MK0-201

Mile2

CPTS - Certified Pen Testing Specialist

Visit: http://www.pass4sureofficial.com/exams.asp?examcode=MK0-201

Pass4sureofficial.com is a reputable IT certification examination guide, study guides and audio exam provider, we not only ensure that you pass your MK0-201 exam in first attempt, but also you can get a high score to acquire Mile2 certification.

If you use pass4sureofficial MK0-201 Certification questions and answers, you will experience actual MK0-201 exam questions/answers. We know exactly what is needed and have all the exam preparation material required to pass the exam. Our Mile2 exam prep covers over 95% of the questions and answers that may be appeared in your MK0-201 exam. Every point from pass4sure MK0-201 PDF, MK0-201 review will help you take Mile2 MK0-201 exam much easier and become Mile2 certified. All the Questions/Answers are taken from real exams.

Here's what you can expect from the Pass4sureOfficial Mile2 MK0-201 course:

** Up-to-Date Mile2 MK0-201 questions taken from the real exam.*
** 100% correct Mile2 MK0-201 answers you simply can't find in other MK0-201 courses.*
** All of our tests are easy to download. Your file will be saved as a MK0-201 PDF.*
** Mile2 MK0-201 brain dump free content featuring the real MK0-201 test questions.*

Mile2 MK0-201 certification exam is of core importance both in your Professional life and Mile2 certification path. With Mile2 certification you can get a good job easily in the market and get on your path for success. Professionals who passed Mile2 MK0-201 exam training are an absolute favorite in the industry. You will pass Mile2 MK0-201 certification test and career opportunities will be open for you.

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 Administrative-level access, why cant the entries in the Event log be trusted with certainty? Choose two.

A. Entries in the event log are not digitally signed
B. The attacker may have been able to simply clear the event log, thus erasing evidence of the method of break-in
C. Tools like Winzapper allow the attacker to selectively delete log entries associated with the initial break-in and subsequent malicious activity

D. Event logs have NTFS permissions of Everyone Full Control and thus can be easily edited

Answer: B, C

Question: 6
Most search engine support Advanced Search Operators; as a Penetration Tester you must be familiar with some of the larger search engines such as Google. There is a wealth of information to be gathered from these public databases. Which of the following operators would you use if you attempt to find an older copy of a website that might have information which is no longer available on the target website?

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

Answer: C

Question: 7
Which of the following items is the least likely to be found while doing Scanning? Choose the best answer.

A. IP addresses
B. Operating System
C. System Owner
D. Services

Answer: C

Question: 8
You are concerned about other people sniffing your data while it is traveling over your local network and the internet.
Which of the following would be the most effective countermeasure to protect your data against sniffing while it is in transit? Choose the best answer.

A. Encryption
B. AntiSniff
C. PromiScan
D. Usage of a switch

Answer: A

Question: 9
When you create a hash value of the message you wish to send, then you encrypt the hash value using your private key before sending it to the receiver in order to prove the authenticity of the message. What would this be called within the cryptography world?

A. Hashing
B. Digital Signature
C. Encryption
D. Diffie-Hillman

Answer: B

Question: 10
Looking at the window presented below:

What type of mail server is running on the remote host?

A. Exchange 8.13.4
B. Hotmail 8.13.4
C. Sendmail 8.13.4
D. Exim Mail 8.13.4

Answer: C

Question: 11
Bob has just produced a very detailed penetration testing report for his client. Bob wishes to ensure that the report will not be changed in storage or in transit. What would be the best tool that Bob can use to assure the integrity of the information and detect any changes that could have happened to the report while being transmitted or stored?

A. A Symmetric Encryption Algorithm
B. An Asymmetric Encryption Algorithm
C. An Hashing Algorithm
D. The ModDetect Algorithm

Answer: C

Question: 12
A malicious hacker has been trying to penetrate company XYZ from an external network location. He has tried every trick in his bag but still did not succeed.
From the choice presented below, what type of logical attempt is he most likely to attempt next?

A. Elevation of privileges
B. Pilfering of data
C. Denial of service

Pass4SureOfficial.com Lifetime Membership Features;

- Pass4SureOfficial Lifetime Membership Package includes over **2500** Exams.
- **All** exams Questions and Answers are included in package.
- **All** Audio Guides are included **free** in package.
- **All** Study Guides are included **free** in package.
- **Lifetime** login access.
- Unlimited download, no account expiry, no hidden charges, just one time $99 payment.
- **Free updates** for Lifetime.
- **Free Download Access** to All new exams added in future.
- Accurate answers with explanations (If applicable).
- Verified answers researched by industry experts.
- Study Material **updated** on regular basis.
- Questions, Answers and Study Guides are downloadable in **PDF** format.
- Audio Exams are downloadable in **MP3** format.
- **No authorization** code required to open exam.
- **Portable** anywhere.
- 100% success ***Guarantee***.
- **Fast**, helpful support 24x7.

View list of All exams (Q&A) downloads
http://www.pass4sureofficial.com/allexams.asp

View list of All Study Guides (SG) downloads
http://www.pass4sureofficial.com/study-guides.asp

View list of All Audio Exams (AE) downloads
http://www.pass4sureofficial.com/audio-exams.asp

Download All Exams Samples
http://www.pass4sureofficial.com/samples.asp

To purchase $99 Lifetime Full Access Membership click here
http://www.pass4sureofficial.com/purchase.asp

3COM	CompTIA	Filemaker	IBM	LPI	OMG	Sun
ADOBE	ComputerAssociates	Fortinet	IISFA	McAfee	Oracle	Sybase
APC	CWNP	Foundry	Intel	McData	PMI	Symantec
Apple	DELL	Fujitsu	ISACA	Microsoft	Polycom	TeraData
BEA	ECCouncil	GuidanceSoftware	ISC2	Mile2	RedHat	TIA
BICSI	EMC	HDI	ISEB	NetworkAppliance	Sair	Tibco
CheckPoint	Enterasys	Hitachi	ISM	Network-General	SASInstitute	TruSecure
Cisco	ExamExpress	HP	Juniper	Nokia	SCP	Veritas
Citrix	Exin	Huawei	Legato	Nortel	See-Beyond	Vmware
CIW	ExtremeNetworks	Hyperion	Lotus	Novell	SNIA