CS0-002 Q&As

CompTIA Cybersecurity Analyst (CySA+)

Pass CompTIA CS0-002 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/cs0-002.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CompTIA Official Exam Center

QUESTION 1

An analyst is reviewing the following log from the company web server:

```
15.34.24 GET /directory/listening.php?user=admin&pass=admin1
15.34.27 GET /directory/listening.php?user=admin&pass=admin2
15.34.29 GET /directory/listening.php?user=admin&pass=1admin
15.34.35 GET /directory/listening.php?user=admin&pass=2admin
```

Which of the following is this an example of?

A. Online rainbow table attack

B. Offline brute force attack

C. Offline dictionary attack

D. Online hybrid attack

Correct Answer: B

QUESTION 2

SIMULATION

You are a penetration tester who is reviewing the system hardening guidelines for a company. Hardening guidelines indicate the following:

1.

There must be one primary server or service per device.

2.

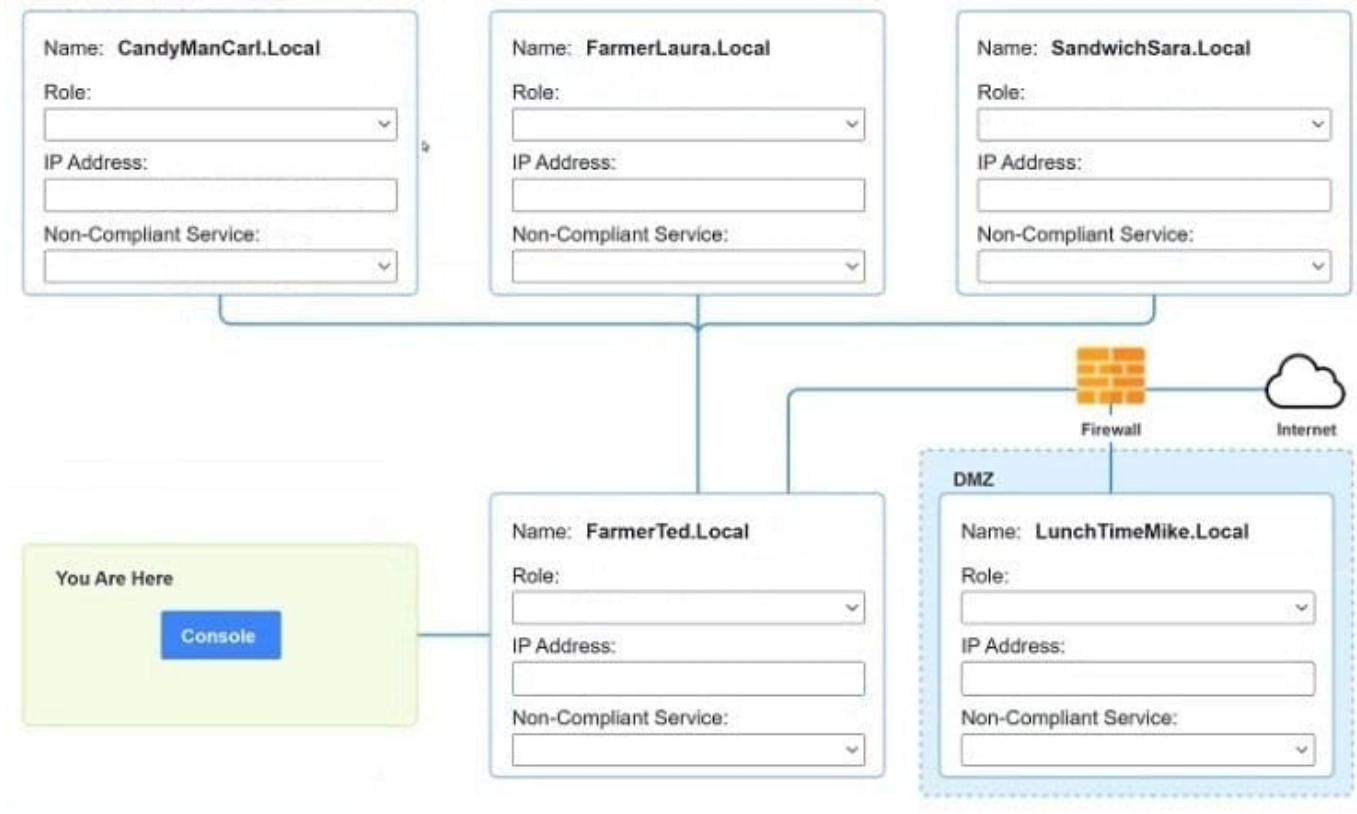
Only default port should be used

3.

