312-50V12^{Q&As}

Certified Ethical Hacker Exam (CEHv12)

Pass EC-COUNCIL 312-50V12 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass2lead.com/312-50v12.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by EC-COUNCIL Official Exam Center

⚙ **Instant Download** After Purchase

⚙ **100% Money Back** Guarantee

⚙ **365 Days** Free Update

⚙ **800,000+** Satisfied Customers

QUESTION 1

During an Xmas scan what indicates a port is closed?

A. No return response

B. RST

C. ACK

D. SYN

Correct Answer: B

QUESTION 2

Why should the security analyst disable/remove unnecessary ISAPI filters?

A. To defend against social engineering attacks

B. To defend against webserver attacks

C. To defend against jailbreaking

D. To defend against wireless attacks

Correct Answer: B

QUESTION 3

Taylor, a security professional, uses a tool to monitor her company\\'s website, analyze the website\\'s traffic, and track the geographical location of the users visiting the company\\'s website. Which of the following tools did Taylor employ in the above scenario?

A. WebSite Watcher

B. web-Stat

C. Webroot

D. WAFW00F

Correct Answer: B

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

QUESTION 4

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

A. Twofish encryption algorithm

B. HMAC encryption algorithm

C. IDEA

D. Blowfish encryption algorithm

Correct Answer: A

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

QUESTION 5

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

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 Creating a phishing email campaign o Leveraging exploit kits and botnets

https://en.wikipedia.org/wiki/Kill_chain

The Cyber Kill Chain consists of 7 steps: Reconnaissance, weaponization, delivery, exploitation, installation, command and control, and finally, actions on objectives. Below you can find detailed information on each.

1.

 Reconnaissance: In this step, the attacker/intruder chooses their target. Then they conduct in-depth research on this target to identify its vulnerabilities that can be exploited.

2.

 Weaponization: In this step, the intruder creates a malware weapon like a virus, worm, or such to exploit the target\\'s vulnerabilities. Depending on the target and the purpose of the attacker, this malware can exploit new, undetected vulnerabilities (also known as the zero-day exploits) or focus on a combination of different vulnerabilities.

3.

 Delivery: This step involves transmitting the weapon to the target. The intruder/attacker can employ different USB drives, e-mail attachments, and websites for this purpose.

4.

 Exploitation: In this step, the malware starts the action. The program code of the malware is triggered to exploit the target\\'s vulnerability/vulnerabilities.

5.

 Installation: In this step, the malware installs an access point for the intruder/attacker. This access point is also known as the backdoor.

6.

 Command and Control: The malware gives the intruder/attacker access to the network/system.

7.

 Actions on Objective: Once the attacker/intruder gains persistent access, they finally take action to fulfill their purposes, such as encryption for ransom, data exfiltration, or even data destruction.

QUESTION 6

To hide the file on a Linux system, you have to start the filename with a specific character. What is the character?

A. Exclamation mark (!)

B. Underscore (_)

C. Tilde H

D. Period (.)

Correct Answer: D

QUESTION 7

Susan has attached to her company\\'s network. She has managed to synchronize her boss\\'s sessions with that of the file server. She then intercepted his traffic destined for the server, changed it the way she wanted to and then placed it on the server in his home directory.

What kind of attack is Susan carrying on?

A. A sniffing attack

B. A spoofing attack

C. A man in the middle attack

D. A denial of service attack

Correct Answer: C

QUESTION 8

Thomas, a cloud security professional, is performing security assessment on cloud services to identify any loopholes. He detects a vulnerability in a bare-metal cloud server that can enable hackers to implant malicious backdoors in its firmware. He also identified that an installed backdoor can persist even if the server is reallocated to new clients or businesses that use it as an IaaS.

What is the type of cloud attack that can be performed by exploiting the vulnerability discussed in the above scenario?

A. Man-in-the-cloud (MITC) attack

B. Cloud cryptojacking

C. Cloudborne attack

D. Metadata spoofing attack

Correct Answer: C

QUESTION 9

What is GINA?

A. Gateway Interface Network Application

B. GUI Installed Network Application CLASS

C. Global Internet National Authority (G-USA)

D. Graphical Identification and Authentication DLL

Correct Answer: D

QUESTION 10

As a securing consultant, what are some of the things you would recommend to a company to ensure DNS security?

