312-50V9 Q&As

Certified Ethical Hacker Exam V9

Pass EC-COUNCIL 312-50V9 Exam with 100% Guarantee

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

https://www.geekcert.com/312-50v9.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

What is the best Nmap command to use when you want to list all devices in the same network quickly after you successfully identified a server whose IP address is 10.10.0.5?

A. nmap -T4 -F 10.10.0.0/24

B. nmap -T4 -q 10.10.0.0/24

C. nmap -T4 -O 10.10.0.0/24

D. nmap -T4 -r 10.10.1.0/24

Correct Answer: A Section: (none)

QUESTION 2

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 Section: (none)

QUESTION 3

Which of the following tools can be used for passive OS fingerprinting?

A. tcpdump

B. nmap

C. ping

D. tracert

Correct Answer: A Section: (none)

The passive operating system fingerprinting is a feature built into both the pf and tcpdump tools.

References: http://geek00l.blogspot.se/2007/04/tcpdump-privilege-dropping-passive-os.html

QUESTION 4

Supposed you are the Chief Network Engineer of a certain Telco. Your company is planning for a big business expansion and it requires that your network authenticate users connecting using analog modems, Digital Subscriber Lines (DSL), wireless data services, and Virtual Private Networks (VPN) over a Frame Relay network. Which AAA protocol would you implement?

A. TACACS+

B. DIAMETER

C. Kerberos

D. RADIUS

Correct Answer: D Section: (none)

QUESTION 5

When a normal TCP connection starts, a destination host receives a SYN (synchronize/start) packet from a source host and sends back a SYN/ACK (synchronize acknowledge). The destination host must then hear an ACK (acknowledge) of the SYN/ACK before the connection is established. This is referred to as the "TCP three-way handshake." While waiting for the ACK to the SYN ACK, a connection queue of finite size on the destination host keeps track of connections waiting to be completed. This queue typically empties quickly since the ACK is expected to arrive a few milliseconds after the SYN ACK. How would an attacker exploit this design by launching TCP SYN attack?

A. Attacker generates TCP SYN packets with random destination addresses towards a victim host

B. Attacker floods TCP SYN packets with random source addresses towards a victim host

C. Attacker generates TCP ACK packets with random source addresses towards a victim host

D. Attacker generates TCP RST packets with random source addresses towards a victim host

Correct Answer: B Section: (none)