

310-301

SUN

Sun Certified Security Administrator for the Solaris 9 Operating System

OfficialCerts.com is a reputable IT certification examination guide, study guides and audio exam provider. We ensure that you pass your 310-301 exam in first attempt and also get high scores to acquire SUN certification.

If you use OfficialCerts 310-301 Certification questions and answers, you will experience actual 310-301 exam questions/answers. We know exactly what is needed and have all the exam preparation material required to pass the exam. Our SUN exam prep covers over 95% of the questions and answers that may be appeared in your 310-301 exam. Every point from pass4sure 310-301 PDF, 310-301 review will help you take SUN 310-301 exam much easier and become SUN certified.

Here's what you can expect from the OfficialCerts SUN 310-301 course:

- * Up-to-Date SUN 310-301 questions as experienced in the real exam.*
- * 100% correct SUN 310-301 answers you simply can't find in other 310-301 courses.*
- * All of our tests are easy to download. Your file will be saved as a 310-301 PDF.*
- * SUN 310-301 brain dump free content featuring the real 310-301 test questions.*

SUN 310-301 certification exam is of core importance both in your Professional life and SUN certification path. With SUN certification you can get a good job easily in the market and get on your path for success. Professionals who passed SUN 310-301 exam training are an absolute favorite in the industry. You will pass SUN 310-301 certification test and career opportunities will be open for you.

<http://news.ift.org/?newsid=exams.asp?examcode=310-301>



Question: 1

Part of a fire protection plan for a computer room should include:

- A. Procedures for an emergency shutdown of equipment.
- B. A sprinkler system that exceeds local code requirements.
- C. The exclusive use of non-flammable materials within the room.
- D. Fireproof doors that can be easily opened if an alarm is sounded.

Answer: A

Question: 2

What network mapping tool uses ICMP (Internet Control Message Protocol)?

- A. Port scanner
- B. Map scanner
- C. Ping scanner
- D. Share scanner

Answer: C

Question: 3

Which of the following would be most effective in preventing network traffic sniffing?

- A. Deploy an IDS (Intrusion Detection System).
- B. Disable promiscuous mode.
- C. Use hubs instead of routers.
- D. Use switches instead of hubs.

Answer: D

Question: 4

A user wants to send an e-mail and ensure that the message is not tampered with while in transit. Which feature of modern cryptographic systems will facilitate this?

- A. Confidentiality
- B. Authentication
- C. Integrity
- D. Non-repudiation

Answer: C

Question: 5

Which of the following type of attack CANNOT be deterred solely through technical means?

- A. Dictionary
- B. Man in the middle
- C. DoS (Denial of Service)
- D. Social engineering

Answer: D

Question: 6

An organization is implementing Kerberos as its primary authentication protocol. Which of the following must be deployed for Kerberos to function?

- A. Dynamic IP (Internet Protocol) routing protocols for routers and servers.
- B. Separate network segments for the realms.
- C. Token authentication devices.
- D. Time synchronization services for clients and servers.

Answer: D

Question: 7

Which of the following is likely to be found after enabling anonymous FTP (File Transfer Protocol) read/write access?

- A. An upload and download directory for each user.
- B. Detailed logging information for each user.
- C. Storage and distribution of unlicensed software.
- D. Fewer server connections and less network bandwidth utilization.

Answer: C

Question: 8

NetBus and Back Orifice are each considered an example of a(n):

- A. Virus
- B. Illicit server
- C. Spoofing tool
- D. Allowable server

Answer: B

Question: 9

Which of the following access control models introduces user security clearance and data classification?

- A. RBAC (Role Based Access Control)
- B. NDAC (Non-Discretionary Access Control)
- C. MAC (Mandatory Access Control)
- D. DAC (Discretionary Access Control)

Answer: C

Question: 10

Why are unique user IDs critical in the review of audit trails?

- A. They CANNOT be easily altered.
- B. They establish individual accountability.
- C. They show which files were changed.
- D. They trigger corrective controls.

Answer: B

Question: 11

Which of the following would NOT be considered a method for managing the administration of accessibility?

- A. DAC (Discretionary Access Control) list
- B. SAC (Subjective Access Control) list

- C. MAC (Mandatory Access Control) list
- D. RBAC (Role Based Access Control) list

Answer: B

Question: 12

In which risk assessment stage does the security auditor map the system and resources on a network?