A. Use the same machines for DNS and other applications

B. Harden DNS servers

C. Use split-horizon operation for DNS servers

D. Restrict Zone transfers

E. Have subnet diversity between DNS servers

Correct Answer: BCDE

QUESTION 11

There have been concerns in your network that the wireless network component is not sufficiently secure. You perform a vulnerability scan of the wireless network and find that it is using an old encryption protocol that was designed to mimic wired encryption, what encryption protocol is being used?

A. WEP

B. RADIUS

C. WPA

D. WPA3

Correct Answer: A

Wired Equivalent Privacy (WEP) may be a security protocol, laid out in the IEEE wireless local area network (Wi-Fi) standard, 802.11b, that\\'s designed to supply a wireless local area network (WLAN) with A level of security and privacy like what\\'s usually expected of a wired LAN. A wired local area network (LAN) is usually protected by physical security mechanisms (controlled access to a building, for example) that are effective for a controlled physical environment, but could also be ineffective for WLANs because radio waves aren\\'t necessarily bound by the walls containing the network. WEP seeks to determine similar protection thereto offered by the wired network\\'s physical security measures by encrypting data transmitted over the WLAN. encoding protects the vulnerable wireless link between clients and

access points; once this measure has been taken, other typical LAN security mechanisms like password protection, end-to-end encryption, virtual private networks (VPNs), and authentication are often put in situ to make sure privacy.A research group from the University of California at Berkeley recently published a report citing "major security flaws" in WEP that left WLANs using the protocol susceptible to attacks (called wireless equivalent privacy attacks). within the course of the group\\'s examination of the technology, they were ready to intercept and modify transmissions and gain access to restricted networks. The Wireless Ethernet Compatibility Alliance (WECA) claims that WEP ?which is included in many networking products ?was never intended to be the only security mechanism for a WLAN, and that, in conjunction with traditional security practices, it\\'s very effective.

QUESTION 12

Sam is a penetration tester hired by Inception Tech, a security organization. He was asked to perform port scanning on a target host in the network. While performing the given task, Sam sends FIN/ACK probes and determines that an RST packet is sent in response by the target host, indicating that the port is closed.

What is the port scanning technique used by Sam to discover open ports?

A. Xmas scan

B. IDLE/IPID header scan

C. TCP Maimon scan

D. ACK flag probe scan

Correct Answer: C

TCP Maimon scan This scan technique is very similar to NULL, FIN, and Xmas scan, but the probe used here is FIN/ACK. In most cases, to determine if the port is open or closed, the RST packet should be generated as a response to a probe request. However, in many BSD systems, the port is open if the packet gets dropped in response to a probe.

https://nmap.org/book/scan-methods-maimon-scan.html

How Nmap interprets responses to a Maimon scan probe

Probe Response Assigned State No response received (even after retransmissions) open|filtered TCP RST packet closed ICMP unreachable error (type 3, code 1, 2, 3, 9, 10, or 13) filtered

QUESTION 13

Yancey is a network security administrator for a large electric company. This company provides power for over 100, 000 people in Las Vegas. Yancey has worked for his company for over 15 years and has become very successful. One day, Yancey comes in to work and finds out that the company will be downsizing and he will be out of a job in two weeks. Yancey is very angry and decides to place logic bombs, viruses, Trojans, and backdoors all over the network to take down the company once he has left. Yancey does not care if his actions land him in jail for 30 or more years, he just wants the company to pay for what they are doing to him.

What would Yancey be considered?

A. Yancey would be considered a Suicide Hacker

B. Since he does not care about going to jail, he would be considered a Black Hat

C. Because Yancey works for the company currently; he would be a White Hat

D. Yancey is a Hacktivist Hacker since he is standing up to a company that is downsizing

Correct Answer: A

QUESTION 14

Which of the following tools can be used to perform a zone transfer?

A. NSLookup

B. Finger

C. Dig

D. Sam Spade

E. Host

F. Netcat

G. Neotrace

Correct Answer: ACDE

QUESTION 15

env x=\\'(){ :;};echo exploit\\' bash -c `cat/etc/passwd\\'

What is the Shellshock bash vulnerability attempting to do on a vulnerable Linux host?

A. Removes the passwd file

B. Changes all passwords in passwd

C. Add new user to the passwd file

D. Display passwd content to prompt

Correct Answer: D

[312-50V12 Study Guide](#)   [312-50V12 Exam Questions](#)   [312-50V12 Braindumps](#)