GIAC Certified Incident Handler

GIAC GCIH

Version Demo

Total Demo Questions: 20

Total Premium Questions: 705

Buy Premium PDF

Topic Break Down

Topic	No. of Questions
Topic 1, Volume A	98
Topic 2, Volume B	96
Topic 3, Volume C	511
Total	705

QUESTION NO: 1

Which of the following steps can be taken as countermeasures against sniffer attacks? Each correct answer represents a complete solution. (Choose all that apply.)

A. Use encrypted protocols for all communications.

B. Use switches instead of hubs since they switch communications, which means that information is delivered only to the predefined host.

C. Use tools such as StackGuard and Immunix System to avoid attacks.

D. Reduce the range of the network to avoid attacks into wireless networks.

ANSWER: A B D

QUESTION NO: 2

Which of the following is a technique for creating Internet maps?

Each correct answer represents a complete solution. (Choose two.)

A. Active Probing

B. AS PATH Inference

C. Object Relational Mapping

D. Network Quota

ANSWER: A B

QUESTION NO: 3

An attacker has tricked a user into executing content he placed on a social networking site. The malicious content executes in the victim's browser and allows the attacker to determine if machines behind the user's firewall are up and running. What type of attack is this?

A. Cross Site Scripting

B. SQL Injection

C. Account Harvesting

D. Session Hijacking

ANSWER: D

QUESTION NO: 4

Which of the following programming languages are NOT vulnerable to buffer overflow attacks?

Each correct answer represents a complete solution. (Choose two.)

A. C

B. Java

C. C++

D. Perl

ANSWER: B D

QUESTION NO: 5

Which of the following protocol loggers is used to detect ping sweep?

A. lppi

B. pitl

C. dpsl

D. ippl

ANSWER: D

QUESTION NO: 6

Which of the following statements about threats are true?

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

A. A threat is a weakness or lack of safeguard that can be exploited by vulnerability, thus causing harm to the information systems or networks.

B. A threat is a potential for violation of security which exists when there is a circumstance, capability, action, or event that could breach security and cause harm.

C. A threat is a sequence of circumstances and events that allows a human or other agent to cause an information-related misfortune by exploiting vulnerability in an IT product.

D. A threat is any circumstance or event with the potential of causing harm to a system in the form of destruction, disclosure, modification of data, or denial of service.

ANSWER: B C D

QUESTION NO: 7

Which of the following can be used as a Trojan vector to infect an information system?

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

A. NetBIOS remote installation

B. Any fake executable

C. Spywares and adware

D. ActiveX controls, VBScript, and Java scripts

ANSWER: A B C D

QUESTION NO: 8

Which of the following statements are true about session hijacking?

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

A. Use of a long random number or string as the session key reduces session hijacking.

B. It is used to slow the working of victim's network resources.

C. TCP session hijacking is when a hacker takes over a TCP session between two machines.

D. It is the exploitation of a valid computer session to gain unauthorized access to information or services in a computer system.

ANSWER: A C D

QUESTION NO: 9

Which of the following tools can be used to force password complexity in Linux?

A. PAM

B. Password Guardian

C. Fast Lane

D. Passfilt.dll

ANSWER: A

Explanation:

On most Linux systems, you can use PAM (the "pluggable authentication module") to enforce password complexity.

QUESTION NO: 10

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\RunServices

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

ANSWER: D

QUESTION NO: 11

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.

ANSWER: A B C

QUESTION NO: 12

Which of the following tools can be used for network sniffing as well as for intercepting conversations through session hijacking?

A. Ethercap

B. Tripwire

C. IPChains

D. Hunt

ANSWER: D

QUESTION NO: 13

John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. He has successfully completed the following steps of the pre-attack phase:

l Information gathering l Determining network range l Identifying active machines l Finding open ports and applications l OS fingerprinting l Fingerprinting services

Now John wants to perform network mapping of the We-are-secure network. Which of the following tools can he use to accomplish his task?

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

A. Ettercap

B. Traceroute

C. Cheops

D. NeoTrace

ANSWER: B C D

QUESTION NO: 14

Which of the following statements about Denial-of-Service (DoS) attack are true? Each correct answer represents a complete solution. (Choose three.)

