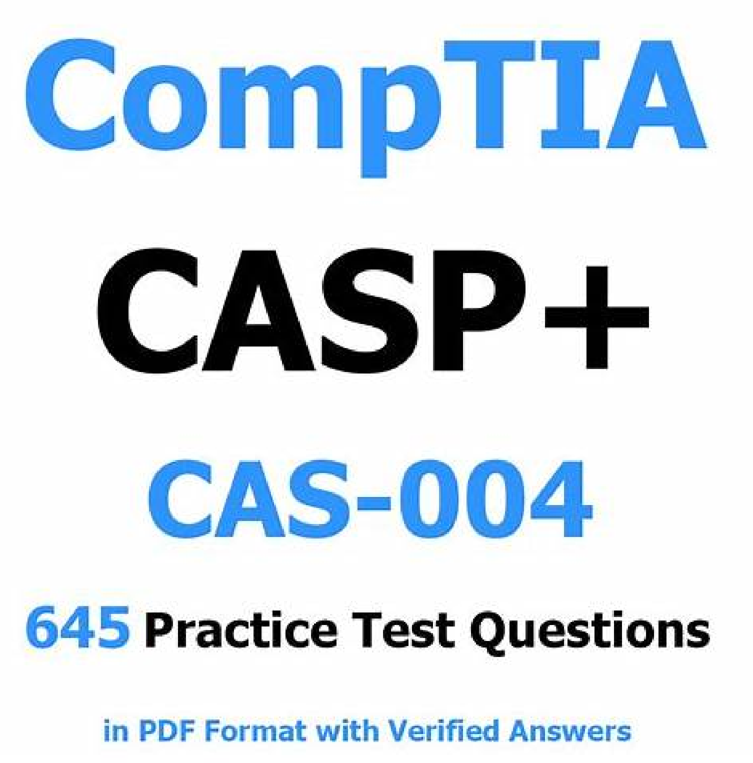
# CAS-004 시험공부, CompTIA Advanced Security Practitioner (CASP+) Exam & CAS-004 VCE버전자료


CompTIA
CASP+
CAS-004
645 Practice Test Questions
in PDF Format with Verified Answers

2026 Itexamdump 최신 CAS-004 PDF 버전 시험 문제집과 CAS-004 시험 문제 및 답변 무료 공유: https://drive.google.com/open?id=16NVZjF2O4I0-8PecIB2XLLAdbIUa5o4O

경쟁율이 점점 높아지는 IT업계에 살아남으려면 국제적으로 인증해주는 IT자격증 몇개쯤은 취득해야 되지 않을가요? CompTIA CAS-004시험으로부터 자격증 취득을 시작해보세요. CompTIA CAS-004 덤프의 모든 문제를 외우기만 하면 시험패스가 됩니다. CompTIA CAS-004덤프는 실제 시험문제의 모든 유형을 포함되어있어 적중율이 최고입니다.

CompTIA CAS-004 시험은 준비가 많이 필요한 어려운 시험입니다. 응시자는 온라인 강좌를 수강하거나 교육 세션에 참여하며, 연습 시험과 스터디 가이드와 같은 학습 자료를 활용하여 시험 준비를 할 수 있습니다. 시험은 90개의 객관식 및 성과 기반 문제로 구성되어 있으며, 165분 안에 완료해야 합니다.

**>> CAS-004시험내용 <<**

## CAS-004퍼펙트 최신 덤프공부 - CAS-004퍼펙트 최신 공부자료

IT국제공인자격증CompTIA CAS-004시험대비덤프를 제공하는 전문적인 사이트로서 회원님의 개인정보를 철저하게 보호해드리고 페이팔을 통한 결제라 안전한 결제를 진행할수 있습니다. CompTIA CAS-004 덤프외에 다른 인증시험덤프에 관심이 있으신 분은 온라인 서비스를 클릭하여 문의해주세요.

CompTIA CASP+ 자격증은 복잡한 기업 환경의 보안에 책임을 지는 전문가들에게 이상적입니다. 시험은 위험 관리, 연구 및 분석, 컴퓨팅, 통신 및 비즈니스 학문의 통합, 기업 구성 요소의 기술적 통합 등 다양한 주제를 다룹니다.

CompTIA CAS-004(CASP+) 시험은 사이버 보안 분야에서 경력을 쌓고자 하는 IT 전문가들에게 필수적인 자격증입니다. 이 자격증은 고급 수준의 주제를 다루며, 후보자의 사이버 보안에 대한 기술적인 지식, 기술 및 전문성을 검증합니다. 시험에 합격하기 위해서는 사이버 보안 개념과 최상의 실천 방법에 대한 깊은 이해와 중요한 준비가 필요합니다.

