EC-Council

Exam Questions 312-50v12

Certified Ethical Hacker Exam (CEHv12)

NEW QUESTION 1
- (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 2
- (Exam Topic 3)
Which among the following is the best example of the third step (delivery) in the cyber kill chain?

A. An intruder sends a malicious attachment via email to a target.
B. An intruder creates malware to be used as a malicious attachment to an email.
C. An intruder's malware is triggered when a target opens a malicious email attachment.
D. An intruder's malware is installed on a target's machine.

Answer: A

NEW QUESTION 3
- (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 4
- (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 5
- (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 6
- (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 7
- (Exam Topic 3)
Dorian Is sending a digitally signed email to Polly, with which key is Dorian signing this message and how is Poly validating It?

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

Answer: C

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

NEW QUESTION 8
- (Exam Topic 3)
Heather's company has decided to use a new customer relationship management tool. After performing the appropriate research, they decided to purchase a subscription to a cloud-hosted solution. The only administrative task that Heather will need to perform is the management of user accounts. The provider will take care of the hardware, operating system, and software administration including patching and monitoring. Which of the following is this type of solution?

A. SaaS
B. IaaS
C. CaaS
D. PasS

Answer: A

Explanation:
Software as a service (SaaS) allows users to attach to and use cloud-based apps over the web. Common examples ar email, calendaring and workplace tool (such as Microsoft workplace 365).
SaaS provides a whole software solution that you get on a pay-as-you-go basis from a cloud service provider. You rent the use of an app for your organisation and your users connect with it over the web, typically with an internet browser. All of the underlying infrastructure, middleware, app software system and app knowledge ar located within the service provider's knowledge center. The service provider manages the hardware and software system and with the appropriate service agreement, can make sure the availability and also the security of the app and your data as well. SaaS allows your organisation to induce quickly up and running with an app at token upfront cost.
Common SaaS scenariosThis tool having used a web-based email service like Outlook, Hotmail or Yahoo! Mail, then you have got already used a form of SaaS. With these services, you log into your account over the web, typically from an internet browser. the e-mail software system is found on the service provider's network and your messages ar hold on there moreover. you can access your email and hold on messages from an internet browser on any laptop or Internet-connected device.
The previous examples are free services for personal use. For organisational use, you can rent productivity apps, like email, collaboration and calendaring; and sophisticated business applications like client relationship management (CRM), enterprise resource coming up with (ERP) and document management. You buy the use of those apps by subscription or per the level of use.
Advantages of SaaSGain access to stylish applications. to supply SaaS apps to users, you don't ought to purchase, install, update or maintain any hardware,

middleware or software system. SaaS makes even sophisticated enterprise applications, like ERP and CRM, affordable for organisations that lack the resources to shop for, deploy and manage the specified infrastructure and software system themselves.
Pay just for what you utilize. you furthermore may economize because the SaaS service automatically scales up and down per the level of usage.
Use free shopper software system. Users will run most SaaS apps directly from their web browser without needing to transfer and install any software system, though some apps need plugins. this suggests that you simply don't ought to purchase and install special software system for your users.
Mobilise your hands simply. SaaS makes it simple to "mobilise" your hands as a result of users will access SaaS apps and knowledge from any Internet-connected laptop or mobile device. You don't ought to worry concerning developing apps to run on differing types of computers and devices as a result of the service supplier has already done therefore. additionally, you don't ought to bring special experience aboard to manage the safety problems inherent in mobile computing. A fastidiously chosen service supplier can make sure the security of your knowledge, no matter the sort of device intense it.
Access app knowledge from anyplace. With knowledge hold on within the cloud, users will access their info from any Internet-connected laptop or mobile device. And once app knowledge is hold on within the cloud, no knowledge is lost if a user's laptop or device fails.

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

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

Answer: D

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

NEW QUESTION 10
- (Exam Topic 3)
Which of the following tactics uses malicious code to redirect users' web traffic?

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

Answer: B

NEW QUESTION 10
- (Exam Topic 3)
Joel, a professional hacker, targeted a company and identified the types of websites frequently visited by its employees. Using this information, he searched for possible loopholes in these websites and injected a malicious script that can redirect users from the web page and download malware onto a victim's machine. Joel waits for the victim to access the infected web application so as to compromise the victim's machine. Which of the following techniques is used by Joel in the above scenario?

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

Answer: B

Explanation:
https://en.wikipedia.org/wiki/Clickjacking
Clickjacking is an attack that tricks a user into clicking a webpage element which is invisible or disguised as another element. This can cause users to unwittingly download malware, visit malicious web pages, provide credentials or sensitive information, transfer money, or purchase products online.

Typically, clickjacking is performed by displaying an invisible page or HTML element, inside an iframe, on top of the page the user sees. The user believes they are clicking the visible page but in fact they are clicking an invisible element in the additional page transposed on top of it.

NEW QUESTION 15
- (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 16
- (Exam Topic 3)
Lewis, a professional hacker, targeted the loT cameras and devices used by a target venture-capital firm. He used an information-gathering tool to collect information about the loT devices connected to a network, open ports and services, and the attack surface area. Using this tool, he also generated statistical reports on broad usage patterns and trends. This tool helped Lewis continually monitor every reachable server and device on the Internet, further allowing him to exploit these devices in the network. Which of the following tools was employed by Lewis in the above scenario?

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

Answer: A

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

NEW QUESTION 20
- (Exam Topic 3)
Which of the following allows attackers to draw a map or outline the target organization's network infrastructure to know about the actual environment that they are going to hack.

