

## **Exam4Test 310-301 Exams**

### *SUN Sun Certified Security Administrator*



**Practice Exam:** 310-301

**Exam Number/Code:** 310-301

**Exam Name:** Sun Certified Security Administrator

**Questions and Answers:** 240 Q&As

### **Exam Description**

Order : [310-301 Exam](#)

1. Exam4Test 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.

Exam4Test **Practice Exams** for 310-301 are written to the highest standards of technical accuracy, provided by our certified subject matter experts and published authors for development.

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

We guarantee your success in the first attempt. If you do not pass the **SCSA10** "310-301" (Sun Certified Security Administrator on your first attempt, send us the official