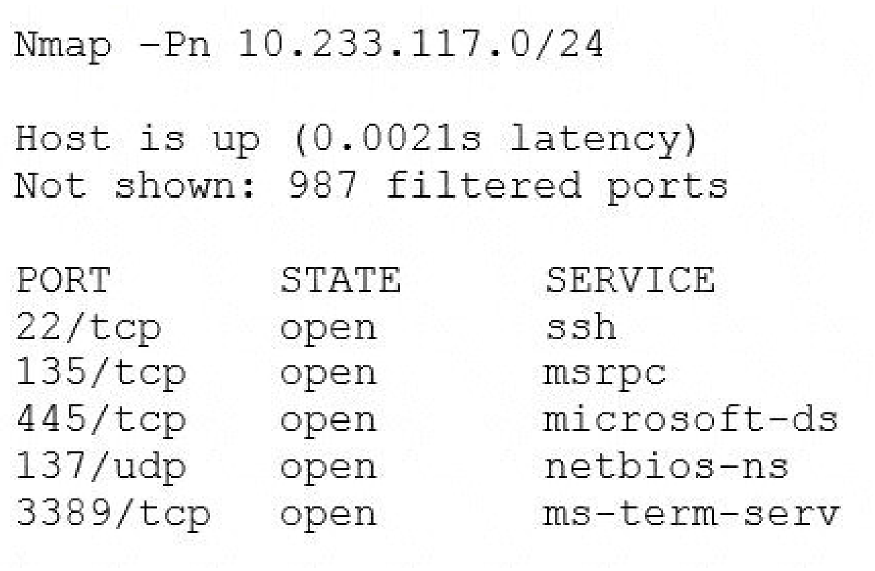
QUESTION 97

A security analyst scanned an internal company subnet and discovered a host with the following Nmap output.



```
Nmap -Pn 10.233.117.0/24

Host is up (0.0021s latency)
Not shown: 987 filtered ports

PORT        STATE      SERVICE
22/tcp      open       ssh
135/tcp     open       msrpc
445/tcp     open       microsoft-ds
137/udp     open       netbios-ns
3389/tcp    open       ms-term-serv
```

Based on the output of this Nmap scan, which of the following should the analyst investigate FIRST?

A. Port 22
B. Port 135
C. Port 445
D. Port 3389

Correct Answer: B

QUESTION 98

A security analyst is generating a list of recommendations for the company's insecure API. Which of the following is the BEST parameter mitigation rec

A. Implement parameterized queries.
B. Use effective authentication and authorization methods.
C. Validate all incoming data.
D. Use TLs for all data exchanges.

Correct Answer: D

QUESTION 99

During an incident response procedure, a security analyst collects a hard drive to analyze a possible vector of compromise. There is a Linux swap partition on the hard drive that needs to be checked. Which of the following should the analyst use to extract human-readable content from the partition?

A. strings
B. head
C. fsstat
D. dd

Correct Answer: A

QUESTION 100
A cybersecurity analyst needs to rearchitect the network using a firewall and a VPN server to achieve the highest level of security. To BEST complete this task, the analyst should place the:

A. firewall behind the VPN server
B. VPN server parallel to the firewall
C. VPN server behind the firewall
D. VPN on the firewall

Correct Answer: C

QUESTION 101
A security analyst suspects a malware infection was caused by a user who downloaded malware after clicking http://<malwaresource>/A.php in a phishing email. To prevent other computers from being infected by the same malware variation, the analyst should create a rule on the.

A. email server that automatically deletes attached executables.
B. IDS to match the malware sample.
C. proxy to block all connections to <malwaresource>.
D. firewall to block connection attempts to dynamic DNS hosts.

Correct Answer: C

QUESTION 102
The SFTP server logs show thousands of failed login attempts from hundreds of IP addresses worldwide. Which of the following controls would BEST protect the service?

A. Whitelisting authorized IP addresses
B. Enforcing more complex password requirements
C. Blacklisting unauthorized IP addresses
D. Establishing a sinkhole service

Correct Answer: C

QUESTION 103
A cybersecurity analyst needs to determine whether a large file named access log from a web server contains the following IoC:

../../../../bin/bash

Which of the following commands can be used to determine if the string is present in the log?

A. echo access.log | grep "../../../../bin/bash"
B. grep "../../../../bin/bash" 1 cat access.log
C. grep "../../../. ./bin/bash" < access.log
D. cat access.log > grep "../../../ ../bin/bash"

Correct Answer: C

QUESTION 104
An audit has revealed an organization is utilizing a large number of servers that are running unsupported operating systems. As part of the management response phase of the audit, which of the following would BEST demonstrate senior management is appropriately aware of and addressing the issue?

A. Copies of prior audits that did not identify the servers as an issue
B. Project plans relating to the replacement of the servers that were approved by management
C. Minutes from meetings in which risk assessment activities addressing the servers were discussed
D. ACLs from perimeter firewalls showing blocked access to the servers
E. Copies of change orders relating to the vulnerable servers

Correct Answer: B

QUESTION 105
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.

