Eccouncil

(ECSAv10)

EC-Council Certified Security Analyst

Total: **150 Questions**

Link:

MYEXAM.FR

In this scenario, the hacker's strategy exemplifies a classic Denial of Service (DoS) attack, where an immense number of invalid requests consume the target's resources. This effectively prevents legitimate users from accessing the service, thus fulfilling the primary characteristic of a DoS attack. The network host's inability to differentiate between valid and invalid requests exacerbates the service disruption, a key element in DoS definitions.

Evaluating incorrect options:

B. Side Channel attacks involve exploiting indirect information gained from a system, such as timing or power consumption, rather than overwhelming a network resource. These tactics do not match the excessive invalid request pattern described.

C. Man-in-the-middle cryptographic attacks focus on intercepting and altering communication between two parties, lacking the resource exhaustion aspect of the scenario. These attacks do not aim to disrupt available resources but rather to eavesdrop or manipulate data in transit.

D. Authentication attacks concentrate on bypassing login credentials or access controls, which does not align with saturating a system with invalid requests. Though they compromise security, they do not directly render a service unavailable, as illustrated in the described case.

For further reading on this topic, refer to the following authoritative sources:

https://www.us-cert.cisa.gov/ncas/tips/Security-Tips-DoS
https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/
https://www.imperva.com/learn/ddos/what-is-a-denial-of-service-attack/

Question: 5

Thomas is an attacker and he skimmed through the HTML source code of an online shopping website for the presence of any vulnerabilities that he can exploit.
He already knows that when a user makes any selection of items in the online shopping webpage, the selection is typically stored as form field values and sent to the application as an HTTP request (GET or POST) after clicking the Submit button. He also knows that some fields related to the selected items are modifiable by the user (like quantity, color, etc.) and some are not (like price). While skimming through the HTML code, he identified that the price field values of the items are present in the HTML code. He modified the price field values of certain items from $200 to $2 in the HTML code and submitted the request successfully to the application.
Identify the type of attack performed by Thomas on the online shopping website?

A. Session poisoning attack
B. Hidden field manipulation attack
C. HTML embedding attack
D. XML external entity attack

Answer: C

Explanation:

C. HTML embedding attack is correct because Thomas manipulated the client-side HTML content of the web application to change the price of items before submitting the request, allowing him to exploit the application's trust in the input data.

In web applications, HTML embedding attacks leverage the fact that client-side code can be altered by users, particularly during form submissions. By modifying the HTML source code with a lower price, Thomas effectively tricked the server into accepting a fraudulent request that bypassed the intended business logic and validation procedures typically enforced on server-side processes.

The specificity and effectiveness of NetBIOS enumeration in acquiring internal network details affirm why option B is the sole correct choice in this context.

References:

https://www.csoonline.com/article/2870884/netbios-101.html
https://www.sans.org/white-papers/100783/
https://networking.ringcentral.com/network-security/netbios-explained.html

Question: 8

Jason is working on a pen testing assignment. He is sending customized ICMP packets to a host in the target network. However, the ping requests to the target failed with `ICMP Time Exceeded Type = 11` error messages. What can Jason do to overcome this error?

A. Set a Fragment Offset
B. Increase the Window size in the packets
C. Increase the TTL value in the packets
D. Increase the ICMP header length

Answer: C

Explanation:

C is correct because increasing the TTL (Time to Live) value prevents packets from being dropped prematurely during routing.

Increasing the TTL enhances the packet's lifespan as it traverses through routers. Each router decrements the TTL upon processing the packet, and once it reaches zero, the packet is discarded, leading to an "ICMP Time Exceeded Type = 11" message. By raising the TTL prior to sending, Jason increases the chances that packets can reach their destination without being dropped due to TTL expiration.

Evaluation of Other Options:

A. Set a Fragment Offset: This option is irrelevant in this context as it pertains to packet fragmentation. Fragmentation does not directly influence TTL decay, and altering the fragment offset will not prevent ICMP Time Exceeded messages.

