

310-301 braindumps

SUN SCSA10

310-301: Sun Certified Security Administrator

Practice Exam: 310-301 Exams

Exam Number/Code: 310-301

Exam Name: Sun Certified Security Administrator

Questions and Answers: 240 Q&As

([SCSA10](#))



Exam : [310-301](#)

"Sun Certified Security Administrator", also known as 310-301 exam, is a SUN certification. With the complete collection of exam questions, Just4Study has assembled to take you through 240 Q&As to your 310-301 exam preparation. In the 310-301 exam resources, you will cover every field and category in SUN Certification helping to ready you for your successful SUN Certification.

The exam questions cover the latest real test and with all the correct answer. we promise the Q&A for SUN SCSA10 310-301 (Sun Certified Security Administrator) examination of original title complete coverage. 310-301 exam questions help you pass the exam.

Just4Study 310-301 Feature:

* High quality - High quality and valued for the 310-301 Exam: 100% Guarantee to Pass Your 310-301 exam and get your SCSA10 certification.

* Authoritative - Authoritative braindumps with complete details about 310-301 exam.

* Cheaper - Our Just4Study products are cheaper than any other website. With our completed SCSA10 resources, you will minimize your **SUN SCSA10** cost and be ready to pass your 310-301 exam on Your First Try, 100% Money Back Guarantee included!

* Free - Try free SCSA10 demo before you decide to buy it in <http://www.Just4Study.com>.

Just4Study Guarantee:

Just4Study provides the most competitive quality of all exams for the customers, we guarantee your success at the first attempt with only our Certification Question&Answers, if you do not pass the 310-301 exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

Free 310-301 Demo Download

Just4Study offers free demo for SCSA10 310-301 exam (Sun Certified Security Administrator). You can check out the interface, question quality and usability of our practice exams before you decide to buy it. We are the only one site can offer demo for almost all products.

The Questions & Answers cover the latest real test and with all the correct answer. we promise the Q&A for **SUN SCSA10 310-301** examination of original title complete coverage. 310-301 Questions & Answers help you pass the exam. Otherwise, we will give you a full refund.

VUE/Prometric Code: 310-301

Exam Name: Sun Certified Security Administrator(SCSA10)

Questions and Answers: 240 Q&A

[SUN 310-301](#) Test belongs to one of the SCSA10 certified test, if needs to obtain the SCSA10 certificate, you also need to participate in other related test, the details you may visit the [SCSA10](#) certified topic, in there, you will see all related SCSA10 certified subject of examination.

Just4Study professional provide SCSA10 310-301 the newest Q&A, completely covers 310-301 test original topic. With our complete SCSA10 resources, you will minimize your SCSA10 cost and be ready to pass your 310-301 tests on Your First Try, 100% Money Back Guarantee included!

Just4Study Help You Pass Any IT Exam

[Just4Study.com](#) offers incredible career enhancing opportunities. We are a team of IT professionals that focus on providing our customers with the most up to date material for any IT certification exam. This material is so effective that we Guarantee you will pass the exam or your money back.

Exam : SUN 310-301

Title : Sun Certified Security Administrator Solaris 9

1. How do you distinguish between denial of service attacks and programming errors?

- A. You cannot make this distinction.
- B. You examine the audit events for the process.
- C. You verify that the process user ID is that of a valid user.
- D. You check the binary against the Solaris Fingerprint Database.

Answer: A

2. Which cryptographic assurances are provided by SSL?

- A. confidentiality, integrity, availability
- B. authorization, confidentiality, message integrity
- C. confidentiality, client authentication, server authentication
- D. authentication, confidentiality, access control, non-repudiation

Answer: C

3. User fred runs a program that consumes all of the system's memory while continuously spawning a new program. You decide to terminate all of fred's programs to put a stop to this. What command should you use?

- A. kill -u fred
- B. pkill -U fred
- C. passwd -l fred
- D. kill `ps -U fred -o pid`

Answer: B

4. What cryptographic assurance is provided by public key cryptography that is NOT provided by secret key cryptography?

- A. integrity
- B. confidentiality
- C. authentication
- D. non-repudiation

Answer: D

5. Which is a public key encryption algorithm?

- A. AH
- B. AES
- C. RSA
- D. PGP
- E. IDEA

Answer: C

6. Which threat can be mitigated by setting the Open Boot PROM security mode to full?

- A. system panics
- B. booting into single user mode
- C. remotely accessing the console
- D. logging in as root at the console

Answer: B

7. Which syslog facility level specification can be used to record unsuccessful attempts to su(1M)?

- A. su.warning
- B. cron.debug
- C. kernel.alert
- D. auth.warning

Answer: D

8. /var/adm/messages contains this output:

Jan 28 21:23:18 mailhost in.telnetd[20911]:

[ID 808958 daemon.warning] refused connect from
ns.foo.com (access denied)

Why was this line generated?

