GCED$^{Q\&As}$

GIAC Certified Enterprise Defender Practice Test

QUESTION 1

How does an Nmap connect scan work?

A. It sends a SYN, waits for a SYN/ACK, then sends a RST.

B. It sends a SYN, waits for a ACK, then sends a RST.

C. It sends a SYN, waits for a ACK, then sends a SYN/ACK.

D. It sends a SYN, waits for a SYN/ACK, then sends a ACK

Correct Answer: A

Explanation: An Nmap connect scan sends a SYN, waits for a SYN/ACK, then sends a ACK to complete the three-way handshake. A Nmap half-open scan sends a SYN, waits for a SYN/ACK, then sends a RST.

QUESTION 2

If a Cisco router is configured with the "service config" configuration statement, which of the following tools could be used by an attacker to apply a new router configuration?

A. TFTPD

B. Hydra

C. Ettercap

D. Yersinia

Correct Answer: A

QUESTION 3

Why would the pass action be used in a Snort configuration file?

A. The pass action simplifies some filtering by specifying what to ignore.

B. The pass action passes the packet onto further rules for immediate analysis.

C. The pass action serves as a placeholder in the snort configuration file for future rule updates.

D. Using the pass action allows a packet to be passed to an external process.

E. The pass action increases the number of false positives, better testing the rules.

Correct Answer: A

Explanation: The pass action is defined because it is sometimes easier to specify the class of data to ignore rather than the data you want to see. This can cut down the number of false positives and help keep down the size of log data. False positives occur because rules failed and indicated a threat that is really not one. They should be minimized whenever possible. The pass action causes the packet to be ignored, not passed on further. It is an active command, not a placeholder.

QUESTION 4

Monitoring the transmission of data across the network using a man-in-the-middle attack presents a threat against which type of data?

A. At-rest

B. In-transit

C. Public

D. Encrypted

Correct Answer: B

QUESTION 5

When attempting to collect data from a suspected system compromise, which of the following should generally be collected first?

A. The network connections and open ports

B. The contents of physical memory

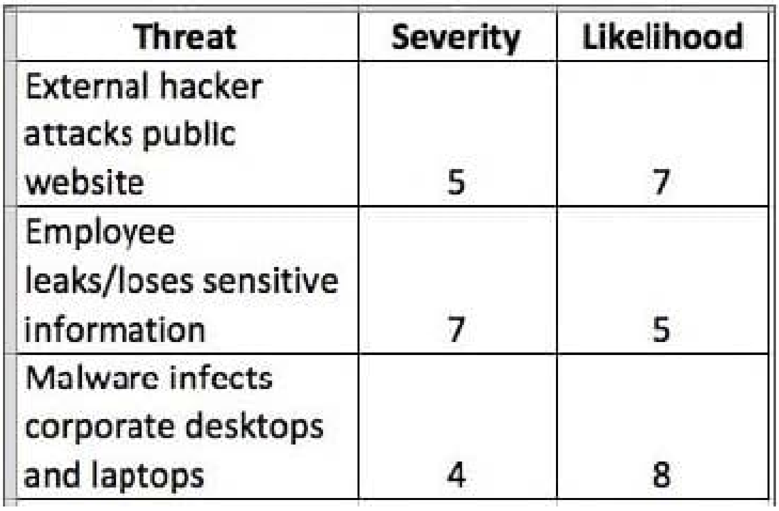
C. The current routing table

D. A list of the running services

Correct Answer: B

QUESTION 6

The matrix in the screen shot below would be created during which process?



Threat	Severity	Likelihood
External hacker attacks public website	5	7
Employee leaks/loses sensitive information	7	5
Malware infects corporate desktops and laptops	4	8

A. Risk Assessment

B. System Hardening

C. Data Classification

D. Vulnerability Scanning

Correct Answer: A

QUESTION 7

Which of the following would be included in a router configuration standard?

A. Names of employees with access rights

B. Access list naming conventions

C. Most recent audit results

D. Passwords for management access

Correct Answer: B

QUESTION 8

Which tool uses a Snort rules file for input and by design triggers Snort alerts?

A. snot

B. stick

C. Nidsbench

D. ftester

Correct Answer: C

QUESTION 9

Which of the following is best defined as "anything that has the potential to target known or existing vulnerabilities in a system?"

A. Vector

B. Gateway

C. Threat

D. Exploit

Correct Answer: A

QUESTION 10

Which of the following is a major problem that attackers often encounter when attempting to develop or use a kernel mode rootkit?

A. Their effectiveness depends on the specific applications used on the target system.

B. They tend to corrupt the kernel of the target system, causing it to crash.

C. They are unstable and are easy to identify after installation

D. They are highly dependent on the target OS.

Correct Answer: B

QUESTION 11

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

Correct 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 12

What would a penetration tester expect to access after the following metasploit payload is delivered successfully?

Set PAYLOAD windows / shell / reverse _ tcp

A. VNC server session on the target

B. A netcat listener on the target

C. A meterpreter prompt on the target

D. A command prompt on the target

Correct Answer: D

Explanation: set PAYLOAD windows/shell/reverse_tcp should get you to a command prompt on the host system. A different payload is used to get a meterpreter session. This payload does not start a VNC server or netcat listener on the target system.

QUESTION 13

What is the most common read-only SNMP community string usually called?

