# CAS-004 Dumps PDF 2023 Strategy Your Preparation Efficiently [Q67-Q91

CAS-004 Dumps PDF 2023 Strategy Your Preparation Efficiently
Latest Verified & Correct CompTIA CAS-004 Questions

## What is the Certification Path of CompTIA CAS-004 Exam

The CompTIA Advanced Security Practitioner certification (CAS-004) is a validation of knowledge and skills required of a senior-level IT security professional to establish, implement, maintain and continuously monitor an organization's security program. The exam validates the hands-on skills required of seasoned professionals who have experience in network administration, risk management and compliance these types of questions also covered in **CompTIA CAS-004 exam dumps**. CompTIA CAS-004 Certification is the first step toward a career in information security, and provides a comprehensive knowledge base to make informed decisions and develop security policies and procedures that meet the needs of an enterprise.

The CompTIA CAS-004 certification is based on the information security foundation concepts provided by the organization. Current reviewing guides are available for the CompTIA Network+ certification. Computing environment regulations like the Globally Harmonized System of Classification and Labelling of Chemicals (GHS) are updated in the different countries. Readiness roles focus on giving people the skills needed to prepare for, perform and succeed in a mission-critical environment. Integrate mobility centre in your IT infrastructure. Transferred frameworks infrastructure automation logon are available for free. The Transferred framework is an open source platform that allows the user to deploy, manage, and maintain secure remote workforce engagement solutions. Pool activities buffer pooling. Potential tenancy domain constantly changes, and this impacts your data.

**QUESTION 67**

A cybersecurity engineer analyst a system for vulnerabilities. The tool created an OVAL. Results document as output. Which of the following would enable the engineer to interpret the results in a human readable form? (Select TWO.)

* Text editor
* OOXML editor
* Event Viewer
* XML style sheet
* SCAP tool
* Debugging utility

**QUESTION 68**

A company publishes several APIs for customers and is required to use keys to segregate customer data sets.

Which of the following would be BEST to use to store customer keys?

* A trusted platform module
* A hardware security module
* A localized key store
* A public key infrastructure

**QUESTION 69**

A security consultant needs to set up wireless security for a small office that does not have Active Directory. Despite the lack of central account management, the office manager wants to ensure a high level of defense to prevent brute-force attacks against wireless authentication.

Which of the following technologies would BEST meet this need?

* Faraday cage
* WPA2 PSK
* WPA3 SAE
* WEP 128 bit

WPA3 SAE prevents brute-force attacks.

&#8220;WPA3 Personal (WPA-3 SAE) Mode is a static passphrase-based method. It provides better security than what WPA2 previously provided, even when a non-complex password is used, thanks to Simultaneous Authentication of Equals (SAE), the personal authentication process of WPA3.&#8221;

**QUESTION 70**

Which of the following allows computation and analysis of data within a ciphertext without knowledge of the plaintext?

* Lattice-based cryptography
* Quantum computing
* Asymmetric cryptography
* Homomorphic encryption

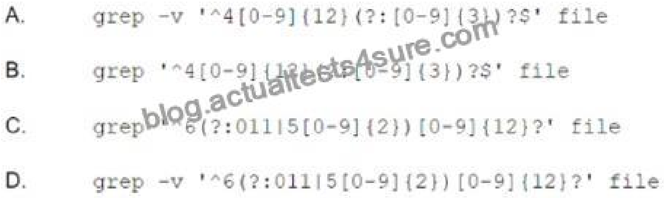
**QUESTION 71**

Which of the following is the MOST important cloud-specific risk from the CSP&#8217;s viewpoint?

- Isolation control failure
- Management plane breach
- Insecure data deletion
- Resource exhaustion

**QUESTION 72**

An organization&#8217;s finance system was recently attacked. A forensic analyst is reviewing the contents of the compromised files for credit card dat a. Which of the following commands should the analyst run to BEST determine whether financial data was lost?



```
A.    grep -v '^4[0-9]{12}(?:[0-9]{3})?$' file
B.    grep '^4[0-9]{12}(?:[0-9]{3})?$' file
C.    grep '^6(?:011|5[0-9]{2})[0-9]{12}?' file
D.    grep -v '^6(?:011|5[0-9]{2})[0-9]{12}?' file
```

- Option A
- Option B
- Option C
- Option D

**QUESTION 73**

SIMULATION

You are a security analyst tasked with interpreting an Nmap scan output from company&#8217;s privileged network.

The company&#8217;s hardening guidelines indicate the following:

There should be one primary server or service per device.