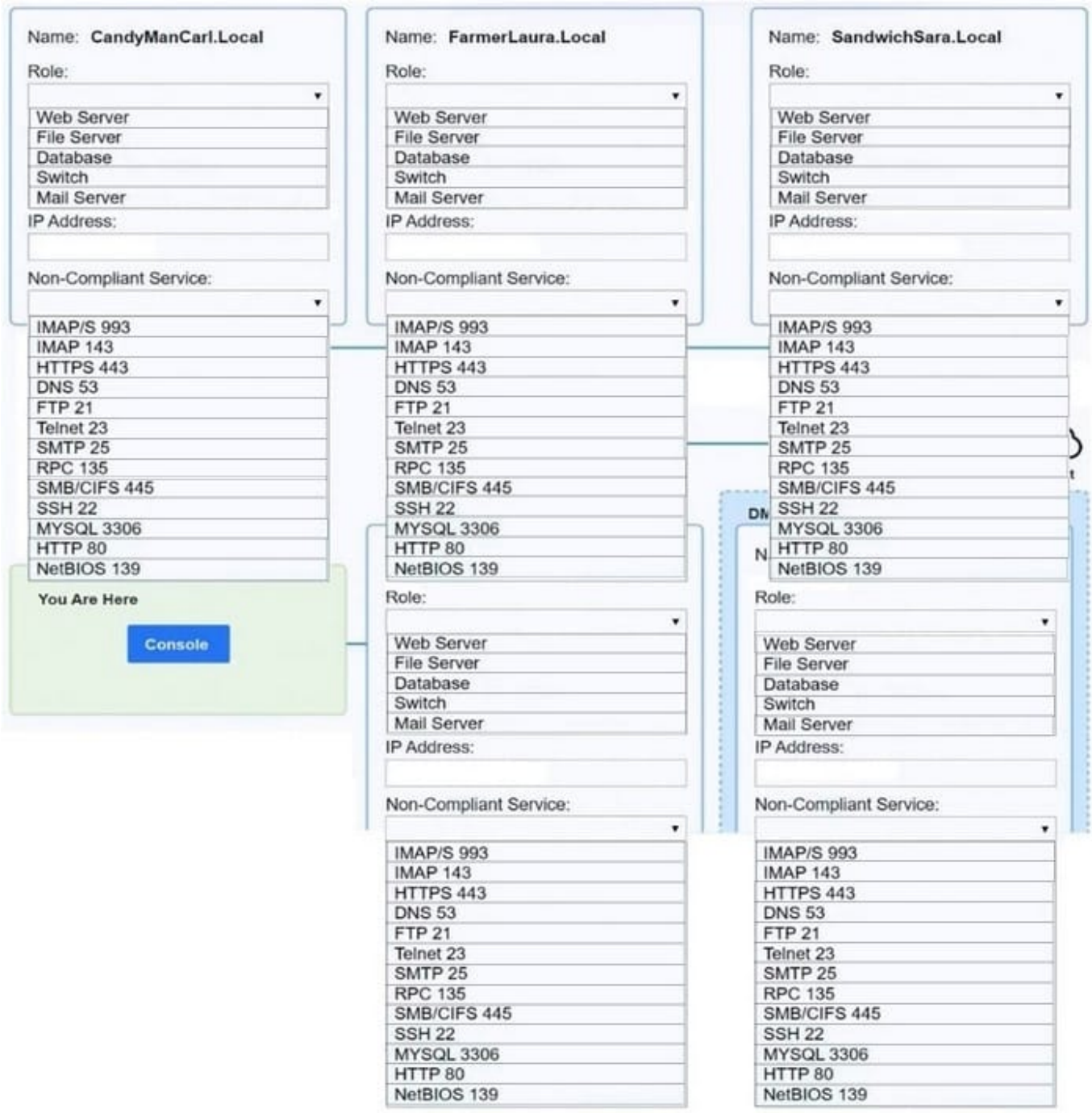
Non- secure protocols should be disabled.

