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.passapply.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

QUESTION 1

What does the this symbol mean?

A. Open Access Point

B. WPA Encrypted Access Point

C. WEP Encrypted Access Point

D. Closed Access Point

Correct Answer: A

This symbol is a "warchalking" symbol for a open node (open circle) with the SSID tsunami and the bandwidth 2.0 Mb/s

QUESTION 2

What is the default Password Hash Algorithm used by NTLMv2?

A. MD4

B. DES

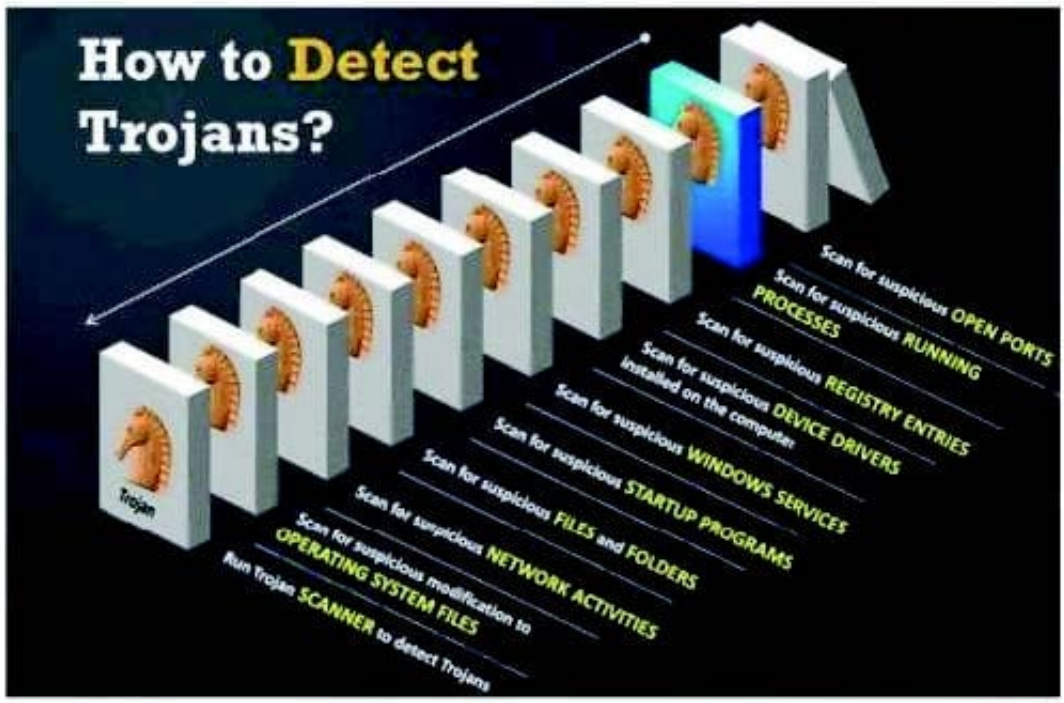
C. SHA-1

D. MD5

Correct Answer: D

QUESTION 3

Your computer is infected by E-mail tracking and spying Trojan. This Trojan infects the computer with a single file - emos.sys Which step would you perform to detect this type of Trojan?



A. Scan for suspicious startup programs using msconfig

B. Scan for suspicious network activities using Wireshark

C. Scan for suspicious device drivers in c:\windows\system32\drivers

D. Scan for suspicious open ports using netstat

Correct Answer: C

QUESTION 4

What is the tool Firewalk used for?

A. To test the IDS for proper operation

B. To test a firewall for proper operation

C. To determine what rules are in place for a firewall

D. To test the webserver configuration

E. Firewalk is a firewall auto configuration tool

Correct Answer: C

Firewalk is an active reconnaissance network security tool that attempts to determine what layer 4 protocols a given IP forwarding device "firewall" will pass. Firewalk works by sending out TCP or UDP packets with a TTL one greater than the targeted gateway. If the gateway allows the traffic, it will forward the packets to the next hop where they will expire and elicit an ICMP_TIME_EXCEEDED message. If the gateway host does not allow the traffic, it will likely drop the

packets and no response will be returned.

QUESTION 5

Maurine is working as a security consultant for Hinklemeir Associate. She has asked the Systems Administrator to create a group policy that would not allow null sessions on the network. The Systems Administrator is fresh out of college and has never heard of null sessions and does not know what they are used for. Maurine is trying to explain to the Systems Administrator that hackers will try to create a null session when footprinting the network.

Why would an attacker try to create a null session with a computer on a network?

A. Enumerate users shares

B. Install a backdoor for later attacks

C. Escalate his/her privileges on the target server

D. To create a user with administrative privileges for later use

Correct Answer: A

The Null Session is often referred to as the "Holy Grail" of Windows hacking. Listed as the number 5 windows vulnerability on the SANS/FBI Top 20 list, Null Sessions take advantage of flaws in the CIFS/SMB (Common Internet File System/ Server Messaging Block) architecture. You can establish a Null Session with a Windows (NT/2000/XP) host by logging on with a null user name and password. Using these null connections allows you to gather the following information from the host:

-

List of users and groups

-

List of machines

-

List of shares

-Users and host SID\\' (Security Identifiers)

QUESTION 6

Eve is spending her day scanning the library computers. She notices that Alice is using a computer whose port 445 is active and listening. Eve uses the ENUM tool to enumerate Alice machine. From the command prompt, she types the following command.

