

310-301 SCSA10

SUN 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 questions and answers, TestInside 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.

Quality and Value for the 310-301 Exam TestInside Practice Exams for SUN **SCSA10** Certification 310-301 are written to the highest standards of technical accuracy, using only certified subject matter experts and published authors for development.

TestInside provide the professional Q&A.

1. We offer free update service for three month.

After you purchase our product, we will offer free update in time for three month.

2. High quality and Value for the 310-301 Exam.

310-301 simulation test questions, including the examination question and the answer, complete by our senior IT lecturers and the SCSA10 product experts, included the current newest 310-301 examination questions.

3. 100% Guarantee to Pass Your SCSA10 exam and get your SCSA10 Certification.

If you do not pass the SUN Certification 310-301 exam (Sun Certified Security Administrator) on your first attempt using our TestInside testing engine and pdf file, we will give you a FULL REFUND of your purchasing fee.

use TestInside 310-301 Q&A ensure you pass the exam at your first try.

TestInside 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!

[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.

TestInside Testing Engine Features

Comprehensive questions and answers about 310-301 exam

310-301 exam questions accompanied by exhibits

Verified Answers Researched by Industry Experts and almost 100% correct

310-301 exam questions updated on regular basis

Same type as the certification exams, 310-301 exam preparation is in multiple-choice questions (MCQs).

Tested by multiple times before publishing

Try free 310-301 exam demo before you decide to buy it in Test-Inside.com.

Note: This pdf demo do not include the question's picture.

Exam : SUN 310-301

Title : Sun Certified Security Administrator Solaris 9

1. 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

2. 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

3. 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

4. /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

5. 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

6. 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

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

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

Answer: C

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

- A. AES

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

Answer: A

14. 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

15. Which is a public key encryption algorithm?

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

Answer: C

16. 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

17. 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

18. 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

19. 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

20. 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

[More 310-301 Information](#)

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

[212-200](#) Sun Certified System Administrator for Solaris 10 OS, Part 1

[212-202](#) Sun Certified System Administrator for Solaris 10 OS, Part 2

Other SUN Exams

[310-812](#) [310-015](#) [310-200](#) [310-814](#) [310-400](#) [310-615](#) [310-560](#) [310-231](#)

[310-092](#) [310-875](#) [212-811](#) [310-810](#) [310-203](#) [310-019](#) [310-035](#) [310-620](#)

[310-813](#) [310-084](#) [212-202](#) [412-600](#)