GIAC Critical Controls Certification (GCCC)

GIAC GCCC

Version Demo

Total Demo Questions: 10

Total Premium Questions: 93

QUESTION NO: 1

Which of the following statements is appropriate in an incident response report?

A. There had been a storm on September 27th that may have caused a power surge

B. The registry entry was modified on September 29th at 22:37

C. The attacker may have been able to access the systems due to missing KB2965111

D. The backup process may have failed at 2345 due to lack of available bandwidth

ANSWER: B

QUESTION NO: 2

What documentation should be gathered and reviewed for evaluating an Incident Response program?

A. Staff member interviews

B. NIST Cybersecurity Framework

C. Policy and Procedures

D. Results from security training assessments

ANSWER: C

QUESTION NO: 3

What could a security team use the command line tool Nmap for when implementing the Inventory and Control of Hardware Assets Control?

A. Control which devices can connect to the network

B. Passively identify new devices

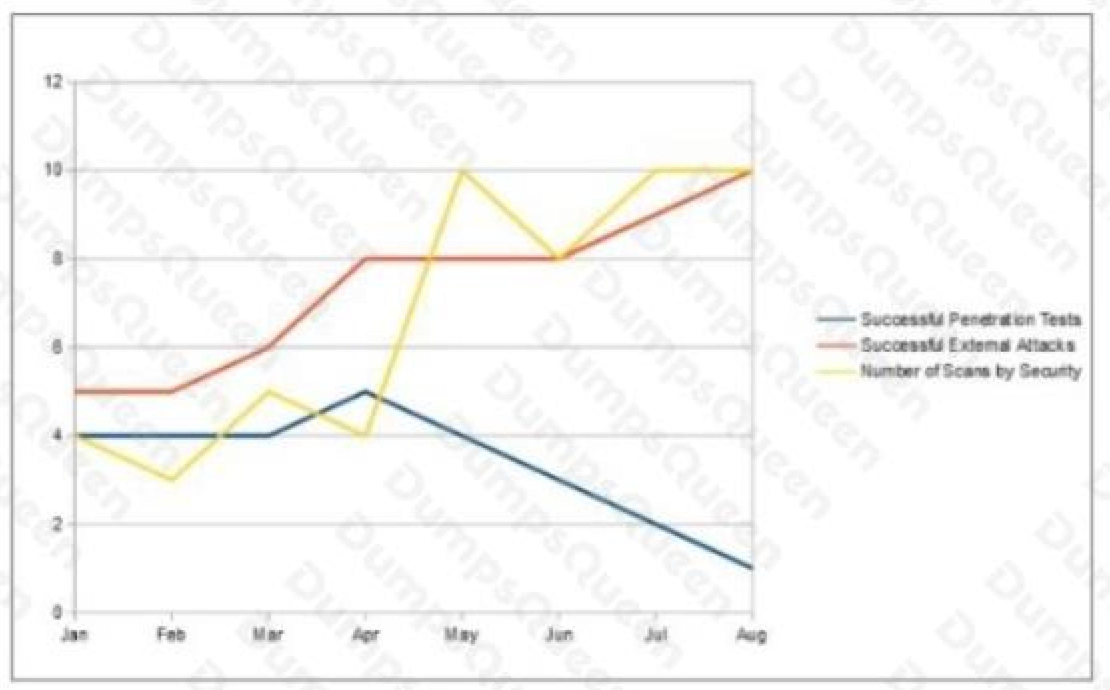
C. Inventory offline databases

D. Actively identify new servers

ANSWER: D

QUESTION NO: 4

An organization has implemented a control for penetration testing and red team exercises conducted on their network. They have compiled metrics showing the success of the penetration testing (Penetration Tests), as well as the number of actual adversary attacks they have sustained (External Attacks). Assess the metrics below and determine the appropriate interpretation with respect to this control.



A. The blue team is adequately protecting the network

B. There are too many internal penetration tests being conducted

C. The methods the red team is using are not effectively testing the network

D. The red team is improving their capability to measure network security

ANSWER: C

QUESTION NO: 5

An organization has implemented a control for Controlled Use of Administrative Privilege. The control requires users to enter a password from their own user account before being allowed elevated privileges, and that no client applications (e.g. web browsers, e-mail clients) can be run with elevated privileges. Which of the following actions will validate this control is implemented properly?

A. Check the log entries to match privilege use with access from authorized users.

B. Run a script at intervals to identify processes running with administrative privilege.

C. Force the root account to only be accessible from the system console.

ANSWER: B

QUESTION NO: 6

An organization has created a policy that allows software from an approved list of applications to be installed on workstations. Programs not on the list should not be installed. How can the organization best monitor compliance with the policy?

A. Performing regular port scans of workstations on the network

B. Auditing Active Directory and alerting when new accounts are created

C. Creating an IDS signature to alert based on unknown “User-Agent ” strings

D. Comparing system snapshots and alerting when changes are made

ANSWER: C

QUESTION NO: 7

As part of a scheduled network discovery scan, what function should the automated scanning tool perform?

A.
Uninstall listening services that have not been used since the last scheduled scan

B. Compare discovered ports and services to a known baseline to report deviations

C. Alert the incident response team on ports and services added since the last scan

D. Automatically close ports and services not included in the current baseline

ANSWER: B

QUESTION NO: 8

What tool creates visual network topology output and results that can be analyzed by Ndiff to determine if a service or network asset has changed?

A. Ngrep

B. CIS-CAT

C. Netscreen

D. Zenmap

ANSWER: D

QUESTION NO: 9

An organization has implemented a policy to detect and remove malicious software from its network. Which of the following actions is focused on correcting rather than preventing attack?

A. Configuring a firewall to only allow communication to whitelisted hosts and ports

B. Using Network access control to disable communication by hosts with viruses

C. Disabling autorun features on all workstations on the network

D. Training users to recognize potential phishing attempts

ANSWER: B

QUESTION NO: 10

How does an organization's hardware inventory support the control for secure configurations?

A. It provides a list of managed devices that should be secured

B. It provides a list of unauthorized devices on the network

C. It provides the MAC addresses for insecure network adapters

D. It identifies the life cycle of manufacturer support for hardware devices

ANSWER: A