Up-to-date Questions and Answers from authentic resources to improve knowledge and pass the exam at very first attempt. ----- Guaranteed.

KILL EXAMS

EC1-350 Dumps
EC1-350 Braindumps
EC1-350 Real Questions
EC1-350 Practice Test
EC1-350 Actual Questions

PASS

EC-Council

EC1-350

Ethical Hacking and Countermeasures V7

QUESTION: 250

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)  246.080 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

Answer: A

QUESTION: 251
Simon is security analyst writing signatures for a Snort node he placed internally that captures all mirrored traffic from his border firewall. From the following signature, what will Snort look for in the payload of the suspected packets?
alert tcp $EXTERNAL_NET any -> $HOME_NET 27374 (msg: "BACKDOOR SIG – SubSseven 22";flags: A+; content: "|0d0a5b52504c5d3030320d0a|"; reference:arachnids,485;) alert

A. The payload of 485 is what this Snort signature will look for.
B. Snort will look for 0d0a5b52504c5d3030320d0a in the payload.
C. Packets that contain the payload of BACKDOOR SIG - SubSseven 22 will be flagged.
D. From this snort signature, packets with HOME_NET 27374 in the payload will be flagged.

Answer: B

QUESTION: 252
You are trying to package a RAT Trojan so that Anti-Virus software will not detect it. Which of the listed technique will NOT be effective in evading Anti-Virus scanner?

A. Convert the Trojan.exe file extension to Trojan.txt disguising as text file
B. Break the Trojan into multiple smaller files and zip the individual pieces
C. Change the content of the Trojan using hex editor and modify the checksum
D. Encrypt the Trojan using multiple hashing algorithms like MD5 and SHA-1

Answer: A

QUESTION: 253
What will the following command produce on a website's login page if executed successfully? SELECT email, passwd, login_id, full_name FROM members WHERE email = 'someone@somewhere.com'; DROP TABLE members; --'

A. This code will insert the someone@somewhere.com email address into the members table.
B. This command will delete the entire members table.
C. It retrieves the password for the first user in the members table.

D. This command will not produce anything since the syntax is incorrect.

Answer: B

QUESTION: 254
Oregon Corp is fighting a litigation suit with Scamster Inc. Oregon has assigned a private investigative agency to go through garbage, recycled paper, and other rubbish at Scamster's office site in order to find relevant information. What would you call this kind of activity?

A. CI Gathering
B. Scanning
C. Dumpster Diving
D. Garbage Scooping

Answer: C

QUESTION: 255
What type of port scan is represented here.

A. Stealth Scan
B. Full Scan
C. XMAS Scan
D. FIN Scan

Answer: A

QUESTION: 256
_____ is found in all versions of NTFS and is described as the ability to fork file data into existing files without affecting their functionality, size, or display to traditional file browsing utilities like dir or Windows Explorer

A. Alternate Data Streams
B. Merge Streams
C. Steganography

D. NetBIOS vulnerability

Answer: A

QUESTION: 257
Justin is checking some network traffic logs on his firewall. Justin finds some IP packets from a computer purporting to be on the internal network. The packets originate from 172.16.1.44 with an IPID number of 3422. The received response from 172.16.1.44 has an IPID number of 512. What can he infer from this traffic log?

A. The traffic from 172.16.1.44 is from a Windows 7 computer.
B. The IPID number differences means the client computer is on wireless.
C. Traffic from 172.16.1.44 was being spoofed.
D. The client computer at 172.16.1.44 is a zombie computer.

Answer: C

QUESTION: 258
A company is legally liable for the content of email that is sent from its systems, regardless of whether the message was sent for private or business-related purposes. This could lead to prosecution for the sender and for the company's directors if, for example, outgoing email was found to contain material that was pornographic, racist, or likely to incite someone to commit an act of terrorism. You can always defend yourself by "ignorance of the law" clause.

A. true
B. false

Answer: B

QUESTION: 259
Paul has just finished setting up his wireless network. He has enabled numerous security features such as changing the default SSID, enabling WPA encryption, and enabling MAC filtering on his wireless router. Paul notices that when he uses his wireless connection, the speed is sometimes 54 Mbps and sometimes it is only 24Mbps or less. Paul connects to his wireless router's management utility and notices that a machine with an unfamiliar name is connected through his wireless connection. Paul checks the router's logs and notices that the unfamiliar machine has the same MAC address as his laptop. What is Paul seeing here?

A. MAC spoofing
B. Macof
C. ARP spoofing
D. DNS spoofing

Answer: A

QUESTION: 260
What two things will happen if a router receives an ICMP packet, which has a TTL value of 1, and the destination host is several hops away? (Select 2 answers)

A. The router will discard the packet
B. The router will decrement the TTL value and forward the packet to the next router on the path to the destination host
C. The router will send a time exceeded message to the source host
D. The router will increment the TTL value and forward the packet to the next router on the path to the destination host.
E. The router will send an ICMP Redirect Message to the source host

Answer: A, C

QUESTION: 261
Which of the following LM hashes represents a password of less than 8 characters?

A. 0182BD0BD4444BF836077A718CCDF409
B. 44EFCE164AB921CQAAD3B435B51404EE
C. BA810DBA98995F1817306D272A9441BB
D. CEC52EB9C8E3455DC2265B23734E0DAC
E. B757BF5C0D87772FAAD3B435B51404EE
F. E52CAC67419A9A224A3B108F3FA6CB6D

Answer: C, E

SAMPLE QUESTIONS

These questions are for demo purpose only. ***Full version*** *is up to date and contains actual questions and answers.*

Killexams.com is an online platform that offers a wide range of services related to certification exam preparation. The platform provides actual questions, exam dumps, and practice tests to help individuals prepare for various certification exams with confidence. Here are some key features and services offered by Killexams.com:

Actual Exam Questions*: Killexams.com provides actual exam questions that are experienced in test centers. These questions are updated regularly to ensure they are up-to-date and relevant to the latest exam syllabus. By studying these actual questions, candidates can familiarize themselves with the content and format of the real exam.*

Exam Dumps*: Killexams.com offers exam dumps in PDF format. These dumps contain a comprehensive collection of questions and answers that cover the exam topics. By using these dumps, candidates can enhance their knowledge and improve their chances of success in the certification exam.*

Practice Tests*: Killexams.com provides practice tests through their desktop VCE exam simulator and online test engine. These practice tests simulate the real exam environment and help candidates assess their readiness for the actual exam. The practice tests cover a wide range of questions and enable candidates to identify their strengths and weaknesses.*

Guaranteed Success*: Killexams.com offers a success guarantee with their exam dumps. They claim that by using their materials, candidates will pass their exams on the first attempt or they will refund the purchase price. This guarantee provides assurance and confidence to individuals preparing for certification exams.*

Updated Content: *Killexams.com regularly updates its question bank and exam dumps to ensure that they are current and reflect the latest changes in the exam syllabus. This helps candidates stay up-to-date with the exam content and increases their chances of success.*

Technical Support*: Killexams.com provides free 24x7 technical support to assist candidates with any queries or issues they may encounter while using their services. Their certified experts are available to provide guidance and help candidates throughout their exam preparation journey.*