A. Enumeration
B. Vulnerability analysis
C. Malware analysis
D. Scanning networks

Answer: D

NEW QUESTION 21
- (Exam Topic 3)
What type of virus is most likely to remain undetected by antivirus software?

A. Cavity virus
B. Stealth virus
C. File-extension virus
D. Macro virus

Answer: B

NEW QUESTION 25
- (Exam Topic 3)
Which of the following is a passive wireless packet analyzer that works on Linux-based systems?

A. Burp Suite
B. OpenVAS
C. tshark
D. Kismet

Answer: C

NEW QUESTION 30
- (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 35
- (Exam Topic 3)
Henry is a penetration tester who works for XYZ organization. While performing enumeration on a client organization, he queries the DNS server for a specific cached DNS record. Further, by using this cached record, he determines the sites recently visited by the organization's user. What is the enumeration technique used by Henry on the organization?

A. DNS zone walking
B. DNS cache snooping
C. DNS SEC zone walking
D. DNS cache poisoning

Answer: B

NEW QUESTION 40
- (Exam Topic 3)
Which of the following Metasploit post-exploitation modules can be used to escalate privileges on Windows systems?

A. getsystem
B. getuid
C. keylogrecorder
D. autoroute

Answer: A

NEW QUESTION 42
- (Exam Topic 3)
Which protocol is used for setting up secure channels between two devices, typically in VPNs?

A. PEM
B. ppp
C. IPSEC
D. SET

Answer: C

NEW QUESTION 46
- (Exam Topic 3)
Kevin, an encryption specialist, implemented a technique that enhances the security of keys used for encryption and authentication. Using this technique, Kevin input an initial key to an algorithm that generated an enhanced key that is resistant to brute-force attacks. What is the technique employed by Kevin to improve the security of encryption keys?

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

Answer: D

NEW QUESTION 50
- (Exam Topic 3)
How can rainbow tables be defeated?

A. Use of non-dictionary words
B. All uppercase character passwords
C. Password salting
D. Lockout accounts under brute force password cracking attempts

Answer: C

Explanation:
https://en.wikipedia.org/wiki/Salt_(cryptography)
A salt is random data that is used as an additional input to a one-way function that hashes data, a password, or passphrase. Salts are used to safeguard passwords in storage. Historically a password was stored in plaintext on a system, but over time additional safeguards were developed to protect a user's password against being read from the system. A salt is one of those methods.

A new salt is randomly generated for each password. In a typical setting, the salt and the password (or its version after key stretching) are concatenated and processed with a cryptographic hash function, and the output hash value (but not the original password) is stored with the salt in a database. Hashing allows for later authentication without keeping and therefore risking exposure of the plaintext password in the event that the authentication data store is compromised.
Salts defend against a pre-computed hash attack, e.g. rainbow tables. Since salts do not have to be memorized by humans they can make the size of the hash table required for a successful attack prohibitively large without placing a burden on the users. Since salts are different in each case, they also protect commonly used passwords, or those users who use the same password on several sites, by making all salted hash instances for the same password different from each other.

NEW QUESTION 51
- (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 55
- (Exam Topic 3)
Which of the following types of SQL injection attacks extends the results returned by the original query, enabling attackers to run two or more statements if they have the same structure as the original one?

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

Answer: D

NEW QUESTION 58
- (Exam Topic 3)
You want to analyze packets on your wireless network. Which program would you use?

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

Answer: A

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

NEW QUESTION 62
- (Exam Topic 3)
What would you enter if you wanted to perform a stealth scan using Nmap?

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

Answer: C

NEW QUESTION 64
- (Exam Topic 3)
if you send a TCP ACK segment to a known closed port on a firewall but it does not respond with an RST. what do you know about the firewall you are scanning?

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

Answer: B

NEW QUESTION 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 74
- (Exam Topic 3)
Bob, your senior colleague, has sent you a mail regarding a deal with one of the clients. You are requested to accept the offer and you oblige. After 2 days, Bab denies that he had ever sent a mail. What do you want to ""know"" to prove yourself that it was Bob who had send a mail?

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

Answer: A

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

NEW QUESTION 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 80
- (Exam Topic 3)
If executives are found liable for not properly protecting their company's assets and information systems, what type of law would apply in this situation?

A. Criminal
B. International
C. Common
D. Civil

Answer: D

NEW QUESTION 83
- (Exam Topic 3)
Sophia is a shopping enthusiast who spends significant time searching for trendy outfits online. Clark, an attacker, noticed her activities several times and sent a fake email containing a deceptive page link to her social media page displaying all-new and trendy outfits. In excitement, Sophia clicked on the malicious link and logged in to that page using her valid credentials. Which of the following tools is employed by Clark to create the spoofed email?

A. PyLoris
B. Slowloris
C. Evilginx
D. PLCinject

Answer: C

NEW QUESTION 85
- (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)
An attacker identified that a user and an access point are both compatible with WPA2 and WPA3 encryption. The attacker installed a rogue access point with only WPA2 compatibility in the vicinity and forced the victim to go through the WPA2 four-way handshake to get connected. After the connection was established, the attacker used automated tools to crack WPA2-encrypted messages. What is the attack performed in the above scenario?

A. Timing-based attack
B. Side-channel attack
C. Downgrade security attack
D. Cache-based attack

Answer: B

NEW QUESTION 91
- (Exam Topic 3)
Miley, a professional hacker, decided to attack a target organization's network. To perform the attack, she used a tool to send fake ARP messages over the target network to link her MAC address with the target system's IP address. By performing this, Miley received messages directed to the victim's MAC address and further used the tool to intercept, steal, modify, and block sensitive communication to the target system. What is the tool employed by Miley to perform the above attack?