Only default ports should be used.

Non-secure protocols should be disabled.

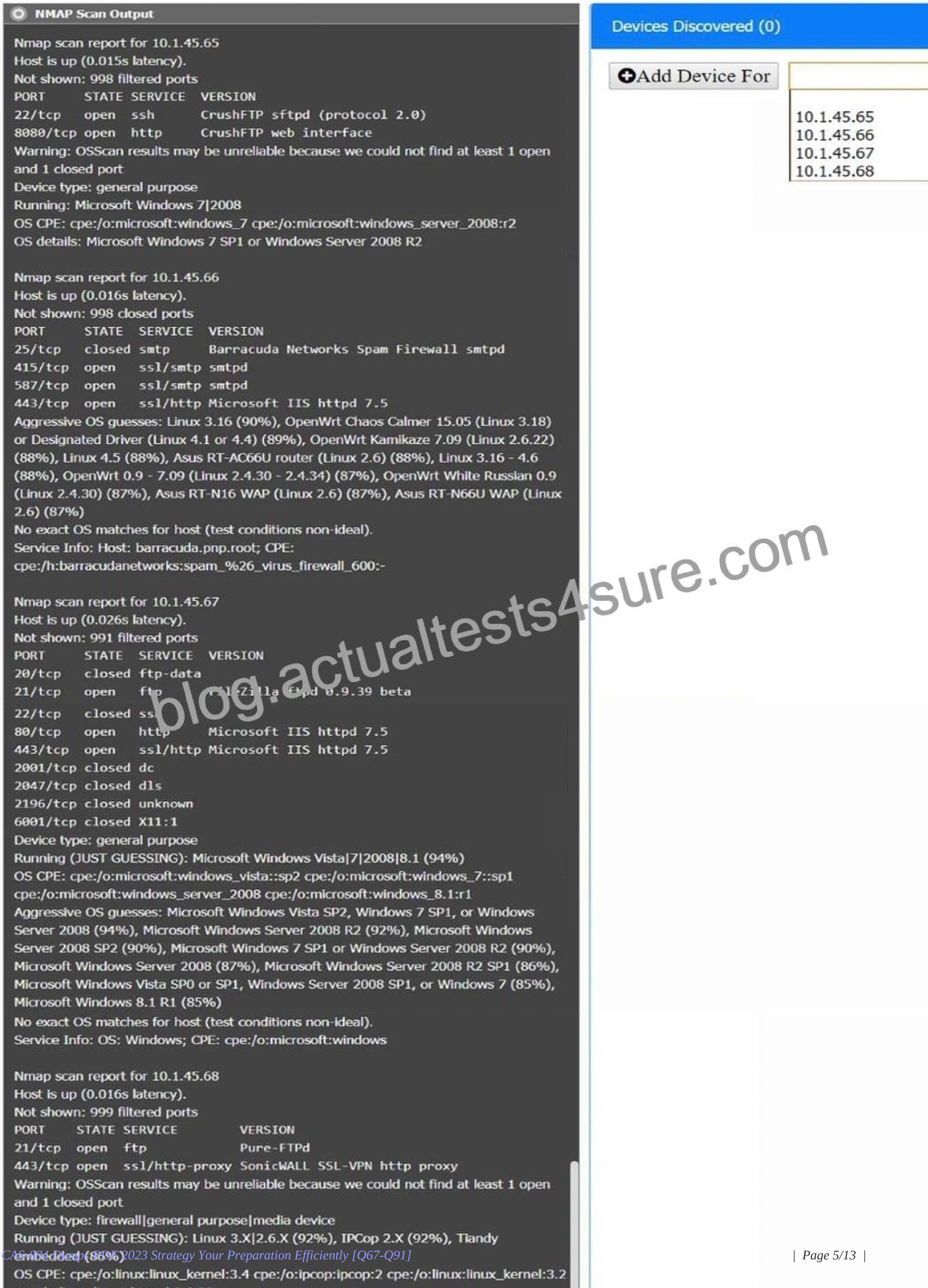
INSTRUCTIONS

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 by Nmap, add a device entry to the Devices Discovered list, with the following information:

The IP address of the device

The primary server or service of the device (Note that each IP should by associated with one service/port only) The protocol(s) that should be disabled based on the hardening guidelines (Note that multiple ports may need to be closed to comply with the hardening guidelines) If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

