Exam Questions 312-50v13

Certified Ethical Hacker v13

https://www.2passeasy.com/dumps/312-50v13/

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

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

Answer: D

NEW QUESTION 2
- (Topic 1)
Study the snort rule given below:

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 135
(msg: "NETBIOS DCERPC ISystemActivator bind attempt";
flow:to_server, established; content: "|05|"; distance: 0; within: 1;
content: "|ob|"; distance: 1; within: 1; byte_test: 1, &, 1, 0, relative;
content: "|A0 01 00 00 00 00 00 00 C0 00 00 00 00 00 00 46|";
distance: 29; within: 16; reference: cve, CAN-2003-0352;
classtype: attempted-admin; sid: 2192; rev: 1;)

alert tcp $EXTERNAL_NET any -> $HOME_NET 445 (msg: "NETBIOS SMB
DCERPC ISystemActivator bind attempt"; flow: to_server, established;
content: "|FF|SMB|25|"; nocase; offset:4, depth:5; content: "|26 00|";
nocase; distance:5; within: 12; content: "|05|"; distance:0; within:1;
content: "|ob|"; distance: 1; within: 1; byte_test: 1, &, 1, 0, relative;
content: "|A0 01 00 00 00 00 00 00 C0 00 00 00 00 00 00 46|";
distance: 29; within: 16; reference: cve, CAN-2003-0352;
classtype: attempted-admin; sid: 2193; rev: 1;)
```

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

A. WebDav
B. SQL Slammer
C. MS Blaster
D. MyDoom

Answer: C

NEW QUESTION 3
- (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

NEW QUESTION 4
- (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.

NEW QUESTION 5
- (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.

NEW QUESTION 6
- (Topic 1)
If a token and 4-digit personal identification number (PIN) are used to access a computer system and the token performs off-line checking for the correct PIN, what type of attack is possible?

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

Answer: B

NEW QUESTION 7
- (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

NEW QUESTION 8
- (Topic 1)
A company??s policy requires employees to perform file transfers using protocols which encrypt traffic. You suspect some employees are still performing file transfers using unencrypted protocols because the employees do not like changes. You have positioned a network sniffer to capture traffic from the laptops used by employees in the data ingest department. Using Wireshark to examine the captured traffic, which command can be used as display filter to find unencrypted file transfers?

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

Answer: A

NEW QUESTION 9
- (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

NEW QUESTION 10
- (Topic 1)
Why would you consider sending an email to an address that you know does not exist within the company you are performing a Penetration Test for?

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

Answer: D

NEW QUESTION 10
- (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

NEW QUESTION 14
- (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

NEW QUESTION 15
- (Topic 1)
Shellshock allowed an unauthorized user to gain access to a server. It affected many Internet-facing services, which OS did it not directly affect?

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

Answer: D

NEW QUESTION 17
- (Topic 1)
Which of the following tools is used to detect wireless LANs using the 802.11a/b/g/n WLAN standards on a linux platform?

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

Answer: A

Explanation:
https://en.wikipedia.org/wiki/Kismet_(software)
Kismet is a network detector, packet sniffer, and intrusion detection system for 802.11 wireless LANs. Kismet will work with any wireless card which supports raw monitoring mode, and can sniff 802.11a, 802.11b, 802.11g, and 802.11n traffic.

NEW QUESTION 20
- (Topic 1)
Tess King is using the nslookup command to craft queries to list all DNS information (such as Name Servers, host names, MX records, CNAME records, glue records (delegation for child Domains), zone serial number, TimeToLive (TTL) records, etc) for a Domain.
What do you think Tess King is trying to accomplish? Select the best answer.

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

Answer: B

NEW QUESTION 22
- (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.

NEW QUESTION 25
- (Topic 1)
Which of the following algorithms can be used to guarantee the integrity of messages being sent, in transit, or stored?

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

Answer: C

NEW QUESTION 26
- (Topic 1)
A new wireless client is configured to join a 802.11 network. This client uses the same hardware and software as many of the other clients on the network. The client can see the network, but cannot connect. A wireless packet sniffer shows that the Wireless Access Point (WAP) is not responding to the association requests being sent by the wireless client. What is a possible source of this problem?

