods, identifies how keys are exchanged, and sets up other parameters that control communications.

Encapsulating Security Payload (ESP) provides both authentication and encryption, while Authentication Header (AH) provides authentication only.

REFERENCES

10.1.7 IPsec Facts

q_ipsec_ah_esp_03_secp7.question.fex

Question 7: ✔ Correct

Which of the following is specifically meant to ensure that a program operates on clean, correct, and useful data?

- Process spawning
- Error and exception handling
- Input validation
- Application hardening

EXPLANATION

Input validation is the process of ensuring that a program operates on clean, correct, and useful data. Input validation uses routines (also called validation rules or check routines) that check for correctness, meaningfulness, and secureness in data input to the system.

Application hardening is the process of preventing vulnerability exploitation in software applications. Error and exception handling is a programming language construct designed to handle the occurrence of exceptions (which are special conditions that change the normal flow of program execution). Process spawning is the creation of a new process (also called a child process) by an existing process (also called a parent process).

REFERENCES

10.3.14 Web Application Attack Facts

q_webattk_input_secp7.question.fex

Question 8: ✔ Correct

You are performing a security test from the outside on a new application that has been deployed.

Which secure testing method are you MOST likely using?

- Interactive
- Static
- Dynamic
- Runtime

EXPLANATION

Dynamic application security testing scans applications after they have been deployed. These tests are performed from the outside.

Static application security testing focuses on analyzing source code, binaries, and byte code early in the development process.

Interactive application security testing is built into static testing and uses source code scanners.

Runtime is a type of coding error that occurs while software is running.

REFERENCES

10.4.3 SDLC and Development Facts

q_sdlc_dynamic_secp7.question.fex

Question 9: ✔ Correct

Which of the following is considered a drawback of the Waterfall application development life cycle?

- Each step in the life cycle only needs to be completed once before moving on to the next one.
- ➡ Requirements are determined at the beginning and are carried through to the end product.
- Development is broken into Sprints.
- Testing is performed throughout development.

EXPLANATION

The Waterfall development life cycle is a slow process and may take months or years to complete. It also lacks flexibility since the requirements determined in the beginning are carried through to the end product.

Development is broken into Sprints when using the Agile development model.

The Agile development model performs testing throughout development.

When using the Waterfall development model, an application likely goes through some of these steps multiple times before moving on to the next step.

REFERENCES

10.4.3 SDLC and Development Facts

q_sdlc_waterfall_secp7.question.fex

Question 10: ✔ Correct

Which rights management category is applied to music, videos, and software that is sold to consumers?

- IRM
- DRM
- Static
- Dynamic

EXPLANATION

Digital Rights Management (DRM) is file-level management applied to rich media like music, videos, and software. This strategy uses security technologies such as encryption, permissions, product keys, limited install applications, and persistent online authentication to prevent editing, sharing, and unauthorized copying.

Dynamic data masking replaces original information with a mask that mimics the original in form and function, making it useful for data that is in use or processing.

Static data masking is helpful for data at rest in a database. Masking this way can be specified by field or column.

Information Rights Management (IRM) focuses on business-to-business transfers for files such as documents, emails, spreadsheets, and financial data.

REFERENCES

10.2.2 DLP Facts

q_dlp_drm_secp7.question.fex

Question 11: ✔ Correct

Which of the following enters random data to the inputs of an application?

- Routines
- Validation rules
- Application hardening
- Fuzzing

EXPLANATION

Fuzz testing (also known as fuzzing) is a software-testing technique that exposes security problems by providing invalid, unexpected, or random data to the inputs of an application. Fuzzing programs come in two types:

- Mutation-based programs, which mutate existing data samples to create test data.
- Generation-based programs, which define new test data based on models of the input.

Input validation is the process of ensuring that a program operates on clean, correct, and useful data. Input validation uses routines (also called validation rules or check routines) that check for correctness, meaningfulness, and secureness in data input to the system. Application hardening is the process of preventing vulnerability exploitation in software applications.

