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.certbus.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 Win32 based command will display DNS record names and types, as well as the current time to live for the record?

A. ipconfig /displaydns

B. ipconfig /showdnsid

C. ipconfig /all

D. ipconfig /registerdns

Correct Answer: A

QUESTION 2

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 3

You want to perform passive footprinting against we-are-secure Inc. Web server. Which of the following tools will you use?

A. Nmap

B. Ethereal

C. Ettercap

D. Netcraft

Correct Answer: D

QUESTION 4

Which of the following is a protocol that, like TFTP, can be used to transfer Netcat to a victim machine in order to open a backdoor listener?

A. DHCP

B. WINS

C. HTTPS

D. SNMP

Correct Answer: C

Note that if outbound TFTP is blocked by a firewall, the attacker can use outbound FTP, SSH, HTTP, HTTPS, or other protocols that might be allowed for communications. SNMP, DHCP, and WINS are not known as file transfer protocols, and are not typically allowed outbound to the internet.

QUESTION 5

Which of the following is a version of netcat with integrated transport encryption capabilities?

A. Encat

B. Nikto

C. Socat

D. Cryptcat

Correct Answer: D

QUESTION 6

You work as a professional Ethical Hacker. You are assigned a project to test the security of www.weare-secure.com. You somehow enter in we-are-secure Inc. main server, which is Windows based.

While you are installing the NetCat tool as a backdoor in the we-are-secure server, you see the file credit.dat having the list of credit card numbers of the company\\'s employees. You want to transfer the credit.dat file in your local computer so that you can sell that information on the internet in the good price. However, you do not want to send the contents of this file in the clear text format since you do not want that the Network Administrator of the we-are-secure Inc. can get any clue of the hacking attempt. Hence, you decide to send the content of the credit.dat file in the encrypted format.

What steps should you take to accomplish the task?

A. You will use the ftp service.

B. You will use Wireshark.

C. You will use CryptCat instead of NetCat.

D. You will use brutus.

Correct Answer: C

QUESTION 7

Which of the following tools will show all TCP and UDP connections on a Windows system?

A. Net

B. TCPView

C. Netcat

D. Psinfo

Correct Answer: B

TCPView shows all TCP and UDP endpoints on your system. The listing includes the name of the process that owns each endpoint, the state of TCP connections, and the remote addresses. Psinfo, net, and netcat do not have this capability.

QUESTION 8

Adam works as an Incident Handler for Umbrella Inc. He has been sent to the California unit to train the members of the incident response team. As a demo project he asked members of the incident response team to perform the following

actions:

Remove the network cable wires.

Isolate the system on a separate VLAN

Use a firewall or access lists to prevent communication into or out of the system.

Change DNS entries to direct traffic away from compromised system

Which of the following steps of the incident handling process includes the above actions?

A. Identification

B. Containment

C. Eradication

D. Recovery

Correct Answer: B

QUESTION 9

How does Karmetasploit acquire the user credentials of wireless clients?

A. Karmetasploit sniffs probe requests form a client, pretends to be its access point, and pretends to be services (HTTP, POP3, and Samba) to the client

B. Karmetasploit sniffs packets utilizing Wire Shark, cracks the WEP key, and views data recorded earlier using the decrypted WEP key

C. Karmetasploit attacks a wireless access point, installs a sniffer on the wireless access point, and sends information back to the attacker via SSH tunnels

D. Karmetasploit acts as a wired bridge between an access point and upstream router, sniffs wired traffic, and sends information back to the attacker via SSH tunnels

Correct Answer: A

Karmetasploit sniffs probe requests from a client, pretends to be its access point, and pretends to be services (HTTP, POP3, and Samba) to the client. Then it can even attack the client.

QUESTION 10

What will the following Enum command display?

C:\> enum -G 127.0.0.1

A. Share list

B. Group and member list

C. LSA policy information

D. Password policy information

Correct Answer: B

QUESTION 11

Which of the following techniques can be used to map \\'open\\' or \\'pass through\\' ports on a gateway?

A. Traceport

B. Tracefire

C. Tracegate

D. Traceroute

Correct Answer: D

QUESTION 12

What will a host do when it receives a packet with an invalid TCP checksum?

A. Drop the packet

B. Hold the packet and wait for a rebroadcast

C. Send an ICMP redirect

D. Reply with a TCP reset

Correct Answer: A

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

A SOC analyst is reviewing event logs from several network devices across the enterprise and notices that there are an abnormally high number of logon attempts across the desktop systems for several user IDs. What should the analyst do next?

A. The desktop teams should be notified to suspend the accounts of the users and reissue new credentials.

B. An IDS signature should be deployed to monitor the user\\'s logon attempts and alert the SOC of new failures.

C. Each device should be examined for any successful logon attempts within the past 24 hours.

D. An event ticket should be created and escalated to the security team to investigate the attempts.

Correct Answer: D

The front line team in the SOC should have the authority to escalate any events that meet the criteria of a security issue to the responsive team. By issuing a ticket to the security team, they are logging the events, collecting the information and applying a service level agreement to the primary business group to handle. Failed logon attempts across multiple desktop systems for several users could indicate a manual or automated (virus/worm) attempt to probe common or collected usernames with a dictionary of pass phrases.

QUESTION 15

A Denial-of-Service (DoS) attack is mounted with the objective of causing a negative impact on the performance of a computer or network. It is also known as network saturation attack or bandwidth consumption attack. Attackers perform DoS attacks by sending a large number of protocol packets to a network. The problems caused by a DoS attack are as

follows:

l Saturation of network resources l Disruption of connections between two computers, thereby preventing communications between services l Disruption of services to a specific computer l Failure to access a Web site l Increase in the amount of spam

Which of the following can be used as countermeasures against DoS attacks?

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

A. Blocking undesired IP addresses

B. Applying router filtering

C. Disabling unneeded network services

D. Permitting network access only to desired traffic

Correct Answer: ABCD