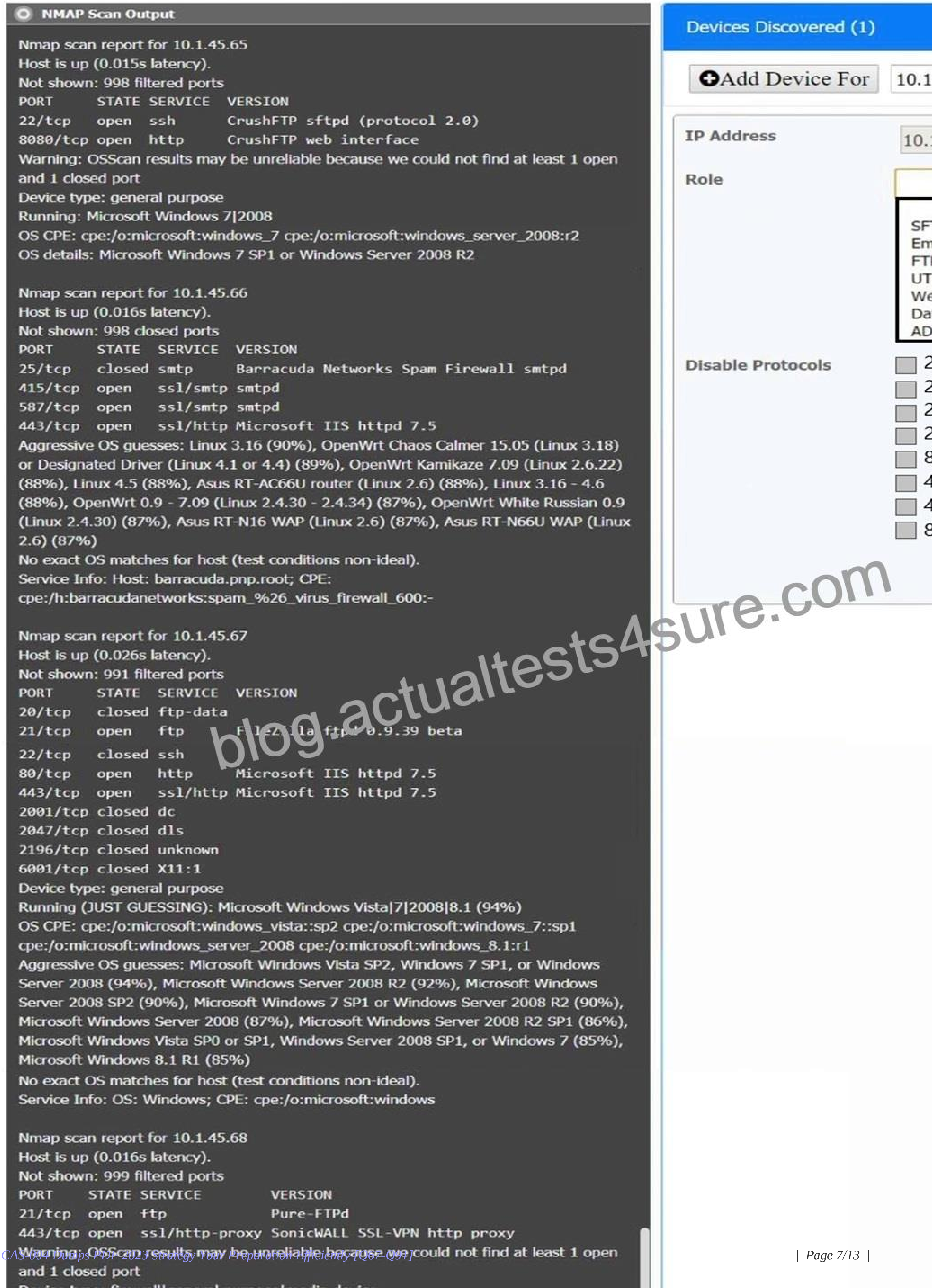


```
Nmap scan report for 10.1.45.65
Host is up (0.015s latency).
Not shown: 998 filtered ports
PORT     STATE SERVICE  VERSION
22/tcp   open  ssh      CrushFTP sftpd (protocol 2.0)
8080/tcp open  http     CrushFTP web interface
Warning: OSScan results may be unreliable because we could not find at least 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 (85%)
OS CPE: cpe:/o:linux:linux_kernel:3.4 cpe:/o:ipcop:ipcop:2 cpe:/o:linux:linux_kernel:3.2
```



```
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
```

Devices Discovered (1)

Add Device For 10.1

IP Address 10.1

Role

SF
Em
FT
UT
We
Da
AD

Disable Protocols

□ 2
□ 2
□ 2
□ 2
□ 8
□ 4
□ 4
□ 8

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 74**

A security architect is tasked with scoping a penetration test that will start next month. The architect wants to define what security controls will be impacted. Which of the following would be the BEST document to consult?

