

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

Send results by email

Name

Enter your name

Email

Enter your email

Send Results

▶ 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 (✖ Missed)
- ☐

☐

☐

Antispyware
- ☐

☐

☐

Malware

🚫 Your answer to this question is incorrect.

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

- ☐

☐

☐

Layer 2 switch
- ☐

☐

☐

Active hub
- ☐

☐

☐

Content filter
- ☐

☒

☐

Router (✖ Missed)

🚫 Your answer to this question is incorrect.

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

- ☐

☐

☐

Tunnel
- ☐

☒

☐

Exception (✖ Missed)
- ☐

☐

☐

Access Point (AP)
- ☐

☐

☐

Entry

🚫 Your answer to this question is incorrect.

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

- ☐

☒

☐

Load balancer (✖ Missed)
- ☐

☐

☐

HIDS
- ☐

☐

☐

Firewall
- ☐

☐


☐

Captive portal



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

 Your answer to this question is incorrect.

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



☐ ☒  True ( Missed)

☐ ☐ ☐ False

 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)

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](#)

☐ ☐ ☐ Layer 3 switch

☐ ☐ ☐ Hardware firewall

 Your answer to this question is incorrect.


► 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.

► **In order to provide you with the best online experience this website uses cookies.**
URL filtering restricts access to Internet sites based on which of the following criteria?

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

☐ ☐ ☐ 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?

☐ ☒  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)

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](#)

☐ ☐ ☐ VLAN tagging

☐ ☐ ☐ Wireless networking

🚩 Your answer to this question is incorrect.

► 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

☐ ☐ ☐ 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.

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](#)

Try Again (/component/communityquiz/quiz/10-comptia-security-plus-certification/53-comptia-security-plus-certification-practice-test-1-exam-sy0-401?Itemid=101)

I agree