CySA+ Final review part 1

Updated 6-21-22

Question 18

A security analyst has received reports of very slow, intermittent access to a public-facing corporate server. Suspecting the system may be compromised, the analyst runs the following commands:

```
[root@www18 /tmp]# uptime
19:23:35 up 2:33, 1 user, load average: 87.22, 79.69, 72.17
[root@www18 /tmp]# crontab -1
* * * * * /tmp/.t/t
[root@www18 /tmp]# ps ax | grep tmp
1325 ? Ss 0:00          /tmp/.t/t
[root@www18 /tmp]# netstat -anlp
tcp 0   0   0.0.0.0:22      172.168.0.0:* ESTABLISHED 1204/sshd
tcp 0   0   127.0.0.1:631   0.0.0.0:*     LISTEN      1214/cupsd
tcp 0   0   0.0.0.0:443     0.0.0.0:*     LISTEN      1267/httpd
```

Based on the output from the above commands, which of the following should the analyst do NEXT to further the investigation?

A. Run crontab -r; rm -rf /tmp/.t to remove and disable the malware on the system.

B. Examine the server logs for further indicators of compromise of a web application.

C. Run kill -9 1325 to bring the load average down so the server is usable again.

D. Perform a binary analysis on the /tmp/.t/t file, as it is likely to be a rogue SSHD server.

Crontab

> You can detect unexpected scheduled tasks in Linux by checking cron. You can check crontab itself by using `cat /etc/crontab`, but you may also want to check `/etc/cron` for anything stashed there. Listing cron jobs is easy as well; use the `crontab -l` command to do so. You should pay particular attention to jobs running as root or equivalent users, and using the `-u` root flag in your crontab list command will do that.

20. Jumpbox

Question #20 *Topic 1*

While planning segmentation for an ICS environment, a security engineer determines IT resources will need access to devices within the ICS environment without compromising security.
To provide the MOST secure access model in this scenario, the jumpbox should be _____.

A. placed in an isolated network segment, authenticated on the IT side, and forwarded into the ICS network.

B. placed on the ICS network with a static firewall rule that allows IT network resources to authenticate.

C. bridged between the IT and operational technology networks to allow authenticated access.

D. placed on the IT side of the network, authenticated, and tunneled into the ICS environment.

Correct Answer: *A*

22. The grep command

Question #22 *Topic 1*

A security analyst is reviewing the logs from an internal chat server. The chat.log file is too large to review manually, so the analyst wants to create a shorter log file that only includes lines associated with a user demonstrating anomalous activity. Below is a snippet of the log:

```
Line   User       Time             Command                  Result
36570  DEV12      02.01.13.151219  KICK DEV27               OK
36571  JAVASHARK  02.01.13.151255  JOIN #CHATOPS e32kk10     OK
36572  DEV12      02.01.13.151325  PART #CHATOPS            OK
36573  CHATTER14  02.01.13.151327  JOIN';CAT ../etc/config' OK
36574  PYTHONFUN  02.01.13.151330  PRIVMSG DEV99 "?"        OK
36575  DEV99      02.01.13.151358  PRIVMSG PYTHONFUN "OK"   OK
```

Which of the following commands would work BEST to achieve the desired result?

A. grep -v chatter14 chat.log

B. grep -i pythonfun chat.log

C. grep -i javashark chat.log

D. grep -v javashark chat.log

E. grep -v pythonfun chat.log

F. grep -i chatter14 chat.log

Correct Answer: *D*

TABLE 10.1 `grep` flags

`grep` flag	Function
`-c`	Counts the number of occurrences
`-i`	Matches both lower and upper case
`-n`	Shows the matching line and line number
`-v`	Shows all lines that do not match the string
`-r`	Reads all files under each directory recursively
`-e`	When followed by a pattern, uses the pattern for a search (allows multiple patterns)

Regular expressions are also commonly used in `grep` searches to match a more flexible set of entries. Using letters between square brackets will match any of a set of characters, whereas an `*` will match any number occurrences of the previous character. Thus, to match all occurrences of text that matches cysa, cysb, and cysc, you could use the following command:

```
grep "cys[abc]" example.txt
```

`grep` is a powerful tool and is frequently combined with other command-line functions to perform complex searches or to prepare data to feed to other tools.