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

Answer: A

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

NEW QUESTION 27
- (Topic 1)
Which of the following is assured by the use of a hash?

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

Answer: D

NEW QUESTION 29
- (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

NEW QUESTION 30
- (Topic 1)
The following is an entry captured by a network IDS. You are assigned the task of analyzing this entry. You notice the value 0x90, which is the most common NOOP instruction for the Intel processor. You figure that the attacker is attempting a buffer overflow attack.
You also notice "/bin/sh" in the ASCII part of the output. As an analyst what would you conclude about the attack?

```
45 00 01 ce 28 1e 40 00 32 06 96 92 d1 3a 18 09 86 9f 18 97 E..Î(.@.2...Ñ:......
06 38 02 03 6f 54 4f a9 01 af fe 78 50 18 7d 78 76 dd 00 00 .8..oTO©.¯þxP.\)
Application "Calculator" "%path:..\dtsapps\calc\dcalc.exe%" " " size 0.75in 0.25in 0.50in
0.05inxvÝ..
42 42 20 f7 ff bf 21 f7 ff bf 22 f7 ff bf 23 f7 ff bf 58 58 BB ÷ÿ¿!÷ÿ¿"÷ÿ¿#÷ÿ¿XX
58 58 58 58 58 58 58 58 58 58 58 58 58 58 58 58 25 2e 32 32 XXXXXXXXXXXXXXXX%.22
34 75 25 33 30 30 24 6e 25 2e 32 31 33 75 25 33 30 31 24 6e 4u%300$n%.213u%301$n
73 65 63 75 25 33 30 32 24 6e 25 2e 31 39 32 75 25 33 30 33 secu%302$n%.192u%303
24 6e 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 $n..................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ....................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ....................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ....................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ....................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ....................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ....................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ....................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ....................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ....................
90 90 31 db 31 c9 31 c0 b0 46 cd 80 89 e5 31 d2 b2 66 89 d0 ..1Û1É1À°FÍ..å1Òªf.Ð
31 c9 89 cb 43 89 5d f8 43 89 5d f4 4b 89 4d fc 8d 4d f4 cd 1É.ËC.]øC.]ôK.Mü.MôÍ
80 31 c9 89 45 f4 43 66 89 5d ec 66 c7 45 ee 0f 27 89 4d f0 .1É.EôCf.]ìfÇEî.'.Mð
8d 45 ec 89 45 f8 c6 45 fc 10 89 d0 8d 4d f4 cd 80 89 d0 43 .Eì.EøÆEü..Ð.MôÍ..ÐC
43 cd 80 89 d0 43 cd 80 89 c3 31 c9 b2 3f 89 d0 cd 80 89 d0 CÍ..ÐCÍ..Ã1É²?.ÐÍ..Ð
41 cd 80 eb 18 5e 89 75 08 31 c0 88 46 07 89 45 0c b0 0b 89 AÍ.ë.^.u.1À.F..E.°..
f3 8d 4d 08 8d 55 0c cd 80 e8 e3 ff ff ff 2f 62 69 6e 2f 73 ó.M..U.Í.èãÿÿÿ/bin/s
68 0a h.
EVENT4: [NOOP:X86] (tcp,dp=515,sp=1592)
```

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

Answer: D

NEW QUESTION 32
- (Topic 1)
The company ABC recently contracts a new accountant. The accountant will be working with the financial statements. Those financial statements need to be approved by the CFO and then they will be sent to the accountant but the CFO is worried because he wants to be sure that the information sent to the accountant was not modified once he approved it. Which of the following options can be useful to ensure the integrity of the data?

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

Answer: A

NEW QUESTION 34

- (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

NEW QUESTION 39
- (Topic 1)
Which is the first step followed by Vulnerability Scanners for scanning a network?

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

Answer: D

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

NEW QUESTION 41
- (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

NEW QUESTION 45
- (Topic 1)
Which of the following is a command line packet analyzer similar to GUI-based Wireshark?

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

Answer: B

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

NEW QUESTION 48
- (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

NEW QUESTION 52
- (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.

NEW QUESTION 54
- (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

NEW QUESTION 56
- (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

NEW QUESTION 60
- (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.

NEW QUESTION 64
- (Topic 1)
Peter is surfing the internet looking for information about DX Company. Which hacking process is Peter doing?