The corporate internet presence should be placed in a protected subnet Instructions :

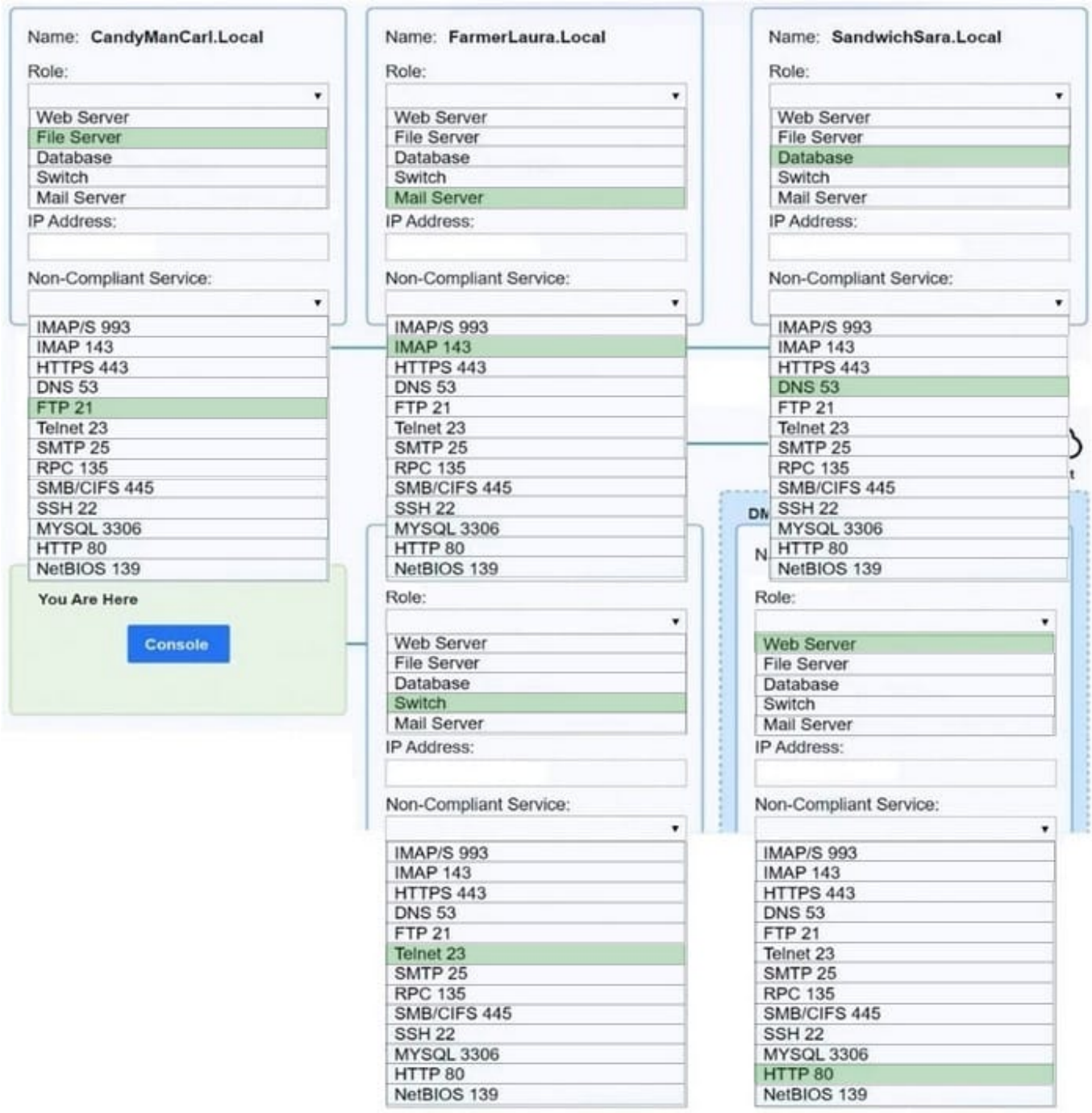
Using the available tools, discover devices on the corporate network and the services running on these devices. You must determine ip address of each device The primary server or service each device The protocols that should be disabled based on the hardening guidelines


