

A security analyst reviews the following aggregated output from an Nmap scan and the border firewall ACL:

Server1	Server2	PC1	PC2
22/tcp open	3389/tcp open	80/tcp open	80/tcp open
80/tcp open	53/udp open	443/tcp open	443/tcp open
443/tcp open			1433/tcp open

Firewall ACL

```

10 permit tcp from: any to: server1: www
15 permit udp from: lan-net to: any: dns
16 permit udp from: any to: server2: dns
20 permit tcp from: any to server1: ssl
25 permit tcp from: lan-net to: any: www
26 permit tcp from: lan-net to: any: ssl
27 permit tcp from: any to pc2: mssql
30 permit tcp from: any to server1: ssh
100 deny ip any any

```

Which of the following should the analyst reconfigure to BEST reduce organizational risk while maintaining current functionality?

- A. PC1
- B. PC2
- C. Server1
- D. Server2
- E. Firewall

During an investigation, a security analyst determines suspicious activity occurred during the night shift over the weekend. Further investigation reveals the activity was initiated from an internal IP going to an external website.

Which of the following would be the MOST appropriate recommendation to prevent the activity from happening in the future?

- A. An IPS signature modification for the specific IP addresses
- B. An IDS signature modification for the specific IP addresses
- C. A firewall rule that will block port 80 traffic
- D. A firewall rule that will block traffic from the specific IP addresses

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 -l
* * * * * /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.

A Chief Information Security Officer (CISO) wants to upgrade an organization's security posture by improving proactive activities associated with attacks from internal and external threats.

Which of the following is the MOST proactive tool or technique that feeds incident response capabilities?

- A. Development of a hypothesis as part of threat hunting
- B. Log correlation, monitoring, and automated reporting through a SIEM platform
- C. Continuous compliance monitoring using SCAP dashboards
- D. Quarterly vulnerability scanning using credentialed scans

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.