



## **EC-Council**

### **Exam Questions 312-50v13**

Certified Ethical Hacker v13

#### NEW QUESTION 1

- (Topic 1)

You are a Network Security Officer. You have two machines. The first machine (192.168.0.99) has snort installed, and the second machine (192.168.0.150) has kiwi syslog installed. You perform a syn scan in your network, and you notice that kiwi syslog is not receiving the alert message from snort. You decide to run Wireshark in the snort machine to check if the messages are going to the kiwi syslog machine. What Wireshark filter will show the connections from the snort machine to kiwi syslog machine?

- A. tcp.srcport= = 514 && ip.src= = 192.168.0.99
- B. tcp.srcport= = 514 && ip.src= = 192.168.150
- C. tcp.dstport= = 514 && ip.dst= = 192.168.0.99
- D. tcp.dstport= = 514 && ip.dst= = 192.168.0.150

**Answer: D**

#### NEW QUESTION 2

- (Topic 1)

A large company intends to use Blackberry for corporate mobile phones and a security analyst is assigned to evaluate the possible threats. The analyst will use the Blackjacking attack method to demonstrate how an attacker could circumvent perimeter defenses and gain access to the Prometric Online Testing – Reports [https://ibt1.prometric.com/users/custom/report\\_queue/rq\\_str...](https://ibt1.prometric.com/users/custom/report_queue/rq_str...) corporate network. What tool should the analyst use to perform a Blackjacking attack?

- A. Paros Proxy
- B. BBProxy
- C. Blooover
- D. BBCrack

**Answer: B**

#### NEW QUESTION 3

- (Topic 1)

Bob, a network administrator at BigUniversity, realized that some students are connecting their notebooks in the wired network to have Internet access. In the university campus, there are many Ethernet ports available for professors and authorized visitors but not for students. He identified this when the IDS alerted for malware activities in the network. What should Bob do to avoid this problem?

- A. Disable unused ports in the switches
- B. Separate students in a different VLAN
- C. Use the 802.1x protocol
- D. Ask students to use the wireless network

**Answer: C**

#### NEW QUESTION 4

- (Topic 1)

If a token and 4-digit personal identification number (PIN) are used to access a computer system and the token performs off-line checking for the correct PIN, what type of attack is possible?

- A. Birthday
- B. Brute force
- C. Man-in-the-middle
- D. Smurf

**Answer: B**

#### NEW QUESTION 5

- (Topic 1)

Peter, a Network Administrator, has come to you looking for advice on a tool that would help him perform SNMP enquires over the network. Which of these tools would do the SNMP enumeration he is looking for? Select the best answers.

- A. SNMPUtil
- B. SNScan
- C. SNMPScan
- D. Solarwinds IP Network Browser
- E. NMap

**Answer: ABD**

#### NEW QUESTION 6

- (Topic 1)

A company's policy requires employees to perform file transfers using protocols which encrypt traffic. You suspect some employees are still performing file transfers using unencrypted protocols because the employees do not like changes. You have positioned a network sniffer to capture traffic from the laptops used by employees in the data ingest department. Using Wireshark to examine the captured traffic, which command can be used as display filter to find unencrypted file transfers?

- A. tcp.port = = 21
- B. tcp.port = 23
- C. tcp.port = = 21 || tcp.port = =22
- D. tcp.port ! = 21

Answer: A

#### NEW QUESTION 7

- (Topic 1)

The establishment of a TCP connection involves a negotiation called three-way handshake. What type of message does the client send to the server in order to begin this negotiation?

- A. ACK
- B. SYN
- C. RST
- D. SYN-ACK

Answer: B

#### NEW QUESTION 8

- (Topic 1)

Eve is spending her day scanning the library computers. She notices that Alice is using a computer whose port 445 is active and listening. Eve uses the ENUM tool to enumerate Alice machine. From the command prompt, she types the following command.

```
For /f "tokens=1 %%a in (hackfile.txt) do net use *
\\10.1.2.3\c$ /user:"Administrator" %%a
```

What is Eve trying to do?

- A. Eve is trying to connect as a user with Administrator privileges
- B. Eve is trying to enumerate all users with Administrative privileges
- C. Eve is trying to carry out a password crack for user Administrator
- D. Eve is trying to escalate privilege of the null user to that of Administrator

Answer: C

#### NEW QUESTION 9

- (Topic 1)

You are tasked to perform a penetration test. While you are performing information gathering, you find an employee list in Google. You find the receptionist's email, and you send her an email changing the source email to her boss's email (boss@company). In this email, you ask for a pdf with information. She reads your email and sends back a pdf with links. You exchange the pdf links with your malicious links (these links contain malware) and send back the modified pdf, saying that the links don't work. She reads your email, opens the links, and her machine gets infected. You now have access to the company network. What testing method did you use?

- A. Social engineering
- B. Piggybacking
- C. Tailgating
- D. Eavesdropping

Answer: A

#### Explanation:

Social engineering is the term used for a broad range of malicious activities accomplished through human interactions. It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information.

Social engineering attacks typically involve some form of psychological manipulation, fooling otherwise unsuspecting users or employees into handing over confidential or sensitive data. Commonly, social engineering involves email or other communication that invokes urgency, fear, or similar emotions in the victim, leading the victim to promptly reveal sensitive information, click a malicious link, or open a malicious file. Because social engineering involves a human element, preventing these attacks can be tricky for enterprises.

#### NEW QUESTION 10

- (Topic 1)

As a securing consultant, what are some of the things you would recommend to a company to ensure DNS security?

- A. Use the same machines for DNS and other applications
- B. Harden DNS servers
- C. Use split-horizon operation for DNS servers
- D. Restrict Zone transfers
- E. Have subnet diversity between DNS servers

Answer: BCDE

#### NEW QUESTION 10

- (Topic 1)

The change of a hard drive failure is once every three years. The cost to buy a new hard drive is \$300. It will require 10 hours to restore the OS and software to the new hard disk. It will require a further 4 hours to restore the database from the last backup to the new hard disk. The recovery person earns \$10/hour. Calculate the SLE, ARO, and ALE. Assume the EF = 1(100%). What is the closest approximate cost of this replacement and recovery operation per year?

- A. \$1320
- B. \$440
- C. \$100

D. \$146

**Answer:** D

**Explanation:**

1. AV (Asset value) = \$300 + (14 \* \$10) = \$440 - the cost of a hard drive plus the work of a recovery person, i.e. how much would it take to replace 1 asset? 10 hours for resorting the OS and soft + 4 hours for DB restore multiplies by hourly rate of the recovery person.

\* 2. SLE (Single Loss Expectancy) = AV \* EF (Exposure Factor) = \$440 \* 1 = \$440

\* 3. ARO (Annual rate of occurrence) = 1/3 (every three years, meaning the probability of occurring during 1 year is 1/3)

\* 4. ALE (Annual Loss Expectancy) = SLE \* ARO = 0.33 \* \$440 = \$145.2

**NEW QUESTION 11**

- (Topic 1)

Email is transmitted across the Internet using the Simple Mail Transport Protocol. SMTP does not encrypt email, leaving the information in the message vulnerable to being read by an unauthorized person. SMTP can upgrade a connection between two mail servers to use TLS. Email transmitted by SMTP over TLS is encrypted. What is the name of the command used by SMTP to transmit email over TLS?

- A. OPPORTUNISTIC TLS
- B. UPGRADE TLS
- C. FORCE TLS
- D. START TLS

**Answer:** D

**NEW QUESTION 16**

- (Topic 1)

Which of the following incident handling process phases is responsible for defining rules, collaborating human workforce, creating a back-up plan, and testing the plans for an organization?

- A. Preparation phase
- B. Containment phase
- C. Identification phase
- D. Recovery phase

**Answer:** A

**NEW QUESTION 17**

- (Topic 1)

Which of the following tools is used to detect wireless LANs using the 802.11a/b/g/n WLAN standards on a linux platform?

- A. Kismet
- B. Abel
- C. Netstumbler
- D. Nessus

**Answer:** A

**Explanation:**

[https://en.wikipedia.org/wiki/Kismet\\_\(software\)](https://en.wikipedia.org/wiki/Kismet_(software))

Kismet is a network detector, packet sniffer, and intrusion detection system for 802.11 wireless LANs. Kismet will work with any wireless card which supports raw monitoring mode, and can sniff 802.11a, 802.11b, 802.11g, and 802.11n traffic.

**NEW QUESTION 18**

- (Topic 1)

Which of the following algorithms can be used to guarantee the integrity of messages being sent, in transit, or stored?

- A. symmetric algorithms
- B. asymmetric algorithms
- C. hashing algorithms
- D. integrity algorithms

**Answer:** C

**NEW QUESTION 21**

- (Topic 1)

A new wireless client is configured to join a 802.11 network. This client uses the same hardware and software as many of the other clients on the network. The client can see the network, but cannot connect. A wireless packet sniffer shows that the Wireless Access Point (WAP) is not responding to the association requests being sent by the wireless client. What is a possible source of this problem?

- A. The WAP does not recognize the client's MAC address
- B. The client cannot see the SSID of the wireless network
- C. Client is configured for the wrong channel
- D. The wireless client is not configured to use DHCP

**Answer:** A

**Explanation:**

[https://en.wikipedia.org/wiki/MAC\\_filtering](https://en.wikipedia.org/wiki/MAC_filtering)

MAC filtering is a security method based on access control. Each address is assigned a 48-bit address, which is used to determine whether we can access a network or not. It helps in listing a set of allowed devices that you need on your Wi-Fi and the list of denied devices that you don't want on your Wi-Fi. It helps in preventing unwanted access to the network. In a way, we can blacklist or white list certain computers based on their MAC address. We can configure the filter to allow connection only to those devices included in the white list. White lists provide greater security than blacklists because the router grants access only to selected devices.

It is used on enterprise wireless networks having multiple access points to prevent clients from communicating with each other. The access point can be configured only to allow clients to talk to the default gateway, but not other wireless clients. It increases the efficiency of access to a network.

The router allows configuring a list of allowed MAC addresses in its web interface, allowing you to choose which devices can connect to your network. The router has several functions designed to improve the network's security, but not all are useful. Media access control may seem advantageous, but there are certain flaws. On a wireless network, the device with the proper credentials such as SSID and password can authenticate with the router and join the network, which gets an IP address and access to the internet and any shared resources.

MAC address filtering adds an extra layer of security that checks the device's MAC address

against a list of agreed addresses. If the client's address matches one on the router's list, access is granted; otherwise, it doesn't join the network.

#### NEW QUESTION 25

- (Topic 1)

Which of the following is assured by the use of a hash?

- A. Authentication
- B. Confidentiality
- C. Availability
- D. Integrity

Answer: D

#### NEW QUESTION 30

- (Topic 1)

What is the way to decide how a packet will move from an untrusted outside host to a protected inside that is behind a firewall, which permits the hacker to determine which ports are open and if the packets can pass through the packet-filtering of the firewall?

- A. Session hijacking
- B. Firewalking
- C. Man-in-the middle attack
- D. Network sniffing

Answer: B

#### NEW QUESTION 34

- (Topic 1)

The company ABC recently contracts a new accountant. The accountant will be working with the financial statements. Those financial statements need to be approved by the CFO and then they will be sent to the accountant but the CFO is worried because he wants to be sure that the information sent to the accountant was not modified once he approved it. Which of the following options can be useful to ensure the integrity of the data?

- A. The CFO can use a hash algorithm in the document once he approved the financial statements
- B. The CFO can use an excel file with a password
- C. The financial statements can be sent twice, one by email and the other delivered in USB and the accountant can compare both to be sure is the same document
- D. The document can be sent to the accountant using an exclusive USB for that document

Answer: A

#### NEW QUESTION 38

- (Topic 1)

Which type of security feature stops vehicles from crashing through the doors of a building?

- A. Bollards
- B. Receptionist
- C. Mantrap
- D. Turnstile

Answer: A

#### NEW QUESTION 41

- (Topic 1)

What is one of the advantages of using both symmetric and asymmetric cryptography in SSL/TLS?

- A. Supporting both types of algorithms allows less-powerful devices such as mobile phones to use symmetric encryption instead.
- B. Symmetric algorithms such as AES provide a failsafe when asymmetric methods fail.
- C. Symmetric encryption allows the server to securely transmit the session keys out-of-band.
- D. Asymmetric cryptography is computationally expensive in comparison
- E. However, it is well-suited to securely negotiate keys for use with symmetric cryptography.

Answer: A

#### NEW QUESTION 46

- (Topic 1)

Joseph was the Web site administrator for the Mason Insurance in New York, who's main Web site was located at [www.masonins.com](http://www.masonins.com). Joseph uses his laptop computer regularly to administer the Web site. One night, Joseph received an urgent phone call from his friend, Smith. According to Smith, the main Mason Insurance web site had been vandalized! All of its normal content was removed and replaced with an attacker's message "Hacker Message: You are dead! Freaks!?? From his office, which was directly connected to Mason Insurance's internal network, Joseph surfed to the Web site using his laptop. In his browser, the Web site looked completely intact.

No changes were apparent. Joseph called a friend of his at his home to help troubleshoot the problem. The Web site appeared defaced when his friend visited using his DSL connection. So, while Smith and his friend could see the defaced page, Joseph saw the intact Mason Insurance web site. To help make sense of this problem, Joseph decided to access the Web site using his dial-up ISP. He disconnected his laptop from the corporate internal network and used his modem to dial up the same ISP used by Smith. After his modem connected, he quickly typed [www.masonins.com](http://www.masonins.com) in his browser to reveal the following web page:

H@cker Mess@ge:  
 Y0u @re De@d! Fre@ks!

After seeing the defaced Web site, he disconnected his dial-up line, reconnected to the internal network, and used Secure Shell (SSH) to log in directly to the Web server. He ran Tripwire against the entire Web site, and determined that every system file and all the Web content on the server were intact. How did the attacker accomplish this hack?

- A. ARP spoofing
- B. SQL injection
- C. DNS poisoning
- D. Routing table injection

**Answer: C**

#### NEW QUESTION 48

- (Topic 1)

What ports should be blocked on the firewall to prevent NetBIOS traffic from not coming through the firewall if your network is comprised of Windows NT, 2000, and XP?

