Free Questions for SY0-601 by ebraindumps

Shared by Rowe on 29-01-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

A company is expanding its threat surface program and allowing individuals to security test the company's internet-facing application. The company will compensate researchers based on the vulnerabilities discovered. Which of the following best describes the program the company is setting up?

Options:

A- Open-source intelligence

B- Bug bounty

C- Red team

D- Penetration testing

Answer:

B

Explanation:

A program that allows individuals to security test the company's internet-facing application and compensates researchers based on the vulnerabilities discovered is best described as a bug bounty program.A bug bounty program is an incentive-based program that rewards ethical hackers for finding and reporting security flaws in software or systems6.

Question 2

Question Type: MultipleChoice

A threat actor used a sophisticated attack to breach a well-known ride-sharing. company. The threat actor posted on social media that this action was in response to the company's treatment of its drivers Which of the following best describes tm type of throat actor?

Options:

A- Nation-slate

B- Hacktivist

C- Organized crime

D- Shadow IT

Answer:

B

Explanation:

A threat actor who used a sophisticated attack to breach a well-known ride-sharing company and posted on social media that this action was in response to the company's treatment of its drivers is most likely a hacktivist.A hacktivist is a person who uses hacking skills to promote a social or political cause, such as human rights, environmentalism, or anti-corporatism5.

Question 3

Question Type: MultipleChoice

Which of the following describes the ability of code to target a hypervisor from inside a guest OS?

Options:

A- Fog computing

B- VM escape

C- Software-defined networking

D- Image forgery

E- Container breakout

Answer:

B

Explanation:

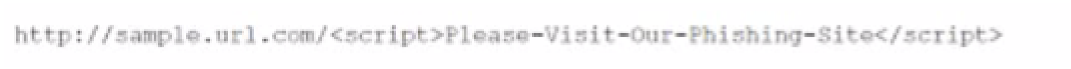
The ability of code to target a hypervisor from inside a guest OS is known as VM escape. This is a serious security threat that can compromise the entire virtualized environment and allow an attacker to access other guest OSes or the host OS.VM escape can be achieved by exploiting vulnerabilities in the hypervisor software, the guest OS, or the virtual hardware devices4.

Question 4

Question Type: MultipleChoice

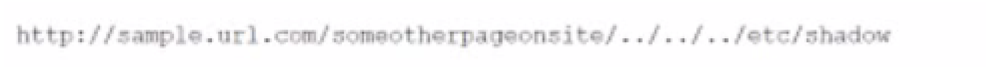
A cybersecurity analyst reviews the log files from a web server end sees a series of files that indicate a directory traversal attack has occurred Which of the following is the analyst most likely seeing?

A.



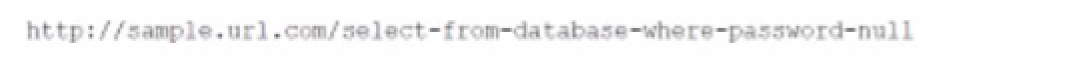
```
http://sample.url.com/<script>Please-Visit-Our-Phishing-Site</script>
```

B.



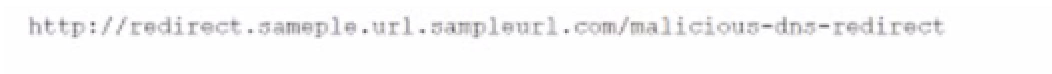
```
http://sample.url.com/someotherpageonsite/../../../etc/shadow
```

C.



```
http://sample.url.com/select-from-database-where-password-null
```

D.



```
http://redirect.sameple.url.sampleurl.com/malicious-dns-redirect
```

Options:

A- Option A

B- Option B

C- Option C

D- Option D

Answer:

C

Explanation:

The log files show that the attacker was able to access files and directories that were not intended to be accessible by web users, such as "/etc/passwd" and "/var/log". This indicates that the attacker was able to exploit a vulnerability in the web server or application that allowed them to manipulate the file path and access arbitrary files on the server.This is a type of attack known as directory traversal, which can lead to information disclosure, privilege escalation, or remote code execution3.

Question 5

Question Type: **MultipleChoice**

A user's login credentials were recently compromised During the investigation, the security analyst determined the user input credentials into a pop-up window when prompted to confirm the username and password However the trusted website does not use a pop-up for entering user colonials Which of the following attacks occurred?