- A. A user connecting from ns.foo.com failed to authenticate.
- B. The user daemon is not allowed to log in from ns.foo.com.
- C. A portscan was run against mailhost from ns.foo.com.
- D. The TCP Wrapper configuration does not allow telnet connections from ns.foo.com.

Answer: D

9. Click the Exhibit button.

Which connection demonstrates that telnet has been denied using TCP Wrappers?

- A. Connection 1
- B. Connection 2
- C. Connection 3
- D. Connection 4

Answer: A

10. Which two regular user PATH assignments expose the user to a Trojan horse attack? (Choose two.)

- A. PATH=/usr/bin:/bin
- B. PATH=/usr/bin:/sbin:/usr/sbin
- C. PATH=/usr/bin:/sbin:/usr/sbin:
- D. PATH=./usr/bin:/sbin:/usr/sbin

Answer: CD

11. Which two types of host keys are supported by Solaris Secure Shell? (Choose two.)

- A. AES
- B. RSA
- C. DSA
- D. DES
- E. 3DES

Answer: BC

12. Which two services support TCP Wrappers by default in the Solaris 9 OE? (Choose two.)

- A. inetd
- B. rpcbind

- C. sendmail
- D. automountd
- E. Solaris Secure Shell

Answer: AE

13. Which evasion technique can NOT be detected by system integrity checks?

- A. installing a rootkit
- B. adding user accounts
- C. abusing an existing user account
- D. installing a loadable kernel module

Answer: C

14. Which command can customize the size for system log file rotation?

- A. dmesg
- B. logger
- C. logadm
- D. syslog
- E. syslogd

Answer: C

15. What command loads a DSA identity into a Solaris Secure Shell authentication agent?

- A. ssh-add
- B. ssh-agent
- C. ssh-keyadd
- D. ssh-keyload
- E. ssh-load-identity

Answer: A

16. Which command generates client key pairs and adds them to the \$HOME/.ssh directory?

- A. ssh-add
- B. ssh-agent
- C. ssh-keygen
- D. ssh-keyadd

Answer: C

17. Which setting in the /etc/system file limits the maximum number of user processes to 100 to prevent a user from executing a fork bomb on a system?

- A. set maxuprc = 100
- B. set maxusers = 100
- C. set user_procs = 100
- D. set max_nprocs = 100

Answer: A

18. Which is uncharacteristic of a Trojan horse program used to escalate privileges?

- A. It is installed in /usr/bin.
- B. It is owned by a normal user.
- C. It has the same name as a common program.
- D. It contains additional functionality which the user does not expect.

Answer: A

19. The system administrator finds a Trojaned login command using md5 and the Solaris Fingerprint Database. What is true about the system administrator's incident response tasks?

- A. The server must be rebuilt.

- B. BSM will identify the attacker.
- C. All other replaced system files can be identified using md5 and the Solaris Fingerprint Database.
- D. All other replaced system files can be identified using md5 and the Solaris Fingerprint Database and replaced with trusted versions.

Answer: A

20. Which statement about denial of service attack is FALSE?

- A. Denial of service is always preventable.
- B. Multiple machines may be used as the source of the attack.
- C. Service is denied on the victim host when a key resource is consumed.
- D. A denial of service attack is an explicit attempt by an attacker to prevent legitimate users of a service from using that service.

Answer: A

[310-301 Braindumps](#)

Related 310-301 Exams

[310-200](#) Sun Certified System Administrator for Solaris 10 OS.Part 1

[310-202](#) Sun Certified System Administrator for Solaris 10 OS.Part 2

[310-302](#) Sun Certified Network Administrator for Solaris 10 OS

[310-303](#) Sun Certified Security Administrator for the Solaris 10 OS

[310-301](#) Sun Certified Security Administrator

Other SUN Exams

[310-878](#) [310-011](#) [310-150](#) [310-035](#) [310-014](#) [310-036](#) [310-200](#) [310-600](#)

[310-625](#) [310-100](#) [311-203](#) [310-044](#) [310-053](#) [310-062](#) [310-610](#) [310-055](#)

[310-](#) [310-045](#) [310-400](#) [310-019](#)

[600Big5](#)