# 최신 CompTIA CASP CAS-004 무료샘플문제 (Q482-Q487):

### 질문 # 482

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?

- A. VLANs enabled by network infrastructure devices
- B. Microsegmentation enabled by software-defined networking
- C. Proxied application data connections enabled by API gateways
- D. Peer-to-peer secure communications enabled by mobile applications

**정답： B**

**설명:**
Microsegmentation enabled by software-defined networking is an architectural design that can meet the requirements of allowing users to access only predefined services, having unique allow lists defined for each user, and constructing one-to-one subject/object access paths dynamically. Microsegmentation is a technique that divides a network into smaller segments or zones based on granular criteria, such as applications, services, users, or devices. Microsegmentation can provide fine-grained access control and isolation for network resources, preventing unauthorized or lateral movements within the network. Software-defined networking is a technology that decouples the control plane from the data plane in network devices, allowing centralized and programmable management of network functions and policies. Software-defined networking can enable microsegmentation by dynamically creating and enforcing network segments or zones based on predefined rules or policies. Peer-to-peer secure communications enabled by mobile applications is not an architectural design that can meet the requirements of allowing users to access only predefined services, having unique allow lists defined for each user, and constructing one-to-one subject/object access paths dynamically, as peer-to-peer secure communications is a technique that allows direct and encrypted communication between two or more parties without relying on a central server or intermediary. Proxied application data connections enabled by API gateways is not an architectural design that can meet the requirements of allowing users to access only predefined services, having unique allow lists defined for each user, and constructing one-to-one subject/object access paths dynamically, as proxied application data connections is a technique that allows indirect and filtered communication between applications or services through an intermediary device or service that can modify or monitor the traffic. VLANs (virtual local area networks) enabled by network infrastructure devices is not an architectural design that can meet the requirements of allowing users to access only predefined services, having unique allow lists defined for each user, and constructing one-to-one subject/object access paths dynamically, as VLANs are logical segments of a physical network that can group devices or users based on common criteria, such as function, department, or location. Verified Reference: https://www.comptia.org/blog/what-is-microsegmentation https://partners.comptia.org/docs/default-source/resources/casp-content-guide

### 질문 # 483

A security engineer is hardening a company's multihomed SFTP server. When scanning a public- facing network interface, the engineer finds the following ports are open:
22
25
110
137
138
139
445
Internal Windows clients are used to transferring files to the server to stage them for customer download as part of the company's distribution process.
Which of the following would be the BEST solution to harden the system?

- A. Close ports 25 and 110. Bind ports 137, 138, 139, and 445 to only the internal interface.
- B. Close ports 22, 137, and 138. Bind ports 110 and 445 to only the internal interface.
- C. Close ports 22 and 139. Bind ports 137, 138, and 445 to only the internal interface.
- D. Close ports 110, 138, and 139. Bind ports 22, 25, and 137 to only the internal interface.

**정답: A**

**설명:**
The engineer should close any unnecessary ports, such as port 25 (SMTP) and port 110 (POP3), which are not used by the SFTP server.
The SFTP server uses port 22 for secure file transfers, so this port should be left open. The engineer should also bind port 22 to only the internal interface, so that it is not accessible from the public internet.
The engineer should also bind ports 137, 138, 139, and 445 to only the internal interface. These ports are used for various networking protocols, such as NetBIOS and SMB, and are not needed for the SFTP server. By binding these ports to only the internal interface, the engineer can further harden the system and prevent external access to these services.

