GCIH Q&As

GIAC Certified Incident Handler

Pass GIAC GCIH Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/gcih.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by GIAC Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

Analyze the following command. What will this command do? $ nc -1 -p 443 -e /bin/csh

A. Provide an encrypted login shell to act as a proxy relay

B. Connect to port 443 of a remote host and provide a shell relay

C. Impersonate the HTTPS process and hide it using a shell process

D. Listen on port 443 and return a shell to connecting hosts

Correct Answer: D

When setting up netcat to listen for connections, the "-e" switch indicated which application to launch when a connection is made. The "-l" switch is used to setup netcat as a listener. The "-p" switch indicates which port the service should listen on. The "-t" switch is used to accept incoming telnet connections.

QUESTION 2

Adam works as a Security Administrator for Umbrella Inc. A project has been assigned to him to test the network security of the company. He created a webpage to discuss the progress of the tests with employees who were interested in

following the test. Visitors were allowed to click on a company\\'s icon to mark the progress of the test. Adam successfully embeds a keylogger. He also added some statistics on the webpage. The firewall protects the network well and allows

strict Internet access.

How was security compromised and how did the firewall respond?

A. The attack was social engineering and the firewall did not detect it.

B. Security was not compromised as the webpage was hosted internally.

C. The attack was Cross Site Scripting and the firewall blocked it.

D. Security was compromised as keylogger is invisible for firewall.

Correct Answer: A

QUESTION 3

A SOC analyst is reviewing event logs from several network devices across the enterprise and notices that there are an abnormally high number of logon attempts across the desktop systems for several user IDs. What should the analyst do next?

A. The desktop teams should be notified to suspend the accounts of the users and reissue new credentials.

B. An IDS signature should be deployed to monitor the user\\'s logon attempts and alert the SOC of new failures.

C. Each device should be examined for any successful logon attempts within the past 24 hours.

D. An event ticket should be created and escalated to the security team to investigate the attempts.

Correct Answer: D

The front line team in the SOC should have the authority to escalate any events that meet the criteria of a security issue to the responsive team. By issuing a ticket to the security team, they are logging the events, collecting the information and applying a service level agreement to the primary business group to handle. Failed logon attempts across multiple desktop systems for several users could indicate a manual or automated (virus/worm) attempt to probe common or collected usernames with a dictionary of pass phrases.

QUESTION 4

What is the primary goal of the Eradication phase of handling an incident?

A. Removing all artifacts left by the attacker

B. Getting the compromised machine back into production

C. Determining if an incident has occurred

D. Creating disk images for forensics purposes

Correct Answer: A

QUESTION 5

You have inserted a Trojan on your friend\\'s computer and you want to put it in the startup so that whenever the computer reboots the Trojan will start to run on the startup. Which of the following registry entries will you edit to accomplish the task?

A. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Startup

B. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Auto

C. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices

D. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Start

Correct Answer: C