- A. 110
- B. 135
- C. 139
- D. 161
- E. 445
- F. 1024

**Answer: BCE**

#### NEW QUESTION 49

- (Topic 1)

Which of the following is a command line packet analyzer similar to GUI-based Wireshark?

- A. nessus
- B. tcpdump
- C. ethereal
- D. jack the ripper

**Answer: B**

#### Explanation:

Tcpdump is a data-network packet analyzer computer program that runs under a command-line interface. It allows the user to display TCP/IP and other packets being transmitted or received over a network to which the computer is attached. Distributed under the BSD license, tcpdump is free software.

<https://www.wireshark.org/>

Wireshark is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education.

NOTE: Wireshark is very similar to tcpdump, but has a graphical front-end, plus some integrated sorting and filtering options.

#### NEW QUESTION 52

- (Topic 1)

Null sessions are un-authenticated connections (not using a username or password.) to an NT or 2000 system. Which TCP and UDP ports must you filter to check null sessions on your network?

- A. 137 and 139
- B. 137 and 443
- C. 139 and 443
- D. 139 and 445

**Answer: D**

#### NEW QUESTION 57

- (Topic 1)

What does the -oX flag do in an Nmap scan?

- A. Perform an eXpress scan
- B. Output the results in truncated format to the screen
- C. Output the results in XML format to a file
- D. Perform an Xmas scan

**Answer:** C

**Explanation:**

<https://nmap.org/book/man-output.html>  
 -oX <filespec> - Requests that XML output be directed to the given filename.

**NEW QUESTION 59**

- (Topic 1)

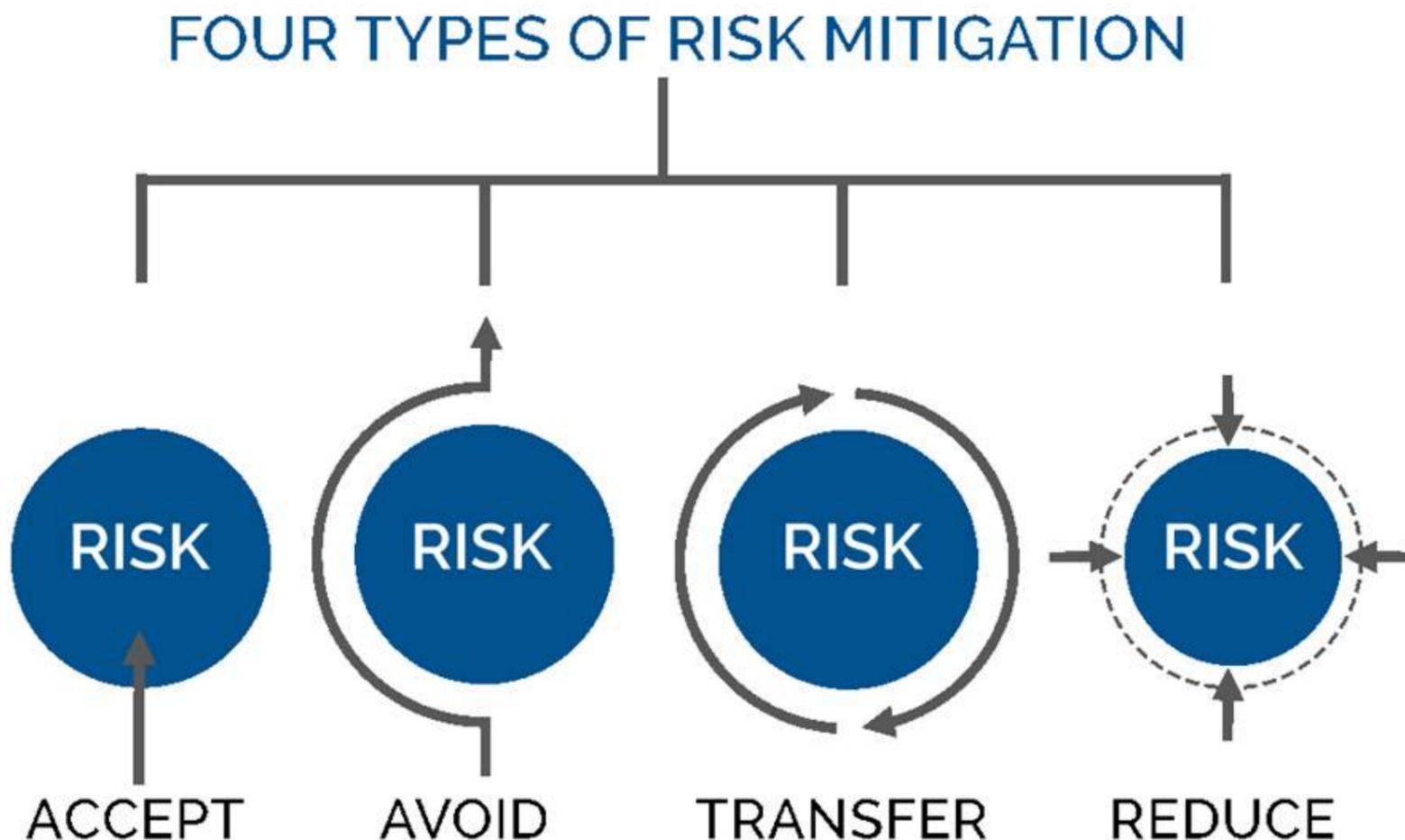
Suppose your company has just passed a security risk assessment exercise. The results display that the risk of the breach in the main company application is 50%. Security staff has taken some measures and implemented the necessary controls. After that, another security risk assessment was performed showing that risk has decreased to 10%. The risk threshold for the application is 20%. Which of the following risk decisions will be the best for the project in terms of its successful continuation with the most business profit?

- A. Accept the risk
- B. Introduce more controls to bring risk to 0%
- C. Mitigate the risk
- D. Avoid the risk

**Answer:** A

**Explanation:**

Risk Mitigation  
 Risk mitigation can be defined as taking steps to reduce adverse effects. There are four types of risk mitigation strategies that hold unique to Business Continuity and Disaster Recovery. When mitigating risk, it's important to develop a strategy that closely relates to and matches your company's profile.



A picture containing diagram  
 Description automatically generated

**Risk Acceptance**

Risk acceptance does not reduce any effects; however, it is still considered a strategy. This strategy is a common option when the cost of other risk management options such as avoidance or limitation may outweigh the cost of the risk itself. A company that doesn't want to spend a lot of money on avoiding risks that do not have a high possibility of occurring will use the risk acceptance strategy.

**Risk Avoidance**

Risk avoidance is the opposite of risk acceptance. It is the action that avoids any exposure to the risk whatsoever. It's important to note that risk avoidance is usually the most expensive of all risk mitigation options.

**Risk Limitation**

Risk limitation is the most common risk management strategy used by businesses. This strategy limits a company's exposure by taking some action. It is a strategy employing a bit of risk acceptance and a bit of risk avoidance or an average of both. An example of risk limitation would be a company accepting that a disk drive may fail and avoiding a long period of failure by having backups.

**Risk Transference**

Risk transference is the involvement of handing risk off to a willing third party. For example, numerous companies outsource certain operations such as customer service, payroll services, etc. This can be beneficial for a company if a transferred risk is not a core competency of that company. It can also be used so a company can focus more on its core competencies.

#### NEW QUESTION 60

- (Topic 1)

What is the proper response for a NULL scan if the port is open?

- A. SYN
- B. ACK
- C. FIN
- D. PSH
- E. RST
- F. No response

**Answer:** F

#### NEW QUESTION 64

- (Topic 1)

An attacker with access to the inside network of a small company launches a successful STP manipulation attack. What will he do next?

- A. He will create a SPAN entry on the spoofed root bridge and redirect traffic to his computer.
- B. He will activate OSPF on the spoofed root bridge.
- C. He will repeat this action so that it escalates to a DoS attack.
- D. He will repeat the same attack against all L2 switches of the network.

**Answer:** A

#### NEW QUESTION 68

- (Topic 1)

During a recent security assessment, you discover the organization has one Domain Name Server (DNS) in a Demilitarized Zone (DMZ) and a second DNS server on the internal network.

What is this type of DNS configuration commonly called?

- A. DynDNS
- B. DNS Scheme
- C. DNSSEC
- D. Split DNS

**Answer:** D

#### NEW QUESTION 69

- (Topic 2)

which of the following information security controls creates an appealing isolated environment for hackers to prevent them from compromising critical targets while simultaneously gathering information about the hacker?

- A. intrusion detection system
- B. Honeypot
- C. Botnet D Firewall

**Answer:** B

#### Explanation:

A honeypot may be a trap that an IT pro lays for a malicious hacker, hoping that they will interact with it during a way that gives useful intelligence. It's one among the oldest security measures in IT, but beware: luring hackers onto your network, even on an isolated system, are often a dangerous game. honeypot may be a good starting place: A honeypot may be a computer or computing system intended to mimic likely targets of cyberattacks. Often a honeypot are going to be deliberately configured with known vulnerabilities in situation to form a more tempting or obvious target for attackers. A honeypot won't contain production data or participate in legitimate traffic on your network — that's how you'll tell anything happening within it's a results of an attack. If someone's stopping by, they're up to no good. That definition covers a various array of systems, from bare-bones virtual machines that only offer a couple of vulnerable systems to ornately constructed fake networks spanning multiple servers. and therefore the goals of these who build honeypots can vary widely also , starting from defense thorough to academic research. additionally , there's now an entire marketing category of deception technology that, while not meeting the strict definition of a honeypot, is certainly within the same family. But we'll get thereto during a moment. honeypots aim to permit close analysis of how hackers do their dirty work. The team controlling the honeypot can watch the techniques hackers use to infiltrate systems, escalate privileges, and otherwise run amok through target networks. These sorts of honeypots are found out by security companies, academics, and government agencies looking to look at the threat landscape. Their creators could also be curious about learning what kind of attacks are out there, getting details on how specific sorts of attacks work, or maybe trying to lure a specific hackers within the hopes of tracing the attack back to its source. These systems are often inbuilt fully isolated lab environments, which ensures that any breaches don't end in non-honeypot machines falling prey to attacks. Production honeypots, on the opposite hand, are usually deployed in proximity to some organization's production infrastructure, though measures are taken to isolate it the maximum amount as possible. These honeypots often serve both as bait to distract hackers who could also be trying to interrupt into that organization's network, keeping them faraway from valuable data or services; they will also function a canary within the coalpit , indicating that attacks are underway and are a minimum of partially succeeding.

#### NEW QUESTION 70

- (Topic 2)

Jim, a professional hacker, targeted an organization that is operating critical Industrial Infrastructure. Jim used Nmap to scan open ports and running services on systems connected to the organization's OT network. He used an Nmap command to identify Ethernet/IP devices connected to the Internet and further gathered Information such as the vendor name, product code and name, device name, and IP address. Which of the following Nmap commands helped Jim retrieve the required information?

- A. nmap -Pn -sT --scan-delay 1s --max-parallelism 1 -p < Port List > < Target IP >
- B. nmap -Pn -sU -p 44818 --script enip-info < Target IP >
- C. nmap -Pn -sT -p 46824 < Target IP >
- D. nmap -Pn -sT -p 102 --script s7-info < Target IP >

**Answer:** B

**Explanation:**

<https://nmap.org/nsedoc/scripts/enip-info.html> Example Usage enip-info:

- nmap --script enip-info -sU -p 44818 <host>

This NSE script is used to send a EtherNet/IP packet to a remote device that has TCP 44818 open. The script will send a Request Identity Packet and once a response is received, it validates that it was a proper response to the command that was sent, and then will parse out the data. Information that is parsed includes Device Type, Vendor ID, Product name, Serial Number, Product code, Revision Number, status, state, as well as the Device IP.

This script was written based of information collected by using the the Wireshark dissector for CIP, and EtherNet/IP, The original information was collected by running a modified version of the ethernetip.py script (<https://github.com/paperwork/pyenip>)

**NEW QUESTION 75**

- (Topic 2)

How is the public key distributed in an orderly, controlled fashion so that the users can be sure of the sender??s identity?

- A. Hash value
- B. Private key
- C. Digital signature
- D. Digital certificate

**Answer:** D

**NEW QUESTION 78**

- (Topic 2)

which of the following protocols can be used to secure an LDAP service against anonymous queries?

- A. SSO
- B. RADIUS
- C. WPA
- D. NTLM

**Answer:** D

**Explanation:**

In a Windows network, nongovernmental organization (New Technology) local area network Manager (NTLM) could be a suite of Microsoft security protocols supposed to produce authentication, integrity, and confidentiality to users. NTLM is that the successor to the authentication protocol in Microsoft local area network Manager (LANMAN), Associate in Nursing older Microsoft product. The NTLM protocol suite is enforced in an exceedingly Security Support supplier, which mixes the local area network Manager authentication protocol, NTLMv1, NTLMv2 and NTLM2 Session protocols in an exceedingly single package. whether or not these protocols area unit used or will be used on a system is ruled by cluster Policy settings, that totally different{completely different} versions of Windows have different default settings. NTLM passwords area unit thought-about weak as a result of they will be brute-forced very simply with fashionable hardware.

NTLM could be a challenge-response authentication protocol that uses 3 messages to authenticate a consumer in an exceedingly affiliation orientating setting (connectionless is similar), and a fourth extra message if integrity is desired.

? First, the consumer establishes a network path to the server and sends a

NEGOTIATE\_MESSAGE advertising its capabilities.

? Next, the server responds with CHALLENGE\_MESSAGE that is employed to determine the identity of the consumer.

? Finally, the consumer responds to the challenge with Associate in Nursing AUTHENTICATE\_MESSAGE.

The NTLM protocol uses one or each of 2 hashed word values, each of that are keep on the server (or domain controller), and that through a scarcity of seasoning area unit word equivalent, that means that if you grab the hash price from the server, you??ll evidence while not knowing the particular word. the 2 area unit the lm Hash (a DES-based operate applied to the primary fourteen chars of the word born-again to the standard eight bit laptop charset for the language), and also the nt Hash (MD4 of the insufficient endian UTF-16 Unicode password). each hash values area unit sixteen bytes (128 bits) every.

The NTLM protocol additionally uses one among 2 a method functions, looking on the NTLM version. National Trust LanMan and NTLM version one use the DES primarily based LanMan a method operate (LMOWF), whereas National TrustLMv2 uses the NT MD4 primarily based a method operate (NTOWF).