To send data from one command-line tool to another, you can use a pipe, represented by the `|` symbol. For example, if you `grep` for a string and know that you will see multiple pages of output and want to paginate the output, you can pipe the output of `grep` into the `more` command:

```
grep cysa example.txt | more
```

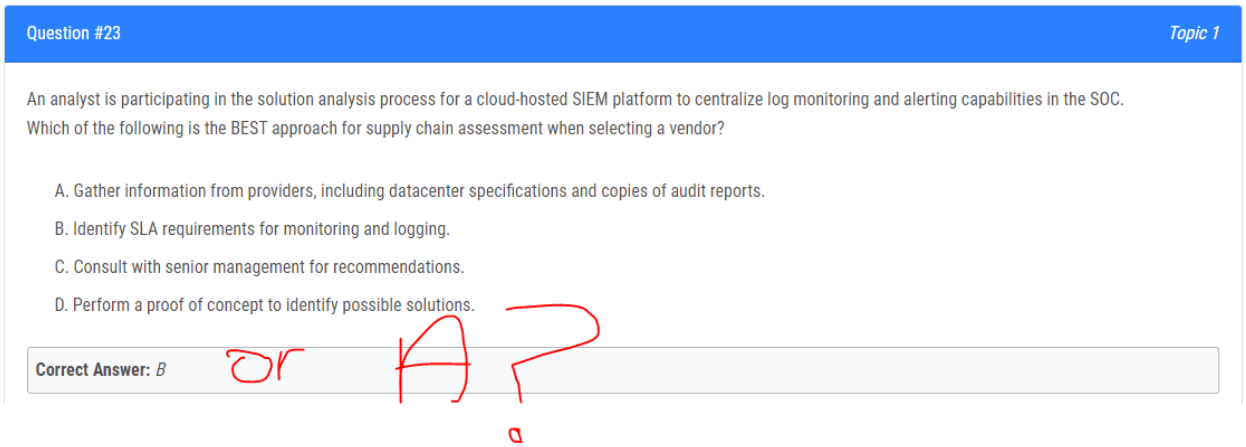
Knowing how to use pipes to combine data from multiple commands is a useful skill for security analysts.

16. Charlene executes the following command against the file shown. What entries will it return?

    ```
    grep -v error /var/log/boot.log
    ```

    1. All lines with the string `"error"` in them
    2. All lines with successful boot messages
    3. All lines without the string `"error"` in them
    4. All lines without successful boot messages

23. ?????



Question #23 *Topic 1*

An analyst is participating in the solution analysis process for a cloud-hosted SIEM platform to centralize log monitoring and alerting capabilities in the SOC. Which of the following is the BEST approach for supply chain assessment when selecting a vendor?

A. Gather information from providers, including datacenter specifications and copies of audit reports.

B. Identify SLA requirements for monitoring and logging.

C. Consult with senior management for recommendations.

D. Perform a proof of concept to identify possible solutions.

Correct Answer: *B*

or A?

29. Credentialed vs. uncredentialed scans

Question #29 *Topic 1*

A security analyst is evaluating two vulnerability management tools for possible use in an organization. The analyst set up each of the tools according to the respective vendor's instructions and generated a report of vulnerabilities that ran against the same target server.

Tool A reported the following:

```
The target host (192.168.10.13) is missing the following patches:
CRITICAL KB50227328: Windows Server 2016 June 2019 Cumulative Update
CRITICAL KB50255293: Windows Server 2016 July 2019 Cumulative Update
HIGH MS19-055: Cumulative Security Update for Edge (2863871)
```

Tool B reported the following:

```
Methods GET HEAD OPTIONS POST TRACE are allowed on 192.168.10.13:80
192.168.10.13:443 uses a self-signed certificate
Apache 4.2.x < 4.2.28 Contains Multiple Vulnerabilities
```

Which of the following BEST describes the method used by each tool? (Choose two.)