Options:

A- Cross-site scripting

B- SOL injection

C- DNS poisoning

D- Certificate forgery

Answer:

D

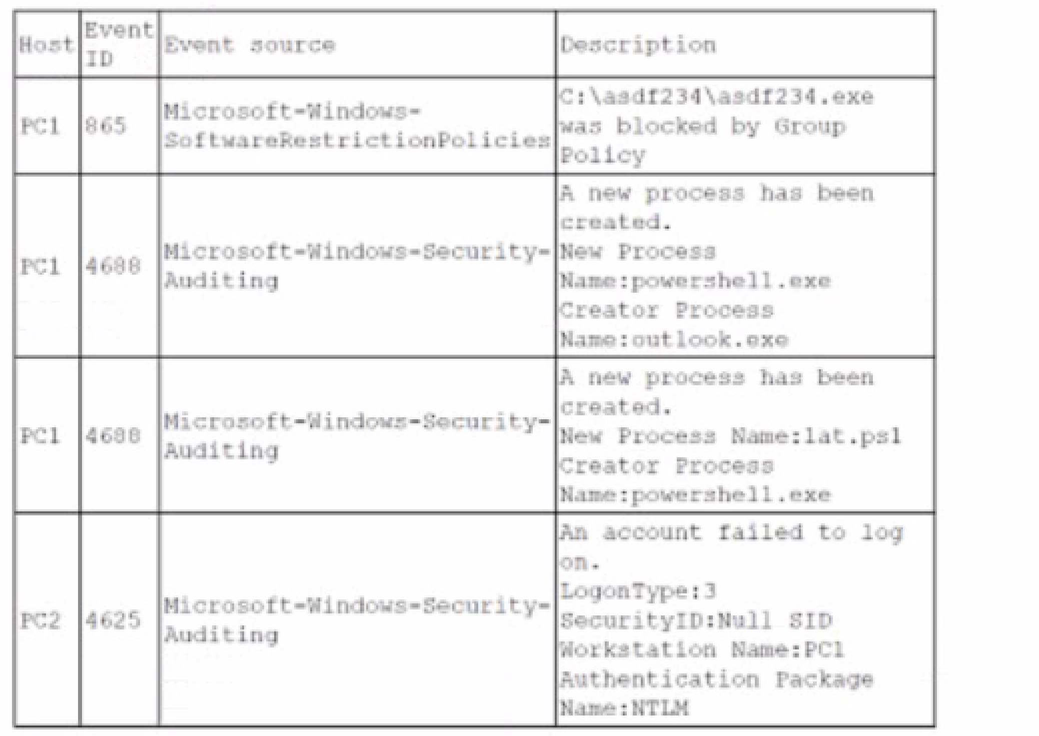
Explanation:

The user input credentials into a pop-up window that was not part of the trusted website. This suggests that the attacker was able to forge a certificate and present a fake website that looked like the legitimate one.This is a type of attack known as certificate forgery, which exploits the trust relationship between users and websites that use SSL/TLS encryption2.

Question 6

Question Type: **MultipleChoice**

A security analyst it investigating an incident to determine what an attacker was able to do on a compromised Laptop. The analyst reviews the following SIEM log:



Host	Event ID	Event source	Description
PC1	865	Microsoft-Windows-SoftwareRestrictionPolicies	C:\asdf234\asdf234.exe was blocked by Group Policy
PC1	4688	Microsoft-Windows-Security-Auditing	A new process has been created. New Process Name:powershell.exe Creator Process Name:outlook.exe
PC1	4688	Microsoft-Windows-Security-Auditing	A new process has been created. New Process Name:lat.ps1 Creator Process Name:powershell.exe
PC2	4625	Microsoft-Windows-Security-Auditing	An account failed to log on. LogonType:3 SecurityID:Null SID Workstation Name:PC1 Authentication Package Name:NTLM

Which of the following describes the method that was used to compromise the laptop?

Options:

A- An attacker was able to move laterally from PC 1 to PC2 using a pass-the-hash attach

B- An attacker was able to bypass the application approve list by emailing a spreadsheet. attachment with an embedded PowerShell in the file.

C- An attacker was able to install malware to the CAasdf234 folder and use it to gain administrator rights and launch Outlook

D- An attacker was able to phish user credentials successfully from an Outlook user profile

Answer:

B

Explanation:

The SIEM log shows that the user opened an email attachment named "Invoice.xlsx" and then executed a PowerShell script that downloaded and ran a malicious file from a remote server. This indicates that the attacker was able to bypass the application approve list by emailing a spreadsheet attachment with an embedded PowerShell in the file.This is a common technique used by malware authors to evade detection and deliver their payloads1.

Question 7

Question Type: MultipleChoice

Which of the following is the correct order of volatility from most to least volatile?

Options:

A- Memory, temporary filesystems. routing tables, disk, network storage

B- Cache, memory, temporary filesystems. disk, archival media

C- Memory, disk, temporary filesystems. cache, archival media

D- Cache, disk, temporary filesystems. network storage, archival media

Answer:

B

Explanation:

The order of volatility is the order of how quickly data can be lost or changed in a system. The order of volatility is important for digital forensics and evidence collection, as it determines the priority and sequence of data preservation. The correct order of volatility from most to least volatile is cache, memory, temporary filesystems, disk, archival media. Cache is the fastest and most volatile type of memory that stores frequently used data. Memory is the main memory or RAM that stores data for active processes. Temporary filesystems are files that are created and deleted during normal system operations, such as swap files, print spool files, etc. Disk is the permanent storage device that stores data on magnetic or solid-state media. Archival media are devices that store data for long-term preservation, such as optical disks, tapes, etc.