



**Exam Code:** MK0-201

**Exam Name:** CPTS - Certified Pen Testing Specialist

**Vendor:** Mile2 Security

**Version:** DEMO

## Part: A

1: By spoofing an IP address and inserting the attacker's 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

**Correct Answers: B**

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

**Correct Answers: A B C**

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

**Correct Answers: C**

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

**Correct Answers: D**

5: If an attacker gets Administrative-level access, why can't 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

**Correct Answers: B C**

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:

**Correct Answers: C**

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

**Correct Answers: C**

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

**Correct Answers: A**

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

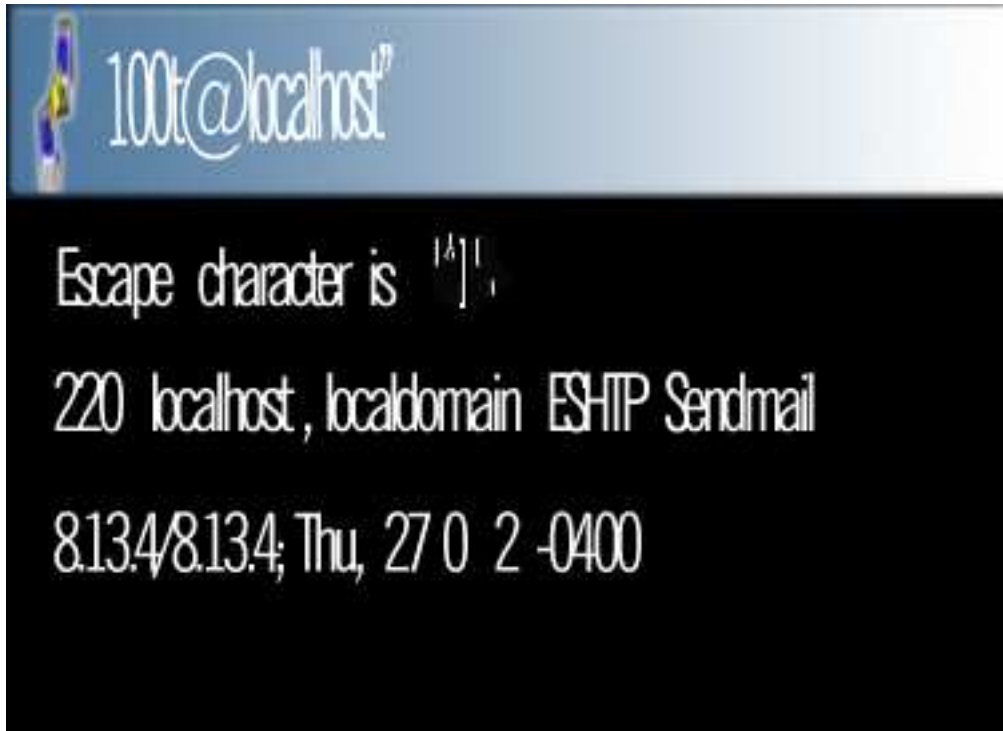
B.Digital Signature

C.Encryption

D.Diffie-Hillman

**Correct Answers: B**

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

**Correct Answers: C**

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

**Correct Answers: C**

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

D.Installation of a back door

**Correct Answers: C**

13: When a piece of malware executes on a computer, what privilege level or account will it

execute under? Choose the best answer.

- A.System
- B.Administrator
- C.Same privilege as the user who installed it
- D.Always runs as System or above

**Correct Answers: C**

14: Software Restriction Policies, if implemented correctly, can help protect against what kinds of threats? Choose two.

- A.Trojans
- B.Malware
- C.Spam
- D.Smurf Attacks

**Correct Answers: A B**

15: What software can alert an administrator to modified files (system or otherwise) by comparing new the hash to the hash on the original trusted file? Choose all that apply. NOTE: The term Choose all that apply in this and additional questions does not necessarily mean that there is more than one answer.

- A.Process Viewer
- B.Paketto Keiretsu
- C.VOMIT
- D.Tripwire

**Correct Answers: D**