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

Answer: B

NEW QUESTION 65
- (Topic 1)
In the field of cryptanalysis, what is meant by a ??rubber-hose?? attack?

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

Answer: C

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

NEW QUESTION 67
- (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 exclusivel
C. Manual testing is outdated because of low speed and possible test setup inconsistencies.
D. Test automation is not usable in security due to the complexity of the tests.
E. It can accelerate benchmark tests and repeat them with a consistent test setu
F. But it cannot replace manual testing completely.

Answer: D

NEW QUESTION 71
- (Topic 1)
What is the proper response for a NULL scan if the port is open?

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

Answer: F

NEW QUESTION 73
- (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

NEW QUESTION 76
- (Topic 2)
SQL injection (SQLi) attacks attempt to inject SQL syntax into web requests, which may Bypass authentication and allow attackers to access and/or modify data attached to a web application.
Which of the following SQLI types leverages a database server's ability to make DNS requests to pass data to an attacker?

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

Answer: B

Explanation:
Out-of-band SQL injection occurs when an attacker is unable to use an equivalent channel to launch the attack and gather results. ?? Out-of-band SQLi techniques would believe the database server??s ability to form DNS or HTTP requests to deliver data to an attacker. Out-of-band SQL injection is not very common, mostly because it depends on features being enabled on the database server being used by the web application. Out-of- band SQL injection occurs when an attacker is unable to use the same channel to launch the attack and gather results.
Out-of-band techniques, offer an attacker an alternative to inferential time-based techniques, especially if the server responses are not very stable (making an inferential time-based attack unreliable).

Out-of-band SQLi techniques would rely on the database server??s ability to make DNS or HTTP requests to deliver data to an attacker. Such is the case with Microsoft SQL Server??s xp_dirtree command, which can be used to make DNS requests to a server an
attacker controls; as well as Oracle Database??s UTL_HTTP package, which can be used to send HTTP requests from SQL and PL/SQL to a server an attacker controls.

NEW QUESTION 77
- (Topic 2)
The Payment Card Industry Data Security Standard (PCI DSS) contains six different categories of control objectives. Each objective contains one or more requirements, which must be followed in order to achieve compliance. Which of the following requirements would best fit under the objective, "Implement strong access control measures"?

A. Regularly test security systems and processes.
B. Encrypt transmission of cardholder data across open, public networks.
C. Assign a unique ID to each person with computer access.
D. Use and regularly update anti-virus software on all systems commonly affected by malware.

Answer: C

NEW QUESTION 79
- (Topic 2)
Bella, a security professional working at an it firm, finds that a security breach has occurred while transferring important files. Sensitive data, employee usernames. and passwords are shared In plaintext, paving the way for hackers 10 perform successful session hijacking. To address this situation. Bella Implemented a protocol that sends data using encryption and digital certificates. Which of the following protocols Is used by Bella?

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

Answer: C

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

NEW QUESTION 83
- (Topic 2)
Sam is working as a system administrator In an organization. He captured the principal characteristics of a vulnerability and produced a numerical score to reflect Its severity using CVSS v3.0 to property assess and prioritize the organization's vulnerability management processes. The base score that Sam obtained after performing cvss rating was 4.0. What is the CVSS severity level of the vulnerability discovered by Sam in the above scenario?

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

Answer: A

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

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

NEW QUESTION 84
- (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)

NEW QUESTION 87
- (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

NEW QUESTION 92
- (Topic 2)
What is the first step for a hacker conducting a DNS cache poisoning (DNS spoofing) attack against an organization?

A. The attacker queries a nameserver using the DNS resolver.
B. The attacker makes a request to the DNS resolver.
C. The attacker forges a reply from the DNS resolver.
D. The attacker uses TCP to poison the ONS resofver.

Answer: B

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

malicious website.

NEW QUESTION 94
- (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.

NEW QUESTION 96
- (Topic 2)
Matthew, a black hat, has managed to open a meterpreter session to one of the kiosk machines in Evil Corp??s lobby. He checks his current SID, which is S-1-5-21-1223352397- 1872883824-861252104-501. What needs to happen before Matthew has full administrator access?

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

Answer: A

NEW QUESTION 97
- (Topic 2)
Gavin owns a white-hat firm and is performing a website security audit for one of his clients. He begins by running a scan which looks for common misconfigurations and outdated software versions. Which of the following tools is he most likely using?