For /f "tokens=1 %%a in (hackfile.txt) do net use * \\10.1.2.3\c$ /user:"Administrator" %%a What is Eve trying to do?

A. Eve is trying to connect as an user with Administrator privileges

B. Eve is trying to enumerate all users with Administrative privileges

C. Eve is trying to carry out a password crack for user Administrator

D. Eve is trying to escalate privilege of the null user to that of Administrator

Correct Answer: C

Eve tries to get a successful login using the username Administrator and passwords from the file hackfile.txt.

QUESTION 7

Which of the following is most effective against passwords ? Select the Answer:

A. Dictionary Attack

B. BruteForce attack

C. Targeted Attack

D. Manual password Attack

Correct Answer: B

The most effective means of password attack is brute force, in a brute force attack the program will attempt to use every possible combination of characters. While this takes longer then a dictionary attack, which uses a text file of real words, it is always capable of breaking the password.

QUESTION 8

What is the IV key size used in WPA2?

A. 32

B. 24

C. 16

D. 48

E. 128

Correct Answer: D

QUESTION 9

Exhibit:

ettercap NCLzs --quiet

What does the command in the exhibit do in "Ettercap"?

A. This command will provide you the entire list of hosts in the LAN

B. This command will check if someone is poisoning you and will report its IP.

C. This command will detach from console and log all the collected passwords from the network to a file.

D. This command broadcasts ping to scan the LAN instead of ARP request of all the subnet IPs.

Correct Answer: C

-N = NON interactive mode (without ncurses)

-C = collect all users and passwords

-L = if used with -C (collector) it creates a file with all the password sniffed in the session in the form "YYYYMMDD-collected-pass.log" -z = start in silent mode (no arp storm on start up)

-s = IP BASED sniffing

--quiet = "demonize" ettercap. Useful if you want to log all data in background.

QUESTION 10

This is an example of whois record.

Registrant
Jason Springfield, Inc
11807 N.E. 99th Street, Suite 1100
New York, NY 98682
USA

Registrar: Jason Springfield (http://www. jspringfield.com)
Domain Name: jspringfield.com
Created on: 29-DEC-10
Expires on: 29-DEC-14
Last Updated on: 23-FEB-11

Administrative Contact:
Contact, Admin Jack_Smith@jspringfield.com
Jason Springfield, Inc
11807 N.E. 99th Street, Suite 1100
New York, NY 98682
USA
360.253.6744
360.253.3556

Technical Contact:
Contact, Technical Sheela_Ravin@jspringfield.com
Jason Springfield, Inc
11807 N.E. 99th Street, Suite 1100
New York, NY 98682
USA
360.253.3456
360.253.2675

Billing Contact:
Contact, Technical David_Bruce@jspringfield.com
Jason Springfield, Inc
11807 N.E. 99th Street, Suite 1100
New York, NY 98682
USA
360.253.5654
360.253.1256

Domain servers (DNS) in listed order:
NS1.jspringfield.com
NS2.jspringfield.com

Sometimes a company shares a little too much information on their organization through public domain records. Based on the above whois record, what can an attacker do? (Select 2 answers)

A. Search engines like Google, Bing will expose information listed on the WHOIS record

B. An attacker can attempt phishing and social engineering on targeted individuals using the information from WHOIS record

C. Spammers can send unsolicited e-mails to addresses listed in the WHOIS record

D. IRS Agents will use this information to track individuals using the WHOIS record information

Correct Answer: BC

QUESTION 11

StackGuard (as used by Immunix), ssp/ProPolice (as used by OpenBSD), and Microsoft\\'s /GS option use _____ defense against buffer overflow attacks.

A. Canary

B. Hex editing

C. Format checking

D. Non-executing stack

Correct Answer: A

Canaries or canary words are known values that are placed between a buffer and control data on the stack to monitor buffer overflows. When the buffer overflows, it will clobber the canary, making the overflow evident. This is a reference to the historic practice of using canaries in coal mines, since they would be affected by toxic gases earlier than the miners, thus providing a biological warning system.