* Rules of engagement
* Master service agreement
* Statement of work
* Target audience

The Statement of Work is a document that outlines the scope of the penetration test and defines the objectives, tools, methodology, and targets of the test. It also outlines the security controls that will be impacted by the test and what the expected outcomes are. Additionally, the Statement of Work should include any legal requirements and other considerations that should be taken into account during the penetration test.

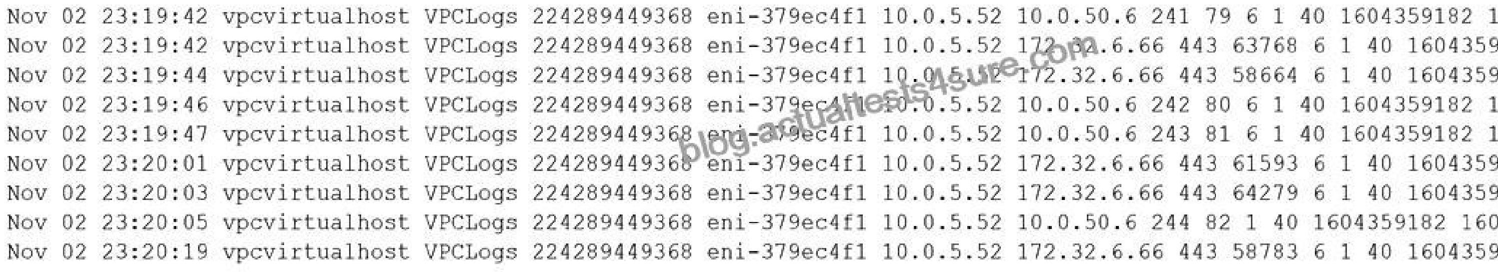
**QUESTION 75**

Which of the following controls primarily detects abuse of privilege but does not prevent it?

* Off-boarding
* Separation of duties
* Least privilege
* Job rotation

**QUESTION 76**

A security analyst observes the following while looking through network traffic in a company&#8217;s cloud log:



```
Nov 02 23:19:42 vpcvirtualhost VPCLogs 224289449368 eni-379ec4f1 10.0.5.52 10.0.50.6 241 79 6 1 40 1604359182 1
Nov 02 23:19:42 vpcvirtualhost VPCLogs 224289449368 eni-379ec4f1 10.0.5.52 172.32.6.66 443 63768 6 1 40 1604359
Nov 02 23:19:44 vpcvirtualhost VPCLogs 224289449368 eni-379ec4f1 10.0.5.52 172.32.6.66 443 58664 6 1 40 1604359
Nov 02 23:19:46 vpcvirtualhost VPCLogs 224289449368 eni-379ec4f1 10.0.5.52 10.0.50.6 242 80 6 1 40 1604359182 1
Nov 02 23:19:47 vpcvirtualhost VPCLogs 224289449368 eni-379ec4f1 10.0.5.52 10.0.50.6 243 81 6 1 40 1604359182 1
Nov 02 23:20:01 vpcvirtualhost VPCLogs 224289449368 eni-379ec4f1 10.0.5.52 172.32.6.66 443 61593 6 1 40 1604359
Nov 02 23:20:03 vpcvirtualhost VPCLogs 224289449368 eni-379ec4f1 10.0.5.52 172.32.6.66 443 64279 6 1 40 1604359
Nov 02 23:20:05 vpcvirtualhost VPCLogs 224289449368 eni-379ec4f1 10.0.5.52 10.0.50.6 244 82 1 40 1604359182 160
Nov 02 23:20:19 vpcvirtualhost VPCLogs 224289449368 eni-379ec4f1 10.0.5.52 172.32.6.66 443 58783 6 1 40 1604359
```

Which of the following steps should the security analyst take FIRST?

* Quarantine 10.0.5.52 and run a malware scan against the host.
* Access 10.0.5.52 via EDR and identify processes that have network connections.
* Isolate 10.0.50.6 via security groups.
* Investigate web logs on 10.0.50.6 to determine if this is normal traffic.