**NEW QUESTION 81**

- (Topic 2)

Boney, a professional hacker, targets an organization for financial benefits. He performs an attack by sending his session ID using an MITM attack technique.

Boney first obtains a valid session ID by logging into a service and later feeds the same session 10 to the target employee. The session ID links the target employee to Boneys account page without disclosing any information to the victim. When the target employee clicks on the link, all the sensitive payment details entered in a form are linked to Boneys account. What is the attack performed by Boney in the above scenario?

- A. Session donation attack
- B. Session fixation attack
- C. Forbidden attack
- D. CRIME attack

**Answer:** A

**Explanation:**

In a session donation attack, the attacker donates their own session ID to the target user. In this attack, the attacker first obtains a valid session ID by logging into a service and later feeds the same session ID to the target user. This session ID links a target user to the attacker's account page without disclosing any information to the victim. When the target user clicks on the link and enters the details (username, password, payment details, etc.) in a form, the entered details are linked to the attacker's account. To initiate this attack, the attacker can send their session ID using techniques such as cross-site cooking, an MITM attack, and session fixation. A session donation attack involves the following steps.

**NEW QUESTION 86**

- (Topic 2)

infecting a system with malware and using phishing to gain credentials to a system or web application are examples of which phase of the ethical hacking methodology?

- A. Reconnaissance
- B. Maintaining access
- C. Scanning
- D. Gaining access

**Answer: D**

**Explanation:**

This phase having the hacker uses different techniques and tools to realize maximum data from the system. they??re → Password cracking – Methods like Bruteforce, dictionary attack, rule-based attack, rainbow table are used. Bruteforce is trying all combinations of the password. Dictionary attack is trying an inventory of meaningful words until the password matches. Rainbow table takes the hash value of the password and compares with pre-computed hash values until a match is discovered. • Password attacks – Passive attacks like wire sniffing, replay attack. Active online attack like Trojans, keyloggers, hash injection, phishing. Offline attacks like pre-computed hash, distributed network and rainbow. Non electronic attack like shoulder surfing, social engineering and dumpster diving.

**NEW QUESTION 91**

- (Topic 2)

George is a security professional working for iTech Solutions. He was tasked with securely transferring sensitive data of the organization between industrial systems. In this process, he used a short-range communication protocol based on the IEEE 203.15.4 standard. This protocol is used in devices that transfer data infrequently at a low rate in a restricted area, within a range of 10-100 m. What is the short-range wireless communication technology George employed in the above scenario?

- A. MQTT
- B. LPWAN
- C. Zigbee
- D. NB-IoT

**Answer: C**

**Explanation:**

Zigbee could be a wireless technology developed as associate open international normal to deal with the unique desires of affordable, low-power wireless IoT networks. The Zigbee normal operates on the IEEE 802.15.4 physical radio specification and operates in unauthorised bands as well as a pair of 4 GHz, 900 MHz and 868 MHz.

The 802.15.4 specification upon that the Zigbee stack operates gained confirmation by the Institute of Electrical and physical science Engineers (IEEE) in 2003. The specification could be a packet-based radio protocol supposed for affordable, battery-operated devices. The protocol permits devices to speak in an exceedingly kind of network topologies and may have battery life lasting many years.

The Zigbee three.0 Protocol

The Zigbee protocol has been created and ratified by member corporations of the Zigbee Alliance. Over three hundred leading semiconductor makers, technology corporations, OEMs and repair corporations comprise the Zigbee Alliance membership. The Zigbee protocol was designed to supply associate easy-to-use wireless information answer characterised by secure, reliable wireless network architectures.

**THE ZIGBEE ADVANTAGE**

The Zigbee 3.0 protocol is intended to speak information through rip-roaring RF environments that area unit common in business and industrial applications. Version 3.0 builds on the prevailing Zigbee normal however unifies the market-specific application profiles to permit all devices to be wirelessly connected within the same network, no matter their market designation and performance. what is more, a Zigbee 3.0 certification theme ensures the ability of product from completely different makers. Connecting Zigbee three.0 networks to the information science domain unveil observance and management from devices like smartphones and tablets on a local area network or WAN, as well as the web, and brings verity net of Things to fruition.

Zigbee protocol options include:

- ? Support for multiple network topologies like point-to-point, point-to-multipoint and mesh networks
- ? Low duty cycle – provides long battery life
- ? Low latency
- ? Direct Sequence unfold Spectrum (DSSS)
- ? Up to 65,000 nodes per network
- ? 128-bit AES encryption for secure information connections
- ? Collision avoidance, retries and acknowledgements

This is another short-range communication protocol based on the IEEE 203.15.4 standard. Zig-Bee is used in devices that transfer data infrequently at a low rate in a restricted area and within a range of 10–100 m.

**NEW QUESTION 92**

- (Topic 2)

Daniel Is a professional hacker who Is attempting to perform an SQL injection attack on a target website. www.movlescope.com. During this process, he encountered an IDS that detects SQL Injection attempts based on predefined signatures. To evade any comparison statement, he attempted placing characters such as ' or '1='1' In any bask injection statement such as " or 1=1." Identify the evasion technique used by Daniel in the above scenario.

- A. Null byte
- B. IP fragmentation
- C. Char encoding
- D. Variation

**Answer: D**

**Explanation:**

One may append the comment ??–?? operator along with the String for the username and whole avoid executing the password segment of the SQL query. Everything when the — operator would be considered as comment and not dead.

To launch such an attack, the value passed for name could be ??OR ??1??=??1?? ; —Statement = ??SELECT \* FROM ??CustomerDB?? WHERE ??name?? = ?? ??+ userName + ?? ?? AND ??password?? = ?? ?? + passwd + ?? ?? ; ??

Statement = ??SELECT \* FROM ??CustomerDB?? WHERE ??name?? = ?? ?? OR ??1??=??1??;- + ?? ?? AND ??password?? = ?? ?? + passwd + ?? ?? ; ?? All the records from the customer database would be listed.

Yet, another variation of the SQL Injection Attack can be conducted in dbms systems that allow multiple SQL injection statements. Here, we will also create use of the vulnerability in sure dbms whereby a user provided field isn??t strongly used in or isn??t checked for sort constraints.

This could take place once a numeric field is to be employed in a SQL statement; but, the programmer makes no checks to validate that the user supplied input is numeric.

Variation is an evasion technique whereby the attacker can easily evade any comparison statement. The attacker does this by placing characters such as '??' or '1='1'?? in any basic injection statement such as ??or 1=1?? or with other accepted SQL comments.

Evasion Technique: Variation is an evasion technique whereby the attacker can easily evade any comparison statement. The attacker does this by placing characters such as '??' or '1='1'?? in any basic injection statement such as ??or 1=1?? or with other accepted SQL comments. The SQL interprets this as a comparison between two strings or characters instead of two numeric values. As the evaluation of two strings yields a true statement, similarly, the evaluation of two numeric values yields a true statement, thus rendering the evaluation of the complete query unaffected. It is also possible to write many other signatures; thus, there are infinite possibilities of variation as well. The main aim of the attacker is to have a WHERE statement that is always evaluated as ??true?? so that any mathematical or string comparison can be used, where the SQL can perform the same.

#### NEW QUESTION 95

- (Topic 2)

You went to great lengths to install all the necessary technologies to prevent hacking attacks, such as expensive firewalls, antivirus software, anti-spam systems and intrusion detection/prevention tools in your company's network. You have configured the most secure policies and tightened every device on your network. You are confident that hackers will never be able to gain access to your network with complex security system in place.

Your peer, Peter Smith who works at the same department disagrees with you.

He says even the best network security technologies cannot prevent hackers gaining access to the network because of presence of "weakest link" in the security chain.

What is Peter Smith talking about?

- A. Untrained staff or ignorant computer users who inadvertently become the weakest link in your security chain
- B. "zero-day" exploits are the weakest link in the security chain since the IDS will not be able to detect these attacks
- C. "Polymorphic viruses" are the weakest link in the security chain since the Anti-Virus scanners will not be able to detect these attacks
- D. Continuous Spam e-mails cannot be blocked by your security system since spammers use different techniques to bypass the filters in your gateway

**Answer:** A

#### NEW QUESTION 98

- (Topic 2)

What is the purpose of DNS AAAA record?

- A. Authorization, Authentication and Auditing record
- B. Address prefix record
- C. Address database record
- D. IPv6 address resolution record

**Answer:** D

#### NEW QUESTION 102

- (Topic 2)

is a tool that can hide processes from the process list, can hide files, registry entries, and intercept keystrokes.

- A. Trojan
- B. RootKit
- C. DoS tool
- D. Scanner
- E. Backdoor

**Answer:** B

#### NEW QUESTION 105

- (Topic 2)

Bob, your senior colleague, has sent you a mail regarding a deal with one of the clients. You are requested to accept the offer and you oblige. After 2 days. Bob denies that he had ever sent a mail. What do you want to ""know"" to prove yourself that it was Bob who had send a mail?

- A. Authentication
- B. Confidentiality
- C. Integrity
- D. Non-Repudiation

**Answer:** D

#### Explanation:

Non-repudiation is the assurance that someone cannot deny the validity of something.

Non-repudiation is a legal concept that is widely used in information security and refers to a service, which provides proof of the origin of data and the integrity of the data. In other words, non-repudiation makes it very difficult to successfully deny who/where a message came from as well as the authenticity and integrity of that message.

#### NEW QUESTION 107

- (Topic 2)

Every company needs a formal written document which spells out to employees precisely what they are allowed to use the company's systems for, what is prohibited, and what will happen to them if they break the rules. Two printed copies of the policy should be given to every employee as soon as possible after they join the organization. The employee should be asked to sign one copy, which should be safely filed by the company. No one should be allowed to use the company's computer systems until they have signed the policy in acceptance of its terms.

What is this document called?

- A. Information Audit Policy (IAP)
- B. Information Security Policy (ISP)
- C. Penetration Testing Policy (PTP)

D. Company Compliance Policy (CCP)

**Answer:** B

#### NEW QUESTION 109

- (Topic 2)

David is a security professional working in an organization, and he is implementing a vulnerability management program in the organization to evaluate and control the risks and vulnerabilities in its IT infrastructure. He is currently executing the process of applying fixes on vulnerable systems to reduce the impact and severity of vulnerabilities. Which phase of the vulnerability-management life cycle is David currently in?

- A. verification
- B. Risk assessment
- C. Vulnerability scan
- D. Remediation

**Answer:** D

#### Explanation:

Vulnerability-Management Life Cycle The vulnerability management life cycle is an important process that helps identify and remediate security weaknesses before they can be exploited. 4.Remediation - applying fixes on vulnerable systems in order to reduce the impact and severity of vulnerabilities. (P.515/499)

#### NEW QUESTION 112

- (Topic 2)

Jane, an ethical hacker, is testing a target organization's web server and website to identify security loopholes. In this process, she copied the entire website and its content on a local drive to view the complete profile of the site's directory structure, file structure, external links, images, web pages, and so on. This information helps Jane map the website's directories and gain valuable information. What is the attack technique employed by Jane in the above scenario?

- A. website mirroring
- B. Session hijacking
- C. Web cache poisoning
- D. Website defacement

**Answer:** A

#### Explanation:

A mirror site may be a website or set of files on a computer server that has been copied to a different computer server in order that the location or files are available from quite one place. A mirror site has its own URL, but is otherwise just like the principal site. Load-balancing devices allow high-volume sites to scale easily, dividing the work between multiple mirror sites. A mirror site is typically updated frequently to make sure it reflects the contents of the first site. In some cases, the first site may arrange for a mirror site at a bigger location with a better speed connection and, perhaps, a better proximity to an outsized audience. If the first site generates an excessive amount of traffic, a mirror site can ensure better availability of the web site or files. For websites that provide copies or updates of widely used software, a mirror site allows the location to handle larger demands and enables the downloaded files to arrive more quickly. Microsoft, Sun Microsystems and other companies have mirror sites from which their browser software are often downloaded. Mirror sites are used to make site access faster when the first site could also be geographically distant from those accessing it. A mirrored web server is usually located on a special continent from the principal site, allowing users on the brink of the mirror site to urge faster and more reliable access. Mirroring an internet site also can be done to make sure that information are often made available to places where access could also be unreliable or censored. In 2013, when Chinese authorities blocked access to foreign media outlets just like the Wall Street Journal and Reuters, site mirroring was used to restore access and circumvent government censorship.

#### NEW QUESTION 116

- (Topic 2)

What is the first step for a hacker conducting a DNS cache poisoning (DNS spoofing) attack against an organization?

- A. The attacker queries a nameserver using the DNS resolver.
- B. The attacker makes a request to the DNS resolver.
- C. The attacker forges a reply from the DNS resolver.
- D. The attacker uses TCP to poison the DNS resolver.

**Answer:** B

#### Explanation:

[https://ru.wikipedia.org/wiki/DNS\\_spoofing](https://ru.wikipedia.org/wiki/DNS_spoofing)

DNS spoofing is a threat that copies the legitimate server destinations to divert the domain's traffic. Ignorant of these attacks, the users are redirected to malicious websites, which results in insensitive and personal data being leaked. It is a method of attack where your DNS server is tricked into saving a fake DNS entry. This will make the DNS server recall a fake site for you, thereby posing a threat to vital information stored on your server or computer.

The cache poisoning codes are often found in URLs sent through spam emails. These emails are sent to prompt users to click on the URL, which infects their computer. When the computer is poisoned, it will divert you to a fake IP address that looks like a real thing. This way, the threats are injected into your systems as well.

Different Stages of Attack of DNS Cache Poisoning:

- The attacker proceeds to send DNS queries to the DNS resolver, which forwards the Root/TLD authoritative DNS server request and awaits an answer.
- The attacker overloads the DNS with poisoned responses that contain several IP addresses of the malicious website. To be accepted by the DNS resolver, the attacker's response should match a port number and the query ID field before the DNS response. Also, the attackers can force its response to increasing their chance of success.
- If you are a legitimate user who queries this DNS resolver, you will get a poisoned response from the cache, and you will be automatically redirected to the malicious website.

#### NEW QUESTION 119

- (Topic 2)

Matthew, a black hat, has managed to open a meterpreter session to one of the kiosk machines in Evil Corp's lobby. He checks his current SID, which is S-1-5-21-1223352397-1872883824-861252104-501. What needs to happen before Matthew has full administrator access?

- A. He must perform privilege escalation.
- B. He needs to disable antivirus protection.
- C. He needs to gain physical access.
- D. He already has admin privileges, as shown by the ??501?? at the end of the SID.

**Answer:** A

#### NEW QUESTION 123

- (Topic 2)

You are trying to break into a highly classified top-secret mainframe computer with highest security system in place at Merclyn Barley Bank located in Los Angeles. You know that conventional hacking doesn't work in this case, because organizations such as banks are generally tight and secure when it comes to protecting their systems.

In other words, you are trying to penetrate an otherwise impenetrable system. How would you proceed?

- A. Look for "zero-day" exploits at various underground hacker websites in Russia and China and buy the necessary exploits from these hackers and target the bank's network
- B. Try to hang around the local pubs or restaurants near the bank, get talking to a poorly- paid or disgruntled employee, and offer them money if they'll abuse their access privileges by providing you with sensitive information
- C. Launch DDOS attacks against Merclyn Barley Bank's routers and firewall systems using 100, 000 or more "zombies" and "bots"
- D. Try to conduct Man-in-the-Middle (MiTM) attack and divert the network traffic going to the Merclyn Barley Bank's Webserver to that of your machine using DNS Cache Poisoning techniques

**Answer:** B

#### NEW QUESTION 125

- (Topic 2)

You have successfully logged on a Linux system. You want to now cover your trade Your login attempt may be logged on several files located in /var/log. Which file does NOT belongs to the list:

- A. user.log
- B. auth.fesg
- C. wtmp
- D. btmp

**Answer:** C

#### NEW QUESTION 130

- (Topic 2)

You work for Acme Corporation as Sales Manager. The company has tight network security restrictions. You are trying to steal data from the company's Sales database (Sales.xls) and transfer them to your home computer. Your company filters and monitors traffic that leaves from the internal network to the Internet. How will you achieve this without raising suspicion?

- A. Encrypt the Sales.xls using PGP and e-mail it to your personal gmail account
- B. Package the Sales.xls using Trojan wrappers and telnet them back your home computer
- C. You can conceal the Sales.xls database in another file like photo.jpg or other files and send it out in an innocent looking email or file transfer using Steganography techniques
- D. Change the extension of Sales.xls to sales.txt and upload them as attachment to your hotmail account

**Answer:** C

#### NEW QUESTION 133

- (Topic 2)

Alice, a professional hacker, targeted an organization's cloud services. She infiltrated the targets MSP provider by sending spear-phishing emails and distributed custom-made malware to compromise user accounts and gain remote access to the cloud service. Further, she accessed the target customer profiles with her MSP account, compressed the customer data, and stored them in the MSP. Then, she used this information to launch further attacks on the target organization. Which of the following cloud attacks did Alice perform in the above scenario?

- A. Cloud hopper attack
- B. Cloud cryptojacking
- C. Cloudborne attack
- D. Man-in-the-cloud (MITC) attack

**Answer:** A

#### Explanation:

Operation Cloud Hopper was an in depth attack and theft of data in 2017 directed at MSP within the uk (U.K.), us (U.S.), Japan, Canada, Brazil, France, Switzerland, Norway, Finland, Sweden, South Africa , India, Thailand, South Korea and Australia. The group used MSP as intermediaries to accumulate assets and trade secrets from MSP client engineering, MSP industrial manufacturing, retail, energy, pharmaceuticals, telecommunications, and government agencies. Operation Cloud Hopper used over 70 variants of backdoors, malware and trojans. These were delivered through spear-phishing emails. The attacks scheduled tasks or leveraged services/utilities to continue Microsoft Windows systems albeit the pc system was rebooted. It installed malware and hacking tools to access systems and steal data.

#### NEW QUESTION 134

- (Topic 2)

Which of the following DoS tools is used to attack target web applications by starvation of available sessions on the web server? The tool keeps sessions at halt using never-ending POST transmissions and sending an arbitrarily large content-length header value.

- A. My Doom

- B. Astacheldraht
- C. R-U-Dead-Yet?(RUDY)
- D. LOIC

**Answer: C**

**NEW QUESTION 139**

- (Topic 2)

Gilbert, a web developer, uses a centralized web API to reduce complexity and increase the Integrity of updating and changing data. For this purpose, he uses a web service that uses HTTP methods such as PUT, POST, GET, and DELETE and can improve the overall performance, visibility, scalability, reliability, and portability of an application. What is the type of web-service API mentioned in the above scenario?

- A. JSON-RPC
- B. SOAP API
- C. RESTful API
- D. REST API

**Answer: C**

**Explanation:**

\*REST is not a specification, tool, or framework, but instead is an architectural style for web services that serves as a communication medium between various systems on the web. \*RESTful APIs, which are also known as RESTful services, are designed using REST principles and HTTP communication protocols RESTful is a collection of resources that use HTTP methods such as PUT, POST, GET, and DELETE

RESTful API: RESTful API is a RESTful service that is designed using REST principles and HTTP communication protocols. RESTful is a collection of resources that use HTTP methods such as PUT, POST, GET, and DELETE. RESTful API is also designed to make applications independent to improve the overall performance, visibility, scalability, reliability, and portability of an application. APIs with the following features can be referred to as to RESTful APIs: o Stateless: The client end stores the state of the session; the server is restricted to save data during the request processing o Cacheable: The client should save responses (representations) in the cache. This feature can enhance API performance pg. 1920 CEHv11 manual.

<https://cloud.google.com/files/apigee/apigee-web-api-design-the-missing-link-ebook.pdf>

The HTTP methods GET, POST, PUT or PATCH, and DELETE can be used with these templates to read, create, update, and delete description resources for dogs and their owners. This API style has become popular for many reasons. It is straightforward and intuitive, and learning this pattern is similar to learning a programming language API. APIs like this one are commonly called RESTful APIs, although they do not display all of the characteristics that define REST (more on REST later).

**NEW QUESTION 143**

- (Topic 2)

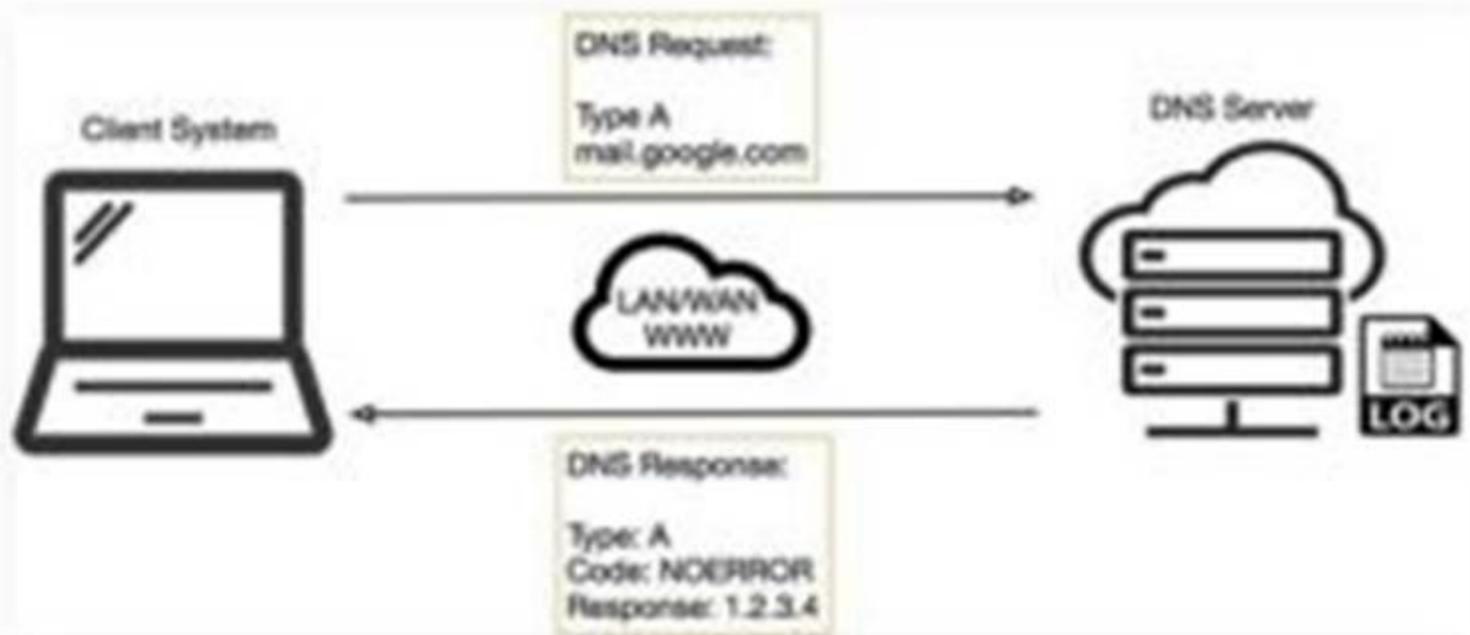
Robin, an attacker, is attempting to bypass the firewalls of an organization through the DNS tunneling method in order to exfiltrate data. He is using the NSTX tool for bypassing the firewalls. On which of the following ports should Robin run the NSTX tool?

- A. Port 53
- B. Port 23
- C. Port 50
- D. Port 80

**Answer: A**

**Explanation:**

DNS uses Ports 53 which is almost always open on systems, firewalls, and clients to transmit DNS queries. instead of the more familiar Transmission Control Protocol (TCP) these queries use User Datagram Protocol (UDP) due to its low-latency, bandwidth and resource usage compared TCP-equivalent queries. UDP has no error or flow-control capabilities, nor does it have any integrity checking to make sure the info arrived intact.How is internet use (browsing, apps, chat etc) so reliable then? If the UDP DNS query fails (it??s a best-effort protocol after all) within the first instance, most systems will retry variety of times and only after multiple failures, potentially switch to TCP before trying again; TCP is additionally used if the DNS query exceeds the restrictions of the UDP datagram size – typically 512 bytes for DNS but can depend upon system settings.Figure 1 below illustrates the essential process of how DNS operates: the client sends a question string (for example, mail.google[.]com during this case) with a particular type – typically A for a number address. I??ve skipped the part whereby intermediate DNS systems may need to establish where ??com?? exists, before checking out where ??google[.]com?? are often found, and so on.



Many worms and scanners are created to seek out and exploit systems running telnet. Given these facts, it??s really no surprise that telnet is usually seen on the highest Ten Target Ports list. Several of the vulnerabilities of telnet are fixed. They require only an upgrade to the foremost current version of the telnet Daemon or OS upgrade. As is usually the case, this upgrade has not been performed on variety of devices. this might flow from to the very fact that a lot of systems administrators and users don??t fully understand the risks involved using telnet. Unfortunately, the sole solution for a few of telnets vulnerabilities is to completely

discontinue its use. the well-liked method of mitigating all of telnets vulnerabilities is replacing it with alternate protocols like ssh. Ssh is capable of providing many of an equivalent functions as telnet and a number of other additional services typical handled by other protocols like FTP and Xwindows. Ssh does still have several drawbacks to beat before it can completely replace telnet. it??s typically only supported on newer equipment. It requires processor and memory resources to perform the info encryption and decryption. It also requires greater bandwidth than telnet thanks to the encryption of the info . This paper was written to assist clarify how dangerous the utilization of telnet are often and to supply solutions to alleviate the main known threats so as to enhance the general security of the web Once a reputation is resolved to an IP caching also helps: the resolved name-to-IP is usually cached on the local system (and possibly on intermediate DNS servers) for a period of your time . Subsequent queries for an equivalent name from an equivalent client then don??t leave the local system until said cache expires. Of course, once the IP address of the remote service is understood , applications can use that information to enable other TCP- based protocols, like HTTP, to try to to their actual work, for instance ensuring internet cat GIFs are often reliably shared together with your colleagues. So, beat all, a couple of dozen extra UDP DNS queries from an organization??s network would be fairly inconspicuous and will leave a malicious payload to beacon bent an adversary; commands could even be received to the requesting application for processing with little difficulty.

#### NEW QUESTION 144

- (Topic 2)

OpenSSL on Linux servers includes a command line tool for testing TLS. What is the name of the tool and the correct syntax to connect to a web server?

- A. openssl s\_client -site www.website.com:443
- B. openssl\_client -site www.website.com:443
- C. openssl s\_client -connect www.website.com:443
- D. openssl\_client -connect www.website.com:443

**Answer:** C

#### NEW QUESTION 145

- (Topic 2)

An attacker redirects the victim to malicious websites by sending them a malicious link by email. The link appears authentic but redirects the victim to a malicious web page, which allows the attacker to steal the victim's data. What type of attack is this?

- A. Phishing
- B. Vishing
- C. Spoofing
- D. DDoS

**Answer:** A

#### Explanation:

<https://en.wikipedia.org/wiki/Phishing>

Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message. The recipient is then tricked into clicking a malicious link, which can lead to the installation of malware, the freezing of the system as part of a ransomware attack, or the revealing of sensitive information.

An attack can have devastating results. For individuals, this includes unauthorized purchases, the stealing of funds, or identify theft.

Moreover, phishing is often used to gain a foothold in corporate or governmental networks as a part of a larger attack, such as an advanced persistent threat (APT) event. In this latter

scenario, employees are compromised in order to bypass security perimeters, distribute malware inside a closed environment, or gain privileged access to secured data.

An organization succumbing to such an attack typically sustains severe financial losses in addition to declining market share, reputation, and consumer trust.

Depending on the scope, a phishing attempt might escalate into a security incident from which a business will have a difficult time recovering.

#### NEW QUESTION 149

- (Topic 2)

The network administrator at Spears Technology, Inc has configured the default gateway Cisco router's access-list as below:

You are hired to conduct security testing on their network.

You successfully brute-force the SNMP community string using a SNMP crack tool. The access-list configured at the router prevents you from establishing a successful connection.

You want to retrieve the Cisco configuration from the router. How would you proceed?

- A. Use the Cisco's TFTP default password to connect and download the configuration file
- B. Run a network sniffer and capture the returned traffic with the configuration file from the router
- C. Run Generic Routing Encapsulation (GRE) tunneling protocol from your computer to the router masking your IP address
- D. Send a customized SNMP set request with a spoofed source IP address in the range - 192.168.1.0

**Answer:** BD

#### NEW QUESTION 154

- (Topic 2)

You need a tool that can do network intrusion prevention and intrusion detection, function as a network sniffer, and record network activity, what tool would you most likely select?

