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: B

QUESTION 31
A security analyst conducted a risk assessment on an organization's wireless network and identified a high-risk element in the implementation of data confidentially protection. Which of the following is the BEST technical security control to mitigate this risk?

A. Switch to RADIUS technology
B. Switch to TACACS+ technology.
C. Switch to 802 IX technology
D. Switch to the WPA2 protocol.

Correct Answer: D

QUESTION 32
A user reports a malware alert to the help desk A technician verifies the alert, determines the workstation is classified as a low-severity device, and uses network controls to block access. The technician then assigns the ticket to a security analyst who will complete the eradication and recovery processes. Which of the following should the security analyst do NEXT?

A. Document the procedures and walk through the incident training guide.
B. Sanitize the workstation and verify countermeasures are restored
C. Reverse engineer the malware to determine its purpose and risk to the organization.
D. Isolate the workstation and issue a new computer to the user.

Correct Answer: B

QUESTION 33
A security team identified some specific known tactics and techniques to help mitigate repeated credential access threats, such as account manipulation and brute forcing. Which of the following frameworks or models did the security team MOST likely use to identify the tactics and techniques'?

A. Kill chain
B. Diamond Model of Intrusion Analysis
C. MITRE ATT&CK
D. ITIL

Correct Answer: C
QUESTION 34
A security analyst received a SIEM alert regarding high levels of memory consumption for a critical system. After several attempts to remediate the issue, the system went down. A root

cause analysis revealed a bad actor forced the application to not reclaim memory. This caused the system to be depleted of resources. Which of the following BEST describes this attack?

A. Injection attack
B. Memory corruption
C. Denial of service
D. Array attack

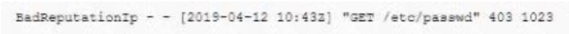
Correct Answer: C

QUESTION 35
Which of the following technologies can be used to house the entropy keys for task encryption on desktops and laptops?

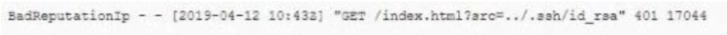
A. Self-encrypting drive
B. Bus encryption
C. TPM
D. HSM

Correct Answer: A

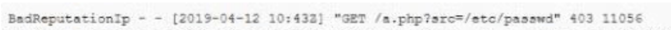
QUESTION 36
During an incident, a cybersecurity analyst found several entries in the web server logs that are related to an IP with a bad reputation . Which of the following would cause the analyst to further review the incident?

A.


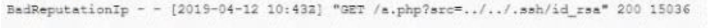
```
BadReputationIp - - [2019-04-12 10:43Z] "GET /etc/passwd" 403 1023
```

B.


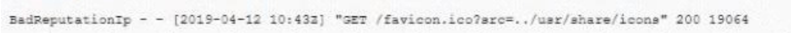
```
BadReputationIp - - [2019-04-12 10:43Z] "GET /index.html?src=../.ssh/id_rsa" 401 17044
```

C.


```
BadReputationIp - - [2019-04-12 10:43Z] "GET /a.php?src=/etc/passwd" 403 11056
```

D.


```
BadReputationIp - - [2019-04-12 10:43Z] "GET /a.php?src=../../.ssh/id_rsa" 200 15036
```

E.


```
BadReputationIp - - [2019-04-12 10:43Z] "GET /favicon.ico?src=../usr/share/icons" 200 19064
```

Correct Answer: D

QUESTION 37
The inability to do remote updates of certificates. keys software and firmware is a security issue commonly associated with:

A. web servers on private networks.
B. HVAC control systems
C. smartphones
D. firewalls and UTM devices

Correct Answer: B

QUESTION 38
A security analyst is handling an incident in which ransomware has encrypted the disks of several company workstations. Which of the following would work BEST to prevent this type of Incident in

the future?

A. Implement a UTM instead of a stateful firewall and enable gateway antivirus.
B. Back up the workstations to facilitate recovery and create a gold Image.
C. Establish a ransomware awareness program and implement secure and verifiable backups.
D. Virtualize all the endpoints with dairy snapshots of the virtual machines.

Correct Answer: C

QUESTION 39
A human resources employee sends out a mass email to all employees that contains their personnel records. A security analyst is called in to address the concern of the human resources director on how to prevent this from happening in the future. Which of the following would be the BEST solution to recommend to the director?

A. Install a data loss prevention system, and train human resources employees on its use. Provide PII training to all employees at the company. Encrypt PII information.
B. Enforce encryption on all emails sent within the company. Create a PII program and policy on how to handle datA. Train all human resources employees.
C. Train all employees. Encrypt data sent on the company network. Bring in privacy personnel to present a plan on how PII should be handled.
D. Install specific equipment to create a human resources policy that protects PII datA. Train company employees on how to handle PII datA. Outsource all PII to another company. Send the human resources director to training for PII handling.