A. private

B. mib

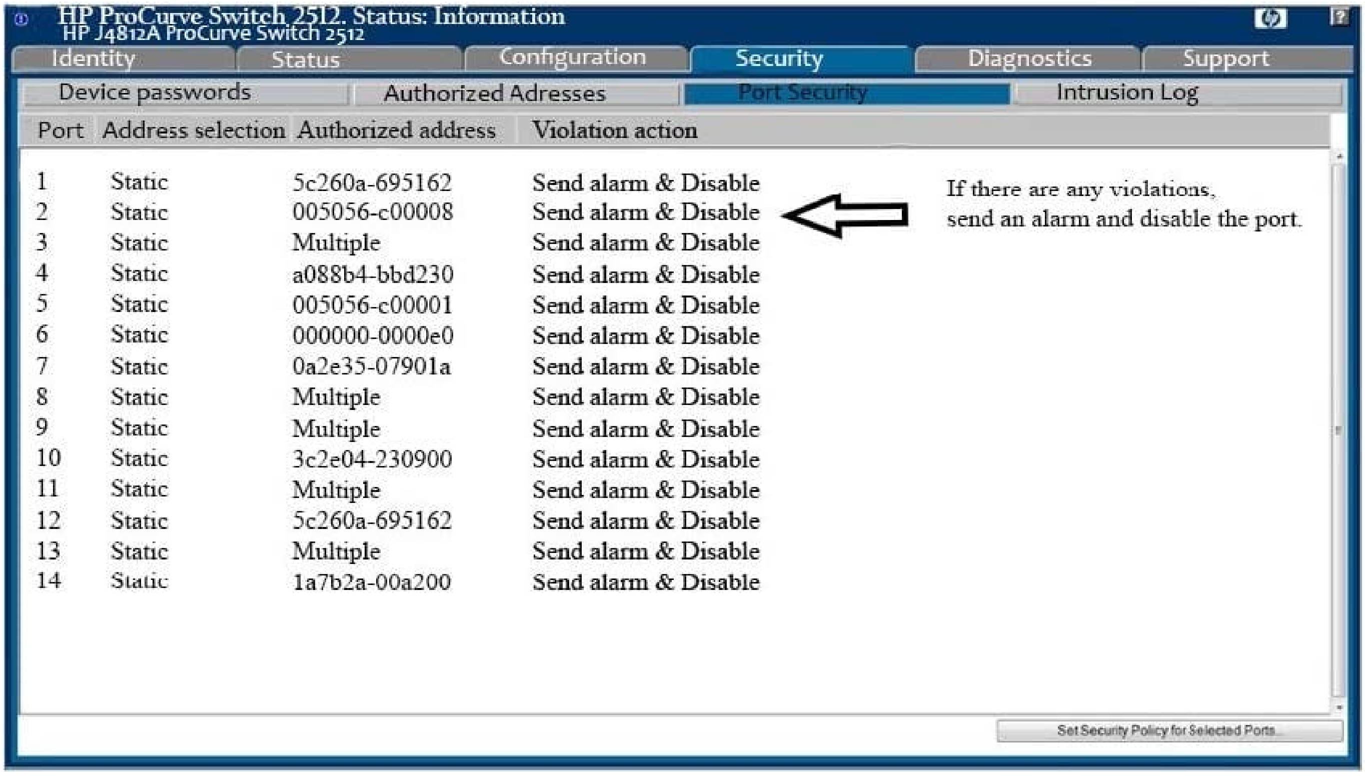
C. open

D. public

Correct Answer: D

QUESTION 14

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



HP ProCurve Switch 2512. Status: Information
HP J4812A ProCurve Switch 2512

Port	Address selection	Authorized address	Violation action
1	Static	5c260a-695162	Send alarm & Disable
2	Static	005056-c00008	Send alarm & Disable
3	Static	Multiple	Send alarm & Disable
4	Static	a088b4-bbd230	Send alarm & Disable
5	Static	005056-c00001	Send alarm & Disable
6	Static	000000-0000e0	Send alarm & Disable
7	Static	0a2e35-07901a	Send alarm & Disable
8	Static	Multiple	Send alarm & Disable
9	Static	Multiple	Send alarm & Disable
10	Static	3c2e04-230900	Send alarm & Disable
11	Static	Multiple	Send alarm & Disable
12	Static	5c260a-695162	Send alarm & Disable
13	Static	Multiple	Send alarm & Disable
14	Static	1a7b2a-00a200	Send alarm & Disable

If there are any violations, send an alarm and disable the port.

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

B. A Replay attack

C. An IP masquerading attack

D. A MAC Flood attack

Correct 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 15

Following a Digital Forensics investigation, which of the following should be included in the final forensics report?

A. An executive summary that includes a list of all forensic procedures performed.

B. A summary of the verified facts of the incident and the analyst\\'s unverified opinions.

C. A summary of the incident and recommended disciplinary actions to apply internally.

D. An executive summary that includes high level descriptions of the overall findings.

Correct Answer: D

Explanation: A professional forensic report should include an executive summary, including a description of the incident and the overall findings.

The written report needs to be factually accurate and free from speculation or bias, meaning that an analyst\\'s unverified or unsubstantiated opinions should not be included in the report. Beyond the executive summary, the detailed report should include a description of the data preserved, a detailed explanation of the procedures performed, and a summary of the facts. Disciplinary action, if needed, would be addressed

through other channels and not included in the forensic analyst\\'s report.