DUMPSARENA

GIAC Certified Enterprise Defender

GIAC GCED

Version Demo

Total Demo Questions: 10

Total Premium Questions: 88

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1

Which of the following is an outcome of the initial triage during incident response?

A. Removal of unnecessary accounts from compromised systems

B. Segmentation of the network to protect critical assets

C. Resetting registry keys that vary from the baseline configuration

D. Determining whether encryption is in use on in scope systems

ANSWER: B

QUESTION NO: 2

Which command is the Best choice for creating a forensic backup of a Linux system?

A. Run form a bootable CD: tar cvzf image.tgz /

B. Run from compromised operating system: tar cvzf image.tgz /

C. Run from compromised operating system: dd if=/ dev/hda1 of=/mnt/backup/hda1.img

D. Run from a bootable CD: dd if=/dev/hda1 of=/mnt/backup/hda1.img

ANSWER: D

Explanation:

Using dd from a bootable CD is the only forensically sound method of creating an image. Using tar does not capture slack space on the disk. Running any command from a compromised operating system will raise integrity issues.

QUESTION NO: 3

Which Unix administration tool is designed to monitor configuration changes to Cisco, Extreme and Foundry infrastructure devices?

A. SNMP

B. Netflow

C. RANCID

D. RMON

ANSWER: C

Explanation:

RANCID is a Unix tool which can be used to monitor changes to the following networked devices and more: IOS, CatOS, PIX, Juniper, Foundry, HP ProCurve, Extreme.

QUESTION NO: 4

A company wants to allow only company-issued devices to attach to the wired and wireless networks. Additionally, devices that are not up-to-date with OS patches need to be isolated from the rest of the network until they are updated. Which technology standards or protocols would meet these requirements?

A. 802.1x and Network Access Control

B. Kerberos and Network Access Control

C. LDAP and Authentication, Authorization and Accounting (AAA)

D. 802.11i and Authentication, Authorization and Accounting (AAA)

ANSWER: A

QUESTION NO: 5

A compromised router is reconfigured by an attacker to redirect SMTP email traffic to the attacker's server before sending packets on to their intended destinations. Which IP header value would help expose anomalies in the path outbound SMTP/ Port 25 traffic takes compared to outbound packets sent to other ports?

A. Checksum

B. Acknowledgement number

C. Time to live

D. Fragment offset

ANSWER: C

Explanation:

In a case study of a redirect tunnel set up on a router, some anomalies were noticed while watching network traffic with the TCPdump packet sniffer.

Packets going to port 25 (Simple Mail Transfer Protocol [SMTP] used by mail servers and other Mail Transfer Agents [MTAs] to send and receive e-mail) were apparently taking a different network path. The TLs were consistently three less than other destination ports, indicating another three network hops were taken.

Other IP header values listed, such as fragment offset. The acknowledgement number is a TCP, not IP, header field.

QUESTION NO: 6

Which type of media should the IR team be handling as they seek to understand the root cause of an incident?

A. Restored media from full backup of the infected host

B. Media from the infected host, copied to the dedicated IR host

C. Original media from the infected host

D. Bit-for-bit image from the infected host

ANSWER: A

Explanation:

By imaging the media with tools such as dd or Ghost and analyzing the copy, you preserve the original media for later analysis so that the results can be recreated by another competent examiner if necessary.

QUESTION NO: 7

How would an attacker use the following configuration settings?

```
interface Tunnel0
ip address 192.168.55.1 255.255.255.0
tunnel source FastEthernet0/0
tunnel destination 192.17.250.2
```

