CompTIA - CAS-004 - CompTIA Advanced Security Practitioner (CASP+) Exam–Efficient Exam Demo

CompTIA Certified professionals are often more sought after than their non-certified counterparts and are more likely to earn higher salaries and promotions. Moreover, cracking the CompTIA Advanced Security Practitioner (CASP+) Exam (CAS-004) exam helps to ensure that you stay up to date with the latest trends and developments in the industry, making you more valuable assets to your organization.

CompTIA CASP+ certification exam is an advanced-level certification designed for cybersecurity professionals who have extensive experience in the field. CompTIA Advanced Security Practitioner (CASP+) Exam certification is designed to validate the candidate's knowledge and skills in advanced-level cybersecurity concepts and practices and to demonstrate to employers that they have the expertise required to design, implement, and manage cybersecurity solutions at the enterprise level. CompTIA Advanced Security Practitioner (CASP+) Exam certification covers a range of topics that are relevant to the day-to-day work of cybersecurity professionals and is designed to be practical and relevant to real-world scenarios.

>> Exam CAS-004 Demo <<

Latest CAS-004 Exam Forum - Valid CAS-004 Test Cram

Now you do not need to worry about the relevancy and top standard of FreeDumps CompTIA Advanced Security Practitioner (CASP+) Exam (CAS-004) exam questions. These CompTIA CAS-004 dumps are designed and verified by qualified CAS-004 exam trainers. Now you can trust FreeDumps CompTIA CAS-004 Practice Questions and start preparation without wasting further time. With the CAS-004 exam questions you will get everything that you need to learn, prepare and pass the challenging CAS-004 exam with good scores.

CompTIA Advanced Security Practitioner (CASP+) Exam Sample Questions (Q139-Q144):

NEW QUESTION # 139
A corporation discovered its internet connection is saturated with traffic originating from multiple IP addresses across the internet. A security analyst needs to find a solution to address future occurrences of this type of attack.
Which of the following would be the BEST solution to meet this goal?

- A. Upgrading the internet link
- B. Provisioning a reverse proxy
- C. Implementing cloud-scrubbing services
- D. Deploying a web application firewall

Answer: C

NEW QUESTION # 140

A network administrator receives a ticket regarding an error from a remote worker who is trying to reboot a laptop. The laptop has not yet loaded the operating system, and the user is unable to continue the boot process.

The administrator is able to provide the user with a recovery PIN, and the user is able to reboot the system and access the device as needed. Which of the following is the MOST likely cause of the error?

- A. Duration of the BitLocker lockout period
- B. Lockout of privileged access account
- C. Failure of the Kerberos time drift sync
- D. Failure of TPM authentication

Answer: D

Explanation:
The most likely cause of the error is the failure of TPM authentication. TPM stands for Trusted Platform Module, which is a hardware component that stores encryption keys and other security information. TPM can be used by BitLocker to protect the encryption keys and verify the integrity of the boot process. If TPM fails to authenticate the laptop, BitLocker will enter recovery mode and ask for a recovery PIN, which is a 48-digit numerical password that can be used to unlock the system. The administrator should check the TPM status and configuration and make sure it is working properly. Verified References:
https://support.microsoft.com/en-us/windows/finding-your-bitlocker-recovery-key-in-windows-6b71ad27-0b89-ea08-f143-056f5ab347d6
https://learn.microsoft.com/en-us/windows/security/operating-system-security/data-protection/bitlocker/bitlocker-recovery-guide-plan
https://docs.sophos.com/esg/sgn/8-1/user/win/en-us/esg/SafeGuard-Enterprise/tasks/BitLockerRecoveryKey.html

NEW QUESTION # 141

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

As part of the image process, which of the following is the FIRST step the analyst should take?

- A. Compare the 'Return-Path'' and ''Received'' fields.
- B. Ignore the emails, as SPF validation is successful, and it is a false positive
- C. Validate the final ''Received'' header against the DNS entry of the domain.
- D. Block the email address carl b@comptia1 com, as it is sending spam to subject matter experts

Answer: A

NEW QUESTION # 142

SIMULATION

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

The company'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 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
                    ☐ 8080/tcp

Answer:

Explanation:
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

NEW QUESTION # 143
A security engineer needs to recommend a solution that will meet the following requirements:

Identify sensitive data in the provider's network
Maintain compliance with company and regulatory guidelines
Detect and respond to insider threats, privileged user threats, and compromised accounts Enforce datacentric security, such as encryption, tokenization, and access control Which of the following solutions should the security engineer recommend to address these requirements?

- A. SWG
- B. CASB
- C. DLP
- D. WAF

Answer: D

NEW QUESTION # 144

......

Our CAS-004 learning guide allows you to study anytime, anywhere. If you are concerned that your study time cannot be guaranteed, then our CAS-004 learning guide is your best choice because it allows you to learn from time to time and make full use of all the time available for learning. Our CAS-004 learning guide is for the world and users are very extensive. In order to give users a better experience, we have been constantly improving. The high quality and efficiency of CAS-004 Test Guide has been recognized by users. The high passing rate of CAS-004 exam training is its biggest feature. As long as you use CAS-004 test guide, you can certainly harvest what you want thing.