

CompTIA Security+ Certification Practice Test 1 (Exam SY0-401)

▶ A software or hardware that checks information coming from the Internet and depending on the applied configuration settings either blocks it or allows it to pass through is called:

☐ ☐ ☐ Antivirus

☐ ☒ ☐ Firewall (✔ Your answer)

☐ ☐ ☐ Antispyware

☐ ☐ ☐ Malware

☒ You correctly answered this question.

▶ A device designed to forward data packets between networks is called:

☐ ☐ ☐ Layer 2 switch

☐ ☐ ☐ Active hub

☐ ☐ ☐ Content filter

☐ ☒ ☐ Router (✔ Your answer)

☒ You correctly answered this question.

▶ Allowing a connection through a firewall is known as creating:

☐ ☐ ☐ Tunnel

☐ ☒ ☐ Exception (✔ Your answer)

☐ ☐ ☐ Access Point (AP)

☐ ☐ ☐ Entry

☒ You correctly answered this question.

▶ A network device designed for managing the optimal distribution of workloads across multiple computing resources is called:

☐ ☒ ☐ Load balancer (✔ Missed)

☐ ☐ ☐ HIDS

☐ ☐ ☐ Firewall

☐ ☐ ☐ Captive portal

☒ Your answer to this question is incorrect.


▶ The last default rule on a firewall is to deny all traffic.

☐ ☒ ☐ True (✔ Missed)

☐ ☐ ☐ False


In order to provide you with the best online experience this website uses cookies.

By using our website, you agree to our use of cookies. [Learn more](#)

 Your answer to this question is incorrect.


► A computer network service that allows clients to make indirect network connections to other network services is called:

☐ ☐ ☐ Load balancing

☐ ☒  Proxy (✖ Missed)

☐ ☐ ☐ Network Access Control (NAC)

☐ ☐ ☐ Backdoor

 Your answer to this question is incorrect.


► Which of the terms listed below refers to a security solution implemented on an individual computer host monitoring that specific system for malicious activities or policy violations?

☐ ☐ ☐ NIPS

☐ ☐ ☐ Content filter

☐ ☐ ☐ Firewall


☐ ☒  HIDS (✖ Missed)

 Your answer to this question is incorrect.

► One of the measures for securing networking devices includes the practice of disabling unused ports.

☐ ☒  True (✖ Missed)

☐ ☐ ☐ False

 Your answer to this question is incorrect.


► Which of the following ensures the privacy of a VPN connection?

☐ ☐ ☐ Hashing

☐ ☒  Tunneling (✖ Missed)


☐ ☐ ☐ Authentication

☐ ☐ ☐ Cleartext credentials

 Your answer to this question is incorrect.


► Which of the following answers refers to a dedicated device for managing secure connections established over an untrusted network, such as the Internet?

☐ ☐ ☐ Load balancer

☐ ☒  VPN concentrator (✖ Missed)

☐ ☐ ☐ Layer 3 switch

☐ ☐ ☐ Hardware firewall

 Your answer to this question is incorrect.

In order to provide you with the best online experience this website uses cookies.

By using our website, you agree to our use of cookies. [Learn more](#)

► Which of the following acronyms refers to a network or host based monitoring system designed to automatically alert administrators of known or suspected unauthorized activity?

✓

🔊

IDS (✖ Missed)

AES

TPM

EFS

Your answer to this question is incorrect.

▶

A software tool used for monitoring and examining contents of the network traffic is known as: (Select all that apply)

Port scanner

✓

🔊

Packet sniffer (✖ Missed)

Vulnerability scanner

✓

🔊

Protocol analyzer (✖ Missed)

Your answer to this question is incorrect.

▶

Which of the following answers list the protocol and port number used by a spam filter? (Select 2 answers)

HTTPS

23

✓

🔊

SMTP (✖ Missed)

443

TELNET

✓

🔊

25 (✖ Missed)

Your answer to this question is incorrect.

▶

Which of the following acronyms refers to a network security solution combining the functionality of a firewall with additional safeguards such as URL filtering, content inspection, or malware inspection?

MTU

STP

✓

🔊

UTM (✖ Missed)

XML

Your answer to this question is incorrect.

▶

URL filtering restricts access to Internet sites based on which of the following criteria?

Virus signature

✓

🔊

Web address (✖ Missed)

Baseline

Data content

Your answer to this question is incorrect.

▶

Which of the following network security solutions inspects network traffic in real-time and has the capability to stop the ongoing attack?

In order to provide you with the best online experience this website uses cookies.

By using our website, you agree to our use of cookies. [Learn more](#)


I agree

☐ ☒  NIPS (✖ Missed)

☐ ☐ ☐ HIDS

☐ ☐ ☐ NIDS

☐ ☐ ☐ NIST

 Your answer to this question is incorrect.


► Which of the following acronyms refers to a firewall controlling access to a web server?

☐ ☐ ☐ WEP

☐ ☐ ☐ WAP

☐ ☐ ☐ WPS

☐ ☒  WAF (✖ Missed)

 Your answer to this question is incorrect.


► Which of the answers listed below refers to a set of rules that specify which users or system processes are granted access to objects as well as what operations are allowed on a given object?

☐ ☐ ☐ CRL

☐ ☐ ☐ NAT

☐ ☐ ☐ BCP

☐ ☒  ACL (✖ Missed)

 Your answer to this question is incorrect.