A. A client based HIDS evasion attack

B. A firewall based DDoS attack

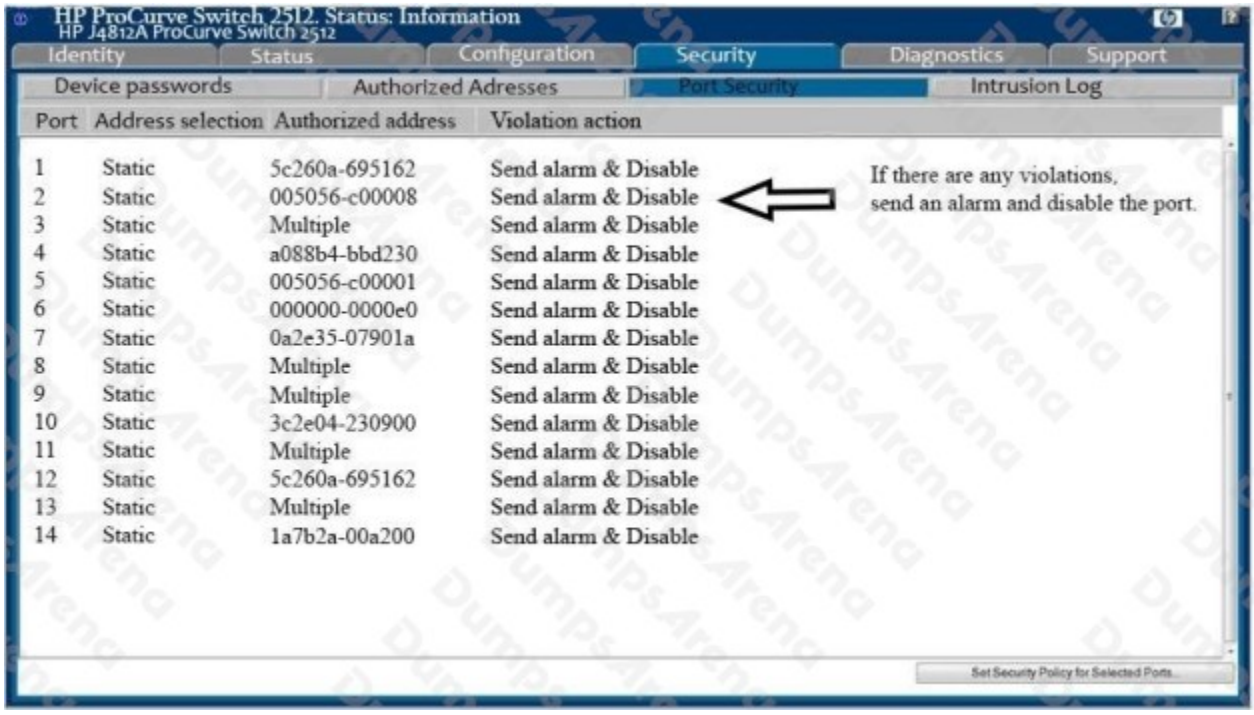
C. A router based MITM attack

D. A switch based VLAN hopping attack

ANSWER: C

QUESTION NO: 8

Analyze the screenshot below. Which of the following attacks can be mitigated by these configuration settings?



A. A Denial-of-Service attack using network broadcasts

B. A Replay attack

C. An IP masquerading attack

D. A MAC Flood attack

ANSWER: D

Explanation:

Both BPDU Guard and Root Guard are used to prevent a new switch from becoming the Root Bridge. They are very similar but use different mechanisms.

Rootguard allows devices to use STP, but if they send superior BDPUs (i.e. they attempt to become the Root Bridge), Root Guard disables the port until the offending BPDUs cease. Recovery is automatic.

If Portfast is enabled on a port, BPDU Guard will disable the port if a BPDU is received. The port stays disabled until it is manually re-enabled. Devices behind such ports cannot use STP, as the port would be disabled as soon as they send BPDUs (which is the default behavior of switches).

QUESTION NO: 9

An internal host at IP address 10.10.50.100 is suspected to be communicating with a command and control whenever a user launches browser window. What features and settings of Wireshark should be used to isolate and analyze this network traffic?

A. Filter traffic using ip.src = = 10.10.50.100 and tcp.srcport = = 80, and use Expert Info

B. Filter traffic using ip.src = = 10.10.50.100 and tcp.dstport = = 53, and use Expert Info

C. Filter traffic using ip.src = = 10.10.50.100 and tcp.dstport = = 80, and use Follow TCP stream

D. Filter traffic using ip.src = = 10.10.50.100, and use Follow TCP stream

ANSWER: C

QUESTION NO: 10

What is the BEST sequence of steps to remove a bot from a system?

A. Terminate the process, remove autoloading traces, delete any malicious files

B. Delete any malicious files, remove autoloading traces, terminate the process

C. Remove autoloading traces, delete any malicious files, terminate the process

D. Delete any malicious files, terminate the process, remove autoloading traces

ANSWER: A