A. Gobbler
B. KDerpNSpoof
C. BetterCAP
D. Wireshark

Answer: C

NEW QUESTION 95
- (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 97
- (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 102
- (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 107
- (Exam Topic 3)
A group of hackers were roaming around a bank office building in a city, driving a luxury car. They were using hacking tools on their laptop with the intention to find a free-access wireless network. What is this hacking process known as?

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

Answer: C

NEW QUESTION 111
- (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 115
- (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 117
- (Exam Topic 3)
Upon establishing his new startup, Tom hired a cloud service provider (CSP) but was dissatisfied with their service and wanted to move to another CSP. What part of the contract might prevent him from doing so?

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

Answer: B

NEW QUESTION 121
- (Exam Topic 3)
Which rootkit is characterized by its function of adding code and/or replacing some of the operating-system kernel code to obscure a backdoor on a system?

A. User-mode rootkit
B. Library-level rootkit
C. Kernel-level rootkit
D. Hypervisor-level rootkit

Answer: C

NEW QUESTION 125
- (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 130

- (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 135
- (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 140
- (Exam Topic 3)
This type of injection attack does not show any error message. It is difficult to exploit as it returns information when the application is given SQL payloads that elicit a true or false response from the server. By observing the response, an attacker can extract sensitive information. What type of attack is this?

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

Answer: D

NEW QUESTION 143
- (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 146
- (Exam Topic 3)
What type of a vulnerability/attack is it when the malicious person forces the user’s browser to send an authenticated request to a server?

A. Session hijacking
B. Server side request forgery
C. Cross-site request forgery
D. Cross-site scripting

Answer: C

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

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

Answer: B

Explanation:
In this attack KRACK is an acronym for Key Reinstallation Attack. KRACK may be a severe replay attack on Wi-Fi Protected Access protocol (WPA2), which secures your Wi-Fi connection. Hackers use KRACK to take advantage of a vulnerability in WPA2. When in close range of a possible victim, attackers can access and skim encrypted data using KRACK.

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

NEW QUESTION 152
- (Exam Topic 3)
You are logged in as a local admin on a Windows 7 system and you need to launch the Computer Management Console from command line.
Which command would you use?

A. c:\compmgmt.msc
B. c:\services.msc
C. c:\ncpa.cp
D. c:\gpedit

Answer: A

Explanation:
To start the Computer Management Console from command line just type compmgmt.msc
/computer:computername in your run box or at the command line and it should automatically open the Computer Management console.
References:
http://www.waynezim.com/tag/compmgmtmsc/

NEW QUESTION 157
- (Exam Topic 3)
An attacker utilizes a Wi-Fi Pineapple to run an access point with a legitimate-looking SSID for a nearby business in order to capture the wireless password. What kind of attack is this?

A. MAC spoofing attack
B. Evil-twin attack
C. War driving attack
D. Phishing attack

Answer: B

NEW QUESTION 158
- (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 159
- (Exam Topic 3)
Which access control mechanism allows for multiple systems to use a central authentication server (CAS) that permits users to authenticate once and gain access to multiple systems?

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

Answer: C

NEW QUESTION 164
- (Exam Topic 3)
In both pharming and phishing attacks, an attacker can create websites that look similar to legitimate sites with the intent of collecting personal identifiable information from its victims.
What is the difference between pharming and phishing attacks?

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

Answer: A

NEW QUESTION 165
- (Exam Topic 3)
Mr. Omkar performed tool-based vulnerability assessment and found two vulnerabilities. During analysis, he found that these issues are not true vulnerabilities.
What will you call these issues?

A. False positives
B. True negatives
C. True positives
D. False negatives

Answer: A

Explanation:
False Positives occur when a scanner, Web Application Firewall (WAF), or Intrusion Prevention System (IPS) flags a security vulnerability that you do not have. A false negative is the opposite of a false positive, telling you that you don't have a vulnerability when, in fact, you do.
A false positive is like a false alarm; your house alarm goes off, but there is no burglar. In web application security, a false positive is when a web application security scanner indicates that there is a vulnerability on your website, such as SQL Injection, when, in reality, there is not. Web security experts and penetration testers use automated web application security scanners to ease the penetration testing process. These tools help them ensure that all web application attack surfaces are correctly tested in a reasonable amount of time. But many false positives tend to break down this process. If the first 20 variants are false, the penetration tester assumes that all the others are false positives and ignore the rest. By doing so, there is a good chance that real web application vulnerabilities will be left undetected.
When checking for false positives, you want to ensure that they are indeed false. By nature, we humans tend to start ignoring false positives rather quickly. For example, suppose a web application security scanner detects 100 SQL Injection vulnerabilities. If the first 20 variants are false positives, the penetration tester assumes that all the others are false positives and ignore all the rest. By doing so, there are chances that real web application vulnerabilities are left undetected. This is why it is crucial to check every vulnerability and deal with each false positive separately to ensure false positives.

NEW QUESTION 167
- (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 172
- (Exam Topic 3)
Which Nmap option would you use if you were not concerned about being detected and wanted to perform a very fast scan?

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

Answer: A

NEW QUESTION 177
- (Exam Topic 3)

Becky has been hired by a client from Dubai to perform a penetration test against one of their remote offices. Working from her location in Columbus, Ohio, Becky runs her usual reconnaissance scans to obtain basic information about their network. When analyzing the results of her Whois search, Becky notices that the IP was allocated to a location in Le Havre, France. Which regional Internet registry should Becky go to for detailed information?

