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.passapply.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

QUESTION 1

Study the snort rule given below:

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 135
(msg: "NETBIOS DCERPC ISystemActivator bind attempt";
flow:to_server, established; content: "|05|"; distance: 0; within: 1;
content: "|ob|"; distance: 1; within: 1; byte_test: 1, &, 1, 0, relative;
content: "|A0 01 00 00 00 00 00 00 C0 00 00 00 00 00 00 46|";
distance: 29; within: 16; reference: cve, CAN-2003-0352;
classtype: attempted-admin; sid: 2192; rev: 1;)

alert tcp $EXTERNAL_NET any -> $HOME_NET 445 (msg: "NETBIOS SMB
DCERPC ISystemActivator bind attempt"; flow: to_server, established;
content: "|FF|SMB|25|"; nocase; offset:4, depth:5; content: "|26 00|";
nocase; distance:5; within: 12; content: "|05|"; distance:0; within:1;
content: "|ob|"; distance: 1; within: 1; byte_test: 1, &, 1, 0, relative;
content: "|A0 01 00 00 00 00 00 00 C0 00 00 00 00 00 00 46|";
distance: 29; within: 16; reference: cve, CAN-2003-0352;
classtype: attempted-admin; sid: 2193; rev: 1;)
```

From the options below, choose the exploit against which this rule applies.

A. WebDav

B. SQL Slammer

C. MS Blaster

D. MyDoom

Correct Answer: C

QUESTION 2

Which of the following is the best countermeasure to encrypting ransomwares?

A. Use multiple antivirus softwares

B. Pay a ransom

C. Keep some generation of off-line backup

D. Analyze the ransomware to get decryption key of encrypted data

Correct Answer: C

QUESTION 3

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 4

Which of the following web vulnerabilities would an attacker be attempting to exploit if they delivered the following input?

] >

A. XXE

B. SQLi

C. IDOR

D. XXS

Correct Answer: A

QUESTION 5

A company\\'s security policy states that all Web browsers must automatically delete their HTTP browser cookies upon terminating. What sort of security breach is this policy attempting to mitigate?

A. Attempts by attackers to access the user and password information stored in the company\\'s SQL database.

B. Attempts by attackers to access Web sites that trust the Web browser user by stealing the user\\'s authentication credentials.

C. Attempts by attackers to access password stored on the user\\'s computer without the user\\'s knowledge.

D. Attempts by attackers to determine the user\\'s Web browser usage patterns, including when sites were visited and for how long.

Correct Answer: B