GCIH Q&As

GIAC Certified Incident Handler

Pass GIAC GCIH Exam with 100% Guarantee

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

https://www.leads4pass.com/gcih.html

100% Passing Guarantee
100% Money Back Assurance

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

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

QUESTION 1

Which of the following statements are true about netcat?

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

A. It provides special tunneling, such as UDP to TCP, with the possibility of specifying all network parameters.

B. It can be used as a file transfer solution.

C. It provides outbound and inbound connections for TCP and UDP ports.

D. The nc -z command can be used to redirect stdin/stdout from a program.

Correct Answer: ABC

QUESTION 2

What do drive-by attacks typically take advantage of when delivering exploits?

A. Server upload policy

B. User\\'s browser

C. Old SSL version

D. Weak passwords

Correct Answer: B

Reference: https://www.kaspersky.com/resource-center/definitions/drive-by-download

QUESTION 3

Which of the following devices would return information about internal targets during an ACK scan?

A. A firewall that does not monitor the connection state of an inbound packet

B. A web-proxy that allows only outbound connections over tcp/8080

C. An IDS connected to a mirror port of the border router

D. A border device that drops inbound connections that use a flag other than SYN

Correct Answer: A

An ACK scan is particularly useful in getting through simple router-based firewalls. If a router allows "established" connections in (and is not using any stateful inspection), an attacker can use ACK scans to send packets into the network. A border device (firewall, advanced router, etc.) that requires state for inbound connections will be definition drop inbound packets with the ACK flag, negating the effectiveness of an ACK scan. A web-proxy that only allows outbound connections will ignore an ACK scan. An IDS connected to a mirror port does not have an IP address to target

with an ACK scan nor is there anything "behind the IDS" to map.

QUESTION 4

Which of the following is an effective method of detecting a covert communication tunnel such as ptunnel?

A. Rejecting incoming UDP packets with source port

B. Capturing outgoing HTTP traffic at unusual times

C. Restricting ICMP port unreachables with a non-zero payload

D. Detecting ICMP packets with uncommon payloads

Correct Answer: C

QUESTION 5

Adam, a malicious hacker purposely sends fragmented ICMP packets to a remote target. The total size of this ICMP packet once reconstructed is over 65,536 bytes. On the basis of above information, which of the following types of attack is Adam attempting to perform?

A. Fraggle attack

B. Ping of death attack

C. SYN Flood attack

D. Land attack

Correct Answer: B

QUESTION 6

Why would an analyst run the following command on a host they suspect is compromised?

C:\> c:\temp\lads\lads /S c:\Windows\System32

A. Find alternate data streams

B. Detect a user-mode rootkit

C. Stop hidden processes from running

D. Remove malicious DLLs from the system folder

Correct Answer: A

QUESTION 7

Which of the following languages are vulnerable to a buffer overflow attack? Each correct answer represents a complete solution. (Choose all that apply.)

A. Java

B. C++

C. C

D. Action script

Correct Answer: BC

QUESTION 8

Which of the following tools can be used as penetration tools in the Information system auditing process?

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

A. Nmap

B. Snort

C. SARA

D. Nessus

Correct Answer: CD

QUESTION 9

Which of the following rootkits adds additional code or replaces portions of an operating system, including both the kernel and associated device drivers?

A. Hypervisor rootkit

B. Boot loader rootkit

C. Kernel level rootkit

D. Library rootkit

Correct Answer: C

QUESTION 10

Which of the following rootkits patches, hooks, or replaces system calls with versions that hide information about the attacker?