REFERENCES

10.4.3 SDLC and Development Facts

q_sdlc_fuzzing_secp7.question.fex

Question 12: ✔ Correct

Which of the following is an attack that injects malicious scripts into web pages to redirect users to fake websites to gather personal information?

- ➡ XSS
- Drive-by download
- SQL injection
- DLL injection

EXPLANATION

Cross-site scripting (XSS) is an attack that injects scripts into web pages. When a user views the web page, the malicious scripts run, allowing the attacker to capture information or perform other actions.

- XSS often relies on social engineering or phishing to entice users to click on links to web pages that contain the malicious scripts.
- Some scripts redirect users to legitimate websites, but run in the background to capture information sent to the legitimate site.
- Scripts can be written to read (steal) cookies that contain identity information (such as session information).
- Scripts can also be designed to run under the security context of the current user. For example, scripts might execute with full privileges on the local system, or the scripts might run using the credentials used on a financial website.

A drive-by download is an attack where software or malware is downloaded and installed without explicit consent from the user. An SQL injection attack occurs when an attacker includes database commands within user data input fields on a form, and those commands subsequently execute on the server. A DLL injection attack occurs when a program is forced to load a dynamic-link library (DLL). This DLL then executes under the security context of the running application, and executes malicious code included with the injected DLL.

REFERENCES

10.3.11 Preventing Cross-Site Scripting

10.3.14 Web Application Attack Facts

q_webattk_cross_secp7.question.fex

Question 13: ✔ Correct

Which of the following functions does a single quote (') perform in an SQL injection?

- Indicates that everything after the single quote is a comment
- ➡ Indicates that data has ended and a command is beginning
- Indicates that the comment has ended and data is being entered
- Indicates that code is ending and a comment is being entered

EXPLANATION

A single quote (') indicates that data has ended and a command is beginning.

The double dashes (--) indicate that code is ending and a comment is being entered. Comments are code that a program does not execute and are usually used for explanations or reminders for the coder. Applications know to ignore the comments.

REFERENCES

10.3.14 Web Application Attack Facts

q_webattk_sql_06_secp7.question.fex

Question 14: ✔ Correct

What is the storage location called that holds all the development source files that version control systems use?

- ➡ Repository
- Stored procedures
- Memory management
- Normalization

EXPLANATION

A version control system uses a repository, which is a storage location that holds all the source files used during development.

Stored procedures are one or more database statements stored as a group in a database's data dictionary.

Normalization is data reorganized in a relational database with the intent to eliminate redundancy by having all related data stored in one place.

Memory management is a resource-management process applied to computer memory.

REFERENCES

10.4.7 Application Development Security Facts

q_app_devsec_repo_secp7.question.fex

Question 15: ✔ Correct

SFTP uses which mechanism to provide security for authentication and data transfer?

- SSL
- Token devices
- IPsec
- SSH

EXPLANATION

SSH File Transfer Protocol uses Secure Shell (SSH) to provide security for authentication and data transfer.

FTPS uses SSL to secure FTP traffic. You can also secure FTP traffic by establishing an IPsec tunnel between the client and the server, but IPsec is established independently of FTP in this case.

REFERENCES

10.1.3 Secure Protocol Facts

q_sec_prot_ssh_02_secp7.question.fex

Question 16: ✔ Correct

Which of the following is the first step in the Waterfall application development model?

- ➡ (●) Requirements
- ( ) Design
- ( ) Maintenance
- ( ) Implementation

EXPLANATION

The Waterfall development life cycle model steps are:

- Requirements
- Design
- Implementation
- Testing
- Development
- Maintenance

REFERENCES

10.4.3 SDLC and Development Facts

q_sdlc_require_secp7.question.fex

Question 17: ✔ Correct

To answer this question, complete the lab using the information below.
You have already answered this question.
You are not allowed to view the lab again.

Launch Lab

You completed the lab correctly.

