MK0-201

(Certified Pen Testing Specialist)

Total Questions: 247
Last Updated: Feb 26, 2009
Document version: 8.27.11

Thanks for purchasing techXams' Study Guide,

techXams' MK0-201 study guide is a comprehensive compilation of questions and answers that have been developed by our team of certified professionals. In order to prepare for the actual exam, all you need is to study the content of this guide. An average of approximately 10 to 20 hours should be spent to study this guide and you will surely pass your exam. It's our guarantee.

Disclaimer

Neither this guide nor any material in this guide is sponsored, endorsed or affiliated with any of the respective vendor. All trademarks are properties of their respective owners.

Guarantee

If you study this guide properly and still unable to pass the exam, please send us a scanned copy of your official score at: **refund@techeXams.ws**. We will happily reimburse the cost of this study guide or send you an exchange of study guide of your choice free of cost.

Feedback

If you find any possible improvement, then please do let us know. We are always interested in improving the quality of this product. Feedback can be send at: **feedback@techeXams.ws**

Copyright

Question: 1

By spoofing an IP address and inserting the attackers MAC address into an unsolicited ARP Reply packet, an attacker is performing what kind of attack? Choose the best answer.

A. Denial of Service
B. Sniffing in a switched network via ARP Poisoning
C. ARP Flood
D. Birthday

Answer: B

Question: 2

Why wouldn't it be surprising to find netcat on a trojaned-computer? Choose three.

A. Netcat can listen on any port and send data to any port
B. Netcat can be used to send or receive files over any port
C. Netcat can be used to perform port scanning
D. Netcat encrypts all communications

Answer: A, B, C

Question: 3

Why would an administrator block ICMP TTL Exceeded error messages at the external gateways of the network? Choose the best answer.

A. To reduce the workload on the routers
B. To prevent Smurf attacks
C. To prevent trace-route software from revealing the IP addresses of these external gateways
D. To prevent fragment-based Denial of Service attacks

Answer: C

Question: 4

Which tools and or techniques can be used to remove an Alternative Data Stream on an NTFS file? Choose two.

A. Ads_cat
B. ADSChecker
C. ADS_Del
D. Copy the NTFS file containing the stream to a FAT partition, delete the original NTFS file, copy the FAT file back to NTFS

Answer: D

Question: 5

If an attacker gets A... he Event log be trusted with certain...

A. Entries in the ev...
B. The attacker ma... ng evidence of the method of break-i...
C. Tools like Winza... ssociated with the initial break-in and...
D. Event logs have... e easily edited

Answer: B, C

Question: 6

Most search engine... on Tester you must be familiar with som... e is a wealth of information to be ga... ollowing operators would you use if you... ght have information which is...

A. Link:
B. InCache:
C. Cache:
D. Related:

Answer: C

Question: 7

the...

A. IP addres...
B. Operating Syst...
C. System Owner
D. Services

Answer: C