Correct Answer: A

QUESTION 40
A forensic analyst took an image of a workstation that was involved in an incident To BEST ensure the image is not tampered with me analyst should use:

A. hashing
B. backup tapes
C. a legal hold
D. chain of custody.

Correct Answer: A

QUESTION 41
Which of the following technologies can be used to store digital certificates and is typically used in highsecurity implementations where integrity is paramount?

A. HSM
B. eFuse
C. UEFI
D. Self-encrypting drive

Correct Answer: A

QUESTION 42

The threat intelligence department recently learned of an advanced persistent threat that is leveraging a new strain of malware, exploiting a system router. The company currently uses the same device mentioned in the threat report. Which of the following configuration changes would BEST improve the organization's security posture?

A. Implement an IPS rule that contains content for the malware variant and patch the routers to protect against the vulnerability
B. Implement an IDS rule that contains the IP addresses from the advanced persistent threat and patch the routers to protect against the vulnerability
C. Implement an IPS rule that contains the IP addresses from the advanced persistent threat and patch the routers to protect against the vulnerability
D. Implement an IDS rule that contains content for the malware variant and patch the routers to protect against the vulnerability

Correct Answer: A

QUESTION 43
During a review of vulnerability scan results an analyst determines the results may be flawed because a control-baseline system which is used to evaluate a scanning tools effectiveness was reported as not vulnerable. Consequently, the analyst verifies the scope of the scan included the control-baseline host which was available on the network during the scan. The use of a control-baseline endpoint in this scenario assists the analyst in confirming.

A. verification of mitigation
B. false positives
C. false negatives
D. the criticality index
E. hardening validation.

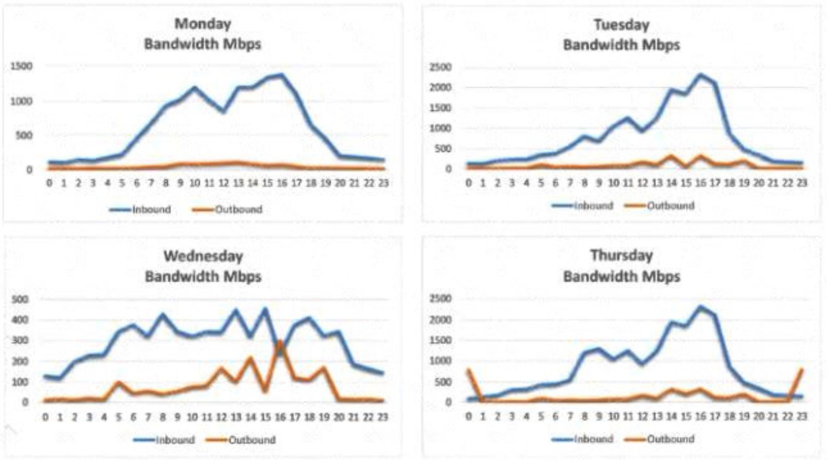
Correct Answer: A

QUESTION 44
A Chief Security Officer (CSO) is working on the communication requirements (or an organization's incident response plan. In addition to technical response activities, which of the following is the main reason why communication must be addressed in an effective incident response program?

A. Public relations must receive information promptly in order to notify the community.
B. Improper communications can create unnecessary complexity and delay response actions.
C. Organizational personnel must only interact with trusted members of the law enforcement community.
D. Senior leadership should act as the only voice for the incident response team when working with forensics teams.

Correct Answer: B

QUESTION 45
A security analyst is conducting a post-incident log analysis to determine which indicators can be used to detect further occurrences of a data exfiltration incident. The analyst determines backups were not performed during this time and reviews the following:



Which of the following should the analyst review to find out how the data was exfilltrated?

A. Monday's logs
B. Tuesday's logs
C. Wednesday's logs
D. Thursday's logs

Correct Answer: D

QUESTION 46
A security analyst is investigating an incident that appears to have started with SOL injection against a publicly available web application. Which of the following is the FIRST step the analyst should take to prevent future attacks?

A. Modify the IDS rules to have a signature for SQL injection.
B. Take the server offline to prevent continued SQL injection attacks.
C. Create a WAF rule In block mode for SQL injection
D. Ask the developers to implement parameterized SQL queries.

Correct Answer: A

QUESTION 47
A cybersecurity analyst is establishing a threat hunting and intelligence group at a growing organization. Which of the following is a collaborative resource that would MOST likely be used for this purpose?

A. Scrum
B. IoC feeds
C. ISAC
D. VSS scores
Correct Answer: C

QUESTION 48