A. Library rootkit

B. Kernel level rootkit

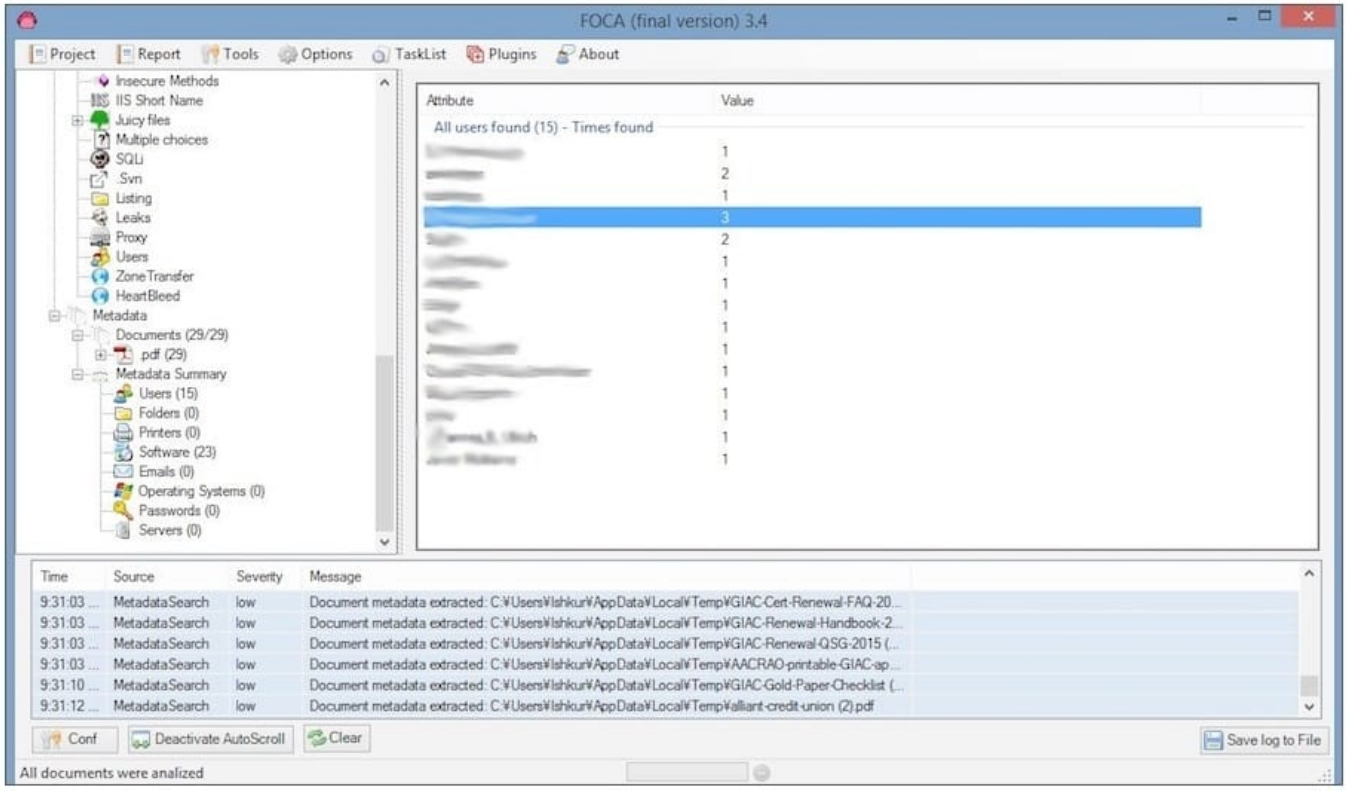
C. Hypervisor rootkit

D. Boot loader rootkit

Correct Answer: A

QUESTION 11

How can the information below be used in a penetration test?



A. Attempt to use an Apache exploit on the server

B. Make a zone transfer request on the DNS server

C. Harvest the user information to attempt to gain access

D. Use the heartbleed vulnerability to pull all user data off the server

Correct Answer: C

The users exposed in metadata can give information for accounts or for attempted exploitation or social engineering.

QUESTION 12

You have forgotten your password of an online shop. The web application of that online shop asks you to enter your

email so that they can send you a new password. You enter your email

you@gmail.com

And press the submit button.

The Web application displays the server error. What can be the reason of the error?

A. You have entered any special character in email.

B. Email entered is not valid.

C. The remote server is down.

D. Your internet connection is slow.

Correct Answer: A

QUESTION 13

Mark works as a Network Administrator for Perfect Inc. The company has both wired and wireless networks. An attacker attempts to keep legitimate users from accessing services that they require. Mark uses IDS/IPS sensors on the wired network to mitigate the attack. Which of the following attacks best describes the attacker\\'s intentions?

A. Internal attack

B. Reconnaissance attack

C. Land attack

D. DoS attack

Correct Answer: D

QUESTION 14

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

Correct Answer: D

QUESTION 15

A user is sending a large number of protocol packets to a network in order to saturate its resources and to disrupt connections to prevent communications between services. Which type of attack is this?

A. Vulnerability attack

B. Impersonation attack

C. Social Engineering attack

D. Denial-of-Service attack

Correct Answer: D