McAfee MA0-150

McAfee Certified Assessment Specialist – Network

Version: 4.0

Topic 1, Volume A

QUESTION NO: 1

An attacker has compromised a Linux/Unix host and discovers a suspicious file called "password" that has no file extension. What command can be used to determine the filetype?

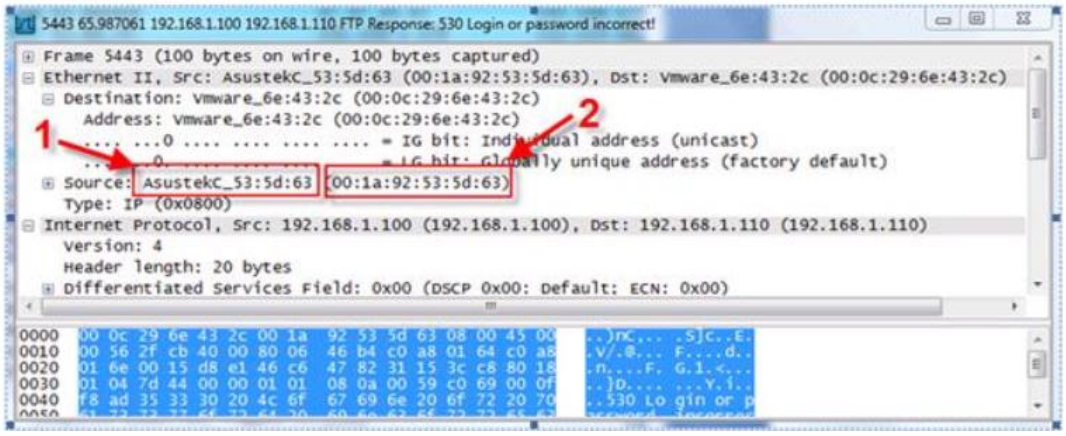
A. filetype
B. file
C. filer
D. fileext

Answer: B

Explanation:

QUESTION NO: 2

Below is a packet capture from Wireshark showing 2 equivalent MAC address in the Source field. Box 1 shows "Asustek..." while Box 2 shows "00:1a:92..".



-Wireshark can determine these are equivalent because MAC addresses can be mapped to

A. Operating systems (and variants)
B. Computer names
C. RFCs
D. Vendors

Answer: D

Explanation:

QUESTION NO: 3

What is the correct syntax to query under which service a user account is running?

A. sc.exe \\192.168.1.1 qc <service>
B. sc.exe \\192.168.1.1 <service>
C. net start \\192.168.1.1 qc
D. net start W192.168.1.1

Answer: A
Explanation:

QUESTION NO: 4

What file indicates and controls where system logs are stored?

A. pam.conf
B. smb.conf
C. authlog.conf
D. syslog.conf

Answer: D
Explanation:

QUESTION NO: 5

The command "grep password *" searches for

A. The word "password" in all files in the current directory.
B. The character "*" in the file "password".
C. The word "password" in all files in the current directory and all subdirectories.
D. All passwords in the file named "*".

Answer: A
Explanation:

QUESTION NO: 6

The following output is generated from cat /etc/shadow:

```
root:$6$GkfJ0/H/
$IDtJEzDO1vh7VyDG5rnnLLMXwZl.cikulTg4wtXjq98Vlcf/PA2D1QsT7
VHSsu46B/od4IJlqENMtc8dSpBEa1:14592:0:99999:7:::
daemon:x:14592:0:99999:7:::
bin:x:14592:0:99999:7:::
```

What hashing algorithm is used to protect the root password?

A. Crypt (DES)
B. MD5
C. Blowfish
D. SHA

Answer: D
Explanation:

QUESTION NO: 7

In computer security, a small piece of code that acts as a payload in which an attacker can control a remote machine is called

A. A buffer overflow.
B. A NOP sled.
C. Shell code.
D. Stack overflow.

Answer: C
Explanation:

QUESTION NO: 8

A person connects to a web application via a mobile device. What request header name can this application use determine which device the person is using?

A. Referer
B. User agent

C. Connection
D. Host

Answer: B
Explanation:

QUESTION NO: 9

What is the proper syntax for enumerating non-hidden shares on a host?

A. net view /domain
B. net view /domain:{domain}
C. net view \\{target}
D. net use \\{target}\ipc$ "" /u:""

Answer: C
Explanation:

QUESTION NO: 10

What is the term used for a technique that runs code within the address space of another process by forcing it to bad a library?

A. Address space layout randomization
B. Overwriting HP
C. DLL injection
D. SQL injection

Answer: C
Explanation:

QUESTION NO: 11

What Microsoft utility encrypts the hashed passwords in a SAM database using 128-bit encryption?

A. ASLR
B. DEP

C. Syskey
D. Kerberos

Answer: C
Explanation:

QUESTION NO: 12

An attacker has just compromised a Linux host. What command can be used to determine the distribution of Linux?

A. cat /etc/crontab
B. cat /etc/passwd
C. cat/etc/issue
D. cat /etc/shadow

Answer: C
Explanation:

QUESTION NO: 13

What is NOT a possible cross-site request forgery attack vector?

A. Captchas
B. Cross-site scripting
C. Email
D. Chat

Answer: A
Explanation:

QUESTION NO: 14

The Xscan tool is a

A. X Windows Brute Forcer
B. Keylogger for X Windows
C. Keylogger for Mac OS X

D. Multi OS port scanner

Answer: B
Explanation:

QUESTION NO: 15

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
Explanation:

QUESTION NO: 16

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

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

Answer: C
Explanation:

QUESTION NO: 17

The datapipe and fpipe tools can be used for

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

Answer: B
Explanation:

QUESTION NO: 18

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
Explanation:

QUESTION NO: 19

What is the magic number for a Linux binary?

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

Answer: D
Explanation:

QUESTION NO: 20

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
Explanation:

QUESTION NO: 21

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
Explanation:

QUESTION NO: 22

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: A,E
Explanation:

QUESTION NO: 23

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

Explanation:

QUESTION NO: 24

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
Explanation:

QUESTION NO: 25

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: A,C,D
Explanation:

QUESTION NO: 26

The Nmap command nmap sV would result in

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

Answer: A
Explanation: