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.certbus.com/ceh-001.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

Which tool would be used to collect wireless packet data?

A. NetStumbler

B. John the Ripper

C. Nessus

D. Netcat

Correct Answer: A

QUESTION 2

Leesa is the senior security analyst for a publicly traded company. The IT department recently rolled out an intranet for company use only with information ranging from training, to holiday schedules, to human resources data. Leesa wants to make sure the site is not accessible from outside and she also wants to ensure the site is Sarbanes-Oxley (SOX) compliant. Leesa goes to a public library as she wants to do some Google searching to verify whether the company\\'s intranet is accessible from outside and has been indexed by Google. Leesa wants to search for a website title of "intranet" with part of the URL containing the word "intranet" and the words "human resources" somewhere in the webpage.

What Google search will accomplish this?

A. related:intranet allinurl:intranet:"human resources"

B. cache:"human resources" inurl:intranet(SharePoint)

C. intitle:intranet inurl:intranet+intext:"human resources"

D. site:"human resources"+intext:intranet intitle:intranet

Correct Answer: C

QUESTION 3

In keeping with the best practices of layered security, where are the best places to place intrusion detection/intrusion prevention systems? (Choose two.)

A. HID/HIP (Host-based Intrusion Detection/Host-based Intrusion Prevention)

B. NID/NIP (Node-based Intrusion Detection/Node-based Intrusion Prevention)

C. NID/NIP (Network-based Intrusion Detection/Network-based Intrusion Prevention)

D. CID/CIP (Computer-based Intrusion Detection/Computer-based Intrusion Prevention)

Correct Answer: AC

QUESTION 4

Neil notices that a single address is generating traffic from its port 500 to port 500 of several other machines on the network. This scan is eating up most of the network bandwidth and Neil is concerned. As a security professional, what would you infer from this scan?

A. It is a network fault and the originating machine is in a network loop

B. It is a worm that is malfunctioning or hardcoded to scan on port 500

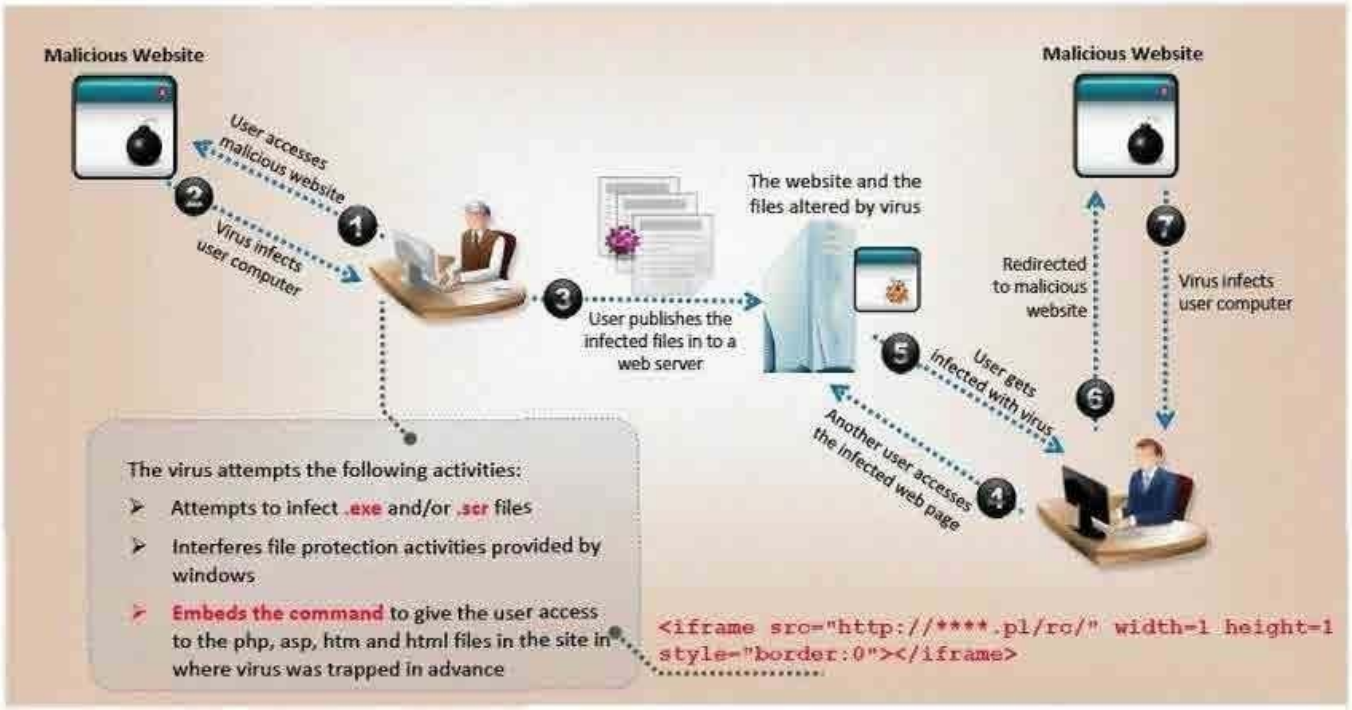
C. The attacker is trying to detect machines on the network which have SSL enabled

D. The attacker is trying to determine the type of VPN implementation and checking for IPSec

Correct Answer: D

QUESTION 5

ViruXine.W32 virus hides their presence by changing the underlying executable code. This Virus code mutates while keeping the original algorithm intact, the code changes itself each time it runs, but the function of the code (its semantics) will not change at all.