A. ARIN
B. APNIC
C. RIPE
D. LACNIC

Answer: C

Explanation:
Regional Internet Registries (RIRs):
ARIN (American Registry for Internet Numbers) AFRINIC (African Network Information Center) APNIC (Asia Pacific Network Information Center)
RIPE (Réseaux IP Européens Network Coordination Centre)
LACNIC (Latin American and Caribbean Network Information Center)

NEW QUESTION 178
- (Exam Topic 3)
Ron, a security professional, was pen testing web applications and SaaS platforms used by his company. While testing, he found a vulnerability that allows hackers to gain unauthorized access to API objects and perform actions such as view, update, and delete sensitive data of the company. What is the API vulnerability revealed in the above scenario?

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

Answer: B

NEW QUESTION 179
- (Exam Topic 3)
A computer science student needs to fill some information into a secured Adobe PDF job application that was received from a prospective employer. Instead of requesting a new document that allowed the forms to be completed, the student decides to write a script that pulls passwords from a list of commonly used passwords to try against the secured PDF until the correct password is found or the list is exhausted.
Which cryptography attack is the student attempting?

A. Man-in-the-middle attack
B. Brute-force attack
C. Dictionary attack
D. Session hijacking

Answer: C

NEW QUESTION 182
- (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 187
- (Exam Topic 2)
what are common files on a web server that can be misconfigured and provide useful Information for a hacker such as verbose error messages?

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

Answer: D

Explanation:
The php.ini file may be a special file for PHP. it's where you declare changes to your PHP settings. The server is already configured with standard settings for

PHP, which your site will use by default. Unless you would like to vary one or more settings, there's no got to create or modify a php.ini file. If you'd wish to make any changes to settings, please do so through the MultiPHP INI Editor.

NEW QUESTION 189
- (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 194
- (Exam Topic 2)
Robin, an attacker, is attempting to bypass the firewalls of an organization through the DNS tunneling method in order to exfiltrate data. He is using the NSTX tool for bypassing the firewalls. On which of the following ports should Robin run the NSTX tool?

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

Answer: A

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

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

NEW QUESTION 197
- (Exam Topic 2)
Bella, a security professional working at an it firm, finds that a security breach has occurred while transferring important files. Sensitive data, employee usernames. and passwords are shared In plaintext, paving the way for hackers 10 perform successful session hijacking. To address this situation. Bella Implemented a protocol that sends data using encryption and digital certificates. Which of the following protocols Is used by Bella?

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

Answer: C

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

NEW QUESTION 198
- (Exam Topic 2)

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

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

Answer: B

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

NEW QUESTION 199
- (Exam Topic 2)
What does the following command in netcat do? nc -l -u -p55555 < /etc/passwd

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

Answer: C

NEW QUESTION 201
- (Exam Topic 2)
What piece of hardware on a computer's motherboard generates encryption keys and only releases a part of the key so that decrypting a disk on a new piece of hardware is not possible?

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

Answer: D

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

NEW QUESTION 205
- (Exam Topic 2)
Switches maintain a CAM Table that maps individual MAC addresses on the network to physical ports on the switch.

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

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

Answer: A

NEW QUESTION 208
- (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 209

- (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 213
- (Exam Topic 2)
A pen tester is configuring a Windows laptop for a test. In setting up Wireshark, what river and library are required to allow the NIC to work in promiscuous mode?

A. Libpcap
B. Awinpcap
C. Winprom
D. Winpcap

Answer: D

NEW QUESTION 218
- (Exam Topic 2)
Andrew is an Ethical Hacker who was assigned the task of discovering all the active devices hidden by a restrictive firewall in the IPv4 range in a given target network.
Which of the following host discovery techniques must he use to perform the given task?

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

Answer: C

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

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

NEW QUESTION 220
- (Exam Topic 2)
ViruXine.W32 virus hides their presence by changing the underlying executable code.
This Virus code mutates while keeping the original algorithm intact, the code changes itself each time it runs, but the function of the code (its semantics) will not change at all.

Here is a section of the Virus code:

What is this technique called?

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

Answer: A

NEW QUESTION 225
- (Exam Topic 2)
in the Common Vulnerability Scoring System (CVSS) v3.1 severity ratings, what range does medium vulnerability fall in?

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

Answer: C

Explanation:

NEW QUESTION 228
- (Exam Topic 2)
Harry. a professional hacker, targets the IT infrastructure of an organization. After preparing for the attack, he attempts to enter the target network using techniques such as sending spear-phishing emails and exploiting vulnerabilities on publicly available servers. Using these techniques, he successfully deployed malware on the target system to establish an outbound connection. What is the APT lifecycle phase that Harry is currently executing?

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

Answer: D

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

NEW QUESTION 229
- (Exam Topic 2)
What type of analysis is performed when an attacker has partial knowledge of inner-workings of the application?

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

Answer: D

NEW QUESTION 232
- (Exam Topic 2)
Which of the following are well known password-cracking programs?

A. L0phtcrack
B. NetCat
C. Jack the Ripper
D. Netbus
E. John the Ripper

Answer: AE

NEW QUESTION 234
- (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 236
- (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 240
- (Exam Topic 2)
George is a security professional working for iTech Solutions. He was tasked with securely transferring sensitive data of the organization between industrial systems. In this process, he used a short-range communication protocol based on the IEEE 203.15.4 standard. This protocol is used in devices that transfer data infrequently at a low rate in a restricted area, within a range of 10-100 m. What is the short-range wireless communication technology George employed in the above scenario?

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

Answer: C

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

Support for multiple network topologies like point-to-point, point-to-multipoint and mesh networks
Low duty cycle – provides long battery life
Low latency
Direct Sequence unfold Spectrum (DSSS)
Up to 65,000 nodes per network
128-bit AES encryption for secure information connections
Collision avoidance, retries and acknowledgements
This is another short-range communication protocol based on the IEEE 203.15.4 standard. Zig-Bee is used in devices that transfer data infrequently at a low rate in a restricted area and within a range of 10–100 m.