B. Increase the Window size in the packets: The TCP window size is used to control data flow in TCP sessions, not applicable to ICMP packets that do not rely on this mechanism. Such an adjustment has no effect on packet routing or TTL expirations.

D. Increase the ICMP header length: This is incorrect as the ICMP header has a defined structure, and modifying its length does not aid in managing TTL. Moreover, uneven header configurations can cause additional issues including routing failures.

Thus, increasing the TTL is the most effective strategy for mitigating the encountered ICMP issues.

Reference:
https://www.cloudflare.com/learning/security/glossary/time-to-live-ttl/" target="_blank">https://www.cloudflare.com/learning/security/glossary/time-to-live-ttl/
https://www.cisco.com/c/en/us/support/docs/ip/internet-control-message-protocol-icmp/137596-icmp-time-exceeded-error.html" target="_blank">https://www.cisco.com/c/en/us/support/docs/ip/internet-control-

A is correct because it specifies a TCP connect scan, which does not utilize stealth techniques and thus does not meet the requirement for evading firewall detection.

When considering the other options:

B (nmap -T4 -A -v zapmaky.com) utilizes the aggressive scan option ("-A"), which includes OS detection and service version detection. These features are likely to trigger security alerts on most firewalls and intrusion detection systems, hence making it ineffective for stealth scanning.

C (nmap -sX -T4 -A -v zapmaky.com) employs an Xmas scan ("-sX"), which may indeed be considered stealthy. However, the addition of the aggressive features undermines stealth by potentially exposing the scan as an attack due to the extensive data collection involved, again drawing attention from firewall defenses.

D (nmap -sN -A zapmaky.com) specifies a null scan ("-sN"), which is a stealth technique but is often less effective against modern firewalls that implement TCP/IP stack fingerprinting. Additionally, like the previous options, the inclusion of "-A" would expose the scan to detection, compromising its stealthy nature.

In summary, while option A does not embody the intended stealthy behavior, it stands as the best among the choices provided since the others either neglect stealth techniques or incorporate aggressive options that would attract attention.

References:

https://nmap.org/book/nmap-usage.html
https://en.wikipedia.org/wiki/Nmap
https://www.acs.com.hk/en/products/1575/acr38-smart-card-reader/

Question: 13

Richard, a penetration tester was asked to assess a web application. During the assessment, he discovered a file upload field where users can upload their profile pictures. While scanning the page for vulnerabilities, Richard found a file upload exploit on the website. Richard wants to test the web application by uploading a malicious PHP shell, but the web page denied the file upload. Trying to get around the security, Richard added the `¯jpg' extension to the end of the file. The new
[1]
successfully upload the PHP shell.
Which of the following techniques has Richard implemented to upload the PHP shell?

A. Session stealing
B. Cookie tampering
C. Cross site scripting
D. Parameter tampering

Answer: D

Explanation:

D is correct as Richard implemented parameter tampering by modifying the file extension to bypass security checks.

Parameter tampering refers to the manipulation of input parameters (in this case, the file upload extension) to alter the behavior of the application. By appending '¯jpg' to the PHP file, Richard effectively tricked the server into accepting a file type that would normally be rejected. This action highlights the inadequacies in the server-side validation processes, where a simple check on file extension alone can be insufficient for security.

Question: 17

An organization has deployed a web application that uses encoding technique before transmitting the data over the Internet. This encoding technique helps the organization to hide the confidential data such as user credentials, email attachments, etc. when in transit. This encoding technique takes 3 bytes of binary data and divides it into four chunks of 6 bits. Each chunk is further encoded into respective printable character.
Identify the encoding technique employed by the organization?

A. Unicode encoding
B. Base64 encoding
C. URL encoding
D. HTMS encoding

Answer: B

Explanation:

B is correct as Base64 encoding specifically transforms 3 bytes of binary data into 4 printable ASCII characters, which fits the described operation.

