312-50V7^{Q&As}

Ethical Hacking and Countermeasures (CEHv7)

Pass EC-COUNCIL 312-50V7 Exam with 100% Guarantee

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

https://www.passapply.com/312-50v7.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

Which of the following ensures that updates to policies, procedures, and configurations are made in a controlled and documented fashion?

A. Regulatory compliance

B. Peer review

C. Change management

D. Penetration testing

Correct Answer: C

QUESTION 2

A security analyst is performing an audit on the network to determine if there are any deviations from the security policies in place. The analyst discovers that a user from the IT department had a dial-out modem installed. Which security policy must the security analyst check to see if dial-out modems are allowed?

A. Firewall-management policy

B. Acceptable-use policy

C. Remote-access policy

D. Permissive policy

Correct Answer: C

QUESTION 3

Wayne is the senior security analyst for his company. Wayne is examining some traffic logs on a server and came across some inconsistencies. Wayne finds some IP packets from a computer purporting to be on the internal network. The packets originate from 192.168.12.35 with a TTL of 15. The server replied to this computer and received a response from 192.168.12.35 with a TTL of 21. What can Wayne infer from this traffic log?

A. The initial traffic from 192.168.12.35 was being spoofed.

B. The traffic from 192.168.12.25 is from a Linux computer.

C. The TTL of 21 means that the client computer is on wireless.

D. The client computer at 192.168.12.35 is a zombie computer.

Correct Answer: A

QUESTION 4

An attacker is attempting to telnet into a corporation\\\'s system in the DMZ. The attacker doesn\\\'t want to get caught and is spoofing his IP address. After numerous tries he remains unsuccessful in connecting to the system. The attacker rechecks that the target system is actually listening on Port 23 and he verifies it with both nmap and hping2. He is still unable to connect to the target system. What could be the reason?

A. The firewall is blocking port 23 to that system

B. He needs to use an automated tool to telnet in

C. He cannot spoof his IP and successfully use TCP

D. He is attacking an operating system that does not reply to telnet even when open

Correct Answer: C

QUESTION 5

During a penetration test, a tester finds a target that is running MS SQL 2000 with default credentials. The tester assumes that the service is running with Local System account. How can this weakness be exploited to access the system?

A. Using the Metasploit psexec module setting the SA / Admin credential

B. Invoking the stored procedure xp_shell to spawn a Windows command shell

C. Invoking the stored procedure cmd_shell to spawn a Windows command shell

D. Invoking the stored procedure xp_cmdshell to spawn a Windows command shell

Correct Answer: D