Name: CandyManCarl.Local
Role:
IP Address:
Non-Compliant Service:
Name: FarmerLaura.Local
Role:
IP Address:
Non-Compliant Service:
Name: SandwichSara.Local
Role:
IP Address:
Non-Compliant Service:
Firewall
Internet
DMZ
You Are Here
Console
Name: FarmerTed.Local
Role:
IP Address:
Non-Compliant Service:
Name: LunchTimeMike.Local
Role:
IP Address:
Non-Compliant Service:

Hot Area:



Correct Answer:

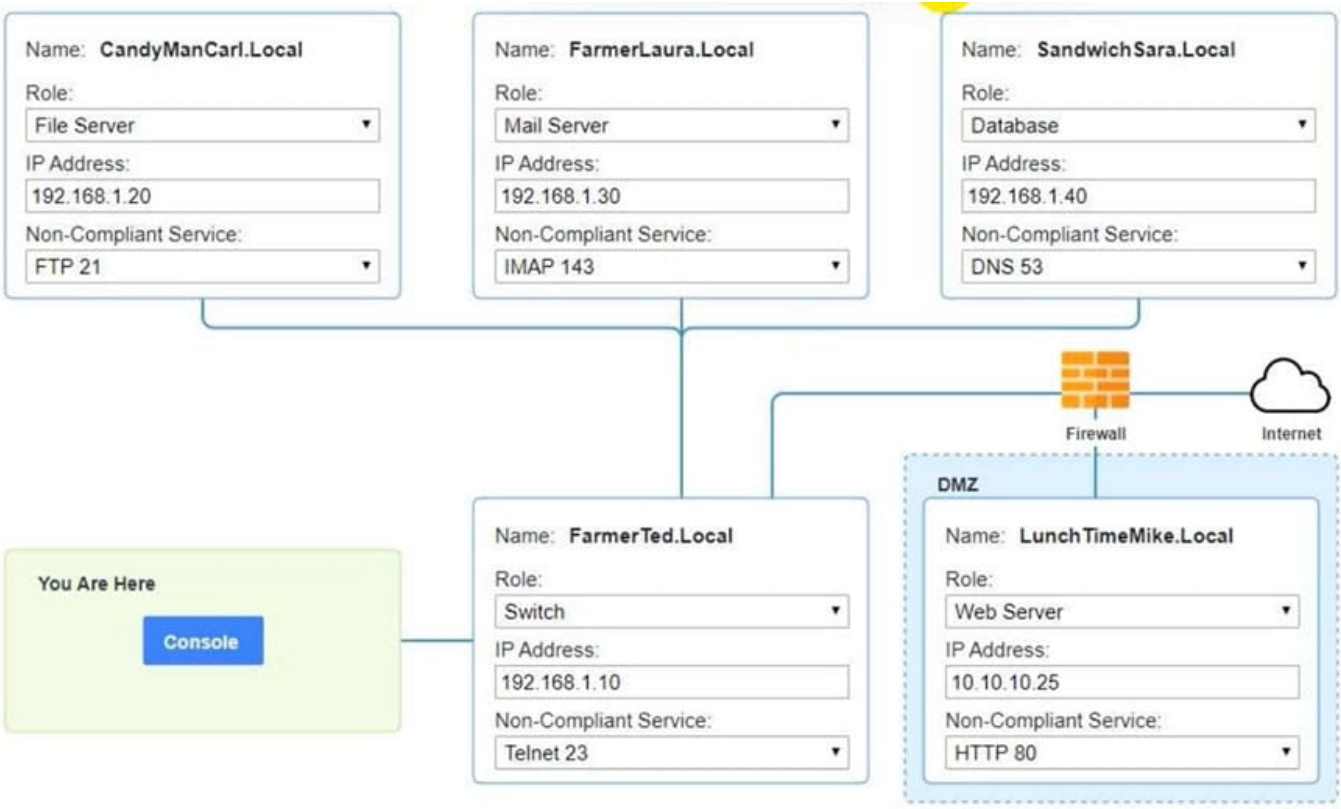


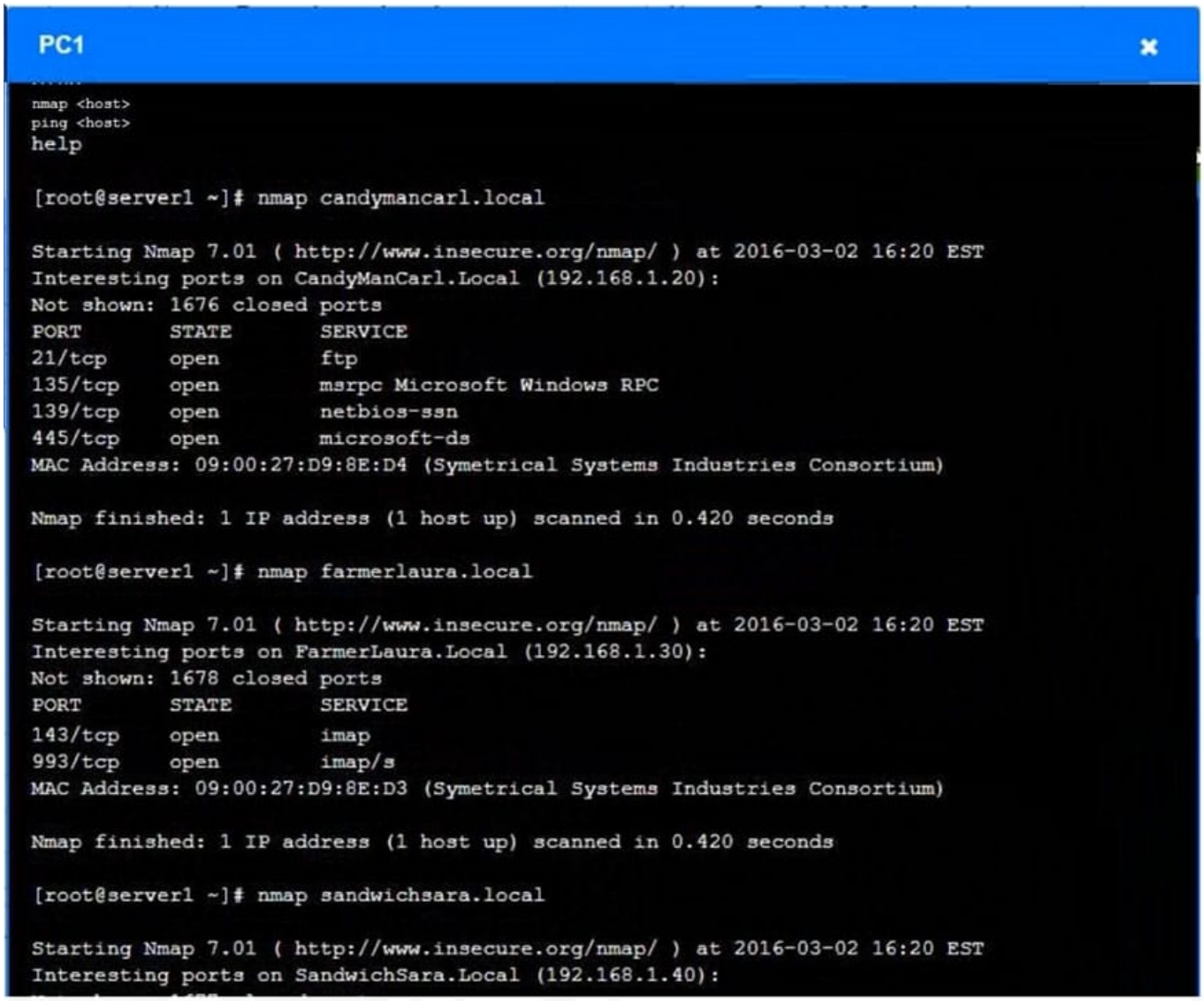
CandyManCarl.Local Role: File Server IP address: 192.168.1.20 Non-Compliant Service: FTP 21 Farmerlaura.Local Role: Mail Server IP address: 192.168.1.30 Non-Compliant Service: IMAP 143