- A. Nmap
- B. Cain & Abel
- C. Nessus
- D. Snort

**Answer:** D

#### NEW QUESTION 158

- (Topic 2)

Log monitoring tools performing behavioral analysis have alerted several suspicious logins on a Linux server occurring during non-business hours. After further examination of all login activities, it is noticed that none of the logins have occurred during typical work hours. A Linux administrator who is investigating this problem realizes the system time on the Linux server is wrong by more than twelve hours. What protocol used on Linux servers to synchronize the time has stopped working?

- A. Time Keeper
- B. NTP
- C. PPP
- D. OSPP

**Answer: B**

#### NEW QUESTION 159

- (Topic 2)

Robin, a professional hacker, targeted an organization's network to sniff all the traffic. During this process.

Robin plugged in a rogue switch to an unused port in the LAN with a priority lower than any other switch in the network so that he could make it a root bridge that will later allow him to sniff all the traffic in the network.

What is the attack performed by Robin in the above scenario?

- A. ARP spoofing attack
- B. VLAN hopping attack
- C. DNS poisoning attack
- D. STP attack

**Answer: D**

#### Explanation:

STP prevents bridging loops in a redundant switched network environment. By avoiding loops, you can ensure that broadcast traffic does not become a traffic storm. STP is a hierarchical tree-like topology with a "root" switch at the top. A switch is elected as root based on the lowest configured priority of any switch (0 through 65,535). When a switch boots up, it begins a process of identifying other switches and determining the root bridge. After a root bridge is elected, the topology is established from its perspective of the connectivity. The switches determine the path to the root bridge, and all redundant paths are blocked. STP sends configuration and topology change notifications and acknowledgments (TCN/TCA) using bridge protocol data units (BPDU).

An STP attack involves an attacker spoofing the root bridge in the topology. The attacker broadcasts out an STP configuration/topology change BPDU in an attempt to force an STP recalculation. The BPDU sent out announces that the attacker's system has a lower bridge priority. The attacker can then see a variety of frames forwarded from other switches to it. STP recalculation may also cause a denial-of-service (DoS) condition on the network by causing an interruption of 30 to 45 seconds each time the root bridge changes. An attacker using STP network topology changes to force its host to be elected as the root bridge.

#### NEW QUESTION 163

- (Topic 2)

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 structure of the server.

What kind of attack is possible in this scenario?

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

**Answer: D**

#### Explanation:

Appropriately controlling admittance to web content is significant for running a safe web worker. Index crossing or Path Traversal is a HTTP assault which permits aggressors to get to limited catalogs and execute orders outside of the web worker's root registry. Web workers give two primary degrees of security instruments ? Access Control Lists (ACLs) ? Root index

An Access Control List is utilized in the approval cycle. It is a rundown which the web worker's manager uses to show which clients or gatherings can get to, change or execute specific records on the worker, just as other access rights.

The root registry is a particular index on the worker record framework in which the clients are kept. Clients can't get to anything over this root.

For instance: the default root registry of IIS on Windows is C:\inetpub\wwwroot and with this arrangement, a client doesn't approach C:\Windows yet approaches C:\inetpub\wwwroot\news and some other indexes and documents under the root catalog (given that the client is confirmed by means of the ACLs).

The root index keeps clients from getting to any documents on the worker, for example, C:\WINDOWS\system32\win.ini on Windows stages and the/and so on/passwd record on Linux/UNIX stages.

This weakness can exist either in the web worker programming itself or in the web application code.

To play out a registry crossing assault, all an assailant requires is an internet browser and some information on where to aimlessly discover any default documents and registries on the framework.

What an assailant can do if your site is defenseless With a framework defenseless against index crossing, an aggressor can utilize this weakness to venture out of the root catalog and access different pieces of the record framework. This may enable the assailant to see confined documents, which could give the aggressor more data needed to additional trade off the framework.

Contingent upon how the site access is set up, the aggressor will execute orders by mimicking himself as the client which is related with "the site". Along these lines everything relies upon what the site client has been offered admittance to in the framework. Illustration of a Directory Traversal assault by means of web application code In web applications with dynamic pages, input is generally gotten from programs through GET or POST solicitation techniques. Here is an illustration of a HTTP GET demand URL

GET http://test.webarticles.com/show.asp?view=oldarchive.html HTTP/1.1 Host: test.webarticles.com

With this URL, the browser requests the dynamic page show.asp from the server and with it also sends the parameter view with the value of oldarchive.html. When this request is

executed on the web server, show.asp retrieves the file oldarchive.html from the server's file system, renders it and then sends it back to the browser which displays it to the user.

The attacker would assume that show.asp can retrieve files from the file system and sends the following custom URL.

GET http://test.webarticles.com/show.asp?view=../../../../../Windows/system.ini HTTP/1.1 Host: test.webarticles.com  
 This will cause the dynamic page to retrieve the file system.ini from the file system and display it to the user. The expression ../ instructs the system to go one directory up which is commonly used as an operating system directive. The attacker has to guess how many directories he has to go up to find the Windows folder on the system, but this is easily done by trial and error.  
 Example of a Directory Traversal attack via web server Apart from vulnerabilities in the code, even the web server itself can be open to directory traversal attacks. The problem can either be incorporated into the web server software or inside some sample script files left available on the server. The vulnerability has been fixed in the latest versions of web server software, but there are web servers online which are still using older versions of IIS and Apache which might be open to directory traversal attacks. Even though you might be using a web server software version that has fixed this vulnerability, you might still have some sensitive default script directories exposed which are well known to hackers.  
 For example, a URL request which makes use of the scripts directory of IIS to traverse directories and execute a command can be  
 GET http://server.com/scripts/..%5c../Windows/System32/cmd.exe?/c+dir+c:\ HTTP/1.1 Host: server.com  
 The request would return to the user a list of all files in the C:\ directory by executing the cmd.exe command shell file and run the command dir c:\ in the shell. The %5c expression that is in the URL request is a web server escape code which is used to represent normal characters. In this case %5c represents the character \.  
 Newer versions of modern web server software check for these escape codes and do not let them through. Some older versions however, do not filter out these codes in the root directory enforcer and will let the attackers execute such commands.

**NEW QUESTION 165**

- (Topic 2)

While examining audit logs, you discover that people are able to telnet into the SMTP server on port 25. You would like to block this, though you do not see any evidence of an attack or other wrong doing. However, you are concerned about affecting the normal functionality of the email server. From the following options choose how best you can achieve this objective?

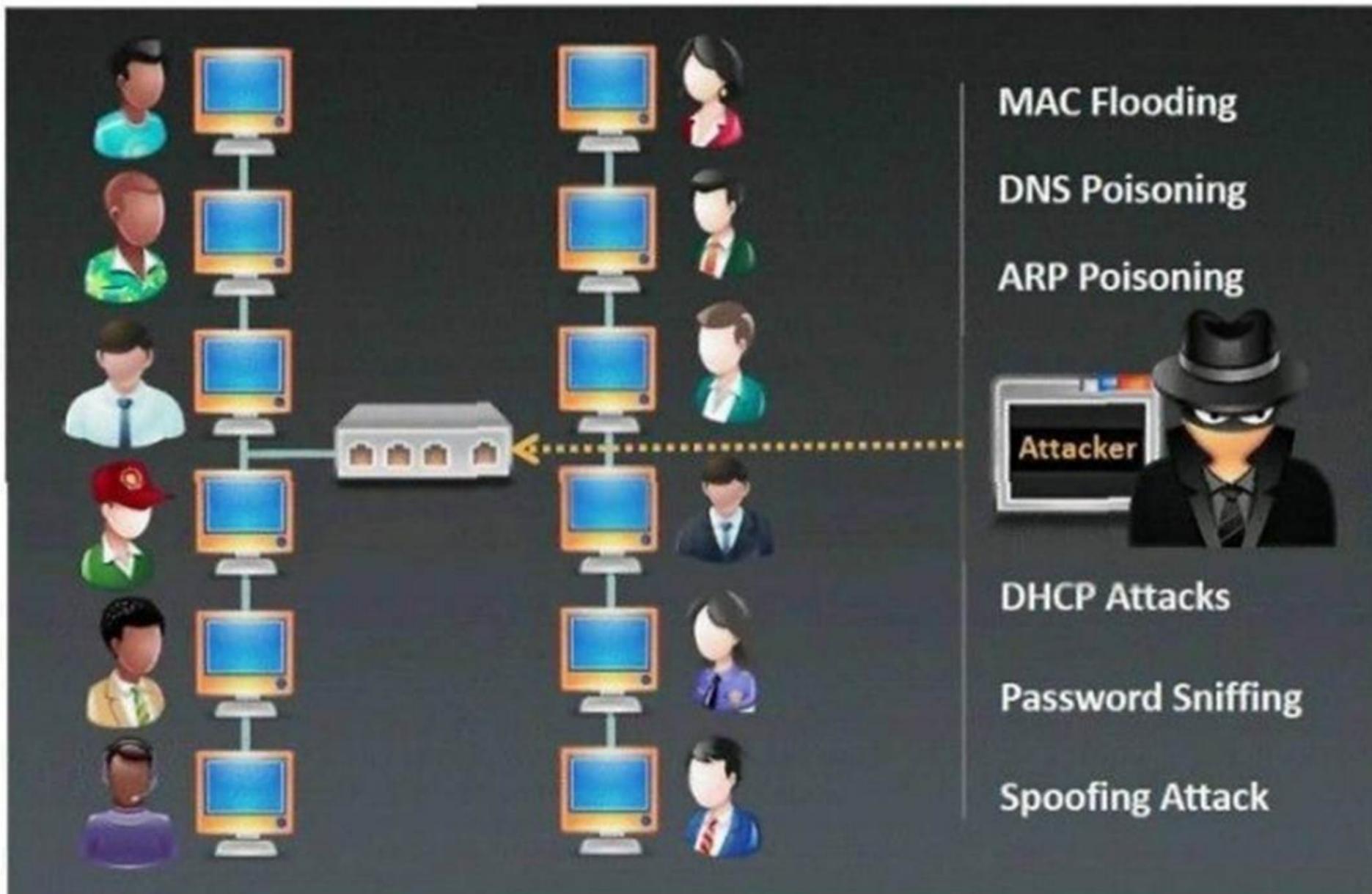
- A. Block port 25 at the firewall.
- B. Shut off the SMTP service on the server.
- C. Force all connections to use a username and password.
- D. Switch from Windows Exchange to UNIX Sendmail.
- E. None of the above.

**Answer: E**

**NEW QUESTION 167**

- (Topic 2)

Which type of sniffing technique is generally referred as MiTM attack?



- A. Password Sniffing
- B. ARP Poisoning
- C. Mac Flooding
- D. DHCP Sniffing

Answer: B

**NEW QUESTION 168**

- (Topic 2)

During the enumeration phase, Lawrence performs banner grabbing to obtain information such as OS details and versions of services running. The service that he enumerated runs directly on TCP port 445.

Which of the following services is enumerated by Lawrence in this scenario?

- A. Server Message Block (SMB)
- B. Network File System (NFS)
- C. Remote procedure call (RPC)
- D. Telnet

Answer: A

**Explanation:**

Worker Message Block (SMB) is an organization document sharing and information texture convention. SMB is utilized by billions of gadgets in a different arrangement of working frameworks, including Windows, MacOS, iOS, Linux, and Android. Customers use SMB to get to information on workers. This permits sharing of records, unified information the board, and brought down capacity limit needs for cell phones. Workers additionally use SMB as a feature of the Software-characterized Data Center for outstanding burdens like grouping and replication.

Since SMB is a far off record framework, it requires security from assaults where a Windows PC may be fooled into reaching a pernicious worker running inside a confided in organization or to a far off worker outside the organization edge. Firewall best practices and arrangements can upgrade security keeping malevolent traffic from leaving the PC or its organization.

For Windows customers and workers that don't have SMB shares, you can obstruct all inbound SMB traffic utilizing the Windows Defender Firewall to keep far off associations from malignant or bargained gadgets. In the Windows Defender Firewall, this incorporates the accompanying inbound principles.

Name	Profile	Enabled
File and Printer Sharing (SMB-In)	All	No
Netlogon Service (NP-In)	All	No
Remote Event Log Management (NP-In)	All	No
Remote Service Management (NP-In)	All	No

You should also create a new blocking rule to override any other inbound firewall rules. Use the following suggested settings for any Windows clients or servers that do not host SMB Shares:

? Name: Block all inbound SMB 445

? Description: Blocks all inbound SMB TCP 445 traffic. Not to be applied to domain controllers or computers that host SMB shares.

? Action: Block the connection

? Programs: All

? Remote Computers: Any

? Protocol Type: TCP

? Local Port: 445

? Remote Port: Any

? Profiles: All

? Scope (Local IP Address): Any

? Scope (Remote IP Address): Any

? Edge Traversal: Block edge traversal

You must not globally block inbound SMB traffic to domain controllers or file servers. However, you can restrict access to them from trusted IP ranges and devices to lower their attack surface. They should also be restricted to Domain or Private firewall profiles and not allow Guest/Public traffic.

**NEW QUESTION 172**

- (Topic 2)

Why containers are less secure than virtual machines?

- A. Host OS on containers has a larger surface attack.
- B. Containers may full fill disk space of the host.
- C. A compromise container may cause a CPU starvation of the host.
- D. Containers are attached to the same virtual network.

Answer: A

**NEW QUESTION 177**

- (Topic 2)

What hacking attack is challenge/response authentication used to prevent?

- A. Replay attacks
- B. Scanning attacks
- C. Session hijacking attacks
- D. Password cracking attacks

**Answer:** A

#### NEW QUESTION 180

- (Topic 2)

Bob, an attacker, has managed to access a target IoT device. He employed an online tool to gather information related to the model of the IoT device and the certifications granted to it. Which of the following tools did Bob employ to gather the above Information?