NEW QUESTION 242
- (Exam Topic 2)
which of the following Bluetooth hacking techniques refers to the theft of information from a wireless device through Bluetooth?

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

Answer: D

Explanation:
Bluesnarfing is the unauthorized access of information from a wireless device through Ba luetooth connection, often between phones, desktops, laptops, and PDAs (personal digital assistant).

NEW QUESTION 246
- (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

NEW QUESTION 248
- (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 253
- (Exam Topic 2)
Which type of sniffing technique is generally referred as MiTM attack?

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

Answer: B

NEW QUESTION 254
- (Exam Topic 2)
Study the snort rule given below and interpret the rule. alert tcp any any --> 192.168.1.0/24 111 (content:"|00 01 86 a5|"; msG. "mountd access";)

A. An alert is generated when a TCP packet is generated from any IP on the 192.168.1.0 subnet and destined to any IP on port 111
B. An alert is generated when any packet other than a TCP packet is seen on the network and destined for the 192.168.1.0 subnet
C. An alert is generated when a TCP packet is originated from port 111 of any IP address to the 192.168.1.0 subnet
D. An alert is generated when a TCP packet originating from any IP address is seen on the network and destined for any IP address on the 192.168.1.0 subnet on port 111

Answer: D

NEW QUESTION 255
- (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 259
- (Exam Topic 2)
What is the purpose of DNS AAAA record?

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

Answer: D

NEW QUESTION 260
- (Exam Topic 2)
Which file is a rich target to discover the structure of a website during web-server footprinting?

A. Document root
B. Robots.txt
C. domain.txt
D. index.html

Answer: B

NEW QUESTION 264
- (Exam Topic 2)
These hackers have limited or no training and know how to use only basic techniques or tools. What kind of hackers are we talking about?

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

Answer: B

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

NEW QUESTION 267
- (Exam Topic 2)
You are performing a penetration test for a client and have gained shell access to a Windows machine on the internal network. You intend to retrieve all DNS records for the internal domain, if the DNS server is at 192.168.10.2 and the domain name is abccorp.local, what command would you type at the nslookup prompt to attempt a zone transfer?

A. list server=192.168.10.2 type=all
B. is-d abccorp.local

C. Iserver 192.168.10.2-t all
D. List domain=Abccorp.local type=zone

Answer: B

NEW QUESTION 270
- (Exam Topic 2)
You work for Acme Corporation as Sales Manager. The company has tight network security restrictions. You are trying to steal data from the company's Sales database (Sales.xls) and transfer them to your home computer. Your company filters and monitors traffic that leaves from the internal network to the Internet. How will you achieve this without raising suspicion?

A. Encrypt the Sales.xls using PGP and e-mail it to your personal gmail account
B. Package the Sales.xls using Trojan wrappers and telnet them back your home computer
C. You can conceal the Sales.xls database in another file like photo.jpg or other files and send it out in aninnocent looking email or file transfer using Steganography techniques
D. Change the extension of Sales.xls to sales.txt and upload them as attachment to your hotmail account

Answer: C

NEW QUESTION 275
- (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 278
- (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 281
- (Exam Topic 2)
This kind of password cracking method uses word lists in combination with numbers and special characters:

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

Answer: A

NEW QUESTION 285
- (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 288
- (Exam Topic 2)
Susan, a software developer, wants her web API to update other applications with the latest information. For this purpose, she uses a user-defined HTTP tailback or push APIs that are raised based on trigger events: when invoked, this feature supplies data to other applications so that users can instantly receive real-time Information.
Which of the following techniques is employed by Susan?

A. web shells
B. Webhooks
C. REST API
D. SOAP API

Answer: B

Explanation:
Webhooks are one of a few ways internet applications will communicate with one another.
It allows you to send real-time data from one application to another whenever a given event happens.
For example, let's say you've created an application using the Foursquare API that tracks when people check into your restaurant. You ideally wish to be able to greet customers by name and provide a complimentary drink when they check in.
What a webhook will is notify you any time someone checks in, therefore you'd be able to run any processes that you simply had in your application once this event is triggered.
The data is then sent over the web from the application wherever the event originally occurred, to the receiving application that handles the data.
Here's a visual representation of what that looks like:

A webhook url is provided by the receiving application, and acts as a phone number that the other application will call once an event happens.
Only it's more complicated than a phone number, because data about the event is shipped to the webhook url in either JSON or XML format. this is known as the "payload."
Here's an example of what a webhook url looks like with the payload it's carrying:

What are Webhooks? Webhooks are user-defined HTTP callback or push APIs that are raised based on events triggered, such as comment received on a post and pushing code to the registry. A webhook allows an application to update other applications with the latest information. Once invoked, it supplies data to the other applications, which means that users instantly receive real-time information. Webhooks are sometimes called "Reverse APIs" as they provide what is required for API specification, and the developer should create an API to use a webhook. A webhook is an API concept that is also used to send text messages and notifications to mobile numbers or email addresses from an application when a specific event is triggered. For instance, if you search for something in the online store and the required item is out of stock, you click on the "Notify me" bar to get an alert from the application when that item is available for purchase. These notifications from the applications are usually sent through webhooks.

NEW QUESTION 292
- (Exam Topic 2)
What is the common name for a vulnerability disclosure program opened by companies In platforms such as HackerOne?

