CEH v13 Certification 312-50v13 Sample Questions Reliable [Q323-Q342

CEH v13 Certification 312-50v13 Sample Questions Reliable Prepare for the Actual CEH v13 312-50v13 Exam Practice Materials Collection Q323. When a normal TCP connection starts, a destination host receives a SYN (synchronize/start) packet from a source host and sends back a SYN/ACK (synchronize acknowledge). The destination host must then hear an ACK (acknowledge) of the SYN/ACK before the connection is established. This is referred to as the &#8220;TCP three-way handshake.&#8221; While waiting for the ACK to the SYN ACK, a connection queue of finite size on the destination host keeps track of connections waiting to be completed. This queue typically empties quickly since the ACK is expected to arrive a few milliseconds after the SYN ACK.

How would an attacker exploit this design by launching TCP SYN attack?
* Attacker generates TCP SYN packets with random destination addresses towards a victim host
* Attacker floods TCP SYN packets with random source addresses towards a victim host
* Attacker generates TCP ACK packets with random source addresses towards a victim host
* Attacker generates TCP RST packets with random source addresses towards a victim host

Q324. Windows LAN Manager (LM) hashes are known to be weak.

Which of the following are known weaknesses of LM? (Choose three.)
* Converts passwords to uppercase.

* Hashes are sent in clear text over the network.
* Makes use of only 32-bit encryption.
* Effective length is 7 characters.

Q325. Which file is a rich target to discover the structure of a website during web-server footprinting?
* Document root
* Robots.txt
* domain.txt
* index.html
Information Gathering from Robots.txt File A website owner creates a robots.txt file to list the files or directories a web crawler should index for providing search results. Poorly written robots.txt files can cause the complete indexing of website files and directories. If confidential files and directories are indexed, an attacker may easily obtain information such as passwords, email addresses, hidden links, and membership areas. If the owner of the target website writes the robots.txt file without allowing the indexing of restricted pages for providing search results, an attacker can still view the robots.txt file of the site to discover restricted files and then view them to gather information. An attacker types URL/robots.txt in the address bar of a browser to view the target website&#8217;s robots.txt file. An attacker can also download the robots.txt file of a target website using the Wget tool. Certified Ethical Hacker(CEH) Version 11 pg 1650

Q326. Dayn, an attacker, wanted to detect if any honeypots are installed in a target network. For this purpose, he used a time-based TCP fingerprinting method to validate the response to a normal computer and the response of a honeypot to a manual SYN request. Which of the following techniques is employed by Dayn to detect honeypots?
* Detecting honeypots running on VMware
* Detecting the presence of Honeyd honeypots
* Detecting the presence of Snort_inline honeypots
* Detecting the presence of Sebek-based honeypots

Q327. Mr. Omkar performed tool-based vulnerability assessment and found two vulnerabilities. During analysis, he found that these issues are not true vulnerabilities.

What will you call these issues?
* False positives
* True negatives
* True positives
* False negatives
False Positives occur when a scanner, Web Application Firewall (WAF), or Intrusion Prevention System (IPS) flags a security vulnerability that you do not have. A false negative is the opposite of a false positive, telling you that you don&#8217;t have a vulnerability when, in fact, you do.

A false positive is like a false alarm; your house alarm goes off, but there is no burglar. In web application security, a false positive is when a web application security scanner indicates that there is a vulnerability on your website, such as SQL Injection, when, in reality, there is not. Web security experts and penetration testers use automated web application security scanners to ease the penetration testing process. These tools help them ensure that all web application attack surfaces are correctly tested in a reasonable amount of time.

But many false positives tend to break down this process. If the first 20 variants are false, the penetration tester assumes that all the others are false positives and ignore the rest. By doing so, there is a good chance that real web application vulnerabilities will be left undetected.

When checking for false positives, you want to ensure that they are indeed false. By nature, we humans tend to start ignoring false positives rather quickly. For example, suppose a web application security scanner detects 100 SQL Injection vulnerabilities. If the first 20 variants are false positives, the penetration tester assumes that all the others are false positives and ignore all the rest. By doing so, there are chances that real web application vulnerabilities are left undetected. This is why it is crucial to check every vulnerability and deal with each false positive separately to ensure false positives.

Q328. Attacker Lauren has gained the credentials of an organization&#8217;s internal server system, and she was often logging in during irregular times to monitor the network activities. The organization was skeptical about the login times and appointed security professional Robert to determine the issue. Robert analyzed the compromised device to find incident details such as the type of attack, its severity, target, impact, method of propagation, and vulnerabilities exploited. What is the incident handling and response (IH&R) phase, in which Robert has determined these issues?
* Preparation
* Eradication
* Incident recording and assignment
* Incident triage
Incident Handling and Response Incident handling and response (IH&R) is the process of taking organized and careful steps when reacting to a security incident or cyberattack. Steps involved in the IH&R process: 3.