- A. search.com
- B. EarthExplorer
- C. Google image search
- D. FCC ID search

**Answer:** D

#### Explanation:

Footprinting techniques are used to collect basic information about the target IoT and OT platforms to exploit them. Information collected through footprinting techniques includes IP address, hostname, ISP, device location, banner of the target IoT device, FCC ID information, certification granted to the device, etc. pg. 5052 ECHv11 manual

[https://en.wikipedia.org/wiki/FCC\\_mark](https://en.wikipedia.org/wiki/FCC_mark)

An FCC ID is a unique identifier assigned to a device registered with the United States Federal Communications Commission. For legal sale of wireless devices in the US, manufacturers must:

- Have the device evaluated by an independent lab to ensure it conforms to FCC standards
- Provide documentation to the FCC of the lab results
- Provide User Manuals, Documentation, and Photos relating to the device
- Digitally or physically label the device with the unique identifier provided by the FCC (upon approved application)

The FCC gets its authority from Title 47 of the Code of Federal Regulations (47 CFR). FCC IDs are required for all wireless emitting devices sold in the USA. By searching an FCC ID, you can find details on the wireless operating frequency (including strength), photos of the device, user manuals for the device, and SAR reports on the wireless emissions

#### NEW QUESTION 181

- (Topic 2)

In the context of password security, a simple dictionary attack involves loading a dictionary file (a text file full of dictionary words) into a cracking application such as L0phtCrack or John the Ripper, and running it against user accounts located by the application. The larger the word and word fragment selection, the more effective the dictionary attack is. The brute force method is the most inclusive, although slow. It usually tries every possible letter and number combination in its automated exploration. If you would use both brute force and dictionary methods combined together to have variation of words, what would you call such an attack?

- A. Full Blown
- B. Thorough
- C. Hybrid
- D. BruteDics

**Answer:** C

#### NEW QUESTION 184

- (Topic 2)

Taylor, a security professional, uses a tool to monitor her company's website, analyze the website's traffic, and track the geographical location of the users visiting the company's website. Which of the following tools did Taylor employ in the above scenario?

- A. WebSite Watcher
- B. web-Stat
- C. Webroot
- D. WAFW00F

**Answer:** B

#### Explanation:

Increase your web site's performance and grow! Add Web-Stat to your site (it's free!) and watch individuals act together with your pages in real time. Learn how individuals realize your web site. Get details concerning every visitor's path through your web site and track pages that flip browsers into consumers. One-click install. observe locations, in operation systems, browsers and screen sizes and obtain alerts for new guests and conversions

#### NEW QUESTION 186

- (Topic 3)

Attempting an injection attack on a web server based on responses to True/False QUESTION NO:s is called which of the following?

- A. Compound SQLi
- B. Blind SQLi
- C. Classic SQLi
- D. DMS-specific SQLi

**Answer:** B

#### Explanation:

[https://en.wikipedia.org/wiki/SQL\\_injection#Blind\\_SQL\\_injection](https://en.wikipedia.org/wiki/SQL_injection#Blind_SQL_injection)

Blind SQL injection is used when a web application is vulnerable to an SQL injection but the results of the injection are not visible to the attacker. The page with the vulnerability may not be one that displays data but will display differently depending on the results of a logical statement injected into the legitimate SQL statement called for that page. This type of attack has traditionally been considered time-intensive because a new statement needed to be crafted for each bit recovered, and depending on its structure, the attack may consist of many unsuccessful requests. Recent advancements have allowed each request to recover multiple bits, with no unsuccessful requests, allowing for more consistent and efficient extraction.

### NEW QUESTION 190

- (Topic 3)

You're the security manager for a tech company that uses a database to store sensitive customer data. You have implemented countermeasures against SQL injection attacks.

Recently, you noticed some suspicious

activities and suspect an attacker is using SQL injection techniques. The attacker is believed to use different forms of payloads in his SQL queries. In the case of a successful SQL injection attack, which of the following payloads would have the most significant impact?

- A. `??OR 'T='1`: This payload manipulates the WHERE clause of an SQL statement, allowing the attacker to view unauthorized data
- B. `??OR username LIKE '%'`: This payload uses the LIKE operator to search for a specific pattern in a column
- C. `OR ??a??='a; DROP TABLE members; --`: This payload combines the manipulation of the WHERE clause with a destructive action, causing data loss
- D. `UNION SELECT NULL, NULL, NULL --`: This payload manipulates the UNION SQL operator, enabling the attacker to retrieve data from different database tables

**Answer: C**

#### Explanation:

The payload that would have the most significant impact in the case of a successful SQL injection attack is `OR ??a??='a; DROP TABLE members; --`. This payload combines the manipulation of the WHERE clause with a destructive action, causing data loss. This payload works as follows:

? The `OR ??a??='a` part of the payload is a logical expression that is always true, regardless of the input or the condition of the SQL statement. This part of the payload allows the attacker to bypass any authentication or authorization checks that may be implemented in the SQL statement, such as a login form or a search query.

? The `;` part of the payload is a statement terminator that marks the end of the current SQL statement and allows the attacker to inject another SQL statement after it. This part of the payload enables the attacker to execute multiple SQL statements in a single query, which is also known as stacked queries or batched queries.

? The `DROP TABLE members` part of the payload is a destructive SQL statement that deletes the entire table named members from the database. This part of the payload causes data loss and may compromise the functionality and integrity of the application that relies on the table. The table name may vary depending on the target database, but the attacker can use other techniques, such as error-based or union-based SQL injection, to discover the table names before executing the drop statement.

? The `--` part of the payload is a comment symbol that tells the SQL engine to ignore the rest of the query. This part of the payload helps the attacker to avoid any syntax errors or unwanted results that may arise from the original query.

The other options are not as impactful as option C for the following reasons:

? A. `??OR 'T='1`: This payload manipulates the WHERE clause of an SQL statement, allowing the attacker to view unauthorized data. This payload is a common and basic SQL injection technique that injects a logical expression that is always true, such as `'OR 'T='1` or `'OR 1=1`, to bypass the authentication or authorization checks of the SQL statement. This payload can allow the attacker to view data that they are not supposed to, such as user credentials, personal information, or financial records. However, this payload does not cause any data loss or modification, and it does not affect the functionality or integrity of the application.

? B. `??OR username LIKE '%'`: This payload uses the LIKE operator to search for a specific pattern in a column. This payload is a variation of the previous payload that injects a logical expression that is always true, such as `'OR username LIKE '%'` or `'OR 1 LIKE '%'`, to bypass the authentication or authorization checks of the SQL statement. The LIKE operator is used to compare a value with a pattern that may contain wildcard characters, such as `%` or `_`, which match any string or character. This payload can allow the attacker to view data that matches the pattern, such as usernames that start with a certain letter or contain a certain substring. However, this payload does not cause any data loss or modification, and it does not affect the functionality or integrity of the application.

? D. `UNION SELECT NULL, NULL, NULL --`: This payload manipulates the UNION SQL operator, enabling the attacker to retrieve data from different database tables. This payload is an advanced SQL injection technique that injects the UNION SQL operator to combine the results of two or more SELECT statements into a single result set, which is then returned as part of the HTTP response. The UNION operator can be used to join the results from different tables that have the same number and type of columns. The NULL values are used to match the column types and avoid any errors. This payload can allow the attacker to retrieve data from tables that are not intended to be accessed by the application, such as system tables, configuration tables, or backup tables. However, this payload does not cause any data loss or modification, and it does not affect the functionality or integrity of the application.

References:

? 1: SQL Injection - OWASP Foundation

? 2: SQL Injection Payloads: How SQLi exploits work - Bright Security

? 3: SQL Injection - HackTricks

### NEW QUESTION 194

- (Topic 3)

Harris is attempting to identify the OS running on his target machine. He inspected the initial TTL in the IP header and the related TCP window size and obtained the following results:

TTL: 64 Window Size: 5840

What is the OS running on the target machine?

- A. Solaris OS
- B. Windows OS
- C. Mac OS
- D. Linux OS

**Answer: D**

### NEW QUESTION 195

- (Topic 3)

A security analyst is preparing to analyze a potentially malicious program believed to have infiltrated an organization's network. To ensure the safety and integrity of the production environment, the analyst decided to use a sheep dip computer for the analysis. Before initiating the analysis, what key step should the analyst take?

- A. Run the potentially malicious program on the sheep dip computer to determine its behavior
- B. Store the potentially malicious program on an external medium, such as a CD-ROM
- C. Connect the sheep dip computer to the organization's internal network
- D. install the potentially malicious program on the sheep dip computer

**Answer: B**

**Explanation:**

A sheep dip computer is a dedicated device that is used to test inbound files or physical media for viruses, malware, or other harmful content, before they are allowed to be used with other computers. The term sheep dip comes from a method of preventing the spread of parasites in a flock of sheep by dipping the new animals that farmers are adding to the flock in a trough of pesticide. A sheep dip computer is isolated from the organization's network and has port monitors, file monitors, network monitors, and antivirus software installed. Before initiating the analysis of a potentially malicious program, the analyst should store the program on an external medium, such as a CD-ROM, and then insert it into the sheep dip computer. This way, the analyst can prevent the program from infecting other devices or spreading over the network, and can safely analyze its behavior and characteristics.

The other options are not correct steps to take before initiating the analysis. Running the potentially malicious program on the sheep dip computer may cause irreversible damage to the device or compromise its security. Connecting the sheep dip computer to the organization's internal network may expose the network to the risk of infection or attack. Installing the potentially malicious program on the sheep dip computer may not be possible or advisable, as the program may require certain dependencies or permissions that the sheep dip computer does not have or allow. References:

? Sheep dip (computing)

? What Does ??Sheep Dip?? Mean in Cyber Security?

? Malware Analysis

? What is a Sheepdip?

**NEW QUESTION 200**

- (Topic 3)

What useful information is gathered during a successful Simple Mail Transfer Protocol (SMTP) enumeration?

- A. The two internal commands VRFY and EXPN provide a confirmation of valid users, email addresses, aliases, and mailing lists.
- B. Reveals the daily outgoing message limits before mailboxes are locked
- C. The internal command RCPT provides a list of ports open to message traffic.
- D. A list of all mail proxy server addresses used by the targeted host

**Answer: A**

**NEW QUESTION 201**

- (Topic 3)

John, a professional hacker, performs a network attack on a renowned organization and gains unauthorized access to the target network. He remains in the network without being detected for a long time and obtains sensitive information without sabotaging the organization. Which of the following attack techniques is used by John?

- A. Advanced persistent theft
- B. threat Diversion theft
- C. Spear-phishing sites
- D. insider threat

**Answer: A**

**Explanation:**

An advanced persistent threat (APT) may be a broad term wont to describe AN attack campaign within which an intruder, or team of intruders, establishes a bootleg, long presence on a network so as to mine sensitive knowledge.

The targets of those assaults, that square measure terribly fastidiously chosen and researched, usually embrace massive enterprises or governmental networks. the implications of such intrusions square measure huge, and include:

? Intellectual property thieving (e.g., trade secrets or patents)

? Compromised sensitive info (e.g., worker and user personal data)

? The sabotaging of essential structure infrastructures (e.g., information deletion)

? Total website takeovers

Executing an APT assault needs additional resources than a regular internet application attack. The perpetrators square measure typically groups of intimate cybercriminals having substantial resource. Some APT attacks square measure government-funded and used as cyber warfare weapons.

APT attacks dissent from ancient internet application threats, in that:

? They??re considerably additional advanced.

? They??re not hit and run attacks—once a network is infiltrated, the culprit remains so as to realize the maximum amount info as potential.

? They??re manually dead (not automated) against a selected mark and indiscriminately launched against an outsized pool of targets.

? They typically aim to infiltrate a complete network, as opposition one specific half. More common attacks, like remote file inclusion (RFI), SQL injection and cross-site scripting (XSS), square measure oftentimes employed by perpetrators to ascertain a footing in a very targeted network. Next, Trojans and backdoor shells square measure typically wont to expand that foothold and make a persistent presence inside the targeted perimeter.

**NEW QUESTION 203**

- (Topic 3)

Which access control mechanism allows for multiple systems to use a central authentication server (CAS) that permits users to authenticate once and gain access to multiple systems?

- A. Role Based Access Control (RBAC)
- B. Discretionary Access Control (DAC)
- C. Single sign-on
- D. Windows authentication

**Answer: C**

**NEW QUESTION 205**

- (Topic 3)

Jake, a professional hacker, installed spyware on a target iPhone to spy on the target user's activities. He can take complete control of the target mobile device by jailbreaking the device remotely and record audio, capture screenshots, and monitor all phone calls and SMS messages. What is the type of spyware that Jake used to infect the target device?

- A. DroidSheep
- B. Androrat

- C. Zscaler
- D. Trident

**Answer:** D

#### NEW QUESTION 207

- (Topic 3)

While performing a security audit of a web application, an ethical hacker discovers a potential vulnerability.

The application responds to logically incorrect queries with detailed error messages that divulge the underlying database's structure. The ethical hacker decides to exploit this vulnerability further. Which type of SQL Injection attack is the ethical hacker likely to use?

- A. UNION SQL Injection
- B. Blind/inferential SQL Injection
- C. In-band SQL Injection
- D. Error-based SQL Injection

**Answer:** D

#### Explanation:

Error-based SQL Injection is a type of in-band SQL Injection attack that relies on error messages thrown by the database server to obtain information about the structure of the database. In some cases, error-based SQL injection alone is enough for an attacker to enumerate an entire database.

The ethical hacker is likely to use this type of SQL Injection attack because the application responds to logically incorrect queries with detailed error messages that divulge the underlying database's structure. This means that the attacker can craft malicious SQL queries that trigger errors and reveal information such as table names, column names, data types, etc. The attacker can then use this information to construct more complex queries that extract data from the database.

For example, if the application uses the following query to display the username of a user based on the user ID:

```
SELECT username FROM users WHERE id = '$id'
```

The attacker can inject a single quote at the end of the user ID parameter to cause a syntax error:

```
SELECT username FROM users WHERE id = '1'
```

The application might display an error message like this:

You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near "1" at line 1

This error message reveals that the database server is MySQL and that the user ID parameter is enclosed in single quotes. The attacker can then use other techniques such as UNION, subqueries, or conditional statements to manipulate the query and retrieve data from other tables or columns.