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

Answer: B

Explanation:
Bug bounty programs allow independent security researchers to report bugs to an companies and receive rewards or compensation. These bugs area unit sometimes security exploits and vulnerabilities, although they will additionally embody method problems, hardware flaws, and so on.
The reports area unit usually created through a program travel by associate degree freelance third party (like Bugcrowd or HackerOne). The companies can got wind of (and run) a program curated to the organization's wants.
Programs is also non-public (invite-only) wherever reports area unit unbroken confidential to the organization or public (where anyone will sign in and join). they will happen over a collection timeframe or with without stopping date (though the second possibility is a lot of common).
Who uses bug bounty programs?Many major organizations use bug bounties as an area of their security program, together with AOL, Android, Apple, Digital Ocean, and goldman Sachs. you'll read an inventory of all the programs offered by major bug bounty suppliers, Bugcrowd and HackerOne, at these links.
Why do corporations use bug bounty programs?Bug bounty programs provide corporations the flexibility to harness an outsized cluster of hackers so as to seek out bugs in their code.
This gives them access to a bigger variety of hackers or testers than they'd be able to access on a one-on-one basis. It {can also|also will|can even|may also|may} increase the probabilities that bugs area unit found and reported to them before malicious hackers can exploit them.
It may also be an honest publicity alternative for a firm. As bug bounties became a lot of common, having a bug bounty program will signal to the general public and even regulators that a corporation incorporates a mature security program.
This trend is likely to continue, as some have began to see bug bounty programs as an business normal that all companies ought to invest in.
Why do researchers and hackers participate in bug bounty programs?Finding and news bugs via a bug bounty program may end up in each money bonuses and recognition. In some cases, it will be a good thanks to show real-world expertise once you are looking for employment, or will even facilitate introduce you to parents on the protection team within an companies.
This can be full time income for a few of us, income to supplement employment, or the way to point out off your skills and find a full time job.
It may also be fun! it is a nice (legal) probability to check out your skills against huge companies and government agencies.
What area unit the disadvantages of a bug bounty program for independent researchers and hackers?A lot of hackers participate in these varieties of programs, and it will be tough to form a major quantity of cash on the platform.

In order to say the reward, the hacker has to be the primary person to submit the bug to the program. meaning that in apply, you may pay weeks searching for a bug to use, solely to be the person to report it and build no cash.
Roughly ninety seven of participants on major bug bounty platforms haven't sold-out a bug.
In fact, a 2019 report from HackerOne confirmed that out of quite three hundred,000 registered users, solely around two.5% received a bounty in their time on the platform.
Essentially, most hackers are not creating a lot of cash on these platforms, and really few square measure creating enough to switch a full time wage (plus they do not have advantages like vacation days, insurance, and retirement planning).
What square measure the disadvantages of bug bounty programs for organizations?These programs square measure solely helpful if the program ends up in the companies realizeing issues that they weren't able to find themselves (and if they'll fix those problems)!
If the companies is not mature enough to be able to quickly rectify known problems, a bug bounty program is not the right alternative for his or her companies.
Also, any bug bounty program is probably going to draw in an outsized range of submissions, several of which can not be high-quality submissions. a corporation must be ready to cope with the exaggerated volume of alerts, and also the risk of a coffee signal to noise magnitude relation (essentially that it's probably that they're going to receive quite few unhelpful reports for each useful report).
Additionally, if the program does not attract enough participants (or participants with the incorrect talent set, and so participants are not able to establish any bugs), the program is not useful for the companies.
The overwhelming majority of bug bounty participants consider web site vulnerabilities (72%, per HackerOn), whereas solely a number of (3.5%) value more highly to seek for package vulnerabilities.
This is probably because of the actual fact that hacking in operation systems (like network hardware and
memory) needs a big quantity of extremely specialised experience. this implies that firms may even see vital come on investment for bug bounties on websites, and not for alternative applications, notably those that need specialised experience.
This conjointly implies that organizations which require to look at AN application or web site among a selected time-frame may not need to rely on a bug bounty as there is no guarantee of once or if they receive reports.
Finally, it are often probably risky to permit freelance researchers to try to penetrate your network. this could end in public speech act of bugs, inflicting name harm within the limelight (which could end in individuals not eager to purchase the organizations' product or service), or speech act of bugs to additional malicious third parties, United Nations agency may use this data to focus on the organization.

NEW QUESTION 294
- (Exam Topic 2)
infecting a system with malware and using phishing to gain credentials to a system or web application are examples of which phase of the ethical hacking methodology?

A. Reconnaissance
B. Maintaining access
C. Scanning
D. Gaining access

Answer: D

Explanation:
This phase having the hacker uses different techniques and tools to realize maximum data from the system.
they're –• Password cracking – Methods like Bruteforce, dictionary attack, rule-based attack, rainbow table a used. Bruteforce is trying all combinations of the password. Dictionary attack is trying an inventory of meaningful words until the password matches. Rainbow table takes the hash value of the password and compares with pre-computed hash values until a match is discovered.• Password attacks – Passive attacks like wire sniffing, replay attack. Active online attack like Trojans, keyloggers, hash injection, phishing. Offline attacks like pre-computed hash, distributed network and rainbow. Non electronic attack like shoulder surfing, social engineering and dumpster diving.

NEW QUESTION 296
- (Exam Topic 2)
Sam is working as a system administrator In an organization. He captured the principal characteristics of a vulnerability and produced a numerical score to reflect Its severity using CVSS v3.0 to property assess and prioritize the organization's vulnerability management processes. The base score that Sam obtained after performing cvss rating was 4.0. What is the CVSS severity level of the vulnerability discovered by Sam in the above scenario?

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

Answer: A

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

NEW QUESTION 298
- (Exam Topic 1)
When analyzing the IDS logs, the system administrator noticed an alert was logged when the external router was accessed from the administrator's Computer to update the router configuration. What type of an alert is this?

