



# McAfee

## MA0-150 Exam

### McAfee Certified Assessment Specialist- UH Exam

Thank you for Downloading MA0-150 exam PDF Demo

You can Buy Latest MA0-150 Full Version Download

<https://www.certkillers.net/Exam/MA0-150>

<https://www.certkillers.net>

---

**Question: 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**

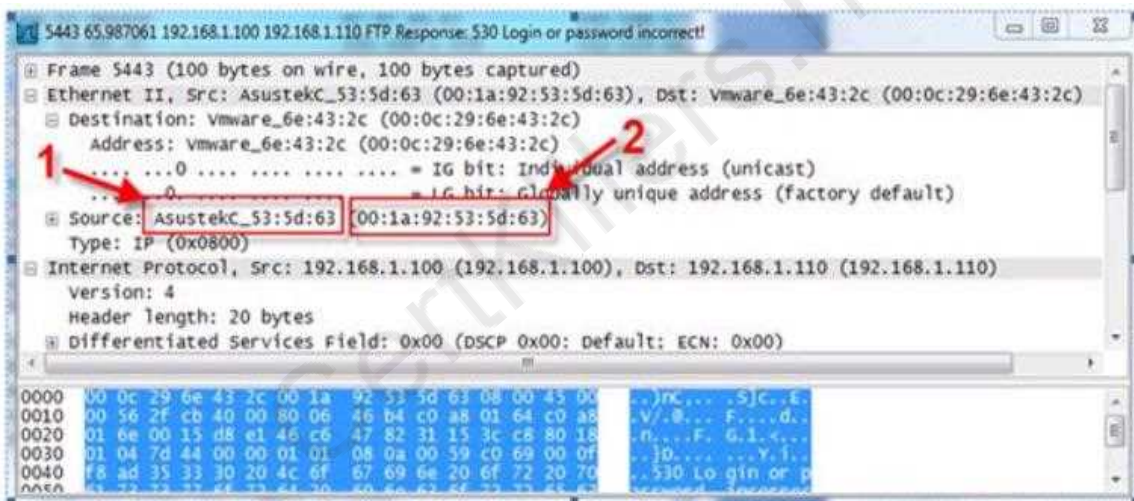
---

---

**Question: 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**

---

---

**Question: 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**

---

---

**Question: 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**

---

---

**Question: 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**

---

---

**Question: 6**

---

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

```
root:$6$GkfJ0/H/
$IDtJEzDO1vh7VyDG5rnLLMXwZl.cikuITg4wtXjq98Vlcf/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**

---

---

**Question: 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**

---

---

**Question: 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**

---

---

**Question: 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**

---

---

**Question: 10**

---

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

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

---

**Answer: C**

---

---

**Question: 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**

---

---

**Question: 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**

---

## Thank You for trying MA0-150 PDF Demo

To Buy Latest MA0-150 Full Version Download visit link below

<https://www.certkillers.net/Exam/MA0-150>

## Start Your MA0-150 Preparation

**[Limited Time Offer]** Use Coupon “CKNET” for Further discount on your purchase. Test your MA0-150 preparation with actual exam questions.

<https://www.certkillers.net>