Loading

REFERENCES

5.6.3 Configure URL Blocking

10.1.5 Allow SSL Connections

10.3.12 SQL Injections

10.3.13 Exploit SQL on a Web Page

10.3.14 Web Application Attack Facts

2173f72e-25f0-4e23-8a29-9acfa75d1f43

Question 18: ✔ Correct

To answer this question, complete the lab using the information below.
You have already answered this question.
You are not allowed to view the lab again.

Launch Lab

You completed the lab correctly.

Loading

REFERENCES

- 2.2.6 Configure Microsoft Defender
- 2.3.11 Identify Social Engineering
- 3.1.3 Implement Physical Security
- 4.2.5 Configure Automatic Updates
- 4.2.7 Configure Microsoft Defender Firewall
- 4.3.5 Configure NTFS Permissions
- 4.3.6 Disable Inheritance
- 5.1.7 Configure a Security Appliance
- 5.1.8 Configure Network Security Appliance Access
- 5.1.10 Configure QoS
- 5.2.3 Configure a DMZ
- 5.3.5 Configure a Perimeter Firewall
- 5.4.3 Configure NAT
- 5.5.4 Configure a Remote Access VPN
- 5.5.5 Configure a VPN Connection iPad
- 5.6.3 Configure URL Blocking
- 5.9.6 Secure a Switch
- 5.11.6 Spoof MAC Addresses with SMAC
- 5.11.9 Harden a Switch
- 5.11.10 Secure Access to a Switch

- 5.11.11 Secure Access to a Switch 2
- 5.12.4 Explore VLANs
- 5.13.5 Restrict Telnet and SSH Access
- 5.13.6 Permit Traffic
- 5.13.7 Block Source Hosts
- 6.5.5 Create OUs
- 6.5.6 Delete OUs
- 6.5.10 Create and Link a GPO
- 6.5.11 Create User Accounts
- 6.5.12 Manage User Accounts
- 6.5.13 Create a Group
- 6.5.14 Create Global Groups
- 6.6.4 Configure Account Password Policies
- 6.6.6 Restrict Local Accounts
- 6.6.7 Secure Default Accounts
- 6.6.8 Enforce User Account Control
- 6.6.11 Configure Smart Card Authentication
- 6.7.4 Create a User Account
- 6.7.5 Rename a User Account
- 6.7.6 Delete a User
- 6.7.7 Change Your Password
- 6.7.8 Change a User's Password
- 6.7.9 Lock and Unlock User Accounts
- 6.8.3 Rename and Create Groups
- 6.8.4 Add Users to a Group
- 6.8.5 Remove a User from a Group
- 6.10.6 Configure Kerberos Policy Settings

- 7.1.11 Hide Files with OpenStego
- 7.3.5 Compare an MD5 Hash
- 7.4.3 Encrypt Files with EFS
- 7.4.8 Configure BitLocker with a TPM
- 7.5.6 Manage Certificates
- 8.1.5 Configure a Wireless Network
- 8.2.6 Configure Rogue Host Protection
- 8.3.6 Harden a Wireless Network
- 8.3.7 Configure WIPS
- 8.3.9 Configuring a Captive Portal
- 9.1.6 Create Virtual Machines
- 9.2.6 Create Virtual Switches
- 9.8.4 Secure an iPad
- 9.8.6 Create a Guest Network for BYOD
- 10.1.5 Allow SSL Connections
- 10.3.10 Clear the Browser Cache
- 10.3.15 Perform an SQL Injection Attack
- 10.4.10 Implement Application Whitelisting with AppLocker
- 10.4.12 Implement Data Execution Preventions
- 11.3.5 Implement Intrusion Prevention
- 11.4.7 Scan for Windows Vulnerabilities
- 11.4.8 Scan for Linux Vulnerabilities
- 11.4.9 Scan for Domain Controller Vulnerabilities
- 11.4.10 Scan for IoT Vulnerabilities
- 11.4.11 Scan for WAP Vulnerabilities
- 11.6.4 Poison ARP and Analyze with Wireshark
- 11.6.6 Poison DNS

