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.geekcert.com/gcih.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

Canaries help to implement what protective mechanisms in the stack?

A. Availability

B. Confidentiality

C. Secrecy

D. Integrity

Correct Answer: D

When the return pointer gets pushed on the stack, the system calculates a keyed hash of the return pointer. This keyed hash result, known as a canary, will be used later as an integrity check of the return pointer to make sure it hasn\\'t been altered by an attacker.

QUESTION 2

Mark works as a Network Administrator for Perfect Inc. The company has both wired and wireless networks. An attacker attempts to keep legitimate users from accessing services that they require. Mark uses IDS/IPS sensors on the wired network to mitigate the attack. Which of the following attacks best describes the attacker\\'s intentions?

A. Internal attack

B. Reconnaissance attack

C. Land attack

D. DoS attack

Correct Answer: D

QUESTION 3

A company is running a Windows network segment with Windows 8 for its users and wants to do a statistical analysis of the workstations to help detect malware. What would be a good way to accomplish this?

A. Use Kansa to grab and sort selected settings across the network

B. Utilize LINReS to pull information and compare information from machines

C. Get the application proxy to give reports on the usage from individual systems

D. Install Redline on all systems and use the report function

Correct Answer: A

Kansa is a good tool that uses Powershell 3.0 or later to pull information across many hosts, and has good statistical tools built in. Powershell 3.0 or later is in Windows 8 and later already.

QUESTION 4

Which of the following is the difference between SSL and S-HTTP?

A. SSL operates at the application layer and S-HTTP operates at the network layer.

B. SSL operates at the application layer and S-HTTP operates at the transport layer.

C. SSL operates at the network layer and S-HTTP operates at the application layer.

D. SSL operates at the transport layer and S-HTTP operates at the application layer.

Correct Answer: D

QUESTION 5

Which of the following statements describes the data below from volatility\\'s pstree plugin?

Name	PID	PPID	Thread	Handle	Time
0xffffa100d5f7f300:winlogon.exe	560	456	4	0	2020-04-10 16:29:41 UTC+0000
. 0xffffa100d5d9b580:userinit.exe	3444	560	0	------	2020-04-10 16:30:14 UTC+0000
.. 0xffffa100d5dad580:explorer.exe	3428	3444	64	0	2020-04-10 16:30:14 UTC+0000
... 0xffffa100d6bbc580:chrmstp.exe	3584	3428	0	------	2020-04-10 16:30:19 UTC+0000
... 0xffffa100d4ae8580:firefox.exe	4952	3428	0	------	2020-04-10 16:37:17 UTC+0000
.... 0xffffa100d4b30580:firefox.exe	5488	4952	0	------	2020-04-10 16:37:17 UTC+0000
... 0xffffa100d4ef3580:cmd.exe	2980	3428	1	0	2020-04-10 17:21:14 UTC+0000
.... 0xffffa100d826a580:powershell.exe	4564	2980	14	0	2020-04-10 17:21:14 UTC+0000
.... 0xffffa100d824e3c0:conhost.exe	1180	2980	3	0	2020-04-10 17:21:14 UTC+0000
... 0xffffa100d6e87080:MSASCuiL.exe	4776	3428	1	0	2020-04-10 16:30:40 UTC+0000
... 0xffffa100d6f19580:OneDrive.exe	4032	3428	19	0	2020-04-10 16:30:40 UTC+0000
... 0xffffa100d4e2f580:cmd.exe	4700	3428	0	------	2020-04-10 16:46:25 UTC+0000
... 0xffffa100d6f76580:notepad.exe	4300	3428	0	------	2020-04-10 16:36:12 UTC+0000

A. Cmd.exe was the child process of OneDrive.exe

B. Chrmstp.exe was launched by MSASCuiL.exe

C. Explorer.exe was the parent process for firefox.exe

D. Notepad.exe was launched with Administrative privileges

Correct Answer: B