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

Answer: B

NEW QUESTION 100
- (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.

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

of malware did the attacker use to bypass the company's application whitelisting?

A. Phishing malware
B. Zero-day malware
C. File-less malware
D. Logic bomb malware

Answer: C

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

NEW QUESTION 105
- (Topic 2)
What port number is used by LDAP protocol?

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

Answer: B

NEW QUESTION 106
- (Topic 2)
Ralph, a professional hacker, targeted Jane, who had recently bought new systems for her company. After a few days, Ralph contacted Jane while masquerading as a legitimate customer support executive, informing that her systems need to be serviced for proper functioning and that customer support will send a computer technician. Jane promptly replied positively. Ralph entered Jane's company using this opportunity and gathered sensitive information by scanning terminals for passwords, searching for important documents in desks, and rummaging bins. What is the type of attack technique Ralph used on jane?

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

Answer: D

NEW QUESTION 111
- (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.

NEW QUESTION 114
- (Topic 2)
Henry Is a cyber security specialist hired by BlackEye - Cyber security solutions. He was tasked with discovering the operating system (OS) of a host. He used the Unkornscan tool to discover the OS of the target system. As a result, he obtained a TTL value, which Indicates that the target system is running a Windows OS. Identify the TTL value Henry obtained, which indicates that the target OS is Windows.

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

Answer: B

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

NEW QUESTION 118
- (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.

NEW QUESTION 122
- (Topic 2)
which type of virus can change its own code and then cipher itself multiple times as it replicates?

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

Answer: A

Explanation:
A stealth virus may be a sort of virus malware that contains sophisticated means of avoiding detection by antivirus software. After it manages to urge into the now-infected machine a stealth viruses hides itself by continually renaming and moving itself round the disc.Like other viruses, a stealth virus can take hold of the many parts of one??s PC. When taking control of the PC and performing tasks, antivirus programs can detect it, but a stealth virus sees that coming and can rename then copy itself to a special drive or area on the disc, before the antivirus software. Once moved and renamed a stealth virus will usually replace the detected ??infected?? file with a clean file that doesn??t trigger anti-virus detection. It??s a never-ending game of cat and mouse.The intelligent architecture of this sort of virus about guarantees it??s impossible to completely rid oneself of it once infected. One would need to completely wipe the pc and rebuild it from scratch to completely eradicate the presence of a stealth virus. Using regularly-updated antivirus software can reduce risk, but, as we all know, antivirus software is additionally caught in an endless cycle of finding new threats and protecting against them. https://www.techslang.com/definition/what-is-a-stealth-virus/

NEW QUESTION 124
- (Topic 2)
Which of the following statements is FALSE with respect to Intrusion Detection Systems?

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

Answer: B

NEW QUESTION 126
- (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

NEW QUESTION 130

- (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: AE

NEW QUESTION 134
- (Topic 2)
Attacker Rony Installed a rogue access point within an organization's perimeter and attempted to Intrude into its internal network. Johnson, a security auditor, identified some unusual traffic in the internal network that is aimed at cracking the authentication mechanism. He immediately turned off the targeted network and tested for any weak and outdated security mechanisms that are open to attack. What is the type of vulnerability assessment performed by Johnson in the above scenario?

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

Answer: B

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

NEW QUESTION 139
- (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

NEW QUESTION 141
- (Topic 2)
The network administrator at Spears Technology, Inc has configured the default gateway Cisco router's access-list as below:
You are hired to conduct security testing on their network.
You successfully brute-force the SNMP community string using a SNMP crack tool. The access-list configured at the router prevents you from establishing a successful
connection.
You want to retrieve the Cisco configuration from the router. How would you proceed?

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

Answer: BD

NEW QUESTION 144
- (Topic 2)
John wants to send Marie an email that includes sensitive information, and he does not trust the network that he is connected to. Marie gives him the idea of using PGP. What should John do to communicate correctly using this type of encryption?

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

Answer: B

Explanation:
When a user encrypts plaintext with PGP, PGP first compresses the plaintext. The session key works with a very secure, fast conventional encryption algorithm to

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

NEW QUESTION 145
- (Topic 2)
what firewall evasion scanning technique make use of a zombie system that has low network activity as well as its fragment identification numbers?