Base64 encoding works by taking groups of 3 bytes (24 bits) of data, dividing them into four 6-bit segments, and mapping each segment to a specific character in the Base64 character set. This method effectively encodes binary data, making it suitable for transmission over protocols that require data to be in a text format, such as email and web forms.

Critical Evaluation of Incorrect Options:

A. **Unicode Encoding**: This technique is intended for representing text in different languages and is not focused on encoding binary data into a specific text format. While Unicode encompasses various encoding formats (e.g., UTF-8), it does not conform to the specific chunking into 6 bits and 4 characters as described.

C. **URL Encoding**: This technique is designed to encode strings so that they can be safely transmitted in URLs, by replacing unsafe ASCII characters with a "%" followed by two hexadecimal digits. URL encoding does not employ a structure of dividing bytes into chunks, nor does it encode in the Base64 manner.

D. **HTML Encoding**: This is primarily used to convert characters into a format that is safe for web pages, specifically for rendering special characters in HTML. It does not involve the systematic transformation of binary data into chunks of bytes like Base64, which is critical for the secure transmission of non-text data.

For further reading:

https://en.wikipedia.org/wiki/Base64
https://www.ietf.org/rfc/rfc3548.txt
https://www.owasp.org/index.php/Encoding

Question: 18

During an internal network audit, you are asked to see if there is any RPC server running on the network and if found, enumerate the associate RPC services.
Which port would you scan to determine the RPC server and which command will you use to enumerate the RPC services?

A. Port 111, rpcinfo
B. Port 111, rpcenum

packets, when reassembled, exceed the maximum allowable size for packets in the IP protocol (65,535 bytes). Many operating systems are unable to properly handle these oversized packets, leading to crashes or denial of service through buffer overflow vulnerabilities. Alisa's action of sending specially crafted ICMP packet fragments with varying offset values directly aligns with this attack methodology, thereby demonstrating the characteristic behavior of a Ping-of-death scenario.

Critically evaluating the other options:

B. Fraggle attack: This is a DDoS attack that exploits UDP and not ICMP. It involves sending UDP packets to broadcast addresses to flood a target with responses, making it conceptually distinct from network fragmentation issues.
C. Session hijacking: This involves taking over a session between two parties, typically through exploiting unprotected session tokens, and thus does not relate to packet fragmentation or ICMP usage.
D. Smurf attack: Similar to Fraggle, this is an amplification DDoS attack that uses ICMP echo requests sent to a broadcast address, and relies on exploiting the ICMP protocol but does not involve fragmentation leading to crashes.

In conclusion, the specific nature of the manipulation in the scenario clearly points to a Ping-of-death attack, with the incorrect options lacking the necessary characteristics of crashing systems through oversized fragment handling.

References:

https://www.cisco.com/c/en/us/support/docs/ip/icmp/13894-icmp.html
https://www.sans.org/white-papers/816/
https://www.us-cert.cisa.gov/ncas/alerts/2016/01/11/ping-death-attacks-and-mitigation

Question: 21

Which of the following roles of Microsoft Windows Active Directory refers to the ability of an active directory to transfer roles to any domain controller (DC) in the enterprise?

A. Master Browser (MB)
B. Global Catalog (GC)
C. Flexible Single Master Operation (FSMO)
D. Rights Management Services (RMS)

Answer: C

Explanation:

C is correct because Flexible Single Master Operation (FSMO) roles in Active Directory are designed to manage specific tasks that ensure the proper functioning of the directory services, including transferring operations to any domain controller in the enterprise.

FSMO encompasses five roles, two of which (Primary Domain Controller Emulator and Infrastructure Master) are critical for inter-domain communications and updates. This capability to transfer roles allows for load balancing and ensures high availability and fault tolerance within Active Directory environments. When a domain controller fails, FSMO roles can be seized or transferred to maintain administrative efficiency and consistency across the network.