Incident Triage &#8211; The IH&R team further analyzes the compromised device to find incident details such as the type of attack, its severity, target, impact, and method of propagation, and any vulnerabilities it exploited. (P.

84/68)

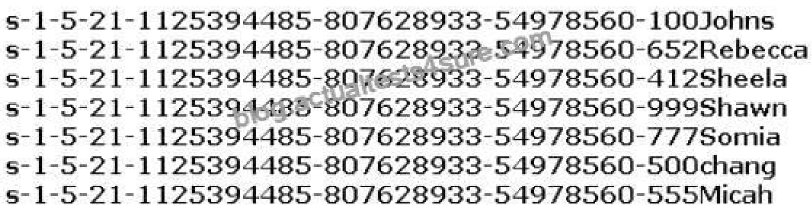
Q329. Which Nmap switch helps evade IDS or firewalls?
* -n/-R
* -0N/-0X/-0G
* -T
* -D

Q330. Which Intrusion Detection System is the best applicable for large environments where critical assets on the network need extra scrutiny and is ideal for observing sensitive network segments?
* Honeypots
* Firewalls
* Network-based intrusion detection system (NIDS)
* Host-based intrusion detection system (HIDS)

Q331. What is the minimum number of network connections in a multi homed firewall?
* 3
* 5
* 4
* 2

Q332. You are attempting to crack LM Manager hashed from Windows 2000 SAM file. You will be using LM Brute force hacking tool for decryption. What encryption algorithm will you be decrypting?
* MD4
* DES
* SHA
* SSL

Q333. Peter extracts the SIDs list from Windows 2000 Server machine using the hacking tool &#8220;SIDExtractor&#8221;. Here is the output of the SIDs:



```
s-1-5-21-1125394485-807628933-54978560-100Johns
s-1-5-21-1125394485-807628933-54978560-652Rebecca
s-1-5-21-1125394485-807628933-54978560-412Sheela
s-1-5-21-1125394485-807628933-54978560-999Shawn
s-1-5-21-1125394485-807628933-54978560-777Somia
s-1-5-21-1125394485-807628933-54978560-500chang
s-1-5-21-1125394485-807628933-54978560-555Micah
```

From the above list identify the user account with System Administrator privileges.
* John
* Rebecca
* Sheela
* Shawn
* Somia
* Chang
* Micah

Q334. Based on the following extract from the log of a compromised machine, what is the hacker really trying to steal?
* har.txt
* SAM file
* wwwroot
* Repair file

Q335. Mason, a professional hacker, targets an organization and spreads Emotet malware through malicious script.

After infecting the victim&#8217;s device. Mason further used Emotet to spread the infection across local networks and beyond to compromise as many machines as possible. In this process, he used a tool, which is a self- extracting RAR file, to retrieve information related to network resources such as writable share drives. What is the tool employed by Mason in the above scenario?
* NetPass.exe
* Outlook scraper
* WebBrowserPassView
* Credential enumerator
https://us-cert.cisa.gov/ncas/alerts/TA18-201A

Currently, Emotet uses five known spreader modules: NetPass.exe, WebBrowserPassView, Mail PassView, Outlook scraper, and a credential enumerator. Credential enumerator is a self-extracting RAR file containing two components: a bypass component and a service component. The bypass component is used for the enumeration of network resources and either finds writable share drives using Server Message Block (SMB) or tries to brute force user accounts, including the administrator account. Once an available system is found, Emotet writes the service component on the system, which writes Emotet onto the disk. Emotet&#8217;s access to SMB can result in the infection of entire domains (servers and clients).

Q336. While testing a web application in development, you notice that the web server does not properly ignore the

&#8220;dot dot slash&#8221; (../) character string and instead returns the file listing of a folder structure of the server.

What kind of attack is possible in this scenario?
* Cross-site scripting
* Denial of service
* SQL injection

* Directory traversal
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&#8217;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&#8217;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&#8217;t get to anything over this root.

For instance: the default root registry of IIS on Windows is C:Inetpubwwwroot and with this arrangement, a client doesn&#8217;t approach C:Windows yet approaches C:Inetpubwwwrootnews and some other indexes and documents under the root catalog (given that the client is confirmed by means of the ACLs).

The root index keeps clients from getting to any documents on the worker, for example, C:WINDOWS

/system32/win.ini on Windows stages and the/and so on/passwd record on Linux/UNIX stages.

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

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

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

Contingent upon how the site access is set up, the aggressor will execute orders by mimicking himself as the client which is related with &#8220;the site&#8221;. Along these lines everything relies upon what the site client has been offered admittance to in the framework.