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

Answer: D

Explanation:
The idle scan could be a communications protocol port scan technique that consists of causing spoofed packets to a pc to seek out out what services square measure
obtainable. this can be accomplished by impersonating another pc whose network traffic is extremely slow or nonexistent (that is, not transmission or receiving information). this might be associate idle pc, known as a ??zombie??.
This action are often done through common code network utilities like nmap and hping. The attack involves causing solid packets to a particular machine target in an attempt to seek out distinct characteristics of another zombie machine. The attack is refined as a result of there??s no interaction between the offender pc and also the target: the offender interacts solely with the ??zombie?? pc.
This exploit functions with 2 functions, as a port scanner and a clerk of sure informatics relationships between machines. The target system interacts with the ??zombie?? pc and distinction in behavior are often discovered mistreatment totally different|completely different ??zombies?? with proof of various privileges granted by the target to different computers.
The overall intention behind the idle scan is to ??check the port standing whereas remaining utterly invisible to the targeted host.??
The first step in execution associate idle scan is to seek out associate applicable zombie. It must assign informatics ID packets incrementally on a worldwide (rather than per-host it communicates with) basis. It ought to be idle (hence the scan name), as extraneous traffic can raise its informatics ID sequence, confusing the scan logic. The lower the latency between the offender and also the zombie, and between the zombie and also the target, the quicker the scan can proceed.
Note that once a port is open, IPIDs increment by a pair of. Following is that the sequence:
? offender to focus on -> SYN, target to zombie ->SYN/ACK, Zombie to focus on -> RST (IPID increment by 1)
? currently offender tries to probe zombie for result. offender to Zombie ->SYN/ACK, Zombie to offender -> RST (IPID increment by 1)
So, during this method IPID increments by a pair of finally.
When associate idle scan is tried, tools (for example nmap) tests the projected zombie and reports any issues with it. If one does not work, attempt another. Enough net hosts square measure vulnerable that zombie candidates are not exhausting to seek out. a standard approach is to easily execute a ping sweep of some network. selecting a network close to your supply address, or close to the target, produces higher results. you??ll be able to attempt associate idle scan mistreatment every obtainable host from the ping sweep results till you discover one that works. As usual, it??s best to raise permission before mistreatment someone??s machines for surprising functions like idle scanning.
Simple network devices typically create nice zombies as a result of {they square measure|they??re} normally each underused (idle) and designed with straightforward network stacks that are susceptible to informatics ID traffic detection.
While distinguishing an acceptable zombie takes some initial work, you??ll be able to keep re-using the nice ones. as an alternative, there are some analysis on utilizing unplanned public internet services as zombie hosts to perform similar idle scans. leverage the approach a number of these services perform departing connections upon user submissions will function some quite poor??s man idle scanning.

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

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

Answer: D

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

NEW QUESTION 150
- (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.

NEW QUESTION 155
- (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

NEW QUESTION 160
- (Topic 2)
Which of the following steps for risk assessment methodology refers to vulnerability identification?

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

Answer: C

NEW QUESTION 161
- (Topic 2)
jane invites her friends Alice and John over for a LAN party. Alice and John access Jane's wireless network without a password. However. Jane has a long, complex password on her router. What attack has likely occurred?