Evaluation of Other Options:

Question: 25

SecGlobal Corporation hired Michael, a penetration tester. Management asked Michael to perform cloud penetration testing on the company's cloud infrastructure.
As a part of his task, he started checking all the agreements with cloud service provider and came to a conclusion that it is not possible to perform penetration testing on the cloud services that are being used by the organization due to the level of responsibilities between company and the Cloud Service Provider (CSP).
Identify the type of cloud service deployed by the organization?

A. Platform as a service (PaaS)
B. Software as a service (SaaS)
C. Anything as a service (XaaS)
D. Infrastructure as a service (IaaS)

Answer: D

Explanation:

D is correct as Infrastructure as a Service (IaaS) typically imposes shared responsibility, limiting the penetration testing capability users can exert over the cloud environment.

IaaS provides fundamental computing resources over the internet and requires users to manage everything above the virtualization layer, including operating systems and applications. The CSP is responsible for the underlying infrastructure while the customer manages their systems within this environment. This shared responsibility often restricts penetration testing due to regulatory compliance or service agreement limitations set by the CSP, as seen in the scenario described.

Evaluation of other options:

A. **Platform as a Service (PaaS)**: PaaS offers a platform allowing users to develop, run, and manage applications. The developer typically has less control over the underlying infrastructure compared to IaaS, which could further restrict the ability to conduct penetration testing, but the focus is primarily on application-level vulnerabilities rather than infrastructure layers.

B. **Software as a Service (SaaS)**: SaaS delivers software applications over the internet, with the CSP managing everything. Users have no control over the underlying infrastructure or platform, ruling out any form of penetration testing, as it only pertains to application security and not to the cloud infrastructure itself.

C. **Anything as a Service (XaaS)**: XaaS is a broad category encompassing all service models. Since it covers all potential service offerings, it cannot specifically denote a limitation in the ability to conduct penetration tests on the infrastructure itself; thus, it lacks the specificity required to answer the question.

In conclusion, IaaS best represents the scenario of limited penetration testing due to the defined responsibilities between the company and the CSP.

References:

https://www.ibm.com/cloud/learn/iaas
https://aws.amazon.com/what-is-iaas/
https://aws.amazon.com/architecture/what-is-architecture/

Question: 26

packet analysis by the IDS, which may not correlate fragmented packets effectively. This strategy leverages the assumption that fragmented packets can bypass certain detection mechanisms, making it a clear example of an evasion tactic defined as an insertion attack through inconsistent packet states.

Evaluation of Other Options:

A. **Bypassing the IDS using a Trojan**: While the action involves deploying a Trojan, it specifically targets packet fragmentation and TTL manipulation, rather than merely employing a Trojan for general evasion, making this option too broad.

B. **Bypassing the IDS using the broadcast address**: This option incorrectly assumes that Peter's approach involves a broadcast address attack, which is not illustrated in the context of his specified methodology regarding fragmentation and TTL values.

C. **Bypassing the IDS using the insertion attack**: Although closely related, insertion attacks typically involve inserting malicious code into legitimate data streams. Peter's fragmented packets do not conform strictly to this definition as they exploit inconsistencies in packet fragment reassembly rather than outright insertion.

In conclusion, Peter's technique showcases a calculated use of packet manipulation to exploit the IDS's processing weaknesses, aligning convincingly with option D.

References:

https://www.cisco.com/c/en/us/products/collateral/security/intrusion-detection-system-ids/white-paper-c11-743952.html
https://www.sans.org/white-papers/2035/
https://www.infosec.edu/sub/infosec-articles/what-is-intrusion-detection-system/#:~:text=An%20intrusion%20detection%20system%20(IDS)

Question: 29

Robert is a network admin in XYZ Inc. He deployed a Linux server in his enterprise network and wanted to share some critical and sensitive files that are present in the Linux server with his subordinates. He wants to set the file access permissions using chmod command in such a way that his subordinates can only read/ view the files but cannot edit or delete the files.
Which of the following chmod commands can Robert use in order to achieve his objective?