A. Tool A is agent based.

B. Tool A used fuzzing logic to test vulnerabilities.

C. Tool A is unauthenticated.

D. Tool B utilized machine learning technology.

E. Tool B is agent based.

F. Tool B is unauthenticated.

Correct Answer: *AF*

Carving

- File carving tools that allow the recovery of files without the filesystem itself available

31. Data carving

Question #31

During an investigation, a security analyst identified machines that are infected with malware the antivirus was unable to detect.
Which of the following is the BEST place to acquire evidence to perform data carving?

A. The system memory

B. The hard drive

C. Network packets

D. The Windows Registry

Correct Answer: *A*
Reference:
https://resources.infosecinstitute.com/memory-forensics/#gref https://www.computerhope.com/jargon/d/data-carving.htm

What is 'fileless' malware?

Fileless malware is a type of malicious software that differs from many other malware threats. Here's why.

Cybercriminals often seek ways to install malicious files on your computer. But a fileless attack doesn't require that. Instead, fileless malware is sneakier in its activation of tools, software and applications that are already built in to your operating system.

That malware then hides in your system.

Fileless malware piggybacks on legitimate scripts by executing malicious activity while the legitimate programs continue to run.

Here's the challenge: Fileless malware can remain undetected because it's memory-based, not file-based.

Antivirus software often works with other types of malware because it detects the traditional "footprints" of a signature.

In contrast, fileless malware leaves no footprints for antivirus products to detect.

32. Automation and orchestration

Question #32

A cybersecurity analyst has access to several threat feeds and wants to organize them while simultaneously comparing intelligence against network traffic. Which of the following would BEST accomplish this goal?

A. Continuous integration and deployment

B. Automation and orchestration

C. Static and dynamic analysis

D. Information sharing and analysis

Correct Answer: *C*

111. B. A SOAR (Security Orchestration, Automation, and Response) tool is focused on exactly what Melissa needs to do. While SIEM provides similar functionality, the key differentiator is the breadth of the platforms that SOAR tools can acquire data from, as well as the process automation capabilities they bring. UEBA (user entity behavior analytics) tools focus on behaviors rather than on a broad set of organizational data, and MDR (managed detection response) systems are used to speed up detection, rather than for compliance and orchestration.

190. C. A workflow orchestration tool is designed to automatically configure, manage, and otherwise oversee systems, applications, and services. Scripts can be used to do this but can be overly complex and failure prone. APIs are used to send and receive data from applications or programs. SCAP (Security Content Automation Protocol) isn't used for this type of task.

34. Risk management

Question #34 *Topic 1*

A security analyst is providing a risk assessment for a medical device that will be installed on the corporate network. During the assessment, the analyst discovers the device has an embedded operating system that will be at the end of its life in two years. Due to the criticality of the device, the security committee makes a risk-based policy decision to review and enforce the vendor upgrade before the end of life is reached.
Which of the following risk actions has the security committee taken?

A. Risk exception
B. Risk avoidance
C. Risk tolerance
D. Risk acceptance

Correct Answer: *D*

35. Limit communication

Question #35

During a cyber incident, which of the following is the BEST course of action?

A. Switch to using a pre-approved, secure, third-party communication system.
B. Keep the entire company informed to ensure transparency and integrity during the incident.
C. Restrict customer communication until the severity of the breach is confirmed.
D. Limit communications to pre-authorized parties to ensure response efforts remain confidential.

Correct Answer: *D*

38. Ip Restrictions

Question #38 *Topic 1*

A security team wants to make SaaS solutions accessible from only the corporate campus.
Which of the following would BEST accomplish this goal?

A. Geofencing
B. IP restrictions
C. Reverse proxy
D. Single sign-on

Correct Answer: *A*
Reference:
https://bluedot.io/library/what-is-geofencing/

41. VLAN

Question #41 *Topic 1*

A security analyst is building a malware analysis lab. The analyst wants to ensure malicious applications are not capable of escaping the virtual machines and pivoting to other networks.
To BEST mitigate this risk, the analyst should use _____.

