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.passapply.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

SATISFACTION GUARANTEED 100% SATISFACTION GUARANTEED

QUESTION 1

In the network logs there are ACK/FIN/PSH/URG packets from a host going to a closed port, and SYN/FIN/URG/PSH packets going to open ports. What is the host likely doing?

A. Active OS fingerprinting

B. Host discovery

C. Passive OS fingerprinting

D. IDS evasion

Correct Answer: B

QUESTION 2

Which of the following BEST represents a true virtual machine escape?

A. An attacker who has compromised a virtual machine using VMcat to run code on the physical host

B. An attacker who has compromised a virtual machine mapping a network drive on the physical host using SMB

C. An attacker who has compromised a virtual machine sniffing network traffic to and from the physical host

D. An attacker who has compromised a virtual machine, able to directly execute code on the physical host

Correct Answer: D

Neither VMcat nor patched VME services are VME escapes, but they are moving in that direction. A "true" VME escape would let an attacker run code inside the guest that would somehow escape the guest and begin running on the underlying host itself. Connecting to a share on the host and sniffing network traffic do not constitute a VM escape.

QUESTION 3

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 4

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

Correct Answer: C

QUESTION 5

Which of the following functionalities is offered by Abel?

A. ARP cache poisoning for traffic redirection

B. Hash calculator for MD5

C. Traceroute via a GUI

D. Remote Windows password hash dumper

Correct Answer: D

Abel runs as a service in the background, giving remote access capabilities to a lot of functionality including a remote command shell, a remote route table manager, remote TCP and UDP port listener and a remote Windows password hash dumper.

QUESTION 6

Which of the following netcat commands will connect to tcp port 2222 on a remote system (10.0.0.1)?

A. C:\>nc.exe 10.0.0.1 2222

B. C:\>nc.exe 10.0.0.1 -l -p 2222

C. C:\>nc.exe 10.0.0.1 -L 2222

D. C:\>nc.exe 10.0.0.1 -p 2222

Correct Answer: B

Reference: https://www.varonis.com/blog/netcat-commands/

QUESTION 7

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()

Correct Answer: AD

QUESTION 8

Which endpoint security bypass technique modifies the assembly of an executable?

A. Living Off the Land

B. Code signing

C. Keyed payload

D. Ghostwriting

Correct Answer: B

QUESTION 9

Which of the following commands will enumerate a list of shares on a Windows target machine?

A. net share \\192.168.99.133

B. net view \\192.168.99.133

C. net use \\192.168.99.133

D. net session \\192.168.99.133

Correct Answer: B

QUESTION 10

Which of the following is one of the fields that Covert TCP uses to transmit data?

A. IP Options

B. Urgent Pointer

C. IP Identification

D. Code Bits

Correct Answer: A

QUESTION 11

You are the leader of an incident handling team for a mid-size manufacturer in the United States. Several of your company\\'s products are patented and several processes used in the manufacturing process are considered trade secrets. A member of your company\\'s firewall team sent you a tcpdump of a firewall log thought looked suspicious. The packets in question had the same external source IP address, the same internal destination IP addresses, and the same source and destination ports were used in each packet. The only difference between the packets was that the TTL\\'s had been incremented. How can you best determine if this is a sign of something malicious or not?

A. Set up a host intrusion detection system on the host with the internal IP address

B. Gather more data from your firewall logs and from other system logs inside your network

C. Check the Internet Storm Center\\'s Top 10 Source IPs Report to see if the external IP address is listed

D. Run a protocol analyzer on your computer with a filter that will only show the internal or external IP address

Correct Answer: A

QUESTION 12

A helpdesk ticket has been escalated to the incident response team. According to the FIRST organization classification guidelines, during which incident response phase should the team document the following information?

Category: Compromised Intellectual Property Criticality: High Sensitivity: Restricted to response team and management

A. Preparation

B. Eradication

C. Lessons Learned

D. Containment

Correct Answer: D

It is important to document various characteristics of the incident early on in the Containment phase. The FIRST organization distributes an incident Case Classification document that recommends characterizing an incident based on three areas: it\\'s general category, the criticality of impacted systems and data, and the sensitivity with which information about the case itself should be treated.

QUESTION 13

An attacker has penetrated a network and is using lateral movement. Which defense will be effective?

A. Prioritizing patches for vulnerabilities affecting public facing servers and web services

B. Configuring alert thresholds for Internet traffic sent to ports commonly used by attackers

C. Setting unique passwords for each local administrator and service account on the network

D. Dual homing hosts that require access to both internal and external resources

Correct Answer: A

Reference: https://www.crowdstrike.com/cybersecurity-101/lateral-movement/

QUESTION 14

An analyst runs the following nmap scan from their Linux computer as a non-privileged user. The target host, 10.0.233.2, has tcp/445 open. What network traffic would be generated by this scan?

```
$ nmap 10.0.233.2
```

A. ICMP echo and reply between the source and destination

B. No traffic will be captured as the scan is passive

C. TCP handshake between the source and destination hosts

D. ACK packets from the source to the destination

Correct Answer: C

A basic nmap scan, when not running as root, does a full TCP connect scan and completes the 3-way handshake.

QUESTION 15

How can you minimize your chances of a mistake, such as not notifying a required party, being made during an incident response?

A. Have management support

B. Have administrative access to all systems

C. Have proper procedures in place

D. Fill out chain of custody forms promptly

Correct Answer: C

Latest GCIH Dumps   GCIH Practice Test   GCIH Exam Questions