- A. Penetration
- B. Cancellation
- C. Activation
- D. Discovery

Answer: D

Question: 13

In a typical corporate environment, which of the following resources demands the highest level of security on the network?

- A. Purchasing
- B. Engineering
- C. Sales
- D. Accounting

Answer: D

Question: 14

What is another term for a network security manager who acts as a potential hacker (a person looking for security loopholes)?

- A. An agent
- B. An auditor
- C. An assessor
- D. An analyzer

Answer: B

Question: 15

What is the essential element in the implementation of any security plan?

- A. Testing to make sure any server-side scripts are secure.
- B. Testing patch levels.
- C. Proper firewall configuration.
- D. Auditing

Answer: D

Question: 16

A malicious user has connected to your system and learned that specifics of your operating system, including its current patch levels and the operating system name. What is the term for this type of scanning attack?

- A. SYN detection
- B. TCP priming

- C. Cache poisoning
- D. Stack fingerprinting

Answer: D

Question: 17

What is the most important step in securing a Web server?

- A. Logging all HTTP activity.
- B. Enabling system-wide encryption.
- C. Placing the operating system, Web server program, and server files on the same partition.
- D. Placing the operating system, Web server program, and server files on separate partitions.

Answer: D

Question: 18

What is the primary security risk in SNMP?

- A. Login names and passwords are not encrypted.
- B. Damaging programs can be executed on the client.
- C. Damaging programs can be executed on the server.
- D. Passwords and data are transferred in cleartext.

Answer: D

Question: 19

Lucy is a systems administrator who wants to block all NNTP traffic between her network and the Internet. How should she configure her firewall?

- A. Configure the firewall to block all incoming and outgoing packets except for those with the source and destination port of 119. Then, allow all traffic with destination ports above 1024 to traverse the firewall.
- B. Configure the firewall to block all incoming packets with the source port of 119, and outgoing Packets with a source port lower than 1024. Then, block all packets with the destination port of 119 and with a source port lower than 1024.
- C. Configure the firewall to block all incoming packets with the destination port of 119, and to Block outgoing packets with the destination port of 119.
- D. Configure the firewall to block all incoming packets with the source port of 119.

Answer: C

Question: 20

Which port or ports are used for SMTP?

- A. 20 and 21
- B. 25
- C. 53
- D. 161 and 162

Answer: B

Question: 21

Which type of attack causes a remote host to crash because it cannot respond to any new TCP connection requests?

OfficialCerts.com Certification Exam Full Version Features;

- Verified answers researched by industry experts.
- Exams **updated** on regular basis.
- Questions, Answers are downloadable in **PDF** format.
- **No authorization** code required to open exam.
- **Portable** anywhere.
- 100% success **Guarantee**.
- **Fast**, helpful support 24x7.

View list of All exams we offer;

<http://www.officialcerts.com/allexams.asp>

To contact our Support;

<http://www.officialcerts.com/support.asp>

View FAQs

<http://www.officialcerts.com/faq.asp>

Download All Exams Samples

<http://www.officialcerts.com/samples.asp>

To purchase Full Version and updated exam;

<http://www.officialcerts.com/allexams.asp>



Shop now using **PayPal**



3COM	CompTIA	Filemaker	IBM	LPI	OMG	Sun
ADOBE	ComputerAssociates	Fortinet	IISFA	McAfee	Oracle	Sybase
APC	CWNP	Foundry	Intel	McData	PMI	Symantec
Apple	DELL	Fujitsu	ISACA	Microsoft	Polycom	TeraData
BEA	ECCouncil	GuidanceSoftware	ISC2	Mile2	RedHat	TIA
BICSI	EMC	HDI	ISEB	NetworkAppliance	Sair	Tibco
CheckPoint	Enterasys	Hitachi	ISM	Network-General	SASInstitute	TruSecure
Cisco	ExamExpress	HP	Juniper	Nokia	SCP	Veritas
Citrix	Exin	Huawei	Legato	Nortel	See-Beyond	Vmware
CIW	ExtremeNetworks	Hyperion	Lotus	Novell	Google	

You have made the
Right Choice

You are becoming member of most comprehensive, accurate, highest quality and lowest cost certification resource in the world.