A. an 802.11ac wireless bridge to create an air gap.
B. a managed switch to segment the lab into a separate VLAN.
C. a firewall to isolate the lab network from all other networks.
D. an unmanaged switch to segment the environments from one another.

Correct Answer: *B*

42. Custom malware

Question #42 *Topic 1*

A security analyst for a large financial institution is creating a threat model for a specific threat actor that is likely targeting an organization's financial assets.
Which of the following is the BEST example of the level of sophistication this threat actor is using?

A. Social media accounts attributed to the threat actor
B. Custom malware attributed to the threat actor from prior attacks
C. Email addresses and phone numbers tied to the threat actor
D. Network assets used in previous attacks attributed to the threat actor
E. IP addresses used by the threat actor for command and control

Correct Answer: *D*

43. Comparability mode

Question #43 *Topic 1*

Bootloader malware was recently discovered on several company workstations. All the workstations run Windows and are current models with UEFI capability. Which of the following UEFI settings is the MOST likely cause of the infections?

A. Compatibility mode

B. Secure boot mode

C. Native mode

D. Fast boot mode

Correct Answer: *A*

What is compatibility mode in BIOS?

Many computers with UEFI firmware will allow you to enable a legacy BIOS compatibility mode. In this mode, **the UEFI firmware functions as a standard BIOS instead of UEFI firmware**. This can help improve compatibility with older operating systems that weren't designed with UEFI in mind — Windows 7, for example. Jul 3, 2017

https://www.howtogeek.com › what-you-need-to-know...

What You Need to Know About Using UEFI Instead of the BIOS

45. DST 172.10.3.5

Question #45

During routine monitoring, a security analyst discovers several suspicious websites that are communicating with a local host. The analyst queries for IP 192.168.50.2 for a 24-hour period:

Time	SRC	DST	Domain	Bytes
6/26/19 10:01	192.168.50.2	138.10.2.5	www.wioapsfeje.co	50
6/26/19 11:05	192.168.50.2	138.10.2.5	www.wioapsfeje.co	1000
6/26/19 13:09	192.168.50.2	138.10.25.5	www.wfaojsjfjoe.co	1000
6/26/19 15:13	192.168.50.2	172.10.25.5	www.wfalksdjflse.co	1000
6/26/19 17:17	192.168.50.2	172.10.45.5	www.wsahlfsdjlfe.co	1000
6/26/19 23:45	192.168.50.2	172.10.3.5	ftp.walksdjgfl.co	50000
6/27/19 10:21	192.168.50.2	175.35.20.5	www.whatsmyip.com	25
6/27/19 11:25	192.168.50.2	175.35.20.5	www.whatsmyip.com	25

To further investigate, the analyst should request PCAP for SRC 192.168.50.2 and _____.

A. DST 138.10.2.5.

B. DST 138.10.25.5.

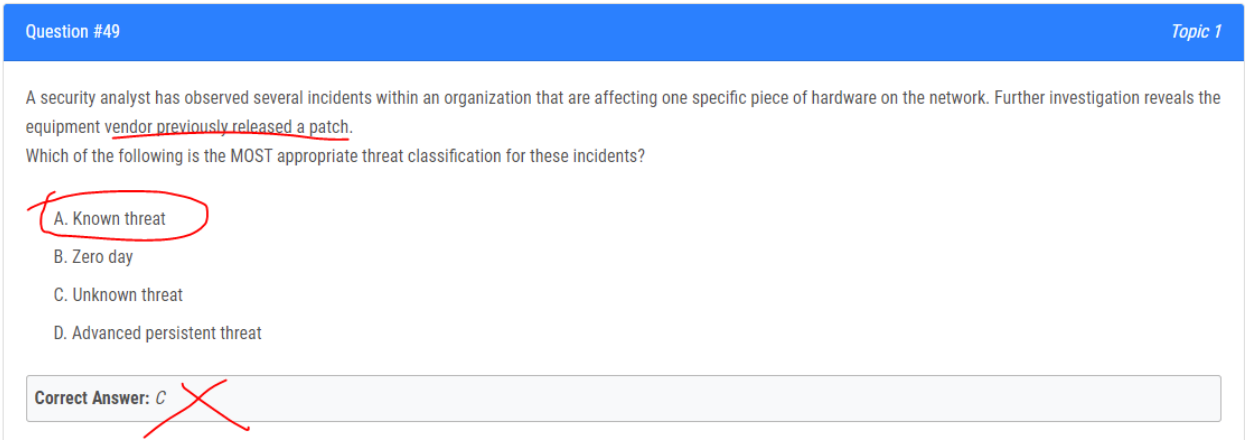
C. DST 172.10.3.5.

