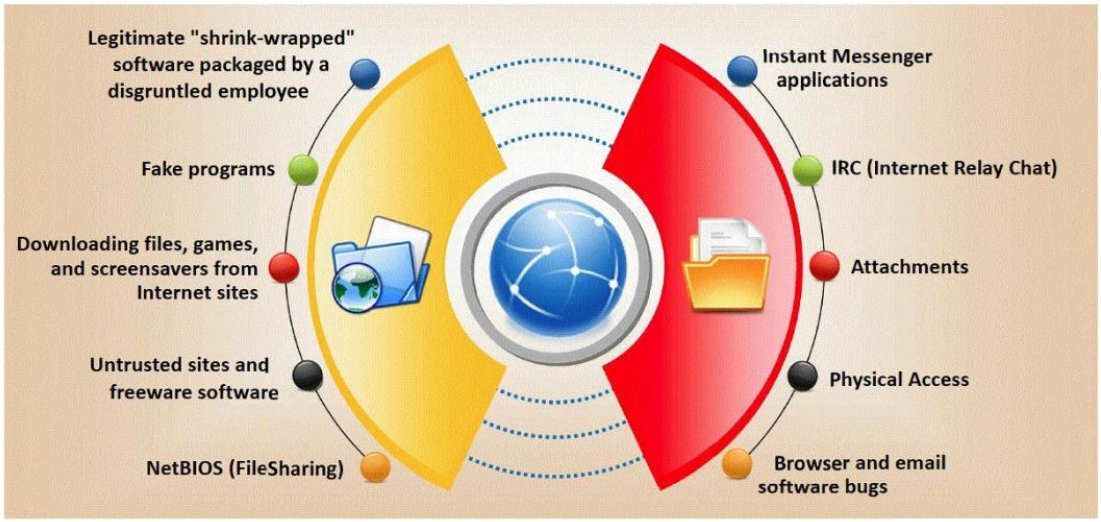
D. 31401

Correct Answer: B

QUESTION 245

Trojan horse attacks pose one of the most serious threats to computer security. The image below shows different ways a Trojan can get into a system. Which are the easiest and most convincing ways to infect a computer?



A. IRC (Internet Relay Chat).
B. Legitimate "shrink-wrapped" software packaged by a disgruntled employee.
C. NetBIOS (File Sharing).
D. Downloading files, games and screensavers from Internet sites.

Correct Answer: B

QUESTION 246

SSL has been seen as the solution to a lot of common security problems. Administrator will often time make use of SSL to encrypt communications from points A to point B. Why do you think this could be a bad idea if there is an Intrusion Detection System deployed to monitor the traffic between point A and B?

A. SSL is redundant if you already have IDS's in place.
B. SSL will trigger rules at regular interval and force the administrator to turn them off.
C. SSL will slow down the IDS while it is breaking the encryption to see the packet content.
D. SSL will blind the content of the packet and Intrusion Detection Systems will not be able to detect them.

Correct Answer: D

QUESTION 247

Jake is a network administrator who needs to get reports from all the computer and network devices on his network. Jake wants to use SNMP but is afraid that won't be secure since passwords and messages are in clear text. How can Jake gather network information in a secure manner?

A. He can use SNMPv3
B. Jake can use SNMPrev5
C. He can use SecWMI
D. Jake can use SecSNMP

Correct Answer: A

QUESTION 248

June, a security analyst, understands that a polymorphic virus has the ability to mutate and can change its known viral signature and hide from signature-based antivirus programs. Can June use an antivirus program in this case and would it be effective against a polymorphic virus?

A. Yes. June can use an antivirus program since it compares the parity bit of executable files to the database of known check sum counts and it is effective on a polymorphic virus.
B. Yes. June can use an antivirus program since it compares the signatures of executable files to the database of known viral signatures and it is very effective against a polymorphic virus.
C. No. June can't use an antivirus program since it compares the signatures of executable files to the database of known viral signatures and in the case the polymorphic viruses cannot be detected by a signature-based anti-virus program.
D. No. June can't use an antivirus program since it compares the size of executable files to the database of known viral signatures and it is effective on a polymorphic virus.

Correct Answer: C

QUESTION 249

Which of the following Exclusive OR transforms bits is NOT correct?

A. 0 xor 0 = 0
B. 1 xor 0 = 1
C. 1 xor 1 = 1
D. 0 xor 1 = 1

Correct Answer: C

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
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 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.

Correct 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.

Correct 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.

Correct 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

Correct Answer: C

QUESTION 255
What type of port scan is represented here?

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

Correct Answer: A

QUESTION 256
One way to defeat a multi-level security solution is to leak data via

A. a bypass regulator
B. steganography
C. a covert channel
D. asymmetric routing