Vendor: McAfee

Exam Code: MA0-150

Exam Name: McAfee Certified Assessment Specialist - Network

Version: DEMO

QUESTION 1
Under UNIX, Pluggable Authentication Modules (PAN) can be used to

A. Implement strong password management.
B. Crack password hashes from /etc/shadow.
C. Crack password hashes from /etc/passwd.
D. Create a certificate authority (CA).

Answer: A

QUESTION 2
What is the quickest protocol to brute force when attacking Windows?

A. SFTP
B. HTTPS
C. SMB
D. SSH

Answer: C

QUESTION 3
The datapipe and fpipe tools can be used for

A. Port scanning.
B. Port redirection.
C. Passing the hash.
D. Directory traversal.

Answer: B

QUESTION 4
What is the basis for Cisco Type 7 passwords?

A. Asymmetric key cryptography
B. Symmetric key cryptography
C. One-way hashing
D. Encoding

Answer: D

QUESTION 5
What is the magic number for a Linux binary?

A. MZ
B. JFIF
C. EXIF
D. ELF

Answer: D

QUESTION 6
Horizontal privilege escalation is a vulnerability of authorization where users act at a privilege level

A. Above one they are entitled to act.
B. Below one they are entitled to act.
C. That they are entitled to but only as a different user.
D. That transfers across another application.

Answer: C

QUESTION 7
A corporate user has just been hacked and shell code is installed. The user logs off, but the hacker remains on the system with NT AUTHORTTY\SYSTEM credentials. What can the attacker use to escalate to the corporate user's permissions?

A. AT scheduler
B. Cached credentials
C. Local windows privilege escalation
D. psexec

Answer: B

QUESTION 8
Which of the following are advantages of maintaining a separate syslog server? (Choose two)

A. Harder for attackers to cover their tracks
B. Easier to implement hard drive backups
C. Easier to implement network time protocol (NTP)
D. Harder to control VPN traffic
E. Harder for rogue network administrator collusion

Answer: AE

QUESTION 9
NetBIOS enumeration requires access to which TCP ports?

A. 389 or 3268
B. 1433 or 1434
C. 135 or 137
D. 139 or 445

Answer: D

QUESTION 10
The nmap command nmap -O would result in

A. Output to a file.
B. Operating System detection.
C. Organizing by port (low to high).
D. Organizing by port (high to low).

Answer: B

QUESTION 11
Which of the following are common vulnerabilities in web applications? (Choose three)

A. SQL Injection
B. CSRF cookies
C. Cross Site Scripting
D. Cross Site Request Forgery
E. Captchas

Answer: ACD

QUESTION 12
The Nmap command nmap sV would result in

A. Version scanning.
B. Verbose output.
C. Very verbose output.
D. Vector initialization.

Answer: A

QUESTION 13
Which of the following are necessary for RFID? (Choose two)

A. Antenna
B. Microchip
C. Encryption
D. Faraday cage
E. RF shielding

Answer: AB

QUESTION 14
Brute force attack tools include which of the following? (Choose three)

A. Hydra
B. Medusa
C. Ettercap
D. Metasploit
E. Dsniff

Answer: ABD

QUESTION 15
Which of the following commands will tell you what version of Microsoft Windows is running? (Choose three)

A. regsvr32
B. windiff
C. ver
D. systeminfo
E. cmd

Answer: CDE

QUESTION 16
During an external penetration test, the consultant identifies a Windows-based server that is running Apache Tomcat Manager with a default username and password combination. After uploading a WAR file, the consultant has the ability to execute commands via a browser under the context of NT AUTHORITY/SYSTEM. Which of the following commands would allow the consultant to create a user and put the newly created user in the administrators group? (Choose two)

A. Net user /add consultant Passwordl23
B. Net localuser /add consultant Passwordl23
C. Net localgroup administrators /add consultant
D. Net administrators /add consultant Passwordl23
E. Creating users under the context of SYSTEM is not allowed

Answer: AC

QUESTION 17
What protocol does the Nmap default scan nmap 192.16S.1.1 use?

A. TCP
B. UDP
C. ICMP
D. ARP

Answer: A

QUESTION 18
Reverse Telnet is an example of a

A. Callback from the compromised host.
B. Technique used to secure UNIX servers from portscans.
C. Honeypot protection mechanism.
D. Port redirection technique.

Answer: A

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

★ More than 99,900 Satisfied Customers Worldwide.

★ Average 99.9% Success Rate.

★ Free Update to match latest and real exam scenarios.

★ Instant Download Access! No Setup required.

★ Questions & Answers are downloadable in PDF format and VCE test engine format.

★ Multi-Platform capabilities - Windows, Laptop, Mac, Android, iPhone, iPod, iPad.

★ 100% Guaranteed Success or 100% Money Back Guarantee.

★ Fast, helpful support 24x7.

View list of all certification exams: http://www.lead2pass.com/all-products.html

10% Discount Coupon Code: **ASTR14**