D. DST 172.10.45.5.

E. DST 175.35.20.5.

Correct Answer: *C*

49. Known threat



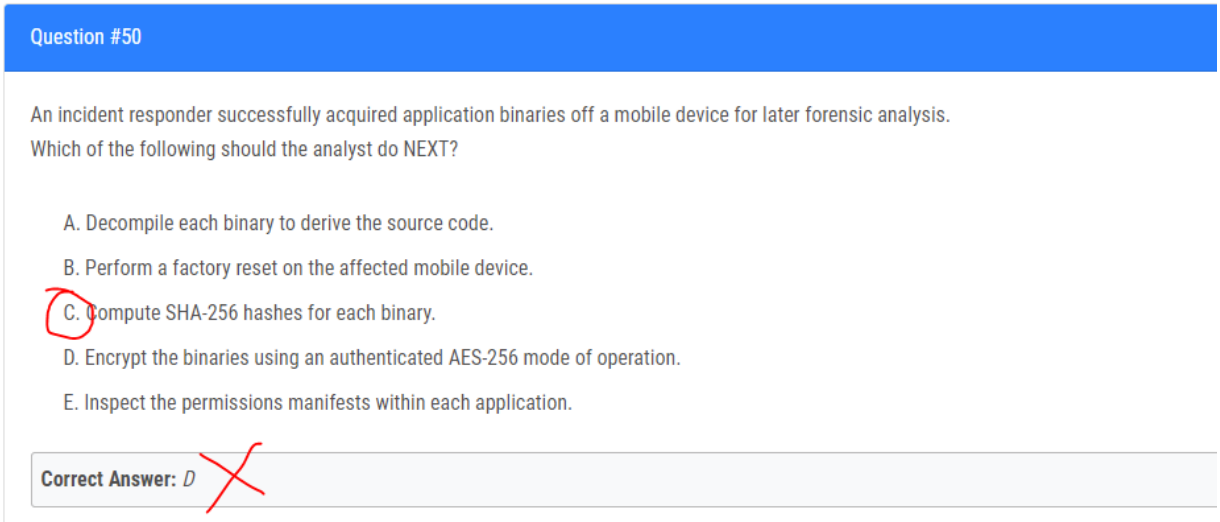
Question #49 — Topic 1

A security analyst has observed several incidents within an organization that are affecting one specific piece of hardware on the network. Further investigation reveals the equipment vendor previously released a patch.
Which of the following is the MOST appropriate threat classification for these incidents?

A. Known threat
B. Zero day
C. Unknown threat
D. Advanced persistent threat

Correct Answer: *C*

50. Hashing



Question #50

An incident responder successfully acquired application binaries off a mobile device for later forensic analysis.
Which of the following should the analyst do NEXT?

A. Decompile each binary to derive the source code.
B. Perform a factory reset on the affected mobile device.
C. Compute SHA-256 hashes for each binary.
D. Encrypt the binaries using an authenticated AES-256 mode of operation.
E. Inspect the permissions manifests within each application.

Correct Answer: *D*

References

https://www.plutora.com/ci-cd-tools/artifacts-management-tools