### 질문 # 484

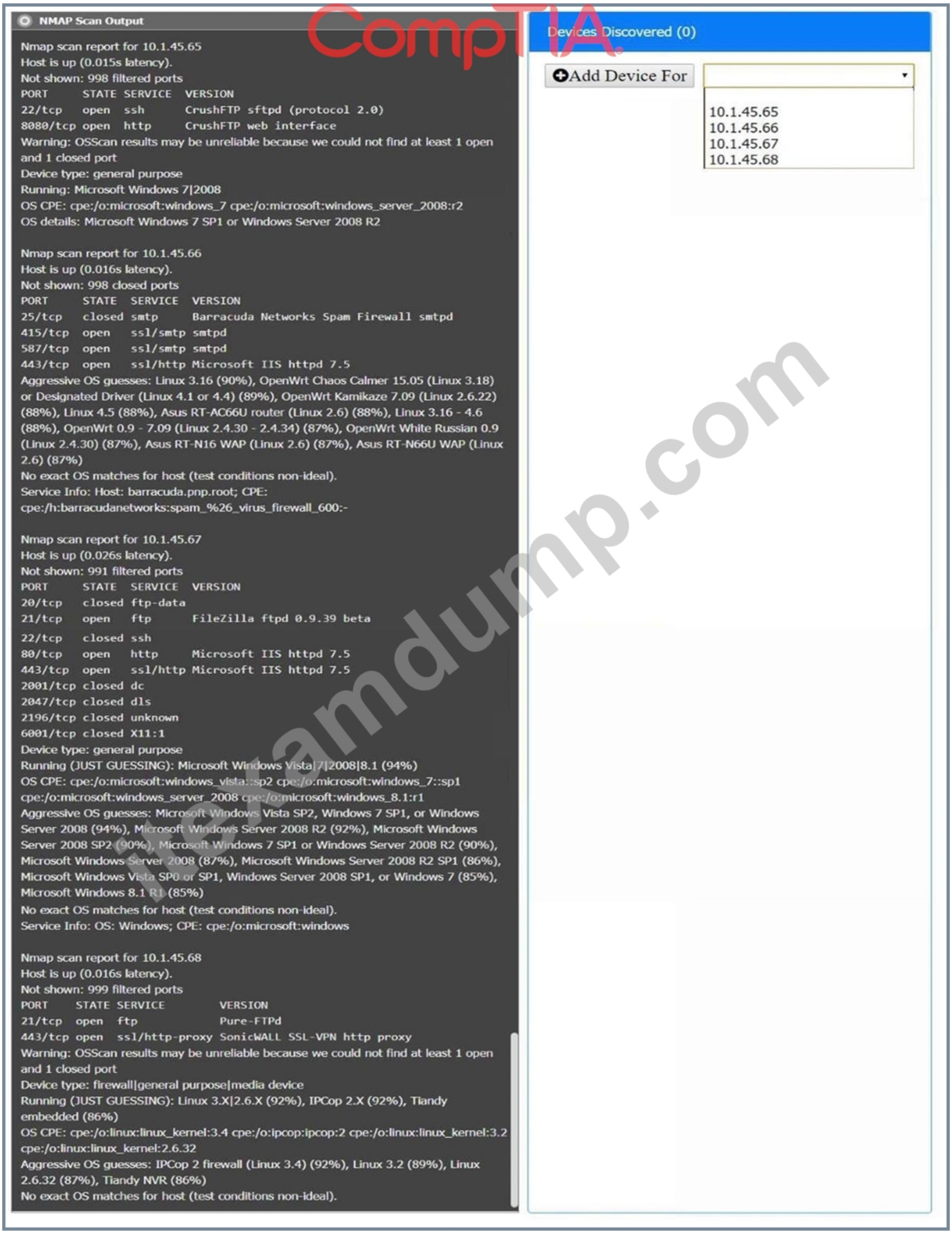
A recent data breach stemmed from unauthorized access to an employee's company account with a cloud-based productivity suite. The attacker exploited excessive permissions granted to a third-party OAuth application to collect sensitive information.
Which of the following BEST mitigates inappropriate access and permissions issues?

- A. WAF
- B. SOAR
- C. CASB
- D. SIEM

**정답: A**

### 질문 # 485

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.