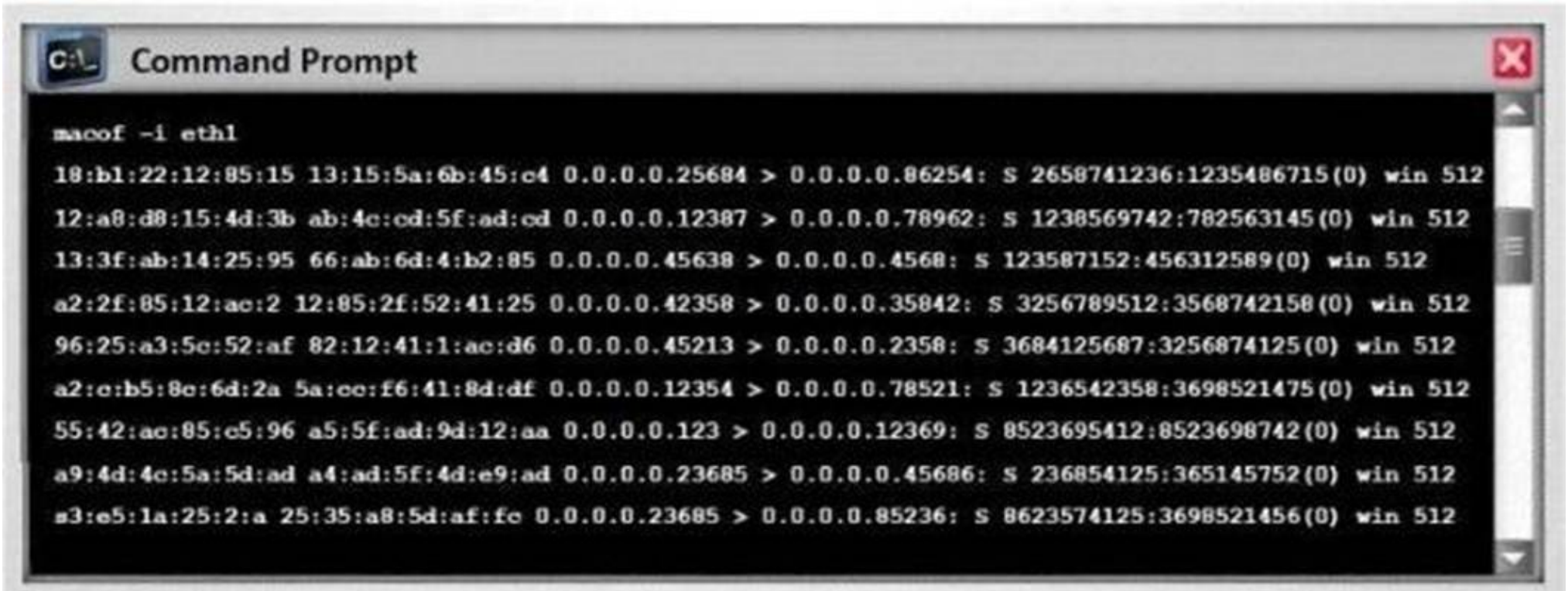
A. Wireless sniffing
B. Piggybacking
C. Evil twin
D. Wardriving

Answer: C

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

twin are often configured to pass Internet traffic through to the legitimate access point while monitoring the victim??s connection, or it can simply say the system is temporarily unavailable after obtaining a username and password.

NEW QUESTION 165
- (Topic 2)
Switches maintain a CAM Table that maps individual MAC addresses on the network to physical ports on the switch.



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

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

Answer: A

NEW QUESTION 166
- (Topic 2)
Sam, a professional hacker. targeted an organization with intention of compromising AWS IAM credentials. He attempted to lure one of the employees of the organization by initiating fake calls while posing as a legitimate employee. Moreover, he sent phishing emails to steal the AWS 1AM credentials and further compromise the employee's account. What is the technique used by Sam to compromise the AWS IAM credentials?

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

Answer: A

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

NEW QUESTION 171
- (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

NEW QUESTION 175
- (Topic 2)
An LDAP directory can be used to store information similar to a SQL database. LDAP uses a database structure instead of SQL??s structure. Because of this, LDAP has difficulty representing many-to-one relationships.

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

Answer: C

NEW QUESTION 176
- (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)

NEW QUESTION 177
- (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.

NEW QUESTION 180
- (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 clausewith 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

NEW QUESTION 182
- (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

NEW QUESTION 184
- (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

NEW QUESTION 188
- (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.

NEW QUESTION 193
- (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

NEW QUESTION 195
- (Topic 3)
An ethical hacker is scanning a target network. They initiate a TCP connection by sending an SYN packet to a target machine and receiving a SYN/ACK packet in response. But instead of completing the three-way handshake with an ACK packet, they send an RST packet. What kind of scan is the ethical hacker likely performing and what is their goal?

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

Answer: A

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

NEW QUESTION 197
- (Topic 3)
You are a cybersecurity consultant for a healthcare organization that utilizes Internet of Medical Things (IoMT) 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 IoMT 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 IoMT devices.
