SANS

Exam SEC504

Hacker Tools, Techniques, Exploits and Incident Handling

Version: 7.1

[Total Questions: 328]

Topic break down

Topic	No. of Questions
Topic 1: Volume A	98
Topic 2: Volume B	96
Topic 3: Volume C	134

Topic 1, Volume A

Question No : 1 - (Topic 1)

Which of the following commands can be used for port scanning?

A. nc -t
B. nc -z
C. nc -w
D. nc -g

Answer: B

Question No : 2 - (Topic 1)

You work as a Network Administrator for Tech Perfect Inc. The company has a TCP/IP-based network. An attacker uses software that keeps trying password combinations until the correct password is found. Which type of attack is this?

A. Denial-of-Service
B. Man-in-the-middle
C. Brute Force
D. Vulnerability

Answer: C

Question No : 3 - (Topic 1)

You work as a Penetration Tester for the Infosec Inc. Your company takes the projects of security auditing. Recently, your company has assigned you a project to test the security of the we-aresecure.com Web site. For this, you want to perform the idle scan so that you can get the ports open in the we-are-secure.com server. You are using Hping tool to perform the idle scan by using a zombie computer. While scanning, you notice that every IPID is being incremented on every query, regardless whether the ports are open or close. Sometimes, IPID is being incremented by more than one value.

What may be the reason?

A. The firewall is blocking the scanning process.
B. The zombie computer is not connected to the we-are-secure.com Web server.
C. The zombie computer is the system interacting with some other system besides your computer.
D. Hping does not perform idle scanning.

Answer: C

Question No : 4 - (Topic 1)

Adam works as an Incident Handler for Umbrella Inc. His recent actions towards the incident are not up to the standard norms of the company. He always forgets some steps and procedures while handling responses as they are very hectic to perform.

Which of the following steps should Adam take to overcome this problem with the least administrative effort?

A. Create incident manual read it every time incident occurs.
B. Appoint someone else to check the procedures.
C. Create incident checklists.
D. Create new sub-team to keep check.

Answer: C

Question No : 5 - (Topic 1)

Which of the following types of attacks is only intended to make a computer resource unavailable to its users?

A. Denial of Service attack
B. Replay attack
C. Teardrop attack
D. Land attack

Answer: A

Question No : 6 - (Topic 1)

Which of the following methods can be used to detect session hijacking attack?

A. nmap
B. Brutus
C. ntop
D. sniffer

Answer: D

Question No : 7 - (Topic 1)

Which of the following tools is an automated tool that is used to implement SQL injections and to retrieve data from Web server databases?

A. Fragroute
B. Absinthe
C. Stick
D. ADMutate

Answer: B

Question No : 8 - (Topic 1)

Your company has been hired to provide consultancy, development, and integration services for a company named Brainbridge International. You have prepared a case study to plan the upgrade for the company. Based on the case study, which of the following steps will you suggest for configuring WebStore1?

Each correct answer represents a part of the solution. Choose two.

A. Customize IIS 6.0 to display a legal warning page on the generation of the 404.2 and 404.3 errors.
B. Move the WebStore1 server to the internal network.
C. Configure IIS 6.0 on WebStore1 to scan the URL for known buffer overflow attacks.
D. Move the computer account of WebStore1 to the Remote organizational unit (OU).

Answer: A,C

Question No : 9 - (Topic 1)

What is the major difference between a *worm* and a *Trojan horse*?

A. A worm spreads via e-mail, while a Trojan horse does not.
B. A worm is a form of malicious program, while a Trojan horse is a utility.
C. A worm is self replicating, while a Trojan horse is not.
D. A Trojan horse is a malicious program, while a worm is an anti-virus software.

Answer: C

Question No : 10 - (Topic 1)

Which of the following functions can be used as a countermeasure to a Shell Injection attack?

Each correct answer represents a complete solution. Choose all that apply.

A. escapeshellarg()
B. mysql_real_escape_string()
C. regenerateid()
D. escapeshellcmd()

Answer: A,D

Question No : 11 - (Topic 1)

Which of the following Denial-of-Service (DoS) attacks employ IP fragmentation mechanism?

Each correct answer represents a complete solution. Choose two.

A. Land attack
B. SYN flood attack
C. Teardrop attack
D. Ping of Death attack

Answer: C,D

Question No : 12 - (Topic 1)

Which of the following are types of access control attacks?

Each correct answer represents a complete solution. Choose all that apply.

A. Spoofing
B. Brute force attack
C. Dictionary attack
D. Mail bombing

Answer: A,B,C

Question No : 13 - (Topic 1)

Adam works as a Security administrator for Umbrella Inc. He runs the following traceroute and notices that hops 19 and 20 both show the same IP address.

