312-50V7$^{\text{Q\&As}}$

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

QUESTION 1

Harold is the senior security analyst for a small state agency in New York. He has no other security professionals that work under him, so he has to do all the security-related tasks for the agency. Coming from a computer hardware background, Harold does not have a lot of experience with security methodologies and technologies, but he was the only one who applied for the position. Harold is currently trying to run a Sniffer on the agency\\'s network to get an idea of what kind of traffic is being passed around, but the program he is using does not seem to be capturing anything. He pours through the Sniffer\\'s manual, but cannot find anything that directly relates to his problem. Harold decides to ask the network administrator if he has any thoughts on the problem. Harold is told that the Sniffer was not working because the agency\\'s network is a switched network, which cannot be sniffed by some programs without some tweaking. What technique could Harold use to sniff his agency\\'s switched network?

A. ARP spoof the default gateway

B. Conduct MiTM against the switch

C. Launch smurf attack against the switch

D. Flood the switch with ICMP packets

Correct Answer: A

QUESTION 2

After a client sends a connection request (SYN) packet to the server, the server will respond (SYN- ACK) with a sequence number of its choosing, which then must be acknowledged (ACK) by the client. This sequence number is predictable; the attack connects to a service first with its own IP address, records the sequence number chosen, and then opens a second connection from a forged IP address. The attack doesn\\'t see the SYN-ACK (or any other packet) from the server, but can guess the correct responses. If the source IP address is used for authentication, then the attacker can use the one-sided communication to break into the server. What attacks can you successfully launch against a server using the above technique?

A. Denial of Service attacks

B. Session Hijacking attacks

C. Web page defacement attacks

D. IP spoofing attacks

Correct Answer: B

QUESTION 3

Which of the following are variants of mandatory access control mechanisms? (Choose two.)

A. Two factor authentication

B. Acceptable use policy

C. Username / password

D. User education program

E. Sign in register

Correct Answer: AC

QUESTION 4

You are footprinting an organization and gathering competitive intelligence. You visit the company\\'s website for contact information and telephone numbers but do not find them listed there. You know they had the entire staff directory listed on their website 12 months ago but now it is not there. Is there any way you can retrieve information from a website that is outdated?

A. Visit Google\\'s search engine and view the cached copy

B. Crawl the entire website and store them into your computer

C. Visit Archive.org web site to retrieve the Internet archive of the company\\'s website

D. Visit the company\\'s partners and customers website for this information

Correct Answer: C

QUESTION 5

How do you defend against Privilege Escalation?

A. Use encryption to protect sensitive data

B. Restrict the interactive logon privileges

C. Run services as unprivileged accounts

D. Allow security settings of IE to zero or Low

E. Run users and applications on the least privileges

Correct Answer: ABCE