B. Disable all wireless connectivity on IoMT devices.
C. Use network segmentation to isolate IoMT devices from the main network.
D. Regularly change the IP addresses of all IoMT devices.

Answer: C

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

names, MAC addresses, or
vulnerabilities. References:
? What Is Internet of Medical Things (IoMT) Security?
? 5 Steps to Secure Internet of Medical Things Devices
? Ransomware in Healthcare: How to Protect Your Organization
? [Network Segmentation: Definition, Benefits, and Best Practices]

NEW QUESTION 198
- (Topic 3)
As a cybersecurity professional, you are responsible for securing a high-traffic web application that uses MySQL as its backend database. Recently, there has been a surge of unauthorized login attempts, and you suspect that a seasoned black-hat hacker is behind them. This hacker has shown proficiency in SQL Injection and appears to be using the 'UNION' SQL keyword to trick the login process into returning additional data.
However, your application's security measures include filtering special characters in user inputs, a method usually effective against such attacks. In this challenging environment, if the hacker still intends to exploit this SQL Injection vulnerability, which strategy is he most likely to employ?

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

Answer: D

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

NEW QUESTION 201
- (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

NEW QUESTION 204
- (Topic 3)
Your organization has signed an agreement with a web hosting provider that requires you to take full responsibility of the maintenance of the cloud-based resources. Which of the following models covers this?

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

Answer: C

NEW QUESTION 208
- (Topic 3)
George, an employee of an organization, is attempting to access restricted websites from an official computer. For this purpose, he used an anonymizer that masked his real IP address and ensured complete and continuous anonymity for all his online activities. Which of the following anonymizers helps George hide his activities?

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

Answer: B

NEW QUESTION 211
- (Topic 3)
Ron, a security professional, was pen testing web applications and SaaS platforms used by his company. While testing, he found a vulnerability that allows hackers to gain unauthorized access to API objects and perform actions such as view, update, and delete sensitive data of the company. What is the API vulnerability revealed in the above scenario?

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

Answer: C

NEW QUESTION 212
- (Topic 3)
You are an ethical hacker contracted to conduct a security audit for a company. During the audit, you discover that the company's wireless network is using WEP encryption. You understand the vulnerabilities associated with WEP and plan to recommend a more secure encryption method. Which of the following would you recommend as a Suitable replacement to enhance the security of the company's wireless network?

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

Answer: B

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

NEW QUESTION 213
- (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.

NEW QUESTION 216
- (Topic 3)
Which of the following tactics uses malicious code to redirect users' web traffic?

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

Answer: B

NEW QUESTION 218
- (Topic 3)
In both pharming and phishing attacks, an attacker can create websites that look similar to legitimate sites with the intent of collecting personal identifiable information from its victims.
What is the difference between pharming and phishing attacks?

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

Answer: A

NEW QUESTION 222
- (Topic 3)
Bob, your senior colleague, has sent you a mail regarding a deal with one of the clients. You are requested to accept the offer and you oblige. After 2 days, Bab denies that he had ever sent a mail. What do you want to ????know???? to prove yourself that it was Bob who had send a mail?

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

Answer: A

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

NEW QUESTION 224
- (Topic 3)
Sam, a web developer, was instructed to incorporate a hybrid encryption software program into a web application to secure email messages. Sam used an encryption software, which is a free implementation of the OpenPGP standard that uses both symmetric-key cryptography and asymmetric-key cryptography for improved speed and secure key exchange. What is the encryption software employed by Sam for securing the email messages?

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

Answer: A

NEW QUESTION 226
- (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

NEW QUESTION 228
- (Topic 3)
Cross-site request forgery involves:

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

Answer: C

Explanation:
https://owasp.org/www-community/attacks/csrf
Cross-Site Request Forgery (CSRF) is an attack that forces an end user to execute unwanted actions on a web application in which they??re currently authenticated. With a little help of social engineering (such as sending a link via email or chat), an attacker may trick the users of a web application into executing actions of the attacker??s choosing. If the victim is a normal user, a successful CSRF attack can force the user to perform state changing requests like transferring funds, changing their email address, and so forth. If the victim is an administrative account, CSRF can compromise the entire web application.
CSRF is an attack that tricks the victim into submitting a malicious request. It inherits the identity and privileges of the victim to perform an undesired function on the victim??s behalf. For most sites, browser requests automatically include any credentials associated with the site, such as the user??s session cookie, IP address, Windows domain credentials, and so forth. Therefore, if the user is currently authenticated to the site, the site will have no way to distinguish between the forged request sent by the victim and a legitimate request sent by the victim.
CSRF attacks target functionality that causes a state change on the server, such as changing the victim??s email address or password, or purchasing something. Forcing the victim to retrieve data doesn??t benefit an attacker because the attacker doesn??t receive the response, the victim does. As such, CSRF attacks target state-changing requests.
It??s sometimes possible to store the CSRF attack on the vulnerable site itself. Such vulnerabilities are called ??stored CSRF flaws??. This can be accomplished by simply storing an IMG or IFRAME tag in a field that accepts HTML, or by a more complex cross-site scripting attack. If the attack can store a CSRF attack in the site, the severity of the attack
is amplified. In particular, the likelihood is increased because the victim is more likely to view the page containing the attack than some random page on the Internet. The likelihood is also increased because the victim is sure to be authenticated to the site already.

NEW QUESTION 230
- (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

NEW QUESTION 231
- (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)

NEW QUESTION 233
- (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:
? 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

NEW QUESTION 238
- (Topic 3)
Upon establishing his new startup, Tom hired a cloud service provider (CSP) but was dissatisfied with their service and wanted to move to another CSP.
What part of the contract might prevent him from doing so?

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

Answer: B

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

NEW QUESTION 242
- (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:
? 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

NEW QUESTION 244
- (Topic 3)
When you are testing a web application, it is very useful to employ a proxy tool to save every request and response. You can manually test every request and analyze the response to find vulnerabilities. You can test parameter and headers manually to get more precise results than if using web vulnerability scanners. What proxy tool will help you find web vulnerabilities?

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

Answer: C

NEW QUESTION 245
- (Topic 3)
Stephen, an attacker, targeted the industrial control systems of an organization. He generated a fraudulent email with a malicious attachment and sent it to employees of the target organization. An employee who manages the sales software of the operational plant opened the fraudulent email and clicked on the malicious attachment. This resulted in the malicious attachment being downloaded and malware being injected into the sales software maintained in the victim's system. Further, the malware propagated itself to other networked systems, finally damaging the industrial automation components. What is the attack technique used by Stephen to damage the industrial systems?

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

Answer: A

NEW QUESTION 247
- (Topic 3)
Jack, a disgruntled ex-employee of Incalsol Ltd., decided to inject fileless malware into Incalsol's systems. To deliver the malware, he used the current employees' email IDs to send fraudulent emails embedded with malicious links that seem to be legitimate. When a victim employee clicks on the link, they are directed to a fraudulent website that automatically loads Flash and triggers the exploit. What is the technique used byjack to launch the fileless malware on the target systems?

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

Answer: B

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

NEW QUESTION 251
- (Topic 3)
Jude, a pen tester working in Keiltech Ltd., performs sophisticated security testing on his company's network infrastructure to identify security loopholes. In this process, he started to circumvent the network protection tools and firewalls used in the company. He employed a technique that can create forged TCP sessions by carrying out multiple SYN, ACK, and RST or FIN packets. Further, this process allowed Jude to execute DDoS attacks that can exhaust the network resources. What is the attack technique used by Jude for finding loopholes in the above scenario?

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

Answer: C

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

NEW QUESTION 256
- (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

NEW QUESTION 259
- (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.

NEW QUESTION 260
- (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

NEW QUESTION 264
- (Topic 3)
A hacker has successfully infected an internet-facing server which he will then use to send junk mail, take part in coordinated attacks, or host junk email content.
Which sort of trojan infects this server?

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

Answer: A

NEW QUESTION 265
- (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/

NEW QUESTION 268
- (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

NEW QUESTION 270
- (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

NEW QUESTION 273
- (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

NEW QUESTION 274
- (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

NEW QUESTION 278

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual 312-50v13 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the 312-50v13 Product From:

https://www.2passeasy.com/dumps/312-50v13/

Money Back Guarantee

312-50v13 Practice Exam Features:

* 312-50v13 Questions and Answers Updated Frequently

* 312-50v13 Practice Questions Verified by Expert Senior Certified Staff

* 312-50v13 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* 312-50v13 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year