CEH-001 Q&As

Certified Ethical Hacker (CEH)

Pass GAQM CEH-001 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.leads4pass.com/ceh-001.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by GAQM Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

Which set of access control solutions implements two-factor authentication?

A. USB token and PIN

B. Fingerprint scanner and retina scanner

C. Password and PIN

D. Account and password

Correct Answer: A

QUESTION 2

Eve is spending her day scanning the library computers. She notices that Alice is using a computer whose port 445 is active and listening. Eve uses the ENUM tool to enumerate Alice machine. From the command prompt, she types the

following command.

For /f "tokens=1 %%a in (hackfile.txt) do net use * \\10.1.2.3\c$ /user:"Administrator" %%a

What is Eve trying to do?

A. Eve is trying to connect as an user with Administrator privileges

B. Eve is trying to enumerate all users with Administrative privileges

C. Eve is trying to carry out a password crack for user Administrator

D. Eve is trying to escalate privilege of the null user to that of Administrator

Correct Answer: C

QUESTION 3

Which of the following does proper basic configuration of snort as a network intrusion detection system require?

A. Limit the packets captured to the snort configuration file.

B. Capture every packet on the network segment.

C. Limit the packets captured to a single segment.

D. Limit the packets captured to the /var/log/snort directory.

Correct Answer: A

QUESTION 4

Which Steganography technique uses Whitespace to hide secret messages?

A. snow

B. beetle

C. magnet

D. cat

Correct Answer: A

QUESTION 5

Samuel is the network administrator of DataX Communications, Inc. He is trying to configure his firewall to block password brute force attempts on his network. He enables blocking the intruder\\'s IP address for a period of 24 hours\\' time after more than three unsuccessful attempts. He is confident that this rule will secure his network from hackers on the Internet.

But he still receives hundreds of thousands brute-force attempts generated from various IP addresses around the world. After some investigation he realizes that the intruders are using a proxy somewhere else on the Internet which has been scripted to enable the random usage of various proxies on each request so as not to get caught by the firewall rule.

Later he adds another rule to his firewall and enables small sleep on the password attempt so that if the password is incorrect, it would take 45 seconds to return to the user to begin another attempt. Since an intruder may use multiple machines to brute force the password, he also throttles the number of connections that will be prepared to accept from a particular IP address. This action will slow the intruder\\'s attempts.

Samuel wants to completely block hackers brute force attempts on his network. What are the alternatives to defending against possible brute-force password attacks on his site?

A. Enforce a password policy and use account lockouts after three wrong logon attempts even though this might lock out legit users

B. Enable the IDS to monitor the intrusion attempts and alert you by e-mail about the IP address of the intruder so that you can block them at the Firewall manually

C. Enforce complex password policy on your network so that passwords are more difficult to brute force

D. You cannot completely block the intruders attempt if they constantly switch proxies

Correct Answer: D

QUESTION 6

Which of the following techniques will identify if computer files have been changed?

A. Network sniffing

B. Permission sets

C. Integrity checking hashes

D. Firewall alerts

Correct Answer: C

QUESTION 7

Attackers target HINFO record types stored on a DNS server to enumerate information. These are information records and potential source for reconnaissance. A network administrator has the option of entering host information specifically the CPU type and operating system when creating a new DNS record. An attacker can extract this type of information easily from a DNS server.

Which of the following commands extracts the HINFO record?

A.
```
c:> nslookup
> Set type=hinfo
> certhack-srv
Server: dns.certifiedhacker.com
Address: 10.0.0.4
sales.certifiedhacker.com      CPU = Intel Quad Chip OS=Linux 2.8
dns.certifiedhacker.com        Internet address = 10.0.0.56
```

B.
```
c:> nslookup
> Set dns=hinfo
> certhack-srv
Server: dns.certifiedhacker.com
IP: 10.0.0.4
sales.certifiedhacker.com      CPU = Intel Quad Chip OS=Linux 2.8
dns.certifiedhacker.com        Internet address = 10.0.0.56
```

C.
```
c:> nslookup
> Set record=hinfo
> certhack-srv
host: dns.certifiedhacker.com
Address: 10.0.0.4
sales.certifiedhacker.com      CPU = Intel Quad Chip OS=Linux 2.8
dns.certifiedhacker.com        Internet address = 10.0.0.56
```

D.
```
c:> nslookup
> Configure type=hinfo
> certhack-srv
Host: dns.certifiedhacker.com
IP: 10.0.0.4
sales.certifiedhacker.com      CPU = Intel Quad Chip OS=Linux 2.8
dns.certifiedhacker.com Internet address = 10.0.0.56
```

