

**Exam : MILE2 Security MK0-201**

**Title : CPTS – Certified Pen Testing Specialist**

**Version : Demo**

## Important Note, Please Read Carefully

### Other VisualExams products

[All visual exams IT Exam Products](#)

### Our products of Offline Testing Engine

Use the offline Testing engine product to practice the questions in an exam environment.

Build a foundation of knowledge which will be useful also after passing the exam.

[visual exams Testing Engine](#)

### Latest Version

We are constantly reviewing our products. New material is added and old material is revised. Free updates are available for 90 days after the purchase. You should check your member zone at VisualExams and update 3-4 days before the scheduled exam date.

Here is the procedure to get the latest version:

1. Go to <http://www.visual exams.com/>
2. Log in the **User Center**
3. The latest versions of all purchased products are downloadable from here. Just click the links.

### Feedback

If you spot a possible improvement then please let us know. We always interested in improving product quality.

Feedback should be send to [Visual exams@hotmail.com](mailto:Visual exams@hotmail.com). You should include the following: Exam number, version, page number, question number, and your login Account.

Our experts will answer your mail promptly.

### Explanations

This product does not include explanations at the moment. If you are interested in providing explanations for this exam, please contact [Visual exams@hotmail.com](mailto:Visual exams@hotmail.com).

### Features

- Comprehensive questions with complete details
- Instant Downloadable in PDF form.
- Verified Answers Researched by Industry Experts
- Questions accompanied by exhibits.
- Drag and Drop questions as experienced in the Actual Exams.
- These questions and answers are backed by our GUARANTEE.
- Questions updated on regular basis.
- Like actual certification exams our product is in multiple-choice questions (MCQs)

**Commitment to Your Success: At VisualTestExam.com, we are committed to you ongoing success. Our exams and questions are constantly being updated and compared to industry standards.**

Want to earn a Microsoft certification like MCSE, MCSE 2003, CCNA, CCNP? Thinking about getting an A+ or CCSP?

A, CCSP or Network+ Certification with less effort and time. You will be astonished at the theoretical and practical knowledge you will acquire in such a short period of time using our Certification Training Products. Our Study material will enable you to pass your Microsoft, Your Cisco and any other certification on the very first attempt.

## **Guarantee**

Visualexams provides the most competitive quality of all exams for the customers, we guarantee your success at the first attempt with only our Certification Question&Answers, if somehow you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

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**

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: ABC**

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**

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: AD**

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: BC**

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**

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**

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**

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**

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**

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**

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

**Answer: 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

**Answer: 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

**Answer: AB**

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

**Answer: D**

16. Why is it so challenging to block packets from Remote Access Trojans that use port 80 for network communications? Choose three.

- A. To a firewall, the traffic appears simply to be from an internal user making an innocuous HTTP GET request
- B. Port 80 outbound is normally open on corporate firewalls
- C. Stateful inspection firewalls will block unsolicited inbound HTTP GET requests
- D. Not all firewalls are capable of inspecting data in the HTTP data fields for evidence of tunneling

**Answer: ABD**

17. To block tunneling remote access trojans like 007Shell, what should you do on your firewall? Choose the best answer.

- A. Block all IGMP
- B. Block UDP port 1900
- C. Block all ICMP
- D. Block TCP port 27374

**Answer: C**

18. What sniffer program is capable of reconstructing associated TCP packets into a session showing application layer data from the client to the server and vice-versa? Choose the best 2 answers.

- A. Packetyzer
- B. Etherape
- C. Ethereal
- D. ARPwatch

**Answer: C**

19. What program can locate computers running sniffers by sending out special ARP packets that only network cards in promiscuous mode will reply to? Choose the best answer.

- A. ARPwatch
- B. Cain and Abel
- C. Macof
- D. Microsoft Network Monitor

**Answer: D**

20. The process of flooding a local segment with thousands of random MAC addresses can result in some switches behaving like a hub. The goal of the hacker is to accomplish what? Choose the best answer.

- A. Denial of service
- B. ARP cache poisoning
- C. Sniffing in a switched network
- D. SYN flood

**Answer: C**

Visualexams.com was founded in 2006. The safer,easier way to help you pass any IT Certification exams . We provide high quality IT Certification exams practice questions and answers(Q&A). Especially Adobe, Apple, Citrix, Comptia, EMC, HP, HuaWei, LPI, Nortel, Oracle, SUN, Vmware and so on. And help you pass any IT Certification exams at the first try.

Web site: <http://www.visualexams.com>

You can reach us at any of the email addresses listed below.

E-Mail: [visualexams \(at\) hotmail.Com](mailto:visualexams@hotmail.com)