Q & A

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

KILL EXAMS

PASS ✓

killexams.com

EC-Council

EC0-349

Computer Hacking Forensic Investigator

ORDER FULL VERSION

B. Trinoo
C. Fraggle
D. SYN flood

Answer: A

QUESTION: 358
Kyle is performing the final testing of an application he developed for the accounting department. His last round of testing is to ensure that the program is as secure as possible. Kyle runs the following command. What is he testing at this point?
#include
#include int main(int argc, char *argv[]) {
char buffer[10];
if (argc < 2) {
fprintf (stderr, "USAGE: %s string\n",
argv[0]);
return 1;
}
strcpy(buffer, argv[1]);
return 0;
}

A. Buffer overflow
B. SQL injection
C. Format string bug
D. Kernal injection

Answer: A

QUESTION: 359
You are running known exploits against your network to test for possible vulnerabilities. To test the strength of your virus software, you load a test network to mimic your production network. Your software successfully blocks some simple macro and encrypted viruses. You decide to really test the software by using virus code where the code rewrites itself entirely and the signatures change from child to child, but the functionality stays the same. What type of virus is this that you are testing?

A. Polymorphic
B. Metamorphic
C. Oligomorhic

D. Transmorphic

Answer: B

QUESTION: 360
What is a good security method to prevent unauthorized users from "tailgating"?

A. Man trap
B. Electronic combination locks
C. Pick-resistant locks
D. Electronic key systems

Answer: A

QUESTION: 361
You are the security analyst working for a private company out of France. Your current assignment is to obtain credit card information from a Swiss bank owned by that company. After initial reconnaissance, you discover that the bank security defenses are very strong and would take too long to penetrate. You decide to get the information by monitoring the traffic between the bank and one of its subsidiaries in London. After monitoring some of the traffic, you see a lot of FTP packets traveling back and forth. You want to sniff the traffic and extract usernames and passwords. What tool could you use to get this information?

A. Airsnort
B. Snort
C. Ettercap
D. RaidSniff

Answer: C

QUESTION: 362
As a security analyst you setup a false survey website that will reQuire users to create a username and a strong password. You send the link to all the employees of the company. What information will you be able to gather?

A. The IP address of the employees computers
B. Bank account numbers and the corresponding routing numbers

C. The employees network usernames and passwords
D. The MAC address of theemployees?computers

Answer: C

QUESTION: 363
Julia is a senior security analyst for Berber Consulting group. She is currently working on a contract for a small accounting firm in Florida. They have given her permission to perform social engineering attacks on the company to see if their in-house training did any good. Julia calls the main number for the accounting firm and talks to the receptionist. Julia says that she is an IT technician from the company's main office in Iowa. She states that she needs the receptionist's network username and password to troubleshoot a problem they are having. Julia says that Bill Hammond, the CEO of the company, reQuested this information. After hearing the name of the CEO, the receptionist gave Julia all the information she asked for. What principal of social engineering did Julia use?

A. Social Validation
B. Scarcity
C. Friendship/Liking
D. Reciprocation

Answer: D

QUESTION: 364
Harold wants to set up a firewall on his network but is not sure which one would be the most appropriate. He knows he needs to allow FTP traffic to one of the servers on his network, but he wants to only allow FTP-PUT. Which firewall would be most appropriate for Harold? needs?

A. Circuit-level proxy firewall
B. Packet filtering firewall
C. Application-level proxy firewall
D. Data link layer firewall

Answer: C

QUESTION: 365
What will the following command accomplish?

A. Test ability of a router to handle over-sized packets
B. Test the ability of a router to handle under-sized packets
C. Test the ability of a WLAN to handle fragmented packets
D. Test the ability of a router to handle fragmented packets

Answer: A

QUESTION: 366
What does ICMP Type 3/Code 13 mean?

A. Host Unreachable
B. Administratively Blocked
C. Port Unreachable
D. Protocol Unreachable

Answer: B

QUESTION: 367
How many bits is Source Port Number in TCP Header packet?

A. 16
B. 32
C. 48
D. 64

Answer: A

QUESTION: 368
After passively scanning the network of Department of Defense (DoD), you switch over to active scanning to identify live hosts on their network. DoD is a lage organization and should respond to any number of scans. You start an ICMP ping sweep by sending an IP packet to the broadcast address. Only five hosts responds to your ICMP pings; definitely not the number of hosts you were expecting. Why did this ping sweep only produce a few responses?

A. Only IBM AS/400 will reply to this scan

B. Only Windows systems will reply to this scan

C. A switched network will not respond to packets sent to the broadcast address

D. Only Unix and Unix-like systems will reply to this scan

Answer: D

QUESTION: 369

Your company's network just finished going through a SAS 70 audit. This audit reported that overall, your network is secure, but there are some areas that needs improvement. The major area was SNMP security. The audit company recommended turning off SNMP, but that is not an option since you have so many remote nodes to keep track of. What step could you take to help secure SNMP on your network?

A. Block all internal MAC address from using SNMP

B. Block access to UDP port 171

C. Block access to TCP port 171

D. Change the default community string names

Answer: D

QUESTION: 370

After attending a CEH security seminar, you make a list of changes you would like to perform on your network to increase its security. One of the first things you change is to switch the RestrictAnonymous setting from 0 to 1 on your servers. This, as you were told, would prevent anonymous users from establishing a null session on the server. Using Userinfo tool mentioned at the seminar, you succeed in establishing a null session with one of the servers. Why is that?

A. RestrictAnonymous must be set to "10" for complete security

B. RestrictAnonymous must be set to "3" for complete security

C. RestrictAnonymous must be set to "2" for complete security

D. There is no way to always prevent an anonymous null session from establishing

Answer: C

QUESTION: 371

In a virtual test environment, Michael is testing the strength and security of BGP using multiple routers to mimic the backbone of the Internet. This project will help him write his doctoral thesis on "bringing down the Internet". Without sniffing the traffic

between the routers, Michael sends millions of RESET packets to the routers in an attempt to shut one or all of them down. After a few hours, one of the routers finally shuts itself down. What will the other routers communicate between themselves?

A. The change in the routing fabric to bypass the affected router
B. More RESET packets to the affected router to get it to power back up
C. RESTART packets to the affected router to get it to power back up
D. STOP packets to all other routers warning of where the attack originated

Answer: A

QUESTION: 372
How many possible sequence number combinations are there in TCP/IP protocol?

A. 1 billion
B. 320 billion
C. 4 billion
D. 32 million

Answer: C

QUESTION: 373
Tyler is setting up a wireless network for his business that he runs out of his home. He has followed all the directions from the ISP as well as the wireless router manual. He does not have any encryption set and the SSID is being broadcast. On his laptop, he can pick up the wireless signal for short periods of time, but then the connection drops and the signal goes away. Eventually the wireless signal shows back up, but drops intermittently. What could be Tyler issue with his home wireless network?

A. Computers on his wired network
B. Satellite television
C. 2.4Ghz Cordless phones
D. CB radio

Answer: C

QUESTION: 374

You are working on a thesis for your doctorate degree in Computer Science. Your thesis is based on HTML, DHTML, and other web-based languages and how they have evolved over the years. You navigate to archive. org and view the HTML code of news.com. You then navigate to the current news.com website and copy over the source code. While searching through the code, you come across something abnormal: What have you found?

A. Web bug
B. CGI code
C. Trojan.downloader
D. Blind bug

Answer: A

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:

ORDER FULL VERSION
Special Discount Coupon

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.