Illustration of a Directory Traversal assault by means of web application codeIn web applications with dynamic pages, input is generally gotten from programs through GET or POST solicitation techniques. Here is an illustration of a HTTP GET demand URL GET

http://test.webarticles.com/show.asp?view=oldarchive.html HTTP/1.1

Host: test.webarticles.com

With this URL, the browser requests the dynamic page show.asp from the server and with it also sends the parameter view with the value of oldarchive.html. When this request is executed on the web server, show.

asp retrieves the file oldarchive.html from the server&#8217;s file system, renders it and then sends it back to the browser which displays it to the user. The attacker would assume that show.asp can retrieve files from the file system and sends the following custom URL.

GET

http://test.webarticles.com/show.asp?view=../../../../../Windows/system.ini HTTP/1.1 Host: test.webarticles.com This will cause the dynamic page to retrieve the file system.ini from the file system and display it to the user.

The expression ../ instructs the system to go one directory up which is commonly used as an operating system directive. The attacker has to guess how many directories he has to go up to find the Windows folder on the system, but this is easily done by trial and error.

Example of a Directory Traversal attack via web serverApart from vulnerabilities in the code, even the web server itself can be open to directory traversal attacks. The problem can either be incorporated into the web server software or inside some sample script files left available on the server.

The vulnerability has been fixed in the latest versions of web server software, but there are web servers online which are still using older versions of IIS and Apache which might be open to directory traversal attacks.

Even though you might be using a web server software version that has fixed this vulnerability, you might still have some sensitive default script directories exposed which are well known to hackers.

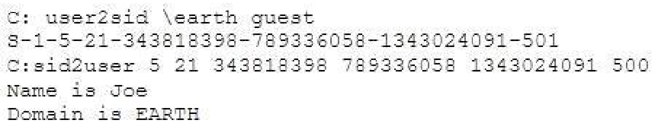
For example, a URL request which makes use of the scripts directory of IIS to traverse directories and execute a command can be GET

http://server.com/scripts/..%5c../Windows/System32/cmd.exe?/c+dir+c: HTTP/1.1 Host: server.com The request would return to the user a list of all files in the C: directory by executing the cmd.exe command shell file and run the command dir c: in the shell. The %5c expression that is in the URL request is a web server escape code which is used to represent normal characters. In this case %5c represents the character .

Newer versions of modern web server software check for these escape codes and do not let them through.

Some older versions however, do not filter out these codes in the root directory enforcer and will let the attackers execute such commands.

Q337. What did the following commands determine?



```
C: user2sid \earth guest
S-1-5-21-343818398-789336058-1343024091-501
C:sid2user 5 21 343818398 789336058 1343024091 500
Name is Joe
Domain is EARTH
```

* That the Joe account has a SID of 500
* These commands demonstrate that the guest account has NOT been disabled
* These commands demonstrate that the guest account has been disabled
* That the true administrator is Joe
* Issued alone, these commands prove nothing

Q338. Peter, a system administrator working at a reputed IT firm, decided to work from his home and login remotely. Later, he

anticipated that the remote connection could be exposed to session hijacking. To curb this possibility, he implemented a technique that creates a safe and encrypted tunnel over a public network to securely send and receive sensitive information and prevent hackers from decrypting the data flow between the endpoints. What is the technique followed by Peter to send files securely through a remote connection?
* DMZ
* SMB signing
* VPN
* Switch network

Q339. Which mode of IPSec should you use to assure security and confidentiality of data within the same LAN?
* ESP transport mode
* ESP confidential
* AH permiscuous
* AH Tunnel mode

Q340. The collection of potentially actionable, overt, and publicly available information is known as
* Open-source intelligence
* Real intelligence
* Social intelligence
* Human intelligence

Q341. The network team has well-established procedures to follow for creating new rules on the firewall. This includes having approval from a manager prior to implementing any new rules. While reviewing the firewall configuration, you notice a recently implemented rule but cannot locate manager approval for it. What would be a good step to have in the procedures for a situation like this?
* Have the network team document the reason why the rule was implemented without prior manager approval.
* Monitor all traffic using the firewall rule until a manager can approve it.
* Do not roll back the firewall rule as the business may be relying upon it, but try to get manager approval as soon as possible.
* Immediately roll back the firewall rule until a manager can approve it

Q342. Ben purchased a new smartphone and received some updates on it through the OTA method. He received two messages: one with a PIN from the network operator and another asking him to enter the PIN received from the operator. As soon as he entered the PIN, the smartphone started functioning in an abnormal manner. What is the type of attack performed on Ben in the above scenario?
* Advanced SMS phishing
* Bypass SSL pinning
* Phishing
* Tap &#8216;n ghost attack

Ace ECCouncil 312-50v13 Certification with Actual Questions Feb 26, 2025 Updated:
https://www.actualtests4sure.com/312-50v13-test-questions.html]