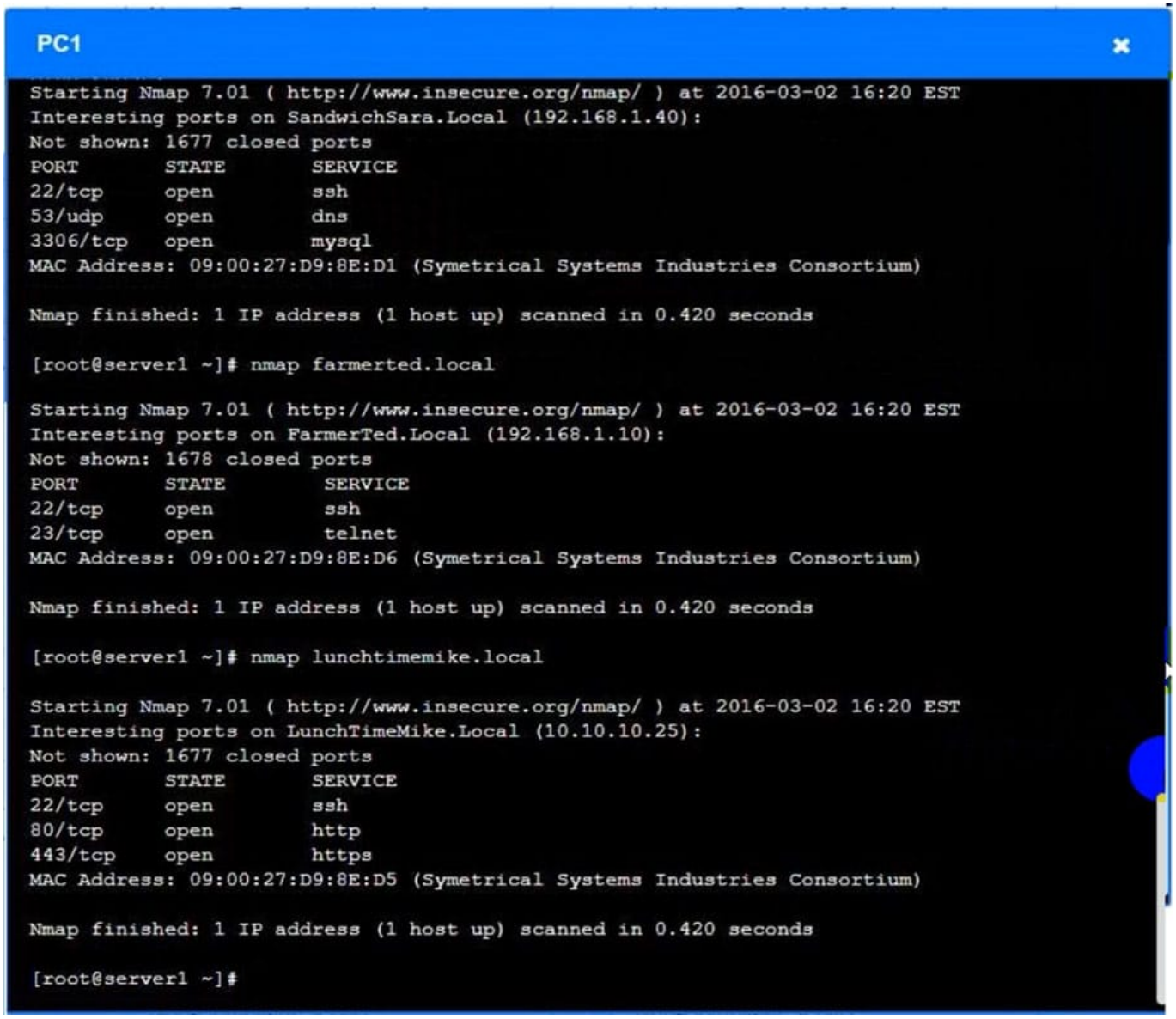
Sandwich $ara.Local Role: Database IP address: 192.168.1.40 Non-Compliant Service: DNS 53

FarmaerTed.Local Role: Switch IP address: 192.168.1.10 Non-Compliant Service: Telnet 23

Lunch TimeMike.Local Role: Web Server IP address: 10.10.10.25 Non-Compliant Service: HTTP 80


Name: CandyManCarl.Local
Role:
File Server
IP Address:
192.168.1.20
Non-Compliant Service:
FTP 21
Name: FarmerLaura.Local
Role:
Mail Server
IP Address:
192.168.1.30
Non-Compliant Service:
IMAP 143
Name: SandwichSara.Local
Role:
Database
IP Address:
192.168.1.40
Non-Compliant Service:
DNS 53
Firewall
Internet
DMZ
You Are Here
Console
Name: FarmerTed.Local
Role:
Switch
IP Address:
192.168.1.10
Non-Compliant Service:
Telnet 23
Name: LunchTimeMike.Local
Role:
Web Server
IP Address:
10.10.10.25
Non-Compliant Service:
HTTP 80


