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.pass2lead.com/gcih.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

Which of the following accurately describes a "Bot"?

A. Bots normally infect a carrier file and need human interaction to spread from computer to computer

B. Bots are distribution channels that worms and viruses use to spread across the network

C. Bots normally infect a carrier file but need no human interaction to spread from computer to computer

D. Bots are software programs that perform an action on behalf of a human

Correct Answer: D

Bots are software programs that perform some action on behalf of a human, typically with little or no human intervention. Bots are specialized backdoors used for controlling systems en masse, with a single attacker controlling groups of bots numbering from a dozen to over a million infected machines. They operate autonomously, and could be used in a variety of ways, including: Maintaining backdoor control of a machine Controlling an IRC channel (one of the earliest and most popular uses of bots) Acting as a mail relay Providing anonomizing HTTP proxies Launching Denial of Service floods Worms and viruses can be distribution channels for bots. Launching Denial of Service floods

Worms and viruses can be distribution channels for bots.

QUESTION 2

You see the career section of a company\\'s Web site and analyze the job profile requirements. You conclude that the company wants professionals who have a sharp knowledge of Windows server 2003 and Windows active directory installation and placement. Which of the following steps are you using to perform hacking?

A. Scanning

B. Covering tracks

C. Reconnaissance

D. Gaining access

Correct Answer: C

QUESTION 3

Which of the following Trojans is used by attackers to modify the Web browser settings?

A. Win32/FlyStudio

B. Trojan.Lodear

C. WMA/TrojanDownloader.GetCodec

D. Win32/Pacex.Gen

Correct Answer: A

QUESTION 4

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 5

You are the Security Consultant and have been hired to check security for a client\\'s network. Your client has stated that he has many concerns but the most critical is the security of Web applications on their Web server. What should be your highest priority then in checking his network?

A. Setting up IDS

B. Port scanning

C. Vulnerability scanning

D. Setting up a honey pot

Correct Answer: C

QUESTION 6

When would a web-based reconnaissance tool be preferred over a direct/local reconnaissance tool?

A. When more comprehensive TCP port scanning is required than what is offered by local tools

B. In the event that the target is running third-party web applications

C. When the target\\'s employees are using a VPN to connect to the central office

D. To keep traffic from the attacker\\'s system from hitting the target network

Correct Answer: C

QUESTION 7

Deleting an attacker\\'s scheduled tasks on a victim host is something that would typically occur during which phase of

incident handling?

A. Identification

B. Recovery

C. Preparation

D. Eradication

Correct Answer: D

QUESTION 8

Which of the following is a technique that can be used to reduce the amount of data to examine during an investigation?

A. Ignore files with known good hashes

B. Ignore malicious file hashes

C. Create file hashes for all directories on the system

D. Request management recommendation for file hashes of interest

Correct Answer: A

QUESTION 9

Which of the following types of malware can an antivirus application disable and destroy?

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

A. Rootkit

B. Trojan

C. Crimeware

D. Worm

E. Adware

F. Virus

Correct Answer: ABDF

QUESTION 10

Which of the following types of scan does not open a full TCP connection?

A. FIN scan

B. ACK scan

C. Stealth scan

D. Idle scan

Correct Answer: C

QUESTION 11

You are responding to an incident in which the organization\\'s Extranet server has been compromised. The Extranet is the browser home page for most users in the organization. You have been instructed to watch the attacker, but minimize the business impact and the risk of further compromise. How can you continue providing services to the organization\\'s users while isolating the compromised server?

A. Point the domain name to the IP address of a secondary, patched production server

B. Change the server IP address to a different IP address

C. Isolate the switch port and put the system on a quarantined VLAN

D. Rebuild the system during a downtime window and restore the service

Correct Answer: A

The server is accessed via domain name by most users in your organization. To continue to provide service to those users, the best approach is to reroute DNS to another server. Chances are good that the attacker is accessing the server via IP address, so he should continue to have access to the server, which enables you to watch his actions while isolating users from the compromised server. Rebuilding the server during downtime would prevent access, prevent you from investigating, and possibly alert the attacker. Changing the IP address would not prevent users from accessing your site, and wouldn\\'t isolate the server. Quarantining the system would prevent legitimate users from accessing services.

QUESTION 12

Which of the following ensures that a party to a dispute cannot deny the authenticity of their signature on a document or the sending of a message that they originated?

A. OS fingerprinting

B. Reconnaissance

C. Non-repudiation

D. Confidentiality

Correct Answer: C

QUESTION 13

An administrator needs to repeatedly scan a very large network with thousands of hosts, what is the best way of accomplishing this very quickly?