► Which of the following actions can be taken by passive IDS? (Select 2 answers)


☐ ☐ ☐ Firewall reconfiguration

☐ ☐ ☐ Closing down connection

☐ ☒  Logging (✖ Missed)

☐ ☐ ☐ Terminating process

☐ ☒  Sending an alert (✖ Missed)

 Your answer to this question is incorrect.


► 802.1x is an IEEE standard defining:

☐ ☐ ☐ Token ring networks

☐ ☒  Port-based network access control (✖ Missed)

☐ ☐ ☐ VLAN tagging

☐ ☐ ☐ Wireless networking

 Your answer to this question is incorrect.

In order to provide you with the best online experience this website uses cookies.

► An access control model in which access to resources is granted or denied depending on Access Control List (ACL) entries is also known as:

☐ ☐ ☐ Mandatory Access Control

I agree

Lattice-Based Access Control

Role-Based Access Control

Rule-Based Access Control (✖ Missed)

Your answer to this question is incorrect.

▶ A type of Intrusion Detection System (IDS) that relies on the previously established baseline of normal network activity in order to detect intrusions is known as a signature-based IDS.

True

False (✖ Missed)

Your answer to this question is incorrect.

▶ Which of the following security solutions provides a countermeasure against denial-of-service attack characterized by increasing number of half-open connections?

Flood guard (✖ Missed)

Captive portal

Protocol analyzer

Firewall

Your answer to this question is incorrect.

▶ Which of the protocols listed below protects against switching loops?

UTP

OCSP

STP (✖ Missed)

HMAC

Your answer to this question is incorrect.

▶ A type of Intrusion Detection System (IDS) that relies on known attack patterns to detect an intrusion is known as a signature-based IDS.

True (✖ Missed)

False

Your answer to this question is incorrect.

Your Final Report		
Total marks		28
Total Questions		25
Questions correctly answered		3
Success ratio		12%
Marks secured	In order to provide you with the best online experience this website uses cookies.	
Percentage secured	By using our website, you agree to our use of cookies. Learn more	10.71%

I agree

Security+

CompTIA Security+ Certification Exam SY0-401 Practice Tests

[Security+ Practice Test 1 \(/comptia-security-plus-practice-test-1-exam-sy0-401\)](/comptia-security-plus-practice-test-1-exam-sy0-401)

[Security+ Practice Test 7 \(/comptia-security-plus-practice-test-7-exam-sy0-401\)](/comptia-security-plus-practice-test-7-exam-sy0-401)

[Security+ Practice Test 2 \(/comptia-security-plus-practice-test-2-exam-sy0-401\)](/comptia-security-plus-practice-test-2-exam-sy0-401)

[Security+ Practice Test 8 \(/comptia-security-plus-practice-test-8-exam-sy0-401\)](/comptia-security-plus-practice-test-8-exam-sy0-401)

[Security+ Practice Test 3 \(/comptia-security-plus-practice-test-3-exam-sy0-401\)](/comptia-security-plus-practice-test-3-exam-sy0-401)

[Security+ Practice Test 9 \(/comptia-security-plus-practice-test-9-exam-sy0-401\)](/comptia-security-plus-practice-test-9-exam-sy0-401)

[Security+ Practice Test 4 \(/comptia-security-plus-practice-test-4-exam-sy0-401\)](/comptia-security-plus-practice-test-4-exam-sy0-401)

[Security+ Practice Test 10 \(/comptia-security-plus-practice-test-10-exam-sy0-401\)](/comptia-security-plus-practice-test-10-exam-sy0-401)

[Security+ Practice Test 5 \(/comptia-security-plus-practice-test-5-exam-sy0-401\)](/comptia-security-plus-practice-test-5-exam-sy0-401)

[Security+ Practice Test 11 \(/comptia-security-plus-practice-test-11-exam-sy0-401\)](/comptia-security-plus-practice-test-11-exam-sy0-401)

[Security+ Practice Test 6 \(/comptia-security-plus-practice-test-6-exam-sy0-401\)](/comptia-security-plus-practice-test-6-exam-sy0-401)

[Security+ Practice Test 12 \(/comptia-security-plus-practice-test-12-exam-sy0-401\)](/comptia-security-plus-practice-test-12-exam-sy0-401)

CompTIA Security+ Certification SY0-401 Practice Tests by Exam Topic

[Malware Quiz \(/malware-quiz\)](/malware-quiz)

[Port Numbers Quiz \(/comptia-security-plus-certification-port-numbers-quiz\)](/comptia-security-plus-certification-port-numbers-quiz)

Exam Glossaries

[Malware Glossary \(/malware-glossary\)](/malware-glossary)

[CompTIA Security+ Certification Exam Acronym Glossary \(/comptia-security-plus-certification-exam-glossary\)](/comptia-security-plus-certification-exam-glossary)

[CompTIA Security+ SY0-401 Exam Objectives \(http://certification.comptia.org/docs/default-source/exam-objectives/comptia-security-sy0-401.pdf\)](http://certification.comptia.org/docs/default-source/exam-objectives/comptia-security-sy0-401.pdf)

[Site Map \(/site-map\)](/site-map)

[Privacy Policy \(/privacy-policy\)](/privacy-policy)

[Terms & Conditions \(/terms-and-conditions\)](/terms-and-conditions)

[Back to top \(https://www.examcompass.com/comptia-security-plus-practice-test-1-exam-sy0-401#top\)](https://www.examcompass.com/comptia-security-plus-practice-test-1-exam-sy0-401#top)

In order to provide you with the best online experience this website uses cookies.

By using our website, you agree to our use of cookies. [Learn more](#)

☐ I agree

