312-50V8 Q&As

Certified Ethical Hacker v8

Pass EC-COUNCIL 312-50V8 Exam with 100% Guarantee

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

https://www.leads4pass.com/312-50v8.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

An incident investigator asks to receive a copy of the event from all firewalls, prosy servers, and Intrusion Detection Systems (IDS) on the network of an organization that has experienced a possible breach of security. When the investigator attempts to correlate the information in all of the logs the sequence of many of the logged events do not match up.

What is the most likely cause?

A. The network devices are not all synchronized

B. The securitybreach was a false positive.

C. The attack altered or erased events from the logs.

D. Proper chain of custody was not observed while collecting the logs.

Correct Answer: C

QUESTION 2

Which of the following resources does NMAP need to be used as a basic vulnerability scanner covering several vectors like SMB, HTTP and FTP?

A. Metasploit scripting engine

B. Nessus scripting engine

C. NMAP scripting engine

D. SAINT scripting engine

Correct Answer: C

QUESTION 3

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 4

Which of the following commands runs snort in packet logger mode?

A. ./snort -dev -h ./log

B. ./snort -dev -l ./log

C. ./snort -dev -o ./log

D. ./snort -dev -p ./log

Correct Answer: B

QUESTION 5

Which type of scan is used on the eye to measure the layer of blood vessels?

A. Facial recognition scan

B. Retinal scan

C. Iris scan

D. Signature kinetics scan

Correct Answer: B