- 11.6.8 Analyze a SYN Flood Attack
- 11.7.4 Crack Password with Rainbow Tables
- 11.7.7 Crack a Password with John the Ripper
- 12.7.6 Configure Fault-Tolerant Volumes
- 12.8.6 Back Up Files with File History
- 12.8.8 Recover a File from File History
- 12.8.10 Backup a Domain Controller
- 13.3.5 Configure Email Filters
- 13.3.7 Secure Email on iPad
- 14.1.4 Configure Advanced Audit Policy
- 14.1.6 Enable Device Logs

c647a5d1-9d4f-4244-88f3-126f7fa59ab9

Question 19: ✔ Correct

Which of the following is a technology that tries to detect and stop sensitive data breaches, or data leakage incidents, in an organization?

- Data transmission security
- Data loss prevention
- Public key cryptography
- Data hashing

EXPLANATION

Data loss prevention (DLP) is a technology that tries to detect and stop sensitive data breaches, or data leakage incidents, in an organization. DLP is used to prevent sensitive data from being disclosed to an unauthorized person, whether it is deliberate or accidental.

Data transmission security is the use of secure protocols to encrypt data when it is transmitted. Hashing takes a variable-length string (message) and compresses and transforms it into a fixed-length value. When received, a hash is decrypted into the actual output so the recipient can understand the message.

Public key infrastructure uses certificates, which are electronic documents that use a digital signature, to bind a public key with an identity.

REFERENCES

10.2.2 DLP Facts

q_dlp_dlp_secp7.question.fex

Question 20: ✔ Correct

Which of the following protocols uses port 443?

- S/MIME
- S-HTTP
- HTTPS
- SSH

EXPLANATION

Hyper Text Transfer Protocol Secure (HTTPS) is a secure form of HTTP that uses either SSL or TLS to encrypt sensitive data before it is transmitted. HTTPS uses port 443.

Secure Hypertext Transfer Protocol (S-HTTP) supports a wide variety of encryption methods, but it does not use port 443. SSH uses port 22. S/MIME is a method for encrypting emails. S/MIME does not communicate over a specific port number.

REFERENCES

10.1.3 Secure Protocol Facts

q_sec_prot_https_01_secp7.question.fex

Question 21: ✔ Correct

Which of the following are the two main causes of software vulnerabilities? (Select two.)

- [ ] Obfuscation
- [x] Design flaws
- [x] Coding errors
- [ ] Normalization
- [ ] Fuzzing

EXPLANATION

Coding errors and design flaws are the main causes of software vulnerabilities.

Fuzz testing (also known as fuzzing) is a software-testing technique that exposes security problems by providing invalid, unexpected, or random data to the inputs of an application.

Normalization is data reorganized in a relational database with the intent to eliminate redundancy. This is done by having all related data stored in one place. This is not one of the main causes of software vulnerabilities.

Obfuscation is the deliberate act of creating source or machine code that is difficult for humans to understand. This is not one of the main causes of software vulnerabilities.

REFERENCES

10.4.3 SDLC and Development Facts

q_sdlc_software_secp7.question.fex

Question 22: ✔ Correct

As you browse the internet, you notice that when you go to some sites, multiple additional windows are opened automatically. Many of these windows contain advertisements for products that are inappropriate for your family to view.

Which tool can you implement to prevent these windows from showing?

- Anti-adware
- Pop-up blocker
- Anti-spyware
- Phishing filter
- Antivirus

EXPLANATION

Use a pop-up blocker to prevent windows from automatically opening when you visit a web site. Pop-up blockers typically do not block pop-ups that show when you click a button or a link, but they do prevent the pop-up windows that open automatically as you navigate to other sites.

Use antivirus software to scan attachments, downloads, or your system for malicious programs. Use anti-adware and anti-spyware software to prevent software that tracks your browsing history. While removing adware might prevent some pop-ups, it does not prevent all pop-ups unless the anti-adware software includes a pop-up blocker. Use a phishing filter to remove phishing emails or to prevent navigating to links that are disguised as legitimate links.