1 172.16.1.254 (172.16.1.254) 0.724 ms 3.285 ms 0.613 ms 2 ip68-98-176-1.nv.nv.cox.net

(68.98.176.1) 12.169 ms 14.958 ms 13.416 ms 3 ip68-98-176-1.nv.nv.cox.net

(68.98.176.1) 13.948 ms ip68-100-0-1.nv.nv. cox.net (68.100.0.1) 16.743 ms 16.207 ms 4 ip68-100-0-137.nv.nv.cox.net (68.100.0.137) 17.324 ms 13.933 ms 20.938 ms 5 68.1.1.4

(68.1.1.4) 12.439 ms 220.166 ms 204.170 ms

6 so-6-0-0.gar2.wdc1.Level3.net (67.29.170.1) 16.177 ms 25.943 ms 14.104 ms 7

unknown.Level3.net (209.247.9.173) 14.227 ms 17.553 ms 15.415 ms "PassGuide" - 8 so-0-1-0.bbr1.NewYork1.level3.net (64.159.1.41) 17.063 ms 20.960 ms 19.512 ms 9 so-7-0-0.gar1. NewYork1.Level3.net (64.159.1.182) 20.334 ms 19.440 ms 17.938 ms 10 so-4-0-0.edge1.NewYork1.Level3.

net (209.244.17.74) 27.526 ms 18.317 ms 21.202 ms 11 uunet-level3-oc48.NewYork1.Level3.net

(209.244.160.12) 21.411 ms 19.133 ms 18.830 ms 12 0.so-6-0-0.XL1.NYC4.ALTER.NET

(152.63.21.78)

21.203 ms 22.670 ms 20.111 ms 13 0.so-2-0-0.TL1.NYC8.ALTER.NET (152.63.0.153) 30.929 ms 24.858 ms

23.108 ms 14 0.so-4-1-0.TL1.ATL5.ALTER.NET (152.63.10.129) 37.894 ms 33.244 ms

33.910 ms 15 0.so-7-0-0.XL1.MIA4.ALTER.NET (152.63.86.189) 51.165 ms 49.935 ms

49.466 ms 16 0.so-3-0-0.XR1.MIA4.ALTER.

NET (152.63.101.41) 50.937 ms 49.005 ms 51.055 ms 17 117.ATM6-0.GW5.MIA1.ALTER.NET (152.63.82.73) 51.897 ms 50.280 ms 53.647 ms 18 PassGuidegw1. customer.alter.net (65.195.239.14) 51.921 ms 51.571 ms 56.855 ms 19 www.PassGuide.com (65.195.239.22) 52.191 ms 52.571 ms 56.855 ms 20 www.PassGuide.com (65.195.239.22) 53.561 ms 54.121 ms 58.333 ms

Which of the following is the most like cause of this issue?

A. An application firewall
B. Intrusion Detection System
C. Network Intrusion system
D. A stateful inspection firewall

Answer: D

Question No : 14 - (Topic 1)

You work as a Network Administrator for InformSec Inc. You find that the TCP port number 23476 is open on your server. You suspect that there may be a Trojan named Donald Dick installed on your server. Now you want to verify whether Donald Dick is installed on it or not. For this, you want to know the process running on port 23476, as well as the process id, process name, and the path of the process on your server. Which of the following applications will you most likely use to accomplish the task?

A. Tripwire
B. SubSeven
C. Netstat
D. Fport

Answer: D

Question No : 15 - (Topic 1)

Buffer overflows are one of the major errors used for exploitation on the Internet today. A buffer overflow occurs when a particular operation/function writes more data into a variable than the variable was designed to hold.

Which of the following are the two popular types of buffer overflows?

Each correct answer represents a complete solution. Choose two.

A. Dynamic buffer overflows
B. Stack based buffer overflow
C. Heap based buffer overflow
D. Static buffer overflows

Answer: B,C

Question No : 16 - (Topic 1)

Which of the following statements are true about a keylogger?

Each correct answer represents a complete solution. Choose all that apply.

A. It records all keystrokes on the victim's computer in a predefined log file.
B. It can be remotely installed on a computer system.
C. It is a software tool used to trace all or specific activities of a user on a computer.
D. It uses hidden code to destroy or scramble data on the hard disk.

Answer: A,B,C

Question No : 17 - (Topic 1)

Adam works as a Security Administrator for Umbrella Inc. A project has been assigned to him to secure access to the network of the company from all possible entry points. He segmented the network into several subnets and installed firewalls all over the network. He has placed very stringent rules on all the firewalls, blocking everything in and out except the ports that must be used. He does need to have port 80 open since his company hosts a website that must be accessed from the Internet. Adam is still worried about the programs

like Hping2 that can get into a network through covert channels.

Which of the following is the most effective way to protect the network of the company from an attacker using Hping2 to scan his internal network?

A. Block all outgoing traffic on port 21
B. Block all outgoing traffic on port 53
C. Block ICMP type 13 messages
D. Block ICMP type 3 messages

Answer: C

Question No : 18 - (Topic 1)

You work as a Network Administrator for Net Perfect Inc. The company has a Windows-based network. The company wants to fix potential vulnerabilities existing on the tested systems. You use Nessus as a vulnerability scanning program to fix the vulnerabilities. Which of the following vulnerabilities can be fixed using Nessus?

Each correct answer represents a complete solution. Choose all that apply.

A. Misconfiguration (e.g. open mail relay, missing patches, etc.)
B. Vulnerabilities that allow a remote cracker to control sensitive data on a system
C. Vulnerabilities that allow a remote cracker to access sensitive data on a system
D. Vulnerabilities that help in Code injection attacks

Answer: A,B,C

Question No : 19 - (Topic 1)

Which of the following commands is used to access Windows resources from Linux workstation?

A. mutt
B. scp
C. rsync
D. smbclient

Answer: D