A. chmod 666
B. chmod 644
C. chmod 755
D. chmod 777

Answer: B

Explanation:

The correct command for Robert to use is B. chmod 644, as it grants read permissions to the owner and the group while restricting write permissions.

This command sets the following permissions:

The owner may read and write (6).
The group may read only (4).
Others may read only (4).

https://www.tldp.org/LDP/nag2/x-087-2-etc-shadow.html
https://www.cyberciti.biz/faq/howto-protect-the-shadow-file-in-linux/
https://www.hackerone.com/blog/Linux-Privilege-Escalation-Quick-References-Through-Shadow-File

Question: 33

An attacker targeted to attack network switches of an organization to steal confidential information such as network subscriber information, passwords, etc. He started transmitting data through one switch to another by creating and sending two 802.1Q tags, one for the attacking switch and the other for victim switch. By sending these frames. The attacker is fooling the victim switch into thinking that the frame is intended for it. The target switch then forwards the frame to the victim port.
Identify the type of attack being performed by the attacker?

A. SNMP brute forcing
B. MAC flooding
C. IP spoofing
D. VLAN hopping

Answer: D

Explanation:

D is correct because the attacker is exploiting VLAN tagging to bypass network segmentation and gain access to sensitive information.

VLAN hopping occurs when an attacker sends traffic to a target switch that appears legitimate due to bogus VLAN tags, enabling unauthorized access to VLANs. By embedding dual 802.1Q tags in frames, the attacker effectively tricks the switch into believing the packets are intended for the target VLAN, leading to the interception of confidential data such as network subscriber information and passwords.

Evaluation of other options:

A. **SNMP brute forcing** involves systematically guessing SNMP community strings to gain unauthorized access to network devices. This attack does not relate to manipulating VLAN tags or forwarding behavior, making it irrelevant in this scenario.

B. **MAC flooding** entails overwhelming a switch's MAC address table with fake MAC addresses, causing the switch to fail open and broadcast frames. While it could allow exposure of data, it does not involve VLAN manipulation or tag spoofing, which is central in the described attack.

C. **IP spoofing** refers to forging the source IP address of packets to gain unauthorized access or impersonate a user. This methodology does not entail the dual tagging mechanism described in the question, nor does it focus on VLANs directly.

In conclusion, VLAN hopping through manipulation of 802.1Q tags constitutes a unique and critical network threat, distinctly separating it from the other potential attacks listed.

References:

https://www.cisco.com/c/en/us/support/docs/security/802-1x/117902-aim.html
https://www.talosintelligence.com/vulnerability_reports/TALOS-2017-0350
https://www.arista.com/en/blog/67/switching-vlan-hopping-explained

Explanation:

C is the correct answer because the chkconfig [service name] off command effectively disables the specified service from starting automatically at boot in Ubuntu systems that use SysVinit.

In Ubuntu, which transitioned to systemd as its init system in later versions, chkconfig is still relevant for managing services and their runlevel settings in older distributions. The “off” option clearly indicates that the service should not initiate with the system.

Evaluation of Other Options:

A. # update-rc.d -f [service name] remove - This command is used for removing a service from the default runlevels, but it is less commonly utilized and may not provide granular control over service management compared to chkconfig. It could inadvertently remove service links rather than merely disabling them.

B. # chkconfig [service name] "del - This command syntax is incorrect due to the quotation marks. Assuming there was no syntax error, "del" is also not a valid argument, making this option ineffective for the intended purpose of disabling services.

D. # service [service name] stop - While this command stops a service that is currently running, it does not prevent it from starting again on the next boot. Therefore, it fails to address the need to disable services on a more permanent basis.