REFERENCES

10.3.14 Web Application Attack Facts

q_webattk_web_01_secp7.question.fex

Question 23: ✔ Correct

Which of the following tools allow remote management of servers? (Select two.)

- [ ] FTP
- [x] Telnet
- [ ] POP3
- [x] SSH
- [ ] SSL

EXPLANATION

Both Telnet and SSH are tools for remote server management.

POP3 is for retrieving email from a remote server, and FTP is for transferring files.

Secure Socket Layer (SSL) secures messages being transmitted on the internet.

REFERENCES

10.1.3 Secure Protocol Facts

q_sec_prot_remote_secp7.question.fex

Question 24: ✔ Correct

When using SSL authentication, what does the client verify first when checking a server's identity?

- ➡ The current date and time must fall within the server's certificate-validity period.
- All DNS resolution must point to the corporate intranet routers.
- The certificate must be non-expiring and self-signed by the sysadmin.
- Master secrets are verifiable from asymmetric keys.

EXPLANATION

An SSL client first checks the server's certificate validity period. The authentication process stops if the current date and time fall outside of the validity period.

SSL clients verify a server's identity using the following steps:

1. The client checks the server's certificate-validity period. The authentication process stops if the current date and time fall outside of the validity period.
2. The client verifies that the issuing certificate authority (CA) is on its list of trusted CAs.
3. The client uses the CA's public key to validate the CA's digital signature on the server certificate. If the digital signature can be verified, the client accepts the server certificate as a valid certificate issued by a trusted CA.
4. To protect against man-in-the-middle attacks, the client compares the actual DNS name of the server to the DNS name on the certificate.

REFERENCES

10.1.3 Secure Protocol Facts

q_sec_prot_ssl_04_secp7.question.fex

Question 25: ✔ Correct

Which of the following protocols are often added to other protocols to provide secure transmission of data? (Select two.)

- [x] SSL
- [x] TLS
- [ ] SMTP
- [ ] SNMP
- [ ] HTTPS

EXPLANATION

Both Secure Sockets Layer (SSL) and Transport Layer Security (TLS) are protocols that are used with other protocols to add security. In addition, Secure Shell (SSH) can be used to add security when using unsecure protocols.

HTTPS is the secure form of HTTP that uses SSL.

SMTP is used for sending email.

SNMP is a network management protocol.

REFERENCES

10.1.3 Secure Protocol Facts

q_sec_prot_ssl_tls_secp7.question.fex

Question 26: ✔ Correct

Having poor software development practices and failing to program input validation checks during development of custom software can result in a system vulnerable to which type of attack?

- Dictionary attack
- Denial-of-service attack
- ➡ Buffer overflow attack
- Superzapping

EXPLANATION

Poor software development practices and failing to program input validation checks can leave a system vulnerable to buffer overflow attacks. A buffer overflow occurs when software code receives more input than it was designed to handle because the programmer of that code failed to include input validation checks. When a buffer overflow occurs, the extra data is pushed into the execution stack and processed with the security context of the system itself. In other words, a buffer overflow attack often allows the attacker to perform any operation on a system.

Denial-of-service attacks exploit vulnerabilities in implementation and coding errors. Dictionary attacks are waged against logon prompts or stolen copies of a security account's database. Superzapping attacks are specific attacks that use a specialized utility named superzap to bypass the security of IBM mainframes to perform system alterations.

REFERENCES

10.3.14 Web Application Attack Facts

q_webattk_buffer_03_secp7.question.fex

Question 27: ✔ Correct

DLP can be used to identify sensitive files in a file system and then embed the organization's security policy within the file.

Which of the following DLP implementations travels with sensitive data files when they are moved or copied?