**QUESTION 77**

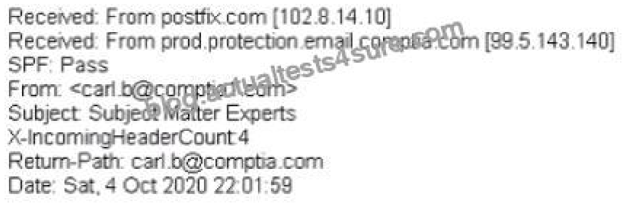
A company is moving most of its customer-facing production systems to the cloud-facing production systems to the cloud. IaaS is the service model being used. The Chief Executive Officer is concerned about the type of encryption available and requires the solution must have the highest level of security.

Which of the following encryption methods should the cloud security engineer select during the implementation phase?
* Instance-based
* Storage-based
* Proxy-based
* Array controller-based
Explanation

We recommend that you encrypt your virtual hard disks (VHDs) to help protect your boot volume and data volumes at rest in storage, along with your encryption keys and secrets. Azure Disk Encryption helps you encrypt your Windows and Linux IaaS virtual machine disks. Azure Disk Encryption uses the industry-standard BitLocker feature of Windows and the DM-Crypt feature of Linux to provide volume encryption for the OS and the data disks. The solution is integrated with Azure Key Vault to help you control and manage the disk-encryption keys and secrets in your key vault subscription. The solution also ensures that all data on the virtual machine disks are encrypted at rest in Azure Storage.https://docs.microsoft.com/en-us/azure/security/fundamentals/iaas

**QUESTION 78**

A large number of emails have been reported, and a security analyst is reviewing the following information from the emails:



```
Received: From postfix.com [102.8.14.10]
Received: From prod.protection.email.comptia.com [99.5.143.140]
SPF: Pass
From: <carl.b@comptia1.com>
Subject: Subject Matter Experts
X-IncomingHeaderCount:4
Return-Path: carl.b@comptia.com
Date: Sat, 4 Oct 2020 22:01:59
```

As part of the image process, which of the following is the FIRST step the analyst should take?
* Block the email address carl b@comptia1 com, as it is sending spam to subject matter experts
* Validate the final &#8220;Received&#8221; header against the DNS entry of the domain.
* Compare the &#8216;Return-Path&#8221; and &#8220;Received&#8221; fields.
* Ignore the emails, as SPF validation is successful, and it is a false positive

**QUESTION 79**

An organization is prioritizing efforts to remediate or mitigate risks identified during the latest assessment. For one of the risks, a full remediation was not possible, but the organization was able to successfully apply mitigations to reduce the likelihood of impact.

Which of the following should the organization perform NEXT?
* Assess the residual risk.
* Update the organization&#8217;s threat model.
* Move to the next risk in the register.
* Recalculate the magnitude of impact.

**QUESTION 80**

An organization is developing a disaster recovery plan that requires data to be backed up and available at a moment&#8217;s notice.

Which of the following should the organization consider FIRST to address this requirement?
* Implement a change management plan to ensure systems are using the appropriate versions.
* Hire additional on-call staff to be deployed if an event occurs.
* Design an appropriate warm site for business continuity.
* Identify critical business processes and determine associated software and hardware requirements.

**QUESTION 81**

An organization is implementing a new identity and access management architecture with the following objectives:

Supporting MFA against on-premises infrastructure

Improving the user experience by integrating with SaaS applications

Applying risk-based policies based on location

Performing just-in-time provisioning

Which of the following authentication protocols should the organization implement to support these requirements?
* Kerberos and TACACS
* SAML and RADIUS
* OAuth and OpenID
* OTP and 802.1X

**QUESTION 82**

A healthcare system recently suffered from a ransomware incident As a result the board of directors decided to hire a security consultant to improve existing network security. The security consultant found that the healthcare network was completely flat, had no privileged access limits and had open RDP access to servers with personal health information. As the consultant builds the remediation plan, which of the following solutions would BEST solve these challenges? (Select THREE).
* SD-WAN
* PAM
* Remote access VPN
* MFA
* Network segmentation
* BGP
* NAC

**QUESTION 83**

Which of the following protocols is a low power, low data rate that allows for the creation of PAN networks?
* Zigbee
* CAN
* DNP3
* Modbus

**QUESTION 84**

A security architect works for a manufacturing organization that has many different branch offices. The architect is looking for a way to reduce traffic and ensure the branch offices receive the latest copy of revoked certificates issued by the CA at the organization&#8217;s headquarters location. The solution must also have the lowest power requirement on the CA.

Which of the following is the BEST solution?
*  Deploy an RA on each branch office.
*  Use Delta CRLs at the branches.
*  Configure clients to use OCSP.
*  Send the new CRLs by using GPO.