A. It disrupts services to a specific computer.

B. It changes the configuration of the TCP/IP protocol.

C. It saturates network resources.

D. It disrupts connections between two computers, preventing communications between services.

ANSWER: A C D

QUESTION NO: 15

Adam, a malicious hacker is sniffing the network to inject ARP packets. He injects broadcast frames onto the wire to conduct Man-in-The-Middle attack. Which of the following is the destination MAC address of a broadcast frame?

A. 0xDDDDDDDDDD

B. 0x00000000000

C. 0xFFFFFFFFFFFF

D. 0xAAAAAAAAAA

ANSWER: C

QUESTION NO: 16

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

Which of the following commands can be used to create a backdoor shell on port 1234 on a Linux or Unix system?

A. nc -p 1234 -e /bin/sh

B. nc -p 1234 -x /bin/sh

C. nc -l 1234 -x /bin/sh

D. nc -l -p 1234 -e /bin/sh

ANSWER: D

Explanation:

The -e command-line option is required to execute a backdoor shell. On Linux and Unix systems, /bin/sh is an appropriate path to a shell. On Windows systems, cmd.exe is an appropriate shell.

QUESTION NO: 18

You enter the following URL on your Web browser:

http://www.we-are-secure.com/scripts/..%co%af../..%co% af../windows/system32/cmd.exe?/c+dir+c:\

What kind of attack are you performing?