QUESTION 12

Which Type of scan sends a packets with no flags set ? Select the Answer

A. Open Scan

B. Null Scan

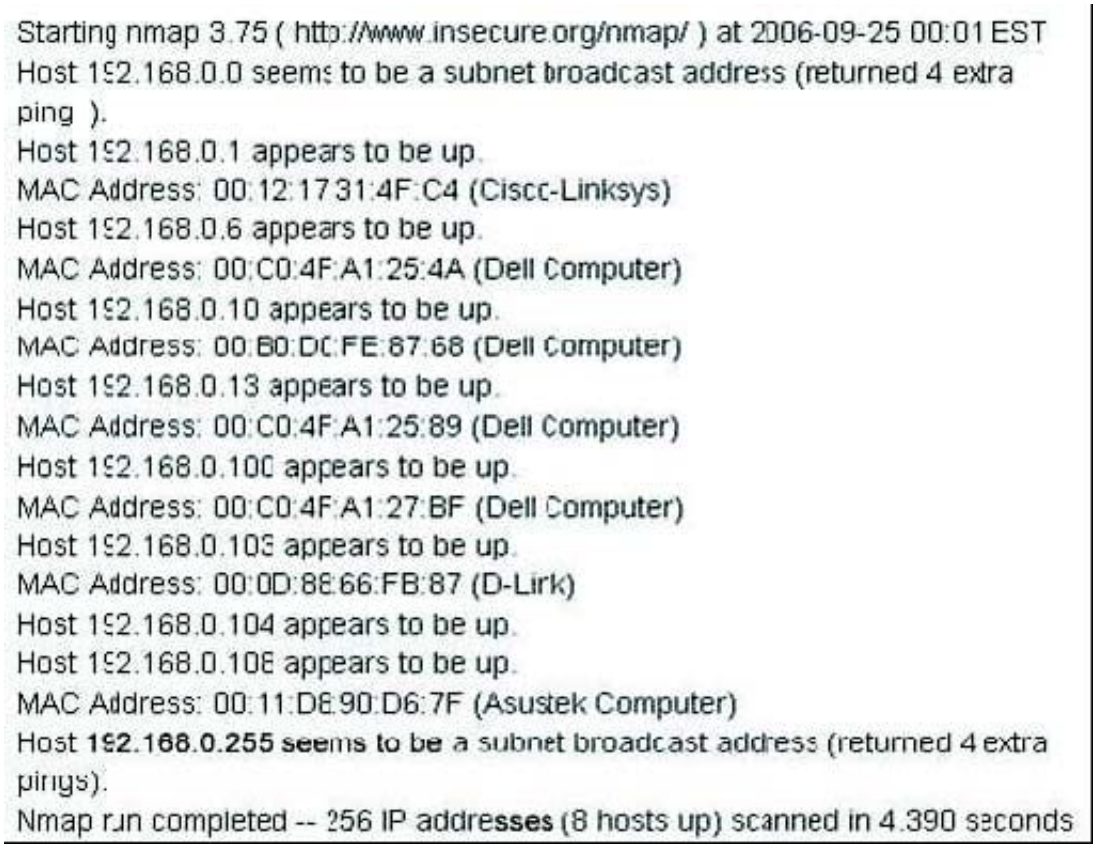
C. Xmas Scan

D. Half-Open Scan

Correct Answer: B

The types of port connections supported are:

QUESTION 13



Which of the following nmap command in Linux procedures the above output?

A. sudo nmap sP 192.168.0.1/24

B. root nmap sA 192.168.0.1/24

C. run nmap TX 192.168.0.1/24

D. launch nmap PP 192.168.0.1/24

Correct Answer: A

This is an output from a ping scan. The option sP will give you a ping scan of the 192.168.0.1/24 network.

QUESTION 14

While footprinting a network, what port/service should you look for to attempt a zone transfer?

A. 53 UDP

B. 53 TCP

C. 25 UDP

D. 25 TCP

E. 161 UDP

F. 22 TCP

G. 60 TCP

Correct Answer: B

IF TCP port 53 is detected, the opportunity to attempt a zone transfer is there.

QUESTION 15

What happens during a SYN flood attack?

A. TCP connection requests floods a target machine is flooded with randomized source address and ports for the TCP ports.

B. A TCP SYN packet, which is a connection initiation, is sent to a target machine, giving the target host\\'s address as both source and destination, and is using the same port on the target host as both source and destination.

C. A TCP packet is received with the FIN bit set but with no ACK bit set in the flags field.

D. A TCP packet is received with both the SYN and the FIN bits set in the flags field.

Correct Answer: A

To a server that requires an exchange of a sequence of messages. The client system begins by sending a SYN message to the server. The server then acknowledges the SYN message by sending a SYN-ACK message to the client. The client then finishes establishing the connection by responding with an ACK message and then data can be exchanged. At the point where the server system has sent an acknowledgment (SYN-ACK) back to client but has not yet received the ACK message, there is a half- open connection. A data structure describing all pending connections is in memory of the server that can be made to overflow by intentionally creating too many partially open connections. Another common attack is the SYN flood, in which a target machine is flooded with TCP connection requests. The source addresses and source TCP ports of the connection request packets are randomized; the purpose is to force the target host to maintain state information for many connections that will never be completed. SYN flood attacks are usually noticed because the target host (frequently an HTTP or SMTP server) becomes extremely slow, crashes, or hangs. It\\'s also possible for the traffic returned from the target host to cause trouble on routers; because this return traffic goes to the randomized source addresses of the original packets, it lacks the locality properties of "real" IP traffic, and may overflow route caches. On Cisco routers, this problem often manifests itself in the router running out of memory.