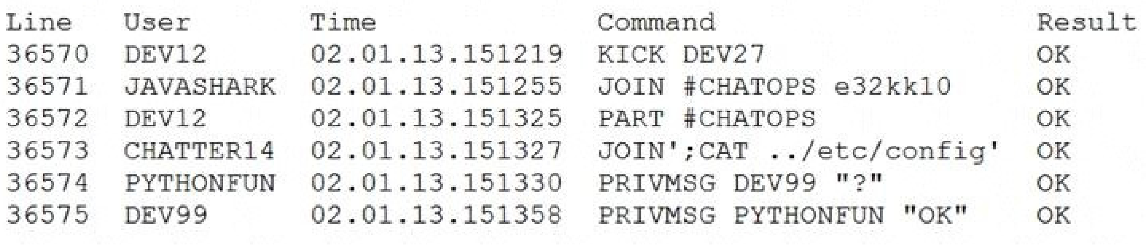
Correct Answer: A

QUESTION 106
A security analyst on the threat-hunting team has developed a list of unneeded, benign services that are currently running as part of the standard OS deployment for workstations. The analyst will provide this list to the operations team to create a policy that will automatically disable the services for all workstations in the organization. Which of the following BEST describes the security analyst's goal?

A. To create a system baseline
B. To reduce the attack surface
C. To optimize system performance
D. To improve malware detection

Correct Answer: B

QUESTION 107
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:



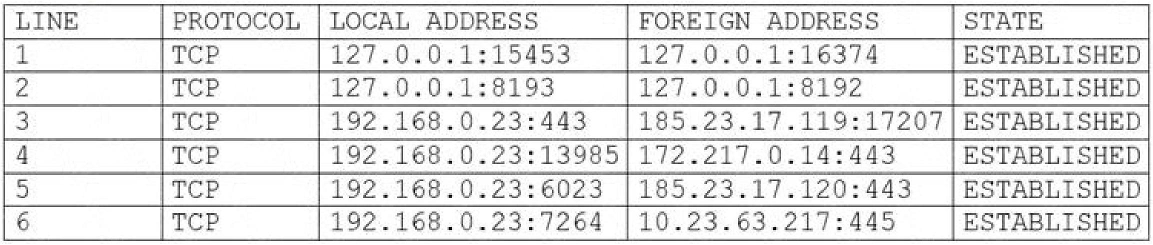
```
Line   User        Time              Command                      Result
36570  DEV12       02.01.13.151219   KICK DEV27                   OK
36571  JAVASHARK   02.01.13.151255   JOIN #CHATOPS e32kk10        OK
36572  DEV12       02.01.13.151325   PART #CHATOPS                OK
36573  CHATTER14   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

QUESTION 108
A user's computer has been running slowly when the user tries to access web pages. A security analyst runs the command netstat -aon from the command line and receives the following output:



LINE	PROTOCOL	LOCAL ADDRESS	FOREIGN ADDRESS	STATE
1	TCP	127.0.0.1:15453	127.0.0.1:16374	ESTABLISHED
2	TCP	127.0.0.1:8193	127.0.0.1:8192	ESTABLISHED
3	TCP	192.168.0.23:443	185.23.17.119:17207	ESTABLISHED
4	TCP	192.168.0.23:13985	172.217.0.14:443	ESTABLISHED
5	TCP	192.168.0.23:6023	185.23.17.120:443	ESTABLISHED
6	TCP	192.168.0.23:7264	10.23.63.217:445	ESTABLISHED

Which of the following lines indicates the computer may be compromised?

A. Line 1
B. Line 2
C. Line 3
D. Line 4
E. Line 5
F. Line 6

Correct Answer: D

QUESTION 109
A company wants to establish a threat-hunting team. Which of the following BEST describes the rationale for integration intelligence into hunt operations?

A. It enables the team to prioritize the focus area and tactics within the company's environment.
B. It provide critically analyses for key enterprise servers and services.
C. It allow analysis to receive updates on newly discovered software vulnerabilities.
D. It supports rapid response and recovery during and followed an incident.

Correct Answer: A

QUESTION 110
A security analyst received a series of antivirus alerts from a workstation segment, and users reported ransomware messages. During lessons-learned activities, the analyst determines the antivirus was able to alert to abnormal behavior but did not stop this newest variant of ransomware. Which of the following actions should be taken to BEST mitigate the effects of this type of threat in the future?

A. Enabling application blacklisting
B. Enabling sandboxing technology
C. Purchasing cyber insurance
D. Installing a firewall between the workstations and Internet

Correct Answer: B

QUESTION 111
A company recently experienced financial fraud, which included shared passwords being compromised and improper levels of access being granted. The company has asked a security analyst to help improve its controls. Which of the following will MOST likely help the security analyst develop better controls?

A. An evidence summarization
B. An indicator of compromise
C. An incident response plan
D. A lessons-learned report

Correct Answer: C

QUESTION 112
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

QUESTION 113
During a routine log review, a security analyst has found the following commands that cannot be identified from the Bash history log on the root user.