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.pass2lead.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

Bob is using a new sniffer called Ethereal.

However,it seems that Bob can only see packets that are sent from and to his own network interface card

(NIC).He cannot see any traffic from the other station.

What could be the cause of Bobs problem?(Select two)

A. The NIC is not in promiscuous mode

B. The network is using UDP traffic

C. Bob is connected to a switched network

D. The sniffer does not support Bobs TCP/IP network stack

Correct Answer: AB

QUESTION 2

Julius has been hired to perform a test on TestKing.com networks.

Julius knows that TestKing.com has a large team of security administrators who are very proactive in their security approach. Most likely there are some Intrusion Detection Systems (IDS) in place that would quickly identify Julius IP

address and he would then be blocked from accessing the network he is supposed to test.

How can Julius avoid having his IP address identified and then blocked?

Which of the following would be the most practical solution and the easiest to implement?

A. By using public key encryption;it is well known that IDS cannot make any sense of encrypted traffic and they would not be able to determine the source of the probes

B. By using Secure Socket Layer (SSL) Which will shield the intruder from the IDS and they wont be able to determine the source of the probes

C. By using only computers within the local internet caf.All traffic will be traced to the internet caf instead of being traced to the security tester

D. By using an internet anonymizer instead of connecting directly to the target.The anonymizer will shield the real source of the probes.

Correct Answer: D

QUESTION 3

An attacker is sending packets with no flag set.This is also known as doing a NULL scan.Usually,operating system networking stacks will respond with a RST packe,however,some operating systems do not conform to this behavior and

respond in appropriately. Such behavior could allow for the identification of the remote OS being used.Which of the following would be one of the Operating systems that responds differently?

A. Solaris

B. Linux

C. Windows

D. HP-UX

Correct Answer: C

QUESTION 4

You have been hired by company WXY to perform a Penetration Test,in this first phase of your test you have been challenged to remain totally stealthy. Which of the following reconnaissance types would best be used in such a scenario?

A. Active

B. Passive

C. Intrusive

D. Allusive

Correct Answer: B

QUESTION 5

Doing Operating System identification remotely is an art that requires analysis of responses from packets being sent.In order to do so efficiently,a methodology called fuzzy logic is often used. Which of the following would best describe what fuzzy logic is?

A. A problem solving control system

B. A special type of port scan

C. An operating system feature

D. A hardware device for OS identification

Correct Answer: A

QUESTION 6

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 7

If IPSec cannot be implemented to secure network communication from sniffing,what program would be an alternative choice for secure terminal logins and file transfers on Windows computers?Choose the best answer.

A. Hyperterm

B. puTTY

C. Sterm

D. WinPCap

Correct Answer: B

QUESTION 8

Which of the following password and encyption cracking methods is guaranteed to successfully crack any password or encryption algorithm?

A. Dictionary

B. Hybrid

C. Brute Force

D. RainbowCrack

Correct Answer: B

QUESTION 9

Which of the following would best describe the meaning of steganography?

A. The art and science of hiding information by embedding messages within other,seemingly harmless messages

B. The art and science of hiding information by encrypting it with a symmetric cipher where the key will be used only once

C. The art and science of hiding information by encrypting it using a public key encryption system where the key pair will be used only once

D. The art and science of hiding information by embedding redundant data within the primary data and then using XOR

against the stream

Correct Answer: A

QUESTION 10

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 changeds that could have happend 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

Correct Answer: C

QUESTION 11

Why are Trojans such as Beast a lot harder to detect?Choose the best answer.

A. They use a well known name to hide themselves

B. They inject themselves into another process

C. They have a polymorphic payload

D. They are self garbling and cannot be detected

Correct Answer: B

QUESTION 12

Why are SYN port scans not as stealthy as what they originally were several years ago?Choose two.

A. Many firewall rulesets detect and block SYN scans

B. IDS systems look for SYN flag packets due to the proliferation of SYN flood-based denial of service attacks

C. RFC 3502 has redefined the TCP three-way handshake thus changing how SYN flags are used

D. The Internet backtone routers all block SYN flag packets according to new RFC 3705

Correct Answer: AB

QUESTION 13

The nbstat tool is used to query the NetBIOS name table from a remote Windows system.The table below shows a sample output of the tool.

The second column is a two digit hexadecimal number that identiifies what the services and entities on the specific machine are.

If you look at line number 3 (in bold below),what does the 20 indiate?

A. The server service is running.

B. The RAS Client service is running.

C. The messenger service is running.

D. The workstation service is running

Correct Answer: A

QUESTION 14

You have been asked to assist an investigation team in collecting data and evidence related to an internal hacking case.

The investigator in charge of the case would like to capture all keystrokes from the suspect but is afraid the employee under investigation who possesses great technical skills might have installed integrity tools on his system that would detect any new software installed.

What solution would be best to use to reach the investigator requirement?

A. Disable the integrity tools in place

B. Install a software key logger that does not show in the process list

C. Install a hardware based key logger

D. Sniff all traffic and keystrokes from the network

Correct Answer: C

QUESTION 15

Which of the following scanning methods would be the most stealthy and best at hiding the source of a scan?

A. TCP Connect()

B. Syn-Ack

C. Fin-Ack

D. Idlescan

Correct Answer: D

Latest MK0-201 Dumps MK0-201 VCE Dumps MK0-201 Practice Test