References:

? [CEHv12 Module 05: Sniffing]

? Types of SQL Injection (SQLi) - GeeksforGeeks

? Types of SQL Injection? - Acunetix

#### NEW QUESTION 210

- (Topic 3)

A post-breach forensic investigation revealed that a known vulnerability in Apache Struts was to blame for the Equifax data breach that affected 143 million customers. A fix was available from the software vendor for several months prior to the intrusion. This is likely a failure in which of the following security processes?

- A. vendor risk management
- B. Security awareness training
- C. Secure deployment lifecycle
- D. Patch management

**Answer:** D

#### Explanation:

Patch management is the method that helps acquire, test and install multiple patches (code changes) on existing applications and software tools on a pc, enabling systems to remain updated on existing patches and determining that patches are the suitable ones. Managing patches so becomes simple and simple.

Patch Management is usually done by software system firms as a part of their internal efforts to mend problems with the various versions of software system programs and also to assist analyze existing software system programs and discover any potential lack of security features or different upgrades.

Software patches help fix those problems that exist and are detected solely once the software's initial unharness. Patches mostly concern security while there are some patches that concern the particular practicality of programs as well.

#### NEW QUESTION 212

- (Topic 3)

A computer science student needs to fill some information into a secured Adobe PDF job application that was received from a prospective employer. Instead of requesting a new document that allowed the forms to be completed, the student decides to write a script that pulls passwords from a list of commonly used passwords to try against the secured PDF until the correct password is found or the list is exhausted.

Which cryptography attack is the student attempting?

- A. Man-in-the-middle attack
- B. Brute-force attack
- C. Dictionary attack
- D. Session hijacking

**Answer:** C

#### NEW QUESTION 217

- (Topic 3)

Mr. Omkar performed tool-based vulnerability assessment and found two vulnerabilities. During analysis, he found that these issues are not true vulnerabilities. What will you call these issues?

- A. False positives
- B. True negatives

- C. True positives
- D. False negatives

**Answer:** A

**Explanation:**

False Positives occur when a scanner, Web Application Firewall (WAF), or Intrusion Prevention System (IPS) flags a security vulnerability that you do not have. A false negative is the opposite of a false positive, telling you that you don't have a vulnerability when, in fact, you do.

A false positive is like a false alarm; your house alarm goes off, but there is no burglar. In web application security, a false positive is when a web application security scanner indicates that there is a vulnerability on your website, such as SQL Injection, when, in reality, there is not. Web security experts and penetration testers use automated web application security scanners to ease the penetration testing process. These tools help them ensure that all web application attack surfaces are correctly tested in a reasonable amount of time. But many false positives tend to break down this process. If the first 20 variants are false, the penetration tester assumes that all the others are false positives and ignore the rest. By doing so, there is a good chance that real web application vulnerabilities will be left undetected.

When checking for false positives, you want to ensure that they are indeed false. By nature, we humans tend to start ignoring false positives rather quickly. For example, suppose a web application security scanner detects 100 SQL Injection vulnerabilities. If the first 20 variants are false positives, the penetration tester assumes that all the others are false positives and ignore all the rest. By doing so, there are chances that real web application vulnerabilities are left undetected. This is why it is crucial to check every vulnerability and deal with each false positive separately to ensure false positives.

**NEW QUESTION 221**

- (Topic 3)

A penetration tester is performing an enumeration on a client's network. The tester has acquired permission to perform enumeration activities. They have identified a remote inter-process communication (IPC) share and are trying to collect more information about it. The tester decides to use a common enumeration technique to collect the desired data. Which of the following techniques would be most appropriate for this scenario?

- A. Brute force Active Directory
- B. Probe the IPC share by attempting to brute force admin credentials
- C. Extract usernames using email IDs
- D. Conduct a DNS zone transfer

**Answer:** B

**Explanation:**

Probing the IPC share by attempting to brute force admin credentials is the most appropriate technique for this scenario, because it can reveal valuable information about the target system, such as its operating system, services, users, groups, and shares. An IPC share is a special share that allows processes to communicate with each other over the network using named pipes. An IPC share can be accessed anonymously or with valid credentials, depending on the security configuration of the target system. A brute force attack is a method of trying different combinations of usernames and passwords until a valid pair is found. By using a brute force attack, the tester can try to access the IPC share with admin credentials, which can grant them more privileges and access to more resources on the target system.

The other options are less suitable or effective techniques for this scenario. Brute forcing Active Directory may not be relevant or feasible, as the target system may not be part of a domain or may have strong password policies. Extracting usernames using email IDs may not provide enough information or access to the target system, as email IDs may not match the usernames or passwords. Conducting a DNS zone transfer may not be possible or useful, as the target system may not be a DNS server or may have restricted zone transfers. A DNS zone transfer is a method of obtaining information about the domain names and IP addresses of the hosts in a network by querying a DNS server. References:

- ? Inter-process communication - Wikipedia
- ? IPC\$ share and null session behavior - Windows Server
- ? Brute Force Attack: Definition, Examples, and Prevention
- ? DNS Zone Transfer: Definition, Types, and Examples

**NEW QUESTION 222**

- (Topic 3)

You are a penetration tester and are about to perform a scan on a specific server. The agreement that you signed with the client contains the following specific condition for the scan: ??The attacker must scan every port on the server several times using a set of spoofed sources IP addresses. ?? Suppose that you are using Nmap to perform this scan. What flag will you use to satisfy this requirement?

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

**Answer:** D

**Explanation:**

flags -source-port and -g are equivalent and instruct nmap to send packets through a selected port. this option is used to try to cheat firewalls whitelisting traffic from specific ports. the following example can scan the target from the port twenty to ports eighty, 22, 21,23 and 25 sending fragmented packets to LinuxHint.

**NEW QUESTION 227**

- (Topic 3)

Which of the following statements is TRUE?

- A. Packet Sniffers operate on the Layer 1 of the OSI model.
- B. Packet Sniffers operate on Layer 2 of the OSI model.
- C. Packet Sniffers operate on both Layer 2 & Layer 3 of the OSI model.
- D. Packet Sniffers operate on Layer 3 of the OSI model.

**Answer:** B

**NEW QUESTION 229**

- (Topic 3)

The security administrator of ABC needs to permit Internet traffic in the host 10.0.0.2 and UDP traffic in the host 10.0.0.3. He also needs to permit all FTP traffic to the rest of the network and deny all other traffic. After he applied his ACL configuration in the router, nobody can access the ftp, and the permitted hosts cannot access the Internet. According to the next configuration, what is happening in the network?

```
access-list 102 deny tcp any any
access-list 104 permit udp host 10.0.0.3 any
access-list 110 permit tcp host 10.0.0.2 eq www any
access-list 108 permit tcp any eq ftp any
```

- A. The ACL 104 needs to be first because is UDP
- B. The first ACL is denying all TCP traffic and the other ACLs are being ignored by the router
- C. The ACL for FTP must be before the ACL 110
- D. The ACL 110 needs to be changed to port 80

**Answer: B**

**Explanation:**

<https://www.cisco.com/c/en/us/support/docs/ip/access-lists/26448-ACLsamples.html> Since the first line prohibits any TCP traffic (access-list 102 deny tcp any any), the lines below will simply be ignored by the router. Below you will find the example from CISCO documentation.

This figure shows that FTP (TCP, port 21) and FTP data (port 20) traffic sourced from NetB destined to NetA is denied, while all other IP traffic is permitted.

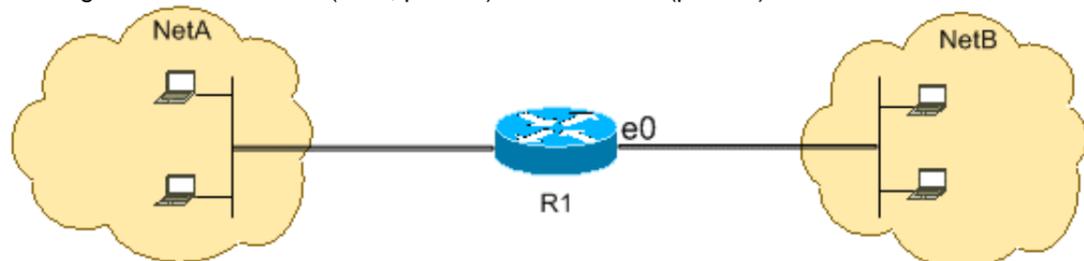


Diagram Description automatically generated

FTP uses port 21 and port 20. TCP traffic destined to port 21 and port 20 is denied and everything else is explicitly permitted.

- ? access-list 102 deny tcp any any eq ftp
- ? access-list 102 deny tcp any any eq ftp-data
- ? access-list 102 permit ip any any

**NEW QUESTION 230**

- (Topic 3)

Ron, a security professional, was pen testing web applications and SaaS platforms used by his company. While testing, he found a vulnerability that allows hackers to gain unauthorized access to API objects and perform actions such as view, update, and delete sensitive data of the company. What is the API vulnerability revealed in the above scenario?

- A. Code injections
- B. Improper use of CORS
- C. No ABAC validation
- D. Business logic flaws

**Answer: C**

**NEW QUESTION 233**

- (Topic 3)

Which protocol is used for setting up secure channels between two devices, typically in VPNs?

- A. PEM
- B. ppp
- C. IPSEC
- D. SET

**Answer: C**

**NEW QUESTION 236**

- (Topic 3)

What would you enter if you wanted to perform a stealth scan using Nmap?

- A. nmap -sM
- B. nmap -sU
- C. nmap -sS
- D. nmap -sT

**Answer: C**

**NEW QUESTION 239**

- (Topic 3)

A large e-commerce organization is planning to implement a vulnerability assessment solution to enhance its security posture. They require a solution that imitates the outside view of attackers, performs well-organized inference-based testing, scans automatically against continuously updated databases, and supports multiple networks. Given these requirements, which type of vulnerability assessment solution would be most appropriate?

- A. Inference-based assessment solution
- B. Service-based solution offered by an auditing firm
- C. Tree-based assessment approach
- D. Product-based solution installed on a private network

**Answer: B**

**Explanation:**

A service-based solution offered by an auditing firm would be the most appropriate type of vulnerability assessment solution for the large e-commerce organization, given their requirements. A service-based solution is a type of vulnerability assessment that is performed by external experts who have the skills, tools, and experience to conduct a thorough and comprehensive analysis of the target system or network. A service-based solution can imitate the outside view of attackers, as the experts are not familiar with the internal details or configurations of the organization. A service-based solution can also perform well-organized inference-based testing, which is a type of testing that uses logical reasoning and deduction to identify and exploit vulnerabilities based on the information gathered from the target. A service-based solution can scan automatically against continuously updated databases, as the experts have access to the latest security intelligence and threat feeds. A service-based solution can also support multiple networks, as the experts can use different techniques and tools to scan different types of networks, such as wired, wireless, cloud, or hybrid.

The other options are not as appropriate as option B for the following reasons:

? A. Inference-based assessment solution: This option is not a type of vulnerability assessment solution, but a type of testing method that can be used by any solution. Inference-based testing is a testing method that uses logical reasoning and deduction to identify and exploit vulnerabilities based on the information gathered from the target. Inference-based testing can be performed by service-based, product-based, or tree-based solutions, depending on the scope, objectives, and resources of the assessment.

? C. Tree-based assessment approach: This option is not a type of vulnerability assessment solution, but a type of testing method that can be used by any solution. Tree-based testing is a testing method that uses a hierarchical structure to organize and prioritize the vulnerabilities based on their severity, impact, and exploitability. Tree-based testing can be performed by service-based, product-based, or inference-based solutions, depending on the scope, objectives, and resources of the assessment.

? D. Product-based solution installed on a private network: This option is a type of vulnerability assessment solution, but it may not meet all the requirements of the large e-commerce organization. A product-based solution is a type of vulnerability assessment that is performed by using software or hardware tools that are installed on the organization's own network. A product-based solution can scan automatically against continuously updated databases, as the tools can be configured to download and apply the latest security updates and patches. However, a product-based solution may not imitate the outside view of attackers, as the tools may have limited access or visibility to the external network or the internet. A product-based solution may also not perform well-organized inference-based testing, as the tools may rely on predefined rules or signatures to detect and report vulnerabilities, rather than using logical reasoning and deduction. A product-based solution may also not support multiple networks, as the tools may be designed or optimized for a specific type of network, such as wired, wireless, cloud, or hybrid.

References:

- ? 1: Vulnerability Assessment Services | Rapid7
- ? 2: Vulnerability Assessment Services | IBM
- ? 3: Inference-Based Vulnerability Testing of Firewall Policies - IEEE Conference Publication
- ? 4: A Tree-Based Approach for Vulnerability Assessment - IEEE Conference Publication
- ? : Vulnerability Assessment Tools | OWASP Foundation
- ? : Vulnerability Assessment Solutions: Why You Need One and How to Choose | Defensible

**NEW QUESTION 243**

- (Topic 3)

Which among the following is the best example of the hacking concept called "clearing tracks"?

- A. After a system is breached, a hacker creates a backdoor to allow re-entry into a system.
- B. During a cyberattack, a hacker injects a rootkit into a server.
- C. An attacker gains access to a server through an exploitable vulnerability.
- D. During a cyberattack, a hacker corrupts the event logs on all machines.

**Answer: D**

**NEW QUESTION 244**

- (Topic 3)

An ethical hacker is hired to evaluate the defenses of an organization's database system which is known to employ a signature-based IDS. The hacker knows that some SQL Injection evasion techniques may allow him to bypass the system's signatures. During the operation, he successfully retrieved a list of usernames from the database without triggering an alarm by employing an advanced evasion technique. Which of the following could he have used?

- A. Utilizing the char encoding function to convert hexadecimal and decimal values into characters that pass-through SQL engine parsing
- B. Using the URL encoding method to replace characters with their ASCII codes in hexadecimal form
- C. Implementing sophisticated matches such as "OR 'john' = john" in place of classical matches like "OR 1=1"
- D. Manipulating white spaces in SQL queries to bypass signature detection

**Answer: D**

**Explanation:**

The hacker could have used the technique of manipulating white spaces in SQL queries to bypass signature detection. This technique involves inserting, removing, or replacing white spaces in SQL queries with other characters or symbols that are either ignored or interpreted as white spaces by the SQL engine, but not by the signature-based IDS. This way, the hacker can alter the appearance of the query and evade the pattern matching of the IDS, while preserving the functionality and logic of the query. For example, the hacker could replace the space character with a tab character, a newline character, a comment symbol, or a URL-encoded value, such as %20.