A. False negative
B. True negative
C. True positive
D. False positive

Answer: D

Explanation:
True Positive - IDS referring a behavior as an attack, in real life it is
True Negative - IDS referring a behavior not an attack and in real life it is not False Positive - IDS referring a behavior as an attack, in real life it is not
False Negative - IDS referring a behavior not an attack, but in real life is an attack. False Negative - is the most serious and dangerous state of all !!!!

NEW QUESTION 303
- (Exam Topic 1)
An attacker with access to the inside network of a small company launches a successful STP manipulation attack. What will he do next?

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

Answer: A

NEW QUESTION 307
- (Exam Topic 1)
You are tasked to perform a penetration test. While you are performing information gathering, you find an employee list in Google. You find the receptionist's email, and you send her an email changing the source email to her boss's email (boss@company). In this email, you ask for a pdf with information. She reads your email and sends back a pdf with links. You exchange the pdf links with your malicious links (these links contain malware) and send back the modified pdf, saying that the links don't work. She reads your email, opens the links, and her machine gets infected. You now have access to the company network. What testing method did you use?

A. Social engineering
B. Piggybacking
C. Tailgating
D. Eavesdropping

Answer: A

Explanation:
Social engineering is the term used for a broad range of malicious activities accomplished through human interactions. It uses psychological manipulation to trick users into making security mistakes or giving away
sensitive information.
Social engineering attacks typically involve some form of psychological manipulation, fooling otherwise unsuspecting users or employees into handing over confidential or sensitive data. Commonly, social engineering involves email or other communication that invokes urgency, fear, or similar emotions in the victim, leading the victim to promptly reveal sensitive information, click a malicious link, or open a malicious file. Because social engineering involves a human element, preventing these attacks can be tricky for enterprises.

NEW QUESTION 311
- (Exam Topic 1)
You have the SOA presented below in your Zone.
Your secondary servers have not been able to contact your primary server to synchronize information. How long will the secondary servers attempt to contact the primary server before it considers that zone is dead and stops responding to queries?
collegae.edu.SOA, cikkye.edu ipad.college.edu. (200302028 3600 3600 604800 3600)

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

Answer: C

NEW QUESTION 316
- (Exam Topic 1)
Null sessions are un-authenticated connections (not using a username or password.) to an NT or 2000 system. Which TCP and UDP ports must you filter to check null sessions on your network?

A. 137 and 139
B. 137 and 443
C. 139 and 443
D. 139 and 445

Answer: D

NEW QUESTION 319
- (Exam Topic 1)
Under what conditions does a secondary name server request a zone transfer from a primary name server?

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

Answer: A

NEW QUESTION 324
- (Exam Topic 1)
The collection of potentially actionable, overt, and publicly available information is known as

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

Answer: A

NEW QUESTION 329
- (Exam Topic 1)
The change of a hard drive failure is once every three years. The cost to buy a new hard drive is $300. It will require 10 hours to restore the OS and software to the new hard disk. It will require a further 4 hours to restore the database from the last backup to the new hard disk. The recovery person earns $10/hour. Calculate the SLE, ARO, and ALE. Assume the EF = 1(100%). What is the closest approximate cost of this replacement and recovery operation per year?

A. $1320
B. $440
C. $100
D. $146

Answer: D

Explanation:
* 1. AV (Asset value) = $300 + (14 * $10) = $440 - the cost of a hard drive plus the work of a recovery person, i.e.how much would it take to replace 1 asset? 10 hours for resorting the OS and soft + 4 hours for DB restore multiplies by hourly rate of the recovery person.
* 2. SLE (Single Loss Expectancy) = AV * EF (Exposure Factor) = $440 * 1 = $440
* 3. ARO (Annual rate of occurrence) = 1/3 (every three years, meaning the probability of occurring during 1 years is 1/3)
* 4. ALE (Annual Loss Expectancy) = SLE * ARO = 0.33 * $440 = $145.2

NEW QUESTION 334
- (Exam Topic 1)
Susan has attached to her company's network. She has managed to synchronize her boss's sessions with that of the file server. She then intercepted his traffic destined for the server, changed it the way she wanted to and then placed it on the server in his home directory.
What kind of attack is Susan carrying on?

A. A sniffing attack
B. A spoofing attack
C. A man in the middle attack
D. A denial of service attack

Answer: C

NEW QUESTION 337
- (Exam Topic 1)
By using a smart card and pin, you are using a two-factor authentication that satisfies

A. Something you are and something you remember
B. Something you have and something you know
C. Something you know and something you are
D. Something you have and something you are

Answer: B

Explanation:
Two-factor Authentication or 2FA is a user identity verification method, where two of the three possible authentication factors are combined to grant access to a website or application.1) something the user knows, 2) something the user has, or 3) something the user is.
The possible factors of authentication are:
· Something the User Knows:
This is often a password, passphrase, PIN, or secret question. To satisfy this authentication challenge, the user must provide information that matches the answers previously provided to the organization by that user, such as “Name the town in which you were born.”
· Something the User Has:
This involves entering a one-time password generated by a hardware authenticator. Users carry around an authentication device that will generate a one-time password on command. Users then authenticate by providing this code to the organization. Today, many organizations offer software authenticators that can be installed on the user’s mobile device.