A. Option A

B. Option B

C. Option C

D. Option D

Correct Answer: A

QUESTION 8

What techniques would you use to evade IDS during a Port Scan? (Select 4 answers)

A. Use fragmented IP packets

B. Spoof your IP address when launching attacks and sniff responses from the server

C. Overload the IDS with Junk traffic to mask your scan

D. Use source routing (if possible)

E. Connect to proxy servers or compromised Trojaned machines to launch attacks

Correct Answer: ABDE

QUESTION 9

You want to capture Facebook website traffic in Wireshark. What display filter should you use that shows all TCP packets that contain the word \\'facebook\\'?

A. display==facebook

B. traffic.content==facebook

C. tcp contains facebook

D. list.display.facebook

Correct Answer: C

QUESTION 10

You have initiated an active operating system fingerprinting attempt with nmap against a target system:

```
[root@ceh NG]# /usr/local/bin/nmap -sT -O 10.0.0.1

Starting nmap 3.28 ( www.insecure.org/nmap/) at 2003-06-18 19:14 IDT
Interesting ports on 10.0.0.1:
(The 1628 ports scanned but not shown below are in state: closed)

Port State Service
21/tcp filtered ftp
22/tcp filtered ssh
25/tcp open smtp
80/tcp open http
135/tcp open loc-srv
139/tcp open netbios-ssn
389/tcp open LDAP
443/tcp open https
465/tcp open smtps
1029/tcp open ms-lsa
1433/tcp open ms-sql-s
2301/tcp open compaqdiag
5555/tcp open freeciv
5800/tcp open vnc-http
5900/tcp open vnc
6000/tcp filtered X11

Remote operating system guess: Windows XP, Windows 2000, NT4 or 95/98/98SE Nmap
run completed -- 1 IP address (1 host up) scanned in 3.334 seconds

Using its fingerprinting tests nmap is unable to distinguish between different groups of
Microsoft based operating systems - Windows XP, Windows 2000, NT4 or 95/98/98SE.
```

What operating system is the target host running based on the open ports shown above?

A. Windows XP

B. Windows 98 SE

C. Windows NT4 Server

D. Windows 2000 Server

Correct Answer: D

QUESTION 11

If the final set of security controls does not eliminate all risk in a system, what could be done next?

A. Continue to apply controls until there is zero risk.

B. Ignore any remaining risk.

C. If the residual risk is low enough, it can be accepted.

D. Remove current controls since they are not completely effective.

Correct Answer: C

QUESTION 12

John is discussing security with Jane. Jane had mentioned to John earlier that she suspects an LKM has been installed on her server. She believes this is the reason that the server has been acting erratically lately. LKM stands for Loadable Kernel Module.

What does this mean in the context of Linux Security?

A. Loadable Kernel Modules are a mechanism for adding functionality to a file system without requiring a kernel recompilation.

B. Loadable Kernel Modules are a mechanism for adding functionality to an operating- system kernel after it has been recompiled and the system rebooted.

C. Loadable Kernel Modules are a mechanism for adding auditing to an operating-system kernel without requiring a kernel recompilation.

D. Loadable Kernel Modules are a mechanism for adding functionality to an operating- system kernel without requiring a kernel recompilation.

Correct Answer: D

QUESTION 13

Every company needs a formal written document which spells out to employees precisely what they are allowed to use the company\\'s systems for, what is prohibited, and what will happen to them if they break the rules. Two printed copies of the policy should be given to every employee as soon as possible after they join the organization. The employee should be asked to sign one copy, which should be safely filed by the company. No one should be allowed to use the company\\'s computer systems until they have signed the policy in acceptance of its terms. What is this document called?

A. Information Audit Policy (IAP)

B. Information Security Policy (ISP)

C. Penetration Testing Policy (PTP)

D. Company Compliance Policy (CCP)

Correct Answer: B

QUESTION 14

In what stage of Virus life does a stealth virus gets activated with the user performing certain actions such as running an infected program?

A. Design

B. Elimination

C. Incorporation

D. Replication

E. Launch

F. Detection

Correct Answer: E

QUESTION 15

Snort is an open source Intrusion Detection system. However, it can also be used for a few other purposes as well.

Which of the choices below indicate the other features offered by Snort?

A. IDS, Packet Logger, Sniffer

B. IDS, Firewall, Sniffer

C. IDS, Sniffer, Proxy

D. IDS, Sniffer, content inspector

Correct Answer: A