- Cloud DLP
- Network DLP
- File-level DLP
- Endpoint DLP

EXPLANATION

File-level DLP is used to identify sensitive files in a file system and then to embed the organization's security policy within the file. This way, the policy travels with the file when it is moved or copied. Since the security policy travels with that file if it's moved or copied, you can continue to control access to the file. For example, you can restrict who it can be transmitted to, even when the file is no longer on your system.

REFERENCES

10.2.2 DLP Facts

q_dlp_file_dlp_secp7.question.fex

Question 28: ✔ Correct

Your organization is having a third party come in and perform an audit on the financial records. You want to ensure that the auditor has access to the data they need while keeping the customers' data secure. To accomplish this goal, you plan to implement a mask that replaces the client names and account numbers with fictional data.

Which masking method are you implementing?

- Static
- Dynamic
- Tokenization
- Encryption

EXPLANATION

Dynamic data masking replaces original information with a mask that mimics the original in form and function, making it useful for data that is in use or processing.

Tokenization replaces actual data with a randomly generated alphanumeric character set called a token.

Static data masking is helpful for data at rest in a database. Masking this way can be specified by field or column.

Encryption happens when plaintext data is changed into unreadable ciphertext using an algorithm.

REFERENCES

10.2.2 DLP Facts

q_dlp_dynamic_01_secp7.question.fex

Question 29: ✔ Correct

Which of the following protocols can TLS use for key exchange? (Select two.)

- [x] Diffie-Hellman
- [x] RSA
- [ ] IKE
- [ ] KEA
- [ ] ECC

EXPLANATION

TLS uses Diffie-Hellman or RSA to exchange session keys.

SSL uses RSA or Key Exchange Protocol (KEA) for key exchange. IPsec uses IKE for key exchange. ECC (elliptic curve cryptography) is a method that can be used in key exchange.

REFERENCES

10.1.3 Secure Protocol Facts

q_sec_prot_tls_secp7.question.fex

Question 30: ✔ Correct

DLP can be implemented as a software or hardware solution that analyzes traffic in an attempt to detect sensitive data that is being transmitted in violation of an organization's security policies.

Which of the following DLP implementations analyzes traffic for data containing such things as financial documents, social security numbers, or key words used in proprietary intellectual property?

- File-level DLP
- Network DLP
- Endpoint DLP
- Cloud DLP

EXPLANATION

Network DLP is a software or hardware solution that is typically installed near the network perimeter. Network DLP analyzes network traffic in an attempt to detect sensitive data that is being transmitted in violation of an organization's security policies.

REFERENCES

10.2.2 DLP Facts

q_dlp_net_dlp_secp7.question.fex

Question 31: ✕ Incorrect

Tokenization is another effective tool in data loss prevention. Tokenization does which of the following? (Select two.)

- [ ] Allows a security policy to travel with a specific file, even when copied or moved
- [x] Protects data on its server with authentication and authorization protocols
- [ ] Allows continued control access to the file, even when it's no longer in your system
- [x] ~~Identifies sensitive files and embeds them within your security policies~~
- [ ] Replaces actual data with a randomly generated alphanumeric character set

EXPLANATION

Tokenization is another effective tool in data loss prevention. Tokenization does the following:

- Replaces actual data with a randomly generated alphanumeric character set called a token
- Stores original data on a server
- Protects data on its server with authentication and authorization protocols
- Allows authorization only when the correct token is presented

Another data protection tool is rights management. Rights management does the following:

- Protects data at the file level
- Identifies sensitive files and embeds them within your security policies
- Allows a security policy to travel with a specific file, even when copied or moved
- Allows continued control access to a file, even when it's no longer in your system

REFERENCES

10.2.2 DLP Facts

q_dlp_token_secp7.question.fex

Question 32: ✔ Correct

What is a set of software development tools called that can be installed as one unit and provides code frameworks or code snippets to help development go faster?

- Memory management
- SDK
- Repository
- Code signing

EXPLANATION

A software development kit (SDK) is a set of software development tools that can be installed as one unit. These tools can provide code frameworks or code snippets to help development go faster.

A version control system uses a repository, which is a storage location that holds all the source files used during development.

Code signing is the process of digitally signing (encrypting) executables and scripts to confirm the software author and guarantee that the code has not been altered or corrupted since it was signed.

Memory management is a resource-management process applied to computer memory.

REFERENCES

10.4.7 Application Development Security Facts

q_app_devsec_sdk_secp7.question.fex

Question 33: ✔ Correct

Which application development model approaches software development as a continuous, changing process with never-ending versions, bug fixes, and enhancements?

- Fuzz testing
- ➡ Agile
- Waterfall
- Code signing

EXPLANATION

The Agile development model approaches software development as a continuous, changing process with never-ending versions, bug fixes, and enhancements.

The Waterfall development model is the most widely used model. It is called this because each step is completed before the next step is begun. This way, each step flows to the next.

Fuzz testing is software testing technique that exposes security problems by providing invalid, unexpected, or random data to the inputs of an application.

Code signing is the process of digitally signing (encrypting) executables and scripts to confirm the software author and guarantee that the code has not been altered or corrupted since it was signed.

REFERENCES

10.4.3 SDLC and Development Facts

q_sdlc_agile_secp7.question.fex

Question 34: ✔ Correct

You have a website that accepts input from users for creating customer accounts. Input on the form is passed to a database server where the user account information is stored.

An attacker is able to insert database commands in the input fields and have those commands execute on the server.

Which type of attack has occurred?

- Buffer overflow
- Cross-site scripting
- DLL injection
- SQL injection

EXPLANATION

A SQL injection attack occurs when an attacker includes database commands within user data input fields on a form, and those commands subsequently execute on the server. The injection attack succeeds if the server does not properly validate the input to restrict entry of characters that could end and begin a database command. SQL injection attacks are prevented by proper programming methods that prevent commands from occurring within form data or that filter data to prevent such attacks.

A buffer overflow occurs when an operating system or application does not properly enforce boundaries for how much and which type of data can be inputted. Hackers submit data beyond the size reserved for the data in the memory buffer, and the extra data overwrites adjacent memory locations. The extra data sent by the attacker could include executable code that might then be able to execute in privileged mode.

Cross-site scripting (XSS) is an attack that injects scripts into web pages. When the user views the web page, the malicious scripts run, allowing the attacker to capture information or perform other actions. A DLL injection attack occurs when a program is forced to load a dynamic-link library (DLL). This DLL then executes under the security context of the running application and executes malicious code included with the injected DLL.

REFERENCES

10.3.14 Web Application Attack Facts

q_webattk_sql_02_secp7.question.fex

Question 35: ✔ Correct

Which DLP method works by replacing sensitive data with realistic fictional data?

- File-level DLP
- Tokenization
- Encryption
- Masking

EXPLANATION

Masking works by replacing sensitive data with realistic fictional data. The two types of masking are dynamic data masking and static data masking.

Tokenization replaces actual data with a randomly generated alphanumeric character set called a token.

File-level DLP is used to identify sensitive files in a file system and then to embed the organization's security policy within the file. This way, the policy travels with the file when it is moved or copied.

Encryption happens when plaintext data is changed through an algorithm into unreadable ciphertext.

REFERENCES

10.2.2 DLP Facts

q_dlp_masking_secp7.question.fex

Question 36: ✔ Correct

You have just finished developing a new application. Before putting it on the website for users to download, you want to provide a checksum to verify that the object has not been modified.

Which of the following would you implement?

- ➡ Code signing
- Code obfuscation
- Normalization
- Memory management

EXPLANATION

Code signing is the process of digitally signing (encrypting) executables and scripts to confirm the software author and guarantee that the code has not been altered or corrupted since it was signed. The process employs the use of a cryptographic hash to validate authenticity and integrity.

