Free Questions for GCCC by certscare

Shared by Rivas on 24-05-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which of the following can be enabled on a Linux based system in order to make it more difficult for an attacker to execute malicious code after launching a buffer overflow attack?

Options:

A- ASLR

B- Tripwire

C- SUID

D- Iptables

E- TCP Wrappers

Answer:

A

Question 2

Question Type: **MultipleChoice**

An organization has failed a test for compliance with a policy of continual detection and removal of malicious software on its network. Which of the following errors is the root cause?

Options:

A- A host ran malicious software that exploited a vulnerability for which there was no patch

B- The security console alerted when a host anti-virus ran whitelisted software

C- The intrusion prevention system failed to update to the newest signature list

D- A newly discovered vulnerability was not detected by the intrusion detection system

Answer:

C

Question 3

Question Type: **MultipleChoice**

After installing a software package on several workstations, an administrator discovered the software opened network port TCP 23456 on each workstation. The port is part of a software management function that is not needed on corporate workstations. Which actions would best protect the computers with the software package installed?

Options:

A- Document the port number and request approval from a change control group

B- Redirect traffic to and from the software management port to a non-default port

C- Block TCP 23456 at the network perimeter firewall

D- Determine which service controls the software management function and opens the port, and disable it

Answer:

D

Question 4

Question Type: **MultipleChoice**

During a security audit which test should result in a source packet failing to reach its intended destination?

Options:

A- A new connection request from the Internet is sent to a host on the company 's internal net work

B- A packet originating from the company's DMZ is sent to a host on the company's internal network

C- A new connection request from the internet is sent to the company's DNS server

D- A packet originating from the company's internal network is sent to the company's DNS server

Answer:

A

Question 5

Question Type: **MultipleChoice**

Which of the following should be measured and analyzed regularly when implementing the Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers CIS Control?

Options:

A- How long does it take to identify new unauthorized listening ports on the network systems

B- How long does it take to remove unauthorized software from the organization's systems

C- What percentage of the organization's applications are using sandboxing products

D- What percentage of assets will have their settings enforced and redeployed

E- What percentage of systems in the organization are using Network Level Authentication (NLA)

Answer:

D

Question 6

Question Type: MultipleChoice

Which approach is recommended by the CIS Controls for performing penetration tests?

Options:

A- Document a single vulnerability per system

B- Utilize a single attack vector at a time

C- Complete intrusive tests on test systems

D- Execute all tests during network maintenance windows

Answer:

C

Question 7

Question Type: MultipleChoice

Which CIS Control includes storing system images on a hardened server, scanning production systems for out-of-date software, and using file integrity assessment tools like tripwire?

Options:

A- Inventory of Authorized and Unauthorized Software

B- Continuous Vulnerability Management

C- Secure Configurations for Network Devices such as Firewalls, Routers and Switches

D- Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers

Answer:

D