SEC504 Q&As

Hacker Tools, Techniques, Exploits and Incident Handling

Pass SANS SEC504 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/sec504.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by SANS Official Exam Center

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

QUESTION 1

When you conduct the XMAS scanning using Nmap, you find that most of the ports scanned do not give a response.

What can be the state of these ports?

A. Filtered

B. Open

C. Closed

Correct Answer: B

QUESTION 2

Which of the following nmap command parameters is used for TCP SYN port scanning?

A. -sF

B. -sU

C. -sX

D. -sS

Correct Answer: D

QUESTION 3

You want to connect to your friend\\'s computer and run a Trojan on it. Which of the following tools will you use to accomplish the task?

A. PSExec

B. Remoxec

C. Hk.exe

D. GetAdmin.exe

Correct Answer: A

QUESTION 4

Many organizations create network maps of their network system to visualize the network and understand the relationship between the end devices and the transport layer that provide services.

Which of the following are the techniques used for network mapping by large organizations? Each correct answer

represents a complete solution. Choose three.

A. Packet crafting

B. Route analytics

C. SNMP-based approaches

D. Active Probing

Correct Answer: BCD

QUESTION 5

Which of the following statements are true about firewalking? Each correct answer represents a complete solution. Choose all that apply.

A. To use firewalking, the attacker needs the IP address of the last known gateway before the firewall and the IP address of a host located behind the firewall.

B. In this technique, an attacker sends a crafted packet with a TTL value that is set to expire one hop past the firewall.

C. A malicious attacker can use firewalking to determine the types of ports/protocols that can bypass the firewall.

D. Firewalking works on the UDP packets.

Correct Answer: ABC

QUESTION 6

Which of the following attacks saturates network resources and disrupts services to a specific computer?

A. Replay attack

B. Teardrop attack

C. Denial-of-Service (DoS) attack

D. Polymorphic shell code attack

Correct Answer: C

QUESTION 7

Address Resolution Protocol (ARP) spoofing, also known as ARP poisoning or ARP Poison Routing (APR), is a technique used to attack an Ethernet wired or wireless network. ARP spoofing may allow an attacker to sniff data frames on a local area network (LAN), modify the traffic, or stop the traffic altogether. The principle of ARP spoofing is to send fake ARP messages to an Ethernet LAN.

What steps can be used as a countermeasure of ARP spoofing? Each correct answer represents a complete solution. Choose all that apply.

A. Using smash guard utility

B. Using ARP Guard utility

C. Using static ARP entries on servers, workstation and routers

D. Using ARP watch utility

E. Using IDS Sensors to check continually for large amount of ARP traffic on local subnets

Correct Answer: BCDE

QUESTION 8

You run the following command while using Nikto Web scanner:

perl nikto.pl -h 192.168.0.1 -p 443

What action do you want to perform?

A. Using it as a proxy server

B. Updating Nikto

C. Seting Nikto for network sniffing

D. Port scanning

Correct Answer: D

QUESTION 9

You enter the netstat -an command in the command prompt and you receive intimation that port number 7777 is open on your computer.

Which of the following Trojans may be installed on your computer?

A. NetBus

B. QAZ

C. Donald Dick

D. Tini

Correct Answer: D

QUESTION 10

John works as a Network Administrator for Net Perfect Inc. The company has a Windows- based network. The company uses Check Point SmartDefense to provide security to the network of the company. On the

HTTP servers of the company, John defines a rule for dropping any kind of userdefined URLs. Which of the following types of attacks can be prevented by dropping the user-defined URLs?

A. Morris worm

B. Code red worm

C. Hybrid attacks

D. PTC worms and mutations

Correct Answer: D

QUESTION 11

Your friend plans to install a Trojan on your computer. He knows that if he gives you a new version of chess.exe, you will definitely install the game on your computer. He picks up a Trojan and joins it to chess.exe. The size of chess.exe was 526,895 bytes originally, and after joining this chess file to the Trojan, the file size increased to 651,823 bytes. When he gives you this new game, you install the infected chess.exe file on your computer. He now performs various malicious tasks on your computer remotely. But you suspect that someone has installed a Trojan on your computer and begin to investigate it. When you enter the netstat command in the command prompt, you get the following results:

C:\WINDOWS>netstat -an | find "UDP" UDP IP_Address:31337 *:*

Now you check the following registry address:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServic es

In the above address, you notice a \\'default\\' key in the \\'Name\\' field having " .exe" value in the corresponding \\'Data\\' field.

Which of the following Trojans do you think your friend may have installed on your computer on the basis of the above evidence?

A. Qaz

B. Donald Dick

C. Tini

D. Back Orifice

Correct Answer: D

QUESTION 12

Which of the following functions in c/c++ can be the cause of buffer overflow? Each correct answer represents a complete solution. Choose two.

A. printf()

B. strcat()

C. strcpy()

D. strlength()

Correct Answer: BC

QUESTION 13

Maria works as a professional Ethical Hacker. She has been assigned the project of testing the security of www.gentech.com. She is using dumpster diving to gather information about Gentech Inc.

In which of the following steps of malicious hacking does dumpster diving come under?

A. Multi-factor authentication

B. Role-based access control

C. Mutual authentication

D. Reconnaissance

Correct Answer: D

QUESTION 14

Adam, a malicious hacker has successfully gained unauthorized access to the Linux system of Umbrella Inc. Web server of the company runs on Apache. He has downloaded sensitive documents and database files from the computer.

After performing these malicious tasks, Adam finally runs the following command on the Linux command box before disconnecting.

for ((i = 0;i