MK0-201 Q&As

CPTS - Certified Pen Testing Specialist

Pass Mile2 MK0-201 Exam with 100% Guarantee

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

https://www.geekcert.com/mk0-201.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Mile2 Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

DNS Spoofing can allow an attacker to sniff traffic that is meant to go to particular web sites.Which of the following tools can perform DNS Spoofing?Choose two.

A. Cain and Abel

B. LC5

C. WinDNSSpoof

D. URLSnarf

Correct Answer: AC

QUESTION 2

Why is it important to ensure that SRV records are not publicly accessible?Choose the best answer.

A. SRV records indicate how long a machine has been up since reboot and hence could indicate patch levels

B. SRV records reveal Active Directory domain controllers

C. SRV records reveal software Update Services computers

D. SRV records are required on NT 4 domains

Correct Answer: B

QUESTION 3

TestKing.com has been getting numerous complaints that one of their employees has been actively probing remote DNS servers and attempting to extact information from them.

After investigation it was detected that jack had used the nslookup command entensively and he also issued commands within nslookup such as server [remoteip]where[remoteip]is the IP address of the target he was probing.

Further investigation also revealed that he used the command is d targetdomain.com where targetdomain.com was the ddomain name he was attempting to get more info about,what was jack really attempting to achieve in this case?

A. See the UNIX permission of files

B. Perform a zone transfer

C. Perform a lookup on user and group permissions of files

D. Perform a zone incremental query

Correct Answer: B

QUESTION 4

Which of the following scan types would be the least accurate scan considering that may other network conditions could indicate that the port is open even though it might not be open?

A. Vanilla TCP Port Scan

B. UDP Port Scan

C. Half-Open Scan

D. Inverse TCP Scan

Correct Answer: B

QUESTION 5

What is one possible method that hackers can use to sniff SSL connections?Choose the best answer.

A. Use dsniff

B. Act as a man in the middle between the client and the webserver and send the client a fake certificate that the user will accept as legitimate

C. Use SSLSniff to sniff the session key exchange

D. Use SSL Relay

Correct Answer: B