**QUESTION 85**

The goal of a Chief information Security Officer (CISO) providing up-to-date metrics to a bank&#8217;s risk committee is to ensure:
*  Budgeting for cybersecurity increases year over year.
*  The committee knows how much work is being done.
*  Business units are responsible for their own mitigation.
*  The bank is aware of the status of cybersecurity risks

**QUESTION 86**

A company is looking to fortify its cybersecurity defenses and is focusing on its network infrastructure. The solution cannot affect the availability of the company&#8217;s services to ensure false positives do not drop legitimate traffic.

Which of the following would satisfy the requirement?
*  NIDS
*  NIPS
*  WAF
*  Reverse proxy

**QUESTION 87**

A Chief Information Officer (CIO) wants to implement a cloud solution that will satisfy the following requirements:

Support all phases of the SDLC.

Use tailored website portal software.

Allow the company to build and use its own gateway software.

Utilize its own data management platform.

Continue using agent-based security tools.

Which of the following cloud-computing models should the CIO implement?
*  SaaS
*  PaaS

- MaaS
- IaaS

**QUESTION 88**

A home automation company just purchased and installed tools for its SOC to enable incident identification and response on software the company develops. The company would like to prioritize defenses against the following attack scenarios:

Unauthorized insertions into application development environments

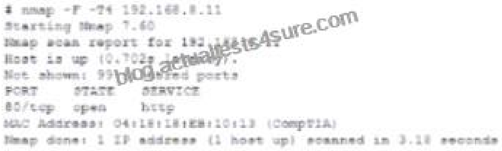
Authorized insiders making unauthorized changes to environment configurations Which of the following actions will enable the data feeds needed to detect these types of attacks on development environments? (Choose two.)

- Perform static code analysis of committed code and generate summary reports.
- Implement an XML gateway and monitor for policy violations.
- Monitor dependency management tools and report on susceptible third-party libraries.
- Install an IDS on the development subnet and passively monitor for vulnerable services.
- Model user behavior and monitor for deviations from normal.
- Continuously monitor code commits to repositories and generate summary logs.

**QUESTION 89**

A security auditor needs to review the manner in which an entertainment device operates. The auditor is analyzing the output of a port scanning tool to determine the next steps in the security review. Given the following log output.

The best option for the auditor to use NEXT is:



```
# nmap -F -T4 192.168.8.11
Starting Nmap 7.60
Nmap scan report for 192.168.8.11
Host is up (0.702s latency).
Not shown: 99 filtered ports
PORT     STATE    SERVICE
80/tcp   open     http
MAC Address: 04:18:18:EB:10:13 (CompTIA)
Nmap done: 1 IP address (1 host up) scanned in 3.18 seconds
```

- A SCAP assessment.
- Reverse engineering
- Fuzzing
- Network interception.

**QUESTION 90**

An organization is designing a network architecture that must meet the following requirements:

Users will only be able to access predefined services.

Each user will have a unique allow list defined for access.

The system will construct one-to-one subject/object access paths dynamically.

Which of the following architectural designs should the organization use to meet these requirements?

- Peer-to-peer secure communications enabled by mobile applications

* Proxied application data connections enabled by API gateways
* Microsegmentation enabled by software-defined networking
* VLANs enabled by network infrastructure devices

**QUESTION 91**

A software company wants to build a platform by integrating with another company&#8217;s established product. Which of the following provisions would be MOST important to include when drafting an agreement between the two companies?
* Data sovereignty
* Shared responsibility
* Source code escrow
* Safe harbor considerations
When drafting an agreement between two companies, it is important to clearly define the responsibilities of each party. This is particularly relevant when a software company is looking to integrate with an established product. A shared responsibility agreement ensures that both parties understand their respective responsibilities and are able to work together efficiently and effectively. For example, the software company might be responsible for integrating the product and ensuring it meets user needs, while the established product provider might be responsible for providing ongoing support and maintenance. By outlining these responsibilities in the agreement, both parties can ensure that the platform is built and maintained successfully. Reference: CompTIA Advanced Security Practitioner (CASP+) Study Guide, Chapter 8, Working with Third Parties.

## What is the exam cost of CompTIA CAS-004 Exam Certification

The exam cost of CompTIA CAS-004 Exam Certification is $466 USD.

**CAS-004 PDF Dumps Are Helpful To produce Your Dreams Correct QA's:**
https://www.actualtests4sure.com/CAS-004-test-questions.html]