Code signing:

- Provides security when deployed.
- Helps prevent namespace conflicts in some programming languages.
- Provides a digital signature mechanism to verify the identity of the author or build system.
- Provides a checksum to verify that the object has not been modified.
- Provides versioning information about an object as well as storing other metadata about the object.

Memory management is a resource-management process applied to computer memory.

Code obfuscation is the deliberate act of creating source or machine code that is difficult for humans to understand.

Normalization is data reorganized in a relational database with the intent to eliminate redundancy by having all related data stored in one place.

REFERENCES

10.4.7 Application Development Security Facts

q_app_devsec_code_secp7.question.fex

Question 37: ✔ Correct

Which of the following DLP implementations can be used to monitor and control access to physical devices on workstations or servers?

- Cloud DLP
- Endpoint DLP
- Network DLP
- File-level DLP

EXPLANATION

Endpoint data loss prevention (DLP) runs on end user workstations and servers. Endpoint DLP is also referred to as a Chinese Wall solution. This could be something as simple as restricting the use of USB devices. Many endpoint-based systems also provide application controls to prevent confidential information transmission and also provide some type of immediate feedback to the user. Giving feedback to the user is based on the concept that not all data leakage incidents are malicious. The employee might not realize that the security-policy violation is inappropriate. The intent is to deter the employee from a similar action in the future.

REFERENCES

10.2.2 DLP Facts

q_dlp_end_dlp_secp7.question.fex

Question 38: ✔ Correct

Which fuzz testing program type defines new test data based on models of the input?

- ➡ (●) Generation-based
- ( ) Code signing
- ( ) Mutation-based
- ( ) Memory management

EXPLANATION

Fuzz testing (also known as fuzzing) is a software-testing technique that exposes security problems by providing invalid, unexpected, or random data to the inputs of an application. Fuzzing program types are:

- Mutation-based programs
  - Mutate existing data samples to create data
- Generation-based programs
  - Define new test data based on models of the input

Code signing is the process of digitally signing (encrypting) executables and scripts to confirm the software author and guarantee that the code has not been altered or corrupted since it was signed.

Memory management is a resource-management process applied to computer memory.

REFERENCES

10.4.7 Application Development Security Facts

q_app_devsec_fuzz_secp7.question.fex

Question 39: ✔ Correct

Which of the following attacks is a form of software exploitation that transmits or submits a longer stream of data than the input variable is designed to handle?

- Time-of-check to time-of-use attack
- Smurf attack
- Buffer overflow attack
- Data diddling

EXPLANATION

A buffer overflow occurs when software code receives more input than it was designed to handle. This normally occurs because the programmer of that code failed to include input validation checks. When a buffer overflow occurs, the extra data is pushed into the execution stack and processed with the security context of the system itself. In other words, a buffer overflow attack often allows the attacker to perform any operation on a system.

A time-of-check to time-of-use (TOCTOU) attack occurs when the results of an attack are realized or initiated after the attack itself is perpetrated. Data diddling is the purposeful altering of data. A smurf attack is a form of distributed-reflective denial of service.

REFERENCES

10.3.14 Web Application Attack Facts

q_webattk_buffer_01_secp7.question.fex

Question 40: ✔ Correct

An attacker inserts SQL database commands into a data input field of an order form used by a web-based application. When submitted, these commands are executed on the remote database server, causing customer contact information from the database to be sent to the malicious user's web browser.

Which practice would have prevented this exploit?

- Installing antivirus, anti-spyware, pop-up blockers, and firewall software
- Implementing a script blocker
- Using the latest browser version and patch level
- ➡ Implementing client-side validation

EXPLANATION

Client-side validation should have been used on the local system to identify input errors in the order form before the data was ever sent to the server. In this example, if the user entered SQL commands in an order form field, the error would have been immediately detected and blocked before the data was submitted to the server.

Using the latest browser version and patch level, installing anti-malware software, and using a script blocker are valuable security measures. But these would not have prevented the exploit in this scenario.

REFERENCES

10.3.14 Web Application Attack Facts

q_webattk_sql_03_secp7.question.fex