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.pass2lead.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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

You want to use netcat to generate huge amount of useless network data continuously for various performance testing between 2 hosts. Which of the following commands accomplish this?

A. Machine A#yes AAAAAAAAAAAAAAAAAAAAA | nc v v l p 2222 > /dev/nullMachine B#yes BBBBBBBBBBBBBBBBBBBBB | nc machinea 2222 > /dev/null

B. Machine Acat somefile | nc v v l p 2222Machine Bcat somefile | nc othermachine 2222

C. Machine Anc l p 1234 | uncompress c | tar xvfpMachine Btar cfp - /some/dir | compress c | nc w 3 machinea 1234

D. Machine Awhile true : donc v l s p 6000 machineb 2Machine Bwhile true ; donc v l s p 6000 machinea 2done

Correct Answer: A

Machine A is setting up a listener on port 2222 using the nc command and then having the letter A sent an infinite amount of times, when yes is used to send data yes NEVER stops until it recieves a break signal from the terminal (Control+C), on the client end (machine B), nc is being used as a client to connect to machine A, sending the letter B and infinite amount of times, while both clients have established a TCP connection each client is infinitely sending data to each other, this process will run FOREVER until it has been stopped by an administrator or the attacker.

QUESTION 2

Jim was having no luck performing a penetration test on his company\\'s network. He was running the test from home and had downloaded every security scanner he could lay his hands on. Despite knowing the IP range of all of the systems and the exact network configuration, Jim was unable to get any useful results. Why is Jim having these problems?

A. Security scanners can\\'t perform vulnerability linkage

B. Security Scanners are not designed to do testing through a firewall

C. Security Scanners are only as smart as their database and can\\'t find unpublished vulnerabilities

D. All of the above

Correct Answer: D

Security scanners are designed to find vulnerabilities but not to use them, also they will only find well known vulnerabilities that and no zero day exploits. Therefore you can\\'t use a security scanner for penetration testing but need a more powerful program.

QUESTION 3

Perimeter testing means determining exactly what your firewall blocks and what it allows. To conduct a good test, you can spoof source IP addresses and source ports. Which of the following command results in packets that will appear to originate from the system at 10.8.8.8? Such a packet is useful for determining whether the firewall is allowing random packets in or out of your network.

A. hping3 -T 10.8.8.8 -S netbios -c 2 -p 80

B. hping3 -Y 10.8.8.8 -S windows -c 2 -p 80

C. hping3 -O 10.8.8.8 -S server -c 2 -p 80

D. hping3 -a 10.8.8.8 -S springfield -c 2 -p 80

Correct Answer: D

QUESTION 4

You are the IT Manager of a large legal firm in California. Your firm represents many important clients whose names always must remain anonymous to the public. Your boss, Mr. Smith is always concerned about client information being leaked or revealed to the pres or public. You have just finished a complete security overhaul of your information system including an updated IPS, new firewall, email encryption and employee security awareness training. Unfortunately, many of your firm\\'s clients do not trust technology to completely secure their information, so couriers routinely have to travel back and forth to and from the office with sensitive information.

Your boss has charged you with figuring out how to secure the information the couriers must transport. You propose that the data be transferred using burned CD\\'s or USB flash drives. You initially think of encrypting the files, but decide against that method for fear the encryption keys could eventually be broken.

What software application could you use to hide the data on the CD\\'s and USB flash drives?

A. Snow

B. File Snuff

C. File Sneaker

D. EFS

Correct Answer: A

The Snow software developed by Matthew Kwan will insert extra spaces at the end of each line. Three bits are encoded in each line by adding between 0 and 7 spaces that are ignored by most display programs including web browsers.

QUESTION 5

Fred is the network administrator for his company. Fred is testing an internal switch. From an external IP address, Fred wants to try and trick this switch into thinking it already has established a session with his computer. How can Fred accomplish this?

A. Fred can accomplish this by sending an IP packet with the RST/SIN bit and the source address of his computer.

B. He can send an IP packet with the SYN bit and the source address of his computer.

C. Fred can send an IP packet with the ACK bit set to zero and the source address of the switch.

D. Fred can send an IP packet to the switch with the ACK bit and the source address of his machine.

Correct Answer: D

312-50 PDF Dumps 312-50 Practice Test 312-50 Study Guide