· Something the User Is:
This third authentication factor requires the user to authenticate using biometric data. This can include fingerprint scans, facial scans, behavioral biometrics, and more.
For example: In internet security, the most used factors of authentication are:
something the user has (e.g., a bank card) andsomething the user knows
., a PIN code). This is
two-factor authentication. Two-factor authentication is also sometimes referred to as strong authentication, Two-Step Verification, or 2FA.
The key difference between Multi-Factor Authentication (MFA) and Two-Factor Authentication (2FA) is that, as the term implies, Two-Factor Authentication utilizes a combination of two out of three possible authentication factors. In contrast, Multi-Factor Authentication could utilize two or more of these authentication factors.

NEW QUESTION 342
- (Exam Topic 1)
While using your bank's online servicing you notice the following string in the URL bar:
"http: // www. MyPersonalBank. com/ account?id=368940911028389&Damount=10980&Camount=21" You observe that if you modify the Damount & Camount values and submit the request, that data on the web
page reflects the changes.
Which type of vulnerability is present on this site?

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

Answer: C

NEW QUESTION 344
- (Exam Topic 1)
A company's policy requires employees to perform file transfers using protocols which encrypt traffic. You suspect some employees are still performing file transfers using unencrypted protocols because the employees do not like changes. You have positioned a network sniffer to capture traffic from the laptops used by employees in the data ingest department. Using Wireshark to examine the captured traffic, which command can be used as display filter to find unencrypted file transfers?

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

Answer: A

NEW QUESTION 348
- (Exam Topic 1)
The Heartbleed bug was discovered in 2014 and is widely referred to under MITRE's Common Vulnerabilities and Exposures (CVE) as CVE-2014-0160. This bug affects the OpenSSL implementation of the Transport Layer Security (TLS) protocols defined in RFC6520.
What type of key does this bug leave exposed to the Internet making exploitation of any compromised system very easy?

A. Public
B. Private
C. Shared
D. Root

Answer: B

NEW QUESTION 352
- (Exam Topic 1)
Study the following log extract and identify the attack.

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

Answer: D

NEW QUESTION 353
- (Exam Topic 1)
What tool can crack Windows SMB passwords simply by listening to network traffic?

A. This is not possible
B. Netbus
C. NTFSDOS
D. L0phtcrack

Answer: D

NEW QUESTION 356
- (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 357
- (Exam Topic 2)
The network administrator at Spears Technology, Inc has configured the default gateway Cisco router's access-list as below:
You are hired to conduct security testing on their network.
You successfully brute-force the SNMP community string using a SNMP crack tool.
The access-list configured at the router prevents you from establishing a successful connection. You want to retrieve the Cisco configuration from the router. How would you proceed?

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

Answer: BD

NEW QUESTION 358
- (Exam Topic 2)
How can you determine if an LM hash you extracted contains a password that is less than 8 characters long?

A. There is no way to tell because a hash cannot be reversed
B. The right most portion of the hash is always the same
C. The hash always starts with AB923D
D. The left most portion of the hash is always the same
E. A portion of the hash will be all 0's

Answer: B

NEW QUESTION 361
- (Exam Topic 2)
During an Xmas scan what indicates a port is closed?

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

Answer: B

NEW QUESTION 362
- (Exam Topic 2)
Abel, a cloud architect, uses container technology to deploy applications/software including all its dependencies, such as libraries and configuration files, binaries, and other resources that run independently from other processes in the cloud environment. For the containerization of applications, he follows the five-tier container technology architecture. Currently. Abel is verifying and validating image contents, signing images, and sending them to the registries. Which of the following tiers of the container technology architecture Is Abel currently working in?

A. Tier-1: Developer machines
B. Tier-4: Orchestrators
C. Tier-3: Registries
D. Tier-2: Testing and accreditation systems

Answer: D

Explanation:
The official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls.
formal declaration by a designated accrediting authority (DAA) or principal accrediting authority (PAA) that an information system is approved to operate at an acceptable level of risk, based on the implementation of an approved set of technical, managerial, and procedural safeguards. See authorization to operate (ATO).
Rationale: The Risk Management Framework uses a new term to refer to this concept, and it is called authorization.
Identifies the information resources covered by an accreditation decision, as distinguished from separately accredited information resources that are interconnected or with which information is exchanged via messaging. Synonymous with Security Perimeter.
For the purposes of identifying the Protection Level for confidentiality of a system to be accredited, the system has a conceptual boundary that extends to all intended users of the system, both directly and indirectly connected, who receive output from the system. See authorization boundary. Rationale: The Risk Management Framework uses a new term to refer to the concept of accreditation, and it is called authorization. Extrapolating, the accreditation boundary would then be referred to as the authorization boundary.

NEW QUESTION 363
- (Exam Topic 2)
Why containers are less secure that virtual machines?

A. Host OS on containers has a larger surface attack.
B. Containers may full fill disk space of the host.
C. A compromise container may cause a CPU starvation of the host.
D. Containers are attached to the same virtual network.

Answer: A

NEW QUESTION 366
- (Exam Topic 2)
What is the BEST alternative if you discover that a rootkit has been installed on one of your computers?

A. Copy the system files from a known good system
B. Perform a trap and trace
C. Delete the files and try to determine the source
D. Reload from a previous backup
E. Reload from known good media

Answer: E

NEW QUESTION 368
- (Exam Topic 2)
What would be the fastest way to perform content enumeration on a given web server by using the Gobuster tool?

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

Answer: A

NEW QUESTION 373
- (Exam Topic 2)
Take a look at the following attack on a Web Server using obstructed URL:

How would you protect from these attacks?

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

Answer: B

NEW QUESTION 375
.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons and Answers in PDF Format

312-50v12 Practice Exam Features:

* 312-50v12 Questions and Answers Updated Frequently

* 312-50v12 Practice Questions Verified by Expert Senior Certified Staff

* 312-50v12 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* 312-50v12 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year