Here is a section of the Virus code: What is this technique called?

```
1.  lots of encrypted code
2.  ...
3.  Decryption_Code:
4.  C = C + 1
5.  A = Encrypted
6.  Loop:
7.  B = *A
8.  C = 3214 * A
9.  B = B XOR CryptoKey
10. *A = B
11. C = 1
12. C = A + B
13. A = A + 1
14. GOTO Loop IF NOT A = Decryption_Code
15. C = C^2
16. GOTO Encrypted
17. CryptoKey:
18. some_random_number
```

A. Polymorphic Virus

B. Metamorphic Virus

C. Dravidic Virus

D. Stealth Virus

Correct Answer: A

QUESTION 6

Which system consists of a publicly available set of databases that contain domain name registration contact information?

A. WHOIS

B. IANA

C. CAPTCHA

D. IETF

Correct Answer: A

QUESTION 7

What is the advantage in encrypting the communication between the agent and the monitor in an Intrusion Detection System?

A. Encryption of agent communications will conceal the presence of the agents

B. The monitor will know if counterfeit messages are being generated because they will not be encrypted

C. Alerts are sent to the monitor when a potential intrusion is detected

D. An intruder could intercept and delete data or alerts and the intrusion can go undetected

Correct Answer: B

QUESTION 8

What is a sheepdip?

A. It is another name for Honeynet

B. It is a machine used to coordinate honeynets

C. It is the process of checking physical media for virus before they are used in a computer

D. None of the above

Correct Answer: C

QUESTION 9

Use the traceroute results shown above to answer the following question:

```
Home/root # traceroute www.targetcorp.com <http://www.targetcorp.com>
traceroute to www.targetcorp.com <http://www.targetcorp.com>
(192.168.12.18), 64 hops may, 40 byte packets

1 router.anon.com (192.13.212.254) 1.373 ms 1.123 ms 1.280 ms

2 192.13.133.121 (192.13.133.121) 3.680 ms 3.506 ms 4.583 ms
3 firewall.anon.com (192.13.192.17) 127.189 ms 257.404 ms 208.484 ms
4 anon-gw.anon.com (192.93.144.89) 471.68 ms 376.875 ms 228.286 ms
5 fe5-0.lin.isp.com (192.162.231.225) 2.961 ms 3.852 ms 2.974 ms
6 fe0-0.lon0.isp.com (192.162.231.234) 3.979 ms 3.243 ms 4.370 ms
7 192.13.133.5 (192.13.133.5) 11.454 ms 4.221 ms 3.333 ms
6 * * *
7 * * *
8

www.targetcorp.com <http://www.targetcorp.com> (192.168.12.18) 5.392 ms 3.348 ms
3.199 ms
```

The perimeter security at targetcorp.com does not permit ICMP TTL-expired packets out.

A. True

B. False

Correct Answer: A

QUESTION 10

A Buffer Overflow attack involves:

A. Using a trojan program to direct data traffic to the target host\\'s memory stack

B. Flooding the target network buffers with data traffic to reduce the bandwidth available to legitimate users

C. Using a dictionary to crack password buffers by guessing user names and passwords

D. Poorly written software that allows an attacker to execute arbitrary code on a target system

Correct Answer: D

QUESTION 11

Which of the following represents the initial two commands that an IRC client sends to join an IRC network?

A. USER, NICK

B. LOGIN, NICK

C. USER, PASS

D. LOGIN, USER

Correct Answer: A

QUESTION 12

The traditional traceroute sends out ICMP ECHO packets with a TTL of one, and increments the TTL until the destination has been reached. By printing the gateways that generate ICMP time exceeded messages along the way, it is able to determine the path packets take to reach the destination.