PC1
nmap <host>
ping <host>
help
[root@server1 ~]# nmap candymancarl.local
Starting Nmap 7.01 (http://www.insecure.org/nmap/) at 2016-03-02 16:20 EST
Interesting ports on CandyManCarl.Local (192.168.1.20):
Not shown: 1676 closed ports
PORT STATE SERVICE
21/tcp open ftp
135/tcp open msrpc Microsoft Windows RPC
139/tcp open netbios-ssn
445/tcp open microsoft-ds
MAC Address: 09:00:27:D9:8E:D4 (Symetrical Systems Industries Consortium)
Nmap finished: 1 IP address (1 host up) scanned in 0.420 seconds
[root@server1 ~]# nmap farmerlaura.local
Starting Nmap 7.01 (http://www.insecure.org/nmap/) at 2016-03-02 16:20 EST
Interesting ports on FarmerLaura.Local (192.168.1.30):
Not shown: 1678 closed ports
PORT STATE SERVICE
143/tcp open imap
993/tcp open imap/s
MAC Address: 09:00:27:D9:8E:D3 (Symetrical Systems Industries Consortium)
Nmap finished: 1 IP address (1 host up) scanned in 0.420 seconds
[root@server1 ~]# nmap sandwichsara.local
Starting Nmap 7.01 (http://www.insecure.org/nmap/) at 2016-03-02 16:20 EST
Interesting ports on SandwichSara.Local (192.168.1.40):



QUESTION 3

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 4

An analyst is reviewing the output from some recent network enumeration activities. The following entry relates to a target on the network:

```
Nmap scan report for 10-112-75-1.biz.bhn.net (10.112.75.1)
Host is up (0.046s latency).
Not shown: 97 closed ports
PORT     STATE SERVICE  VERSION
21/tcp   open  ftp      FileZilla ftpd
80/tcp   open  http     Microsoft IIS httpd 7.5
8443/tcp open  ssl/http SonicWALL firewall http config
Device type: broadband router|WAP|general purpose|VoIP phone| storage-misc
Running (JUST GUESSING): Asus embedded (89%), Linux 2.6.X|2.4.X (89%),
OpenBSD 4.X (87%), FreeBSD 5.X (87%), Digium embedded (87%), HP embedded (87%)
OS CPE: cpe:/h:asus:rt-ac66u cpe:/o:linux:linux_kernel:2.6 cpe/h:asus:rt-n16 cpe:/o:linux:linux_kernel:2.4
cpe:/o:openbsd:openbsd:4.3 cpe:/o:freebsd:freebsd:5.4 cpe:/h:digium:d70 cpe:/h:hp:p2000_g3
Aggressive OS guesses: Asus RT-AC66U router (Linux 2.6) (89%), Asus RT-N16 WAP (Linux 2.6) (89%), Asus RT-N66U WAP (Linux 2.6)
(89%), Tomato 1.28 (Linux 2.6.22) (89%), OpenWrt Kamikaze 7.09 (Linux 2.6.22) (89%), OpenWrt 0.9 - 7.09 (Linux 2.4.30 - 2.4.34)
(88%), OpenWrt White Russian 0.9 (Linux 2.4.30) (88%), OpenBSD 4.3 (87%), FreeBSD 5.4-RELEASE (87%), Digium D70 IP phone (87%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Windows; Device: firewall; CPE: cpe:/o:microsoft:windows
```

Based on the above output, which Of the following tools or techniques is MOST likely being used?

A. Web application firewall

B. Port triggering

C. Intrusion prevention system

D. Port isolation

E. Port address translation

Correct Answer: A

Filezilla ftpd and Microsoft IIS httpd 7.5 are running on ports 21 and 80, respectively.

QUESTION 5

An information security analyst discovered a virtual machine server was compromised by an attacker. Which of the following should be the FIRST step to confirm and respond to the incident?

A. Pause the virtual machine,

B. Shut down the virtual machine.

C. Take a snapshot of the virtual machine.

D. Remove the NIC from the virtual machine.

Correct Answer: A

Enumeration is the process of discovering and listing information. Network enumeration is the process of discovering pieces of information that might be helpful in a network attack or compromise. There are several techniques used to perform enumeration and several tools that make the process easier for both testers and attackers. Let\\'s take a look at these techniques and tools.