312-50V7 Q&As

Ethical Hacking and Countermeasures (CEHv7)

Pass EC-COUNCIL 312-50V7 Exam with 100% Guarantee

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

https://www.pass4itsure.com/312-50v7.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

An engineer is learning to write exploits in C++ and is using the exploit tool Backtrack. The engineer wants to compile the newest C++ exploit and name it calc.exe. Which command would the engineer use to accomplish this?

A. g++ hackersExploit.cpp -o calc.exe

B. g++ hackersExploit.py -o calc.exe

C. g++ -i hackersExploit.pl -o calc.exe

D. g++ --compile i hackersExploit.cpp -o calc.exe

Correct Answer: A

QUESTION 2

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 3

Which type of scan measures a person\\'s external features through a digital video camera?

A. Iris scan

B. Retinal scan

C. Facial recognition scan

D. Signature kinetics scan

Correct Answer: C

QUESTION 4

A tester is attempting to capture and analyze the traffic on a given network and realizes that the network has several switches. What could be used to successfully sniff the traffic on this switched network? (Choose three.)

A. ARP spoofing

B. MAC duplication

C. MAC flooding

D. SYN flood

E. Reverse smurf attack

F. ARP broadcasting

Correct Answer: ABC

QUESTION 5

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 (4.69.148.186)  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)  246.030 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