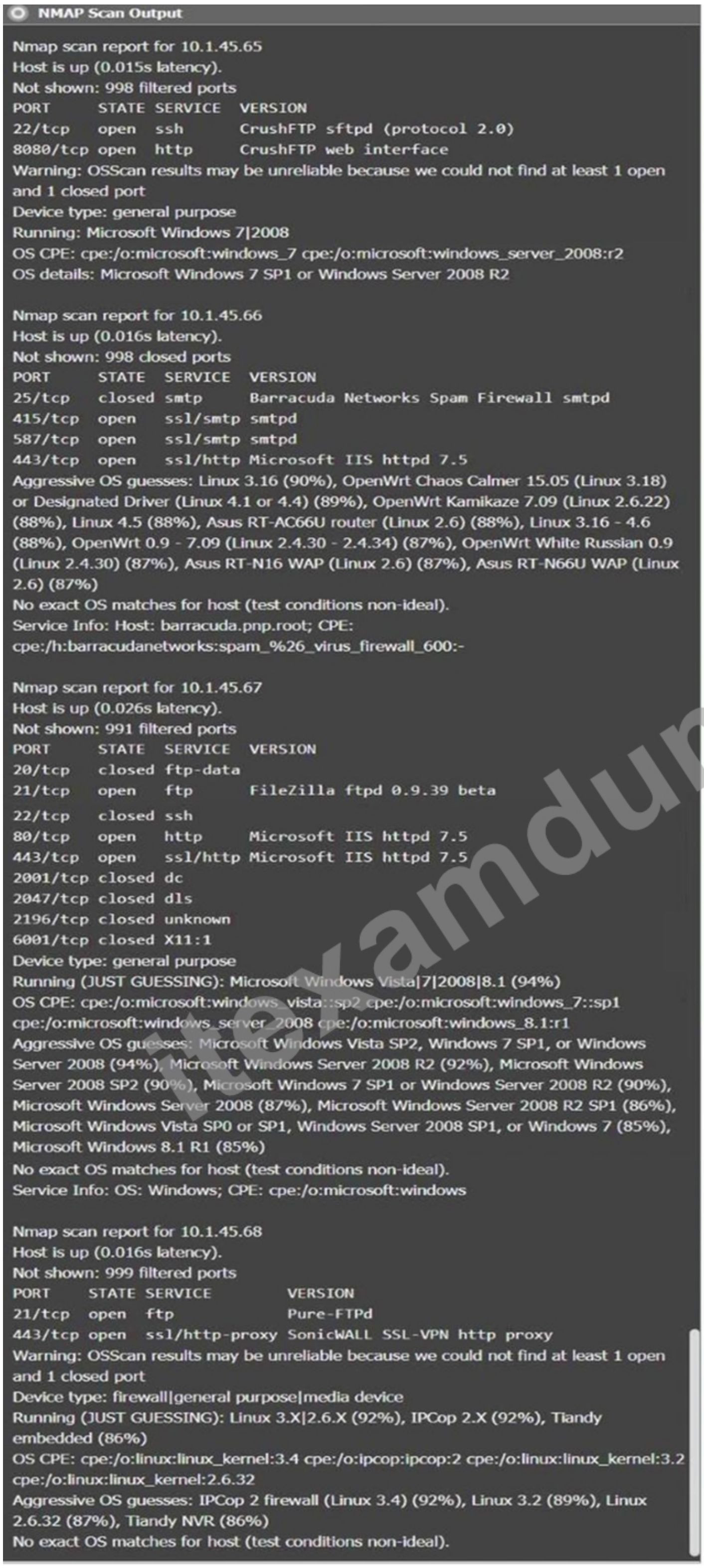


```
Nmap scan report for 10.1.45.65
Host is up (0.015s latency).
Not shown: 998 filtered ports
PORT     STATE SERVICE  VERSION
22/tcp   open  ssh      CrushFTP sftpd (protocol 2.0)
8080/tcp open  http     CrushFTP web interface
Warning: OSScan results may be unreliable because we could not find at least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



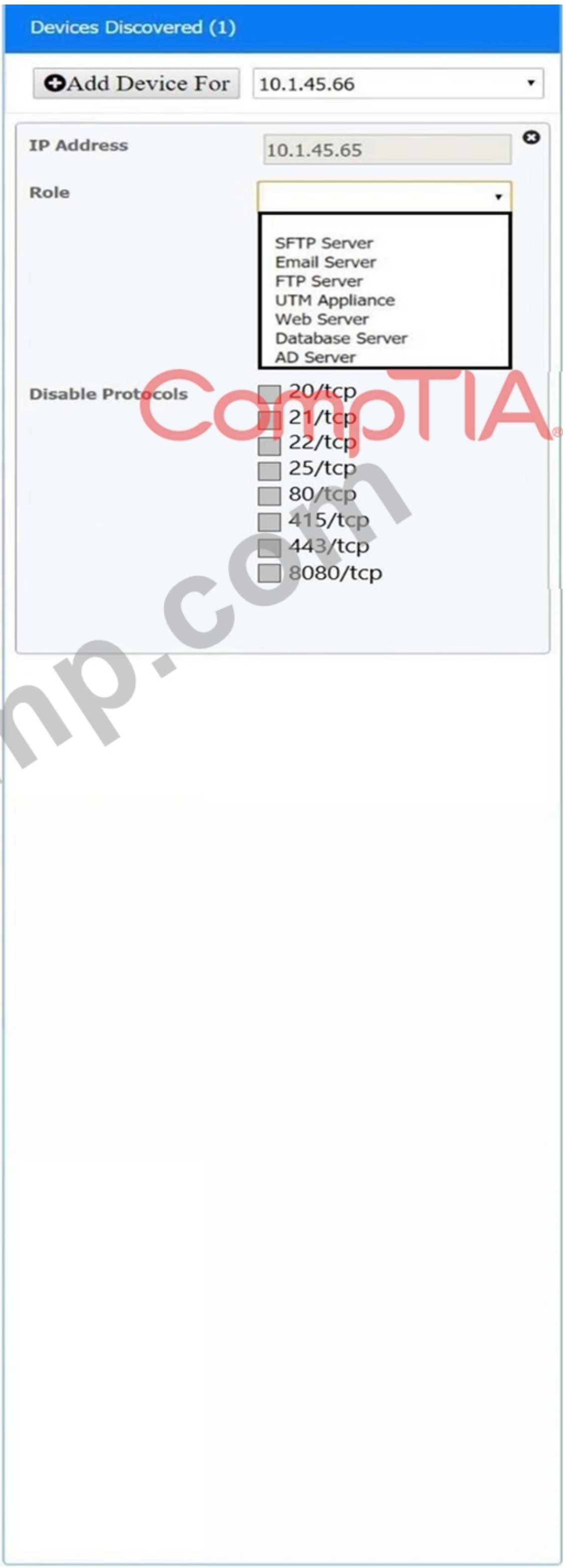
NMAP Scan Output