The problem is that with the widespread use of firewalls on the Internet today, many of the packets that traceroute sends out end up being filtered, making it impossible to completely trace the path to the destination.

```
Juggyboy$ traceroute www.eccouncil.org
traceroute to www.eccouncil.org (64.147.99.90), 30 hops max, 52 byte packets
 1  * * *
 2  * * *
 3  ras.beamtele.net (183.82.15.69)  1.579 ms  1.513 ms  1.444 ms
 4  115.113.205.29.static-hyderabad.vsnl.net.in (115.113.205.29)  2.093 ms  1.963 ms  1.948 ms
 5  59.163.16.54.static.vsnl.net.in (59.163.16.54)  13.062 ms  13.094 ms  13.102 ms
 6  if-5-0-0-550.core2.cfo-chennai.as6453.net (116.0.84.69)  13.371 ms  13.103 ms  13.285 ms
 7  if-10-1-1-0.tcore2.cxr-chennai.as6453.net (180.87.37.18)  183.760 ms  165.805 ms  165.756 ms
 8  if-9-2.tcore2.mlv-mumbai.as6453.net (180.87.37.10)  172.479 ms  162.924 ms  162.835 ms
 9  if-6-2.tcore1.178-london.as6453.net (80.231.130.5)  151.203 ms  156.257 ms  150.901 ms
10  vlan704.icore1.ldn-london.as6453.net (80.231.130.10)  151.268 ms  152.167 ms  161.829 ms
11  * * *
12  ae-34-52.ebr2.london1.level3.net (4.69.139.97)  157.454 ms  151.607 ms  151.777 ms
13  ae-23-23.ebr2.frankfurt1.level3.net (4.69.148.194)  162.926 ms
    ae-22-22.ebr2.frankfurt1.level3.net (4.69.148.190)  170.020 ms
    ae-21-21.ebr2.frankfurt1.level3.net (4.69.148.166)  166.144 ms
14  ae-43-43.ebr2.washington1.level3.net (4.69.137.58)  236.524 ms
    ae-44-44.ebr2.washington1.level3.net (4.69.137.62)  246.080 ms  254.330 ms
15  ae-3-3.ebr1.newyork2.level3.net (4.69.132.90)  237.647 ms  252.050 ms
    ae-5-5.ebr2.washington12.level3.net (4.69.143.222)  258.821 ms
16  4.69.148.49 (4.69.148.49)  240.058 ms
    ae-4-4.ebr1.newyork1.level3.net (4.69.141.17)  242.545 ms
    4.69.148.49 (4.69.148.49)  240.874 ms
17  ae-61-61.csw1.newyork1.level3.net (4.69.134.66)  250.844 ms
    ae-71-71.csw2.newyork1.level3.net (4.69.134.70)  256.370 ms  242.690 ms
18  ae-34-89.car4.newyork1.level3.net (4.68.16.134)  250.200 ms
    ae-24-79.car4.newyork1.level3.net (4.68.16.70)  236.524 ms
    ae-14-69.car4.newyork1.level3.net (4.68.16.6)  255.573 ms
19  the-new-yor.car4.newyork1.level3.net (63.208.174.50)  249.250 ms  247.363 ms  243.364 ms
20  cs-nyi-gigalan-114.nyinternet.net (64.147.101.114)  240.236 ms  241.212 ms  240.654 ms
21  * * *          Request timed out
22  * * *          Request timed out
23  * * *          Request timed out
24  * * *          Request timed out
25  * * *          Request timed out
26  * * *          Request timed out
27  * * *          Request timed out
28  * * *          Request timed out
29  * * *          Request timed out
30  * * *          Request timed out

Destination Reached in 251 ms. Connection established to 64.147.99.90
Trace complete.
```

How would you overcome the Firewall restriction on ICMP ECHO packets?

A. Firewalls will permit inbound TCP packets to specific ports that hosts sitting behind the firewall are listening for connections. By sending out TCP SYN packets instead of ICMP ECHO packets, traceroute can bypass the most common firewall filters.

B. Firewalls will permit inbound UDP packets to specific ports that hosts sitting behind the firewall are listening for connections. By sending out TCP SYN packets instead of ICMP ECHO packets, traceroute can bypass the most common firewall filters.

C. Firewalls will permit inbound UDP packets to specific ports that hosts sitting behind the firewall are listening for connections. By sending out TCP SYN packets instead of ICMP ECHO packets, traceroute can bypass the most common firewall filters.

D. Do not use traceroute command to determine the path packets take to reach the destination instead use the custom hacking tool JOHNTHETRACER and run with the command

E. \> JOHNTHETRACER www.eccouncil.org -F -evade

Correct Answer: A

QUESTION 13

John the Ripper is a technical assessment tool used to test the weakness of which of the following?

A. Usernames

B. File permissions

C. Firewall rulesets

D. Passwords

Correct Answer: D

QUESTION 14

Which of the following ICMP message types are used for destinations unreachables?

A. 0

B. 3

C. 11

D. 13

E. 17

Correct Answer: B

QUESTION 15

Exhibit

```
05/20-17:06:45.061034 192.160.13.4:31337 -> 172.16.1.101:1 TCP TTL:44 TOS:0x10 ID:242
***FRP** Seq: 0XA1D95 Ack: 0x53 Win: 0x400
...
05/20-17:06:58.685879 192.160.13.4:31337 ->
172.16.1.101:1024
TCP TTL:44 TOS:0x10 ID:242
***FRP** Seq: 0XA1D95 Ack: 0x53 Win: 0x400
```

(Note: the student is being tested on concepts learnt during passive OS fingerprinting, basic TCP/IP connection concepts and the ability to read packet signatures from a sniff dump.)

Snort has been used to capture packets on the network. On studying the packets, the penetration tester finds it to be abnormal. If you were the penetration tester, why would you find this abnormal?

What is odd about this attack? Choose the best answer.

A. This is not a spoofed packet as the IP stack has increasing numbers for the three flags.

B. This is back orifice activity as the scan comes form port 31337.

C. The attacker wants to avoid creating a sub-carries connection that is not normally valid.

D. These packets were crafted by a tool, they were not created by a standard IP stack.

Correct Answer: B