The other options are not correct for the following reasons:

? A. Utilizing the char encoding function to convert hexadecimal and decimal values into characters that pass-through SQL engine parsing: This option is not feasible because the char encoding function is not supported by all SQL engines, and it may not be able to convert all hexadecimal and decimal values into valid characters. Moreover, the char encoding function may not be able to bypass the signature detection of the IDS, as it may still match the keywords or syntax of the SQL query.

? B. Using the URL encoding method to replace characters with their ASCII codes in hexadecimal form: This option is not effective because the URL encoding method is not applicable to SQL queries, as it is designed for encoding special characters in URLs. The URL encoding method may not be able to replace all characters with their ASCII codes, and it may not be able to preserve the functionality and logic of the SQL query. Furthermore, the URL encoding method may not be able to evade the signature detection of the IDS, as it may still match the keywords or syntax of the SQL query.

? C. Implementing sophisticated matches such as "OR 'john' = john" in place of classical matches like "OR 1=1": This option is not advanced because it is a common and basic SQL injection technique that does not involve any evasion or obfuscation. This technique involves injecting a logical expression that is always true, such as "OR 'john' = john" or "OR 1=1", to bypass the authentication or authorization checks of the SQL query. However, this technique may not be able to bypass the signature detection of the IDS, as it may easily match the keywords or syntax of the SQL query.

References:

- ? 1: SQL Injection Evasion Detection - F5
- ? 2: Mastering SQL Injection with SQLmap: A Comprehensive Evasion Techniques Cheatsheet
- ? 3: SQL Injection Prevention - OWASP Cheat Sheet Series
- ? 4: URL Encoding - W3Schools
- ? : SQL Injection - OWASP Foundation

#### NEW QUESTION 249

- (Topic 3)

On performing a risk assessment, you need to determine the potential impacts when some of the critical business processes of the company interrupt its service. What is the name of the process by which you can determine those critical businesses?

- A. Emergency Plan Response (EPR)
- B. Business Impact Analysis (BIA)
- C. Risk Mitigation
- D. Disaster Recovery Planning (DRP)

**Answer: B**

#### NEW QUESTION 253

- (Topic 3)

In a large organization, a network security analyst discovered a series of packet captures that seem unusual.

The network operates on a switched Ethernet environment. The security team suspects that an attacker might be using a sniffer tool. Which technique could the attacker be using to successfully carry out this attack, considering the switched nature of the network?

- A. The attacker might be compromising physical security to plug into the network directly
- B. The attacker might be implementing MAC flooding to overwhelm the switch's memory
- C. The attacker is probably using a Trojan horse with in-built sniffing capability
- D. The attacker might be using passive sniffing, as it provides significant stealth advantages

**Answer: B**

#### Explanation:

A sniffer tool is a software or hardware device that can capture and analyze network traffic. In a switched Ethernet environment, where each port on a switch is connected to a single device, a sniffer tool can only see the traffic that is destined for or originated from the device it is attached to. However, an attacker can use various techniques to overcome this limitation and sniff the traffic of other devices on the same network. One of these techniques is MAC flooding, which exploits the finite memory of the switch's MAC address table. The attacker sends a large number of frames with different source MAC addresses to the switch, which fills up the MAC address table and causes the switch to enter a fail-open mode, where it broadcasts all incoming frames to all ports, regardless of the destination MAC address. This way, the attacker can see all the traffic on the network and capture it with a sniffer tool.

The other options are less likely or less effective techniques for sniffing a switched Ethernet network. Compromising physical security to plug into the network directly may allow the attacker to sniff the traffic of the device they are connected to, but not the traffic of other devices on the network. Using a Trojan horse with in-built sniffing capability may allow the attacker to sniff the traffic of the infected device, but not the traffic of other devices on the network, unless the Trojan horse also performs MAC flooding or other techniques to bypass the switch. Using passive sniffing, which involves listening to the network traffic without sending any packets, may provide significant stealth advantages, but it does not help the attacker to see the traffic of other devices on the network, unless the switch is already in fail-open mode or the attacker uses other techniques to induce it. References:

- ? Sniffing: A Beginners Guide In 4 Important Points
- ? How can I run a packet sniffer on a Router or Switch
- ? Detection of Sniffers in an Ethernet Network

#### NEW QUESTION 255

- (Topic 3)

During a penetration testing assignment, a Certified Ethical Hacker (CEH) used a set of scanning tools to create a profile of the target organization. The CEH wanted to scan for live hosts, open ports, and services on a target network. He used Nmap for network inventory and Hping3 for network security auditing. However, he wanted to spoof IP addresses for anonymity during probing. Which command should the CEH use to perform this task?

- A. Hping3 -110.0.0.25 --ICMP
- B. Nmap -sS -Pn -n -vw --packet-trace -p- --script discovery -T4
- C. Hping3 -S 192.168.1.1 -a 192.168.1.254 -p 22 -flood
- D. Hping3-210.0.0.25-p 80

**Answer: C**

#### Explanation:

The command C. Hping3 -S 192.168.1.1 -a 192.168.1.254 -p 22 -flood is the correct one to spoof IP addresses for anonymity during probing. This command sends SYN packets (-S) to the target IP 192.168.1.1 with a spoofed source IP (-a) 192.168.1.254 on port 22 (-p) and floods the target with packets (-flood). This way, the CEH can hide his real IP address and avoid detection by the target's firewall or IDS.

The other commands are incorrect for the following reasons:

- ? A. Hping3 -110.0.0.25 --ICMP: This command sends ICMP packets (--ICMP) to the target IP 10.0.0.25, but does not spoof the source IP. Therefore, the CEH's real IP address will be exposed to the target.
- ? B. Nmap -sS -Pn -n -vw --packet-trace -p- --script discovery -T4: This command performs a stealthy SYN scan (-sS) on all ports (-p) of the target without pinging it (-Pn) or resolving DNS names (-n). It also enables verbose output (-v), packet tracing (--packet-trace), and discovery scripts (--script discovery) with an aggressive timing (-T4). However, this command does not spoof the source IP, and in fact, reveals more information about the scan to the target by using packet tracing and discovery scripts.
- ? D. Hping3-210.0.0.25-p 80: This command sends TCP packets (default) to the target IP 10.0.0.25 on port 80 (-p), but does not spoof the source IP. Therefore, the CEH's real IP address will be exposed to the target.

References:

- ? 1: Master hping3 and Enhance Your Network Strength | GoLinuxCloud
- ? 2: Spoofing Packets with Hping3 - YouTube

#### NEW QUESTION 257

- (Topic 3)

An ethical hacker is hired to conduct a comprehensive network scan of a large organization that strongly suspects potential intrusions into their internal systems. The hacker decides to employ a combination of scanning tools to obtain a detailed understanding of the network. Which sequence of actions would provide the most comprehensive information about the network's status?

- A. Initiate with Nmap for a ping sweep, then use Metasploit to scan for open ports and services, and finally use Hping3 to perform remote OS fingerprinting
- B. Use Hping3 for an ICMP ping scan on the entire subnet, then use Nmap for a SYN scan on identified active hosts, and finally use Metasploit to exploit identified vulnerabilities
- C. Start with Hping3 for a UDP scan on random ports, then use Nmap for a version detection scan, and finally use Metasploit to exploit detected vulnerabilities
- D. Begin with NetScanTools Pro for a general network scan, then use Nmap for OS detection and version detection, and finally perform an SYN flooding with Hping3

**Answer: B**

**Explanation:**

The sequence of actions that would provide the most comprehensive information about the network's status is to use Hping3 for an ICMP ping scan on the entire subnet, then use Nmap for a SYN scan on identified active hosts, and finally use Metasploit to exploit identified vulnerabilities. This sequence of actions works as follows:

? Use Hping3 for an ICMP ping scan on the entire subnet: This action is used to discover the active hosts on the network by sending ICMP echo request packets to each possible IP address on the subnet and waiting for ICMP echo reply packets from the hosts. Hping3 is a command-line tool that can craft and send custom packets, such as TCP, UDP, or ICMP, and analyze the responses. By using Hping3 for an ICMP ping scan, the hacker can quickly and efficiently identify the live hosts on the network, as well as their response times and packet loss rates<sup>12</sup>.

? Use Nmap for a SYN scan on identified active hosts: This action is used to scan the open ports and services on the active hosts by sending TCP SYN packets to a range of ports and analyzing the TCP responses. Nmap is a popular and powerful tool that can perform various types of network scans, such as port scanning, service detection, OS detection, and vulnerability scanning. By using Nmap for a SYN scan, the hacker can determine the state of the ports on the active hosts, such as open, closed, filtered, or unfiltered, as well as the services and protocols running on them. A SYN scan is also known as a stealth scan, as it does not complete the TCP three-way handshake and thus avoids logging on the target system<sup>34</sup>.

? Use Metasploit to exploit identified vulnerabilities: This action is used to exploit the vulnerabilities on the active hosts by using pre-built or custom modules that leverage the open ports and services. Metasploit is a framework that contains a collection of tools and modules for penetration testing and exploitation. By using Metasploit, the hacker can launch various attacks on the active hosts, such as remote code execution, privilege escalation, or backdoor installation, and gain access to the target system or data. Metasploit can also be used to perform post-exploitation tasks, such as gathering information, maintaining persistence, or pivoting to other systems .

The other options are not as comprehensive as option B for the following reasons:

? A. Initiate with Nmap for a ping sweep, then use Metasploit to scan for open ports and services, and finally use Hping3 to perform remote OS fingerprinting: This option is not optimal because it does not use the tools in the most efficient and effective way. Nmap can perform a ping sweep, but it is slower and less flexible than Hping3, which can craft and send custom packets. Metasploit can scan for open ports and services, but it is more suitable for exploitation than scanning, and it relies on Nmap for port scanning anyway. Hping3 can perform remote OS fingerprinting, but it is less accurate and reliable than Nmap, which can use various techniques and probes to determine the OS type and version<sup>13</sup> .

? C. Start with Hping3 for a UDP scan on random ports, then use Nmap for a version detection scan, and finally use Metasploit to exploit detected vulnerabilities: This option is not effective because it does not use the best scanning methods and techniques. Hping3 can perform a UDP scan, but it is slower and less reliable than a TCP scan, as UDP is a connectionless protocol that does not always generate responses. Scanning random ports is also inefficient and incomplete, as it may miss important ports or services. Nmap can perform a version detection scan, but it is more useful to perform a port scan first, as it can narrow down the scope and speed up the scan. Metasploit can exploit detected vulnerabilities, but it is not clear how the hacker can identify the vulnerabilities without performing a vulnerability scan first<sup>13</sup> .

? D. Begin with NetScanTools Pro for a general network scan, then use Nmap for OS detection and version detection, and finally perform an SYN flooding with Hping3: This option is not comprehensive because it does not cover all the aspects and objectives of a network scan. NetScanTools Pro is a graphical tool that can perform various network tasks, such as ping, traceroute, DNS lookup, or port scan, but it is less powerful and versatile than Nmap or Hping3, which can perform more advanced and customized scans. Nmap can perform OS detection and version detection, but it is more useful to perform a port scan first, as it can provide more information and insights into the target system. Performing an SYN flooding with Hping3 is not a network scan, but a denial-of-service attack, which can disrupt the network and alert the target system, and it is not an ethical or legal action for a hired hacker<sup>13</sup> .

References:

- ? 1: Hping - Wikipedia
- ? 2: Hping3 Examples - NetworkProGuide
- ? 3: Nmap - Wikipedia
- ? 4: Nmap Tutorial: From Discovery to Exploits – Part 1: Introduction to Nmap | HackerTarget.com
- ? : Metasploit Project - Wikipedia
- ? : Metasploit Unleashed - Offensive Security
- ? : NetScanTools Pro - Northwest Performance Software, Inc.

**NEW QUESTION 259**

- (Topic 3)

An IT security team is conducting an internal review of security protocols in their organization to identify potential vulnerabilities. During their investigation, they encounter a suspicious program running on several computers. Further examination reveals that the program has been logging all user keystrokes. How can the security team confirm the type of program and what countermeasures should be taken to ensure the same attack does not occur in the future?

- A. The program is a Trojan; the team should regularly update antivirus software and install a reliable firewall
- B. The program is spyware; the team should use password managers and encrypt sensitive data
- C. The program is a keylogger; the team should employ intrusion detection systems and regularly update the system software
- D. The program is a keylogger; the team should educate employees about phishing attacks and maintain regular backups

**Answer: C**

**Explanation:**

A keylogger is a type of spyware that can record and steal consecutive keystrokes (and much more) that the user enters on a device. Keyloggers are a common tool for cybercriminals, who use them to capture passwords, credit card numbers, personal information, and other sensitive data. Keyloggers can be installed on a device through various methods, such as phishing emails, malicious downloads, or physical access. To confirm the type of program, the security team can use a web search tool, such as Bing, to look for keylogger programs and compare their features and behaviors with the suspicious program they encountered. Alternatively, they can use a malware analysis tool, such as Malwarebytes, to scan and identify the program and its characteristics.

To prevent the same attack from occurring in the future, the security team should employ intrusion detection systems (IDS) and regularly update the system software. An IDS is a system that monitors network traffic and system activities for signs of malicious or unauthorized behavior, such as keylogger installation or

communication. An IDS can alert the security team of any potential threats and help them respond accordingly. Regularly updating the system software can help patch any vulnerabilities or bugs that keyloggers may exploit to infect the device. Additionally, the security team should also remove the keylogger program from the affected computers and change any compromised passwords or credentials. References:

- ? Keylogger | What is a Keylogger? How to protect yourself
- ? How to Detect and Remove a Keylogger From Your Computer
- ? Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS)
- ? What is a Keylogger? | Keystroke Logging Definition | Avast
- ? Keylogger Software: 11 Best Free to Use in 2023

#### NEW QUESTION 261

.....

## Thank You for Trying Our Product

### We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

### 312-50v13 Practice Exam Features:

- \* 312-50v13 Questions and Answers Updated Frequently
- \* 312-50v13 Practice Questions Verified by Expert Senior Certified Staff
- \* 312-50v13 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- \* 312-50v13 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

**100% Actual & Verified — Instant Download, Please Click**  
[Order The 312-50v13 Practice Test Here](#)