In conclusion, option C stands out as the most appropriate choice for disabling unnecessary services systematically within Ubuntu environments.

References:

https://help.ubuntu.com/community/UbuntuStart
https://linux.die.net/man/8/chkconfig
https://manpages.ubuntu.com/manpages/focal/man8/update-rc.d.8.html

Question: 38

Jack, a network engineer, is working on an IPv6 implementation for one of his clients. He deployed IPv6 on IPv4 networks using a mechanism where a node can choose from IPv6 or IPv4 based on the DNS value. This makes the network resources work simpler.
What kind of technique did Jack use?

A. Dual stacks
B. Filtering
C. Translation
D. Tunneling

Answer: A

Explanation:

A. Dual stacks is correct because this configuration allows a node to utilize both IPv4 and IPv6 protocols simultaneously.

The dual stack technique facilitates network readiness during the transition from IPv4 to IPv6, where nodes can operate on both protocols based on the DNS resolution. This approach ensures backward compatibility and provides flexibility, enabling seamless communication regardless of the protocol used by other nodes. By

In summary, option B directly addresses the need for specific network data essential for effective penetration testing, while the other options divert from the technical requirements of the task.

References:

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

Question: 41

Karen is a Network engineer at ITSec, a reputed MNC based in Philadelphia, USA. She wants to retrieve the DNS records from the publicly available servers. She searched using Google for the providers DNS Information and found the following sites: http://www.dnsstuff.com https://dnsquery.org
Through these sites she got the DNS records information as she wished.
What information is contained in DNS records?

A. Information about the DNS logs.
B. Information about local MAC addresses.
C. Information such as mail server extensions, IP addresses etc.
D. Information about the database servers and its services.

Answer: C

Explanation:

C is correct because DNS records provide critical details like IP addresses, mail server extensions, and other essential domain-specific information.

DNS (Domain Name System) records serve as a fundamental component of the internet's infrastructure, facilitating the translation of human-readable domain names into machine-readable IP addresses. The most common types of DNS records include A records, which map domains to IP addresses, MX records for mail exchange servers, and CNAME records for aliasing one domain to another. These records are indispensable for both website functionality and email delivery, making option C fundamentally aligned with the core purpose of DNS.

Evaluation of Other Options:

A. Information about the DNS logs.
This option is incorrect because DNS logs pertain to operational data like query logs and server activity, which are not stored within DNS records. DNS records do not provide historical tracking or auditing functionality.

B. Information about local MAC addresses.
This option is also incorrect as DNS operates at the network layer, primarily focusing on the IP layer. MAC addresses are localized to the local network segment and are not part of DNS records, which operate globally on the internet.

D. Information about the database servers and its services.
While database servers may have associated DNS records, the records themselves do not contain intrinsic information about the servers and services. DNS records are focused on name resolution rather than service details, thus making this option misleading.

In summary, option C accurately captures the essence of what DNS records are designed to convey, while the other options fail to align with established DNS functionalities.

command. This technique enables the execution of arbitrary SQL code, enhancing an attacker's control over the database environment.

Evaluation of Incorrect Options:

B. File inclusion: This vulnerability occurs when a web application includes files erroneously, leading to the execution of untrusted files. It is unrelated to direct SQL command manipulation and does not pertain to command execution in SQL databases.

C. Buffer Overflow: This attack targets memory management vulnerabilities by overflowing a buffer in an application to execute arbitrary code. This technique does not apply to SQL injection scenarios where direct query manipulation is used to exploit SQL servers.

D. Code injection: While related to injecting code, this term is broader and often pertains to injecting scripts into applications. Function call injection focuses specifically on SQL operational contexts, making it a more precise term for this SQL injection technique.

For further examination of SQL injection techniques and their implications:

1. https://owasp.org/www-community/attacks/SQL_Injection
2. https://www.veracode.com/security/sql-injection
3. https://www.csoonline.com/article/2200952/sql-injection-explained.html