```
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:

Disable Protocols

□ 20/tcp
□ 21/tcp
□ 22/tcp
□ 25/tcp
□ 80/tcp
□ 415/tcp
□ 443/tcp
□ 8080/tcp

**정답：**

**설명：**

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

## 질문 # 486

A company created an external, PHP-based web application for its customers. A security researcher reports that the application has the Heartbleed vulnerability. Which of the following would BEST resolve and mitigate the issue? (Select TWO).

- A. Fixing the PHP code
- B. UsingSSLv3
- C. Changing the web server from HTTPS to HTTP
- D. Updating the OpenSSL library
- E. Deploying a WAF signature
- F. Changing the code from PHP to ColdFusion

**정답：D,E**

**설명：**
Explanation
Deploying a web application firewall (WAF) signature is a way to detect and block attempts to exploit the Heartbleed vulnerability on the web server. A WAF signature is a pattern that matches a known attack vector, such as a malicious heartbeat request. By deploying a WAF signature, the company can protect its web application from Heartbleed attacks until the underlying vulnerability is fixed.
Updating the OpenSSL library is the ultimate way to fix and mitigate the Heartbleed vulnerability. The OpenSSL project released version 1.0.1g on April 7, 2014, which patched the bug by adding a bounds check to the heartbeat function. By updating the OpenSSL library on the web server, the company can eliminate the vulnerability and prevent any future exploitation.
B: Fixing the PHP code is not a way to resolve or mitigate the Heartbleed vulnerability, because the vulnerability is not in the PHP code, but in the OpenSSL library that handles the SSL/TLS encryption for the web server.
C: Changing the web server from HTTPS to HTTP is not a way to resolve or mitigate the Heartbleed vulnerability, because it would expose all the web traffic to eavesdropping and tampering by attackers. HTTPS provides confidentiality, integrity, and authentication for web communications, and should not be disabled for security reasons.
D: Using SSLv3 is not a way to resolve or mitigate the Heartbleed vulnerability, because SSLv3 is an outdated and insecure protocol that has been deprecated and replaced by TLS. SSLv3 does not support modern cipher suites, encryption algorithms, or security features, and is vulnerable to various attacks, such as POODLE.
E: Changing the code from PHP to ColdFusion is not a way to resolve or mitigate the Heartbleed vulnerability, because the vulnerability is not related to the programming language of the web application, but to the OpenSSL library that handles the SSL/TLS encryption for the web server.
https://owasp.org/www-community/vulnerabilities/Heartbleed_Bug
https://heartbleed.com/

**질문 # 487**
......

십시오CAS-004최신 시험대비자료

- CAS-004최신 업데이트버전 공부문제 □ CAS-004시험대비 덤프 최신 샘플문제 □ CAS-004최신 업데이트인증공부자료 □ { www.itdumpskr.com }에서➠ CAS-004 □를 검색하고 무료 다운로드 받기CAS-004시험패스 가능한 공부자료
- CAS-004인증덤프 샘플문제 □ CAS-004시험대비 덤프 최신 샘플문제 □ CAS-004최신 업데이트버전 공부문제 □ 오픈 웹 사이트□ kr.fast2test.com □검색□ CAS-004 □무료 다운로드CAS-004덤프문제은행
- myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, study.stcs.edu.np, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, Disposable vapes

참고: Itexamdump에서 Google Drive로 공유하는 무료 2026 CompTIA CAS-004 시험 문제집이 있습니다: https://drive.google.com/open?id=16NVZjF2O4I0-8PecIB2XLLAdbIUa5o4O