A. Directory traversal

B. Replay

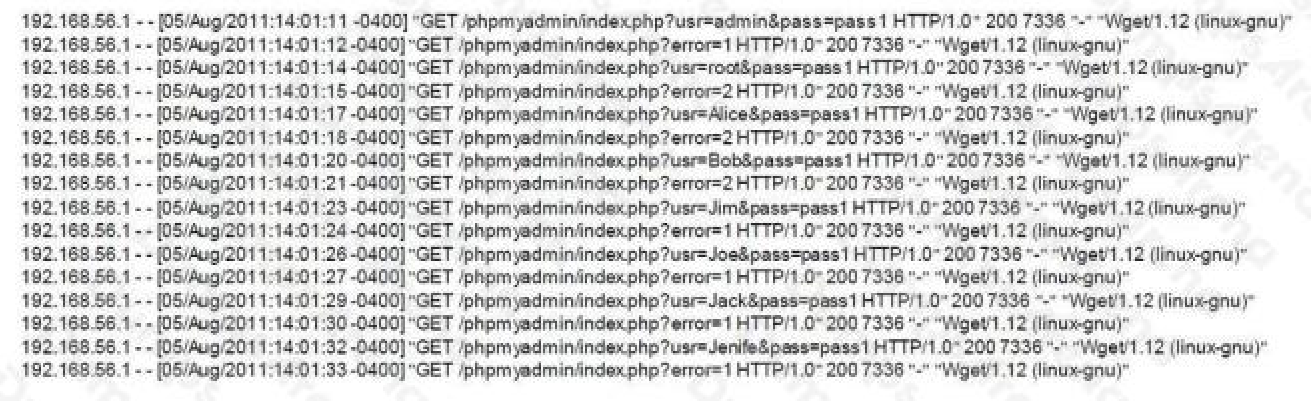
C. Session hijacking

D. URL obfuscating

ANSWER: A

QUESTION NO: 19

What step would mitigate the risk of the specific type of the web attack that produced the web server logs presented below?



```
192.168.56.1 - - [05/Aug/2011:14:01:11 -0400] "GET /phpmyadmin/index.php?usr=admin&pass=pass1 HTTP/1.0" 200 7336 "-" "Wget/1.12 (linux-gnu)"
192.168.56.1 - - [05/Aug/2011:14:01:12 -0400] "GET /phpmyadmin/index.php?error=1 HTTP/1.0" 200 7336 "-" "Wget/1.12 (linux-gnu)"
192.168.56.1 - - [05/Aug/2011:14:01:14 -0400] "GET /phpmyadmin/index.php?usr=root&pass=pass1 HTTP/1.0" 200 7336 "-" "Wget/1.12 (linux-gnu)"
192.168.56.1 - - [05/Aug/2011:14:01:15 -0400] "GET /phpmyadmin/index.php?error=2 HTTP/1.0" 200 7336 "-" "Wget/1.12 (linux-gnu)"
192.168.56.1 - - [05/Aug/2011:14:01:17 -0400] "GET /phpmyadmin/index.php?usr=Alice&pass=pass1 HTTP/1.0" 200 7336 "-" "Wget/1.12 (linux-gnu)"
192.168.56.1 - - [05/Aug/2011:14:01:18 -0400] "GET /phpmyadmin/index.php?error=2 HTTP/1.0" 200 7336 "-" "Wget/1.12 (linux-gnu)"
192.168.56.1 - - [05/Aug/2011:14:01:20 -0400] "GET /phpmyadmin/index.php?usr=Bob&pass=pass1 HTTP/1.0" 200 7336 "-" "Wget/1.12 (linux-gnu)"
192.168.56.1 - - [05/Aug/2011:14:01:21 -0400] "GET /phpmyadmin/index.php?error=2 HTTP/1.0" 200 7336 "-" "Wget/1.12 (linux-gnu)"
192.168.56.1 - - [05/Aug/2011:14:01:23 -0400] "GET /phpmyadmin/index.php?usr=Jim&pass=pass1 HTTP/1.0" 200 7336 "-" "Wget/1.12 (linux-gnu)"
192.168.56.1 - - [05/Aug/2011:14:01:24 -0400] "GET /phpmyadmin/index.php?error=1 HTTP/1.0" 200 7336 "-" "Wget/1.12 (linux-gnu)"
192.168.56.1 - - [05/Aug/2011:14:01:26 -0400] "GET /phpmyadmin/index.php?usr=Joe&pass=pass1 HTTP/1.0" 200 7336 "-" "Wget/1.12 (linux-gnu)"
192.168.56.1 - - [05/Aug/2011:14:01:27 -0400] "GET /phpmyadmin/index.php?error=1 HTTP/1.0" 200 7336 "-" "Wget/1.12 (linux-gnu)"
192.168.56.1 - - [05/Aug/2011:14:01:29 -0400] "GET /phpmyadmin/index.php?usr=Jack&pass=pass1 HTTP/1.0" 200 7336 "-" "Wget/1.12 (linux-gnu)"
192.168.56.1 - - [05/Aug/2011:14:01:30 -0400] "GET /phpmyadmin/index.php?error=1 HTTP/1.0" 200 7336 "-" "Wget/1.12 (linux-gnu)"
192.168.56.1 - - [05/Aug/2011:14:01:32 -0400] "GET /phpmyadmin/index.php?usr=Jenife&pass=pass1 HTTP/1.0" 200 7336 "-" "Wget/1.12 (linux-gnu)"
192.168.56.1 - - [05/Aug/2011:14:01:33 -0400] "GET /phpmyadmin/index.php?error=1 HTTP/1.0" 200 7336 "-" "Wget/1.12 (linux-gnu)"
```

A. HTTPS should be used instead of HTTP

B. The root account should not be available via a web interface

C. Users should not share the same password

D. Authentication error messages must be consistent

E. The application should require stronger passwords

ANSWER: D

Explanation:

In these specific logs, we can observe that the parameters named “usr” and “pass” are passed to phpmyadmin/index.php using GET requests, and after each one of them there is another GET request where the parameter “error” is passed to the same web page. However, the value passed to the “error” parameter is either “1” or “2”, which shows an inconsistency to the error messages. Such an inconsistency can be exploited by attackers in several ways, as for example in account harvesting attacks, where they attempt to find valid usernames. Such a risk can be mitigated using consistent (authentication) error messages.

From these specific logs we cannot conclude whether users use simple passwords or that they share the same passwords, since “pass1” is just a password tried by the attacker and not a valid one. Moreover, there is no indication if the root account is accessible via the web interface. Finally, although https protocol should be used instead of http to avoid transmitting usernames and passwords in cleartext, this would not prevent an account harvesting attack or any other attack whose cause would be the inconsistency in error messages.

QUESTION NO: 20

Which of the following is the most effective technique for identifying live client systems on a LAN?

A. ICMP Echo Requests

B. TCP FIN scanning

C. Traceroute

D. DNS Zone Transfer

ANSWER: C