Free Questions for GCED by dumpshq

Shared by Kelley on 24-05-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

An analyst will capture traffic from an air-gapped network that does not use DNS. The analyst is looking for unencrypted Syslog data being transmitted. Which of the following is most efficient for this purpose?

Options:

A- tcpdump --s0 --i eth0 port 514

B- tcpdump --nnvvX --i eth0 port 6514

C- tcpdump --nX --i eth0 port 514

D- tcpdump --vv --i eth0 port 6514

Answer:

B

Explanation:

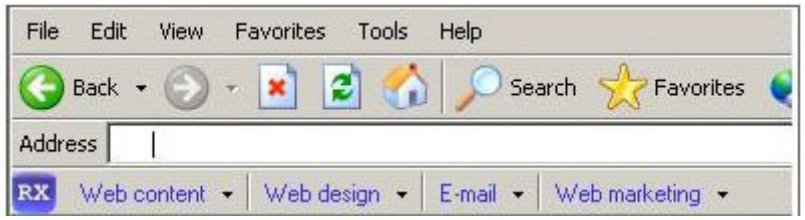
When using tcpdump, a --n switch will tell the tool to not resolve hostnames; as this network makes no use of DNS this is efficient. The --vv switch increases the tools output verbosity. The --s0 increases the snaplength to "all" rather than the default of 96 bytes. The --nnvvX

would make sense here except that the port in the filter is 6514 which is the default port for encrypted Syslog transmissions.

Question 2

Question Type: MultipleChoice

Which of the following tools is the most capable for removing the unwanted add-on in the screenshot below?



Options:

A- ProcessExplorer

B- Taskkill

C- Paros

D- Hijack This

Answer:

B

Question 3

Question Type: MultipleChoice

In order to determine if network traffic adheres to expected usage and complies with technical standards, an organization would use a device that provides which functionality?

Options:

A- Stateful packet filtering

B- Signature matching

C- Protocol anomaly detection

D- CRC checking

E- Forward error correction

Answer:

C

Explanation:

In addition to standards compliance, Protocol Anomaly Detection determines whether data within the protocol adheres to expected usage. Even if a communication stream complies with a protocol standard, the way in which the protocol is being used may be inconsistent with what is expected. Perimeter devices that perform protocol anomaly detection contain in-depth knowledge of protocol standards and expected usage and are able to detect traffic that does not comply with those guidelines.

Question 4

Question Type: MultipleChoice

Why would a Cisco network device with the latest updates and patches have the service config setting enabled, making the device vulnerable to the TFTP Server Attack?

Options:

A- Disabling telnet enables the setting on the network device.

B- This setting is enabled by default in the current Cisco IOS.

C- Allowing remote administration using SSH under the Cisco IOS also enables the setting.

D- An attack by Cisco Global Exploiter will automatically enable the setting.

E- This older default IOS setting was inherited from an older configuration despite the upgrade.

Answer:

B

Explanation:

Enabling the service config setting causes a Cisco router to be vulnerable to the TFTP Server Attack since it will actively try to retrieve a new configuration file from the nearest TFTP server. An attacker can insert a malicious update file in this process to compromise the Cisco router.

The service config setting was disabled by default in the Cisco IOS in version 12.0, but had been enabled by default in the 11.x series of the IOS trains. This feature is often enabled in later versions since organizations don't always realize the risk of this setting and will leave it enabled as the migrate through multiple IOS upgrades.

The other items listed don't enable the service config setting.

Question 5

Question Type: MultipleChoice

Which of the following is an operational security control that is used as a prevention mechanism?

Options:

A- Labeling of assets

B- Heat detectors

C- Vibration alarms

D- Voltage regulators

Answer:

A

Explanation:

The following are considered operational security prevention controls: Security gates, guards, and dogs; Heating, ventilation, and air conditioning (HVAC); Fire suppressant; Labeling of assets (classification and responsible agents); Off-site storage (recovery); Safes and locks. The other distractors are considered operational security detection controls.

Question 6

Question Type: MultipleChoice

Requiring background checks for employees who access protected data is an example of which type of data loss control?

Options:

A- Mitigation

B- Prevention

C- Monitoring

D- Identification

Answer:

B

Explanation:

Once sensitive data is identified and classified, preventive measures can be taken. Among these are software-based controls, such as auditing and access control, as well as human controls such as background checks, psychological examinations, and such.

Question 7

Question Type: MultipleChoice

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

Set PAYLOAD windows / shell / reverse _ tcp

Options:

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

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 8

Question Type: MultipleChoice

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

Options:

A- private

B- mib

C- open

D- public

Answer:

D

Question 9

Question Type: MultipleChoice

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
```

Options:

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 10

Question Type: MultipleChoice

Which control would BEST help detect a potential insider threat?

Options:

A- Mandatory approval process for executive and administrative access requests.

B- Providing the same access to all employees and monitoring sensitive file access.

C- Multiple scheduled log reviews of all employee access levels throughout the year

D- Requiring more than one employee to be trained on each task or job duty.

Answer:

A

Question 11

Question Type: MultipleChoice

How does the Cisco IOS IP Source Guard feature help prevent spoofing attacks?

Options:

A- Filters traffic based on IP address once a DHCP address has been assigned

B- Prevents unauthorized MAC addresses from receiving an IP address on the network

C- Blocks unsolicited ARP packets after a client has received an IP address

D- Rate limits client traffic to prevent CAM table flooding

Answer:

A

Question 12

Question Type: MultipleChoice

What should happen before acquiring a bit-for-bit copy of suspect media during incident response?

Options:

A- Encrypt the original media to protect the data

B- Create a one-way hash of the original media

C- Decompress files on the original media

D- Decrypt the original media

Answer:

B