A. Nessus

B. Nmap

C. Masscan

D. Hping3

Correct Answer: C

QUESTION 14

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

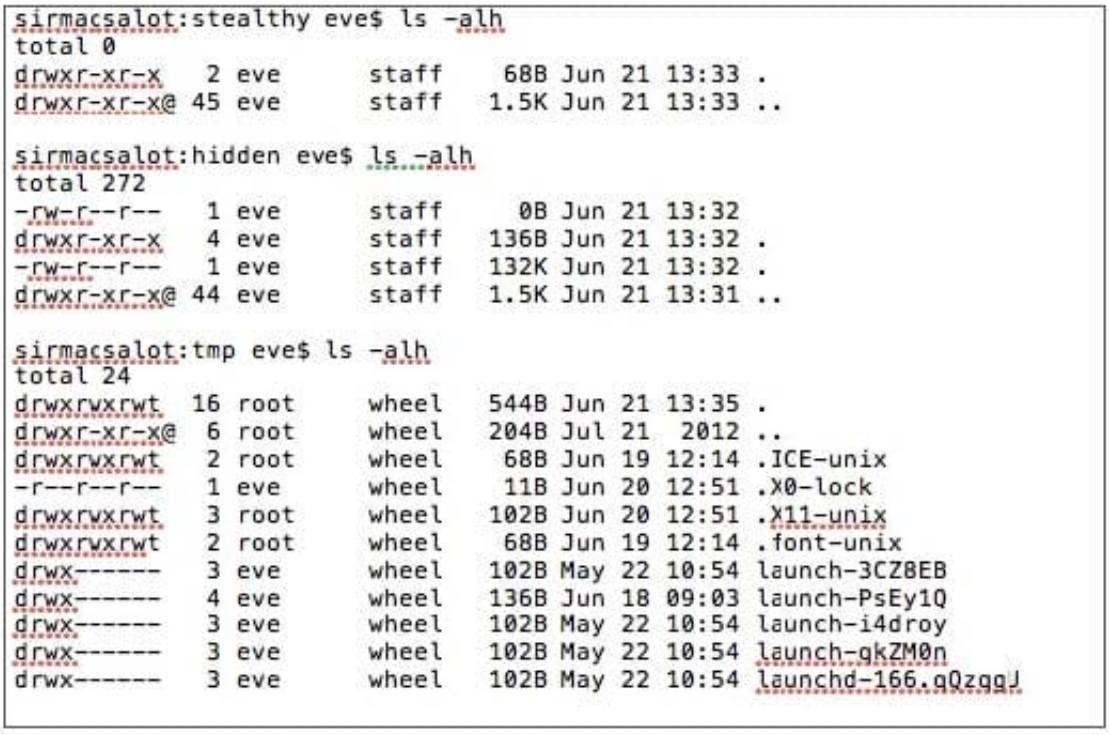
C. Hypervisor rootkit

D. Boot loader rootkit

Correct Answer: A

QUESTION 15

Examine the image below. Which of the following directories should be examined for suspicious entries?



```
sirmacsalot:stealthy eve$ ls -alh
total 0
drwxr-xr-x   2 eve      staff    68B Jun 21 13:33 .
drwxr-xr-x@ 45 eve      staff   1.5K Jun 21 13:33 ..

sirmacsalot:hidden eve$ ls -alh
total 272
-rw-r--r--   1 eve      staff     0B Jun 21 13:32
drwxr-xr-x   4 eve      staff   136B Jun 21 13:32 .
-rw-r--r--   1 eve      staff   132K Jun 21 13:32 .
drwxr-xr-x@ 44 eve      staff   1.5K Jun 21 13:31 ..

sirmacsalot:tmp eve$ ls -alh
total 24
drwxrwxrwt  16 root     wheel   544B Jun 21 13:35 .
drwxr-xr-x@  6 root     wheel   204B Jul 21  2012 ..
drwxrwxrwt   2 root     wheel    68B Jun 19 12:14 .ICE-unix
-r--r--r--   1 eve      wheel    11B Jun 20 12:51 .X0-lock
drwxrwxrwt   3 root     wheel   102B Jun 20 12:51 .X11-unix
drwxrwxrwt   2 root     wheel    68B Jun 19 12:14 .font-unix
drwx------   3 eve      wheel   102B May 22 10:54 launch-3CZ8EB
drwx------   4 eve      wheel   136B Jun 18 09:03 launch-PsEy1Q
drwx------   3 eve      wheel   102B May 22 10:54 launch-i4droy
drwx------   3 eve      wheel   102B May 22 10:54 launch-gkZM0n
drwx------   3 eve      wheel   102B May 22 10:54 launchd-166.qQzqqJ
```

A. stealthy

B. tmp

C. hidden

Correct Answer: C

The directory hidden has two hidden entries, a zero-byte file called " " (space) and a second 136 byte file called "." Both of these files should be investigated and are considered to be suspicious. The stealthy directory is empty and the tmp directory is a regular tmp directory from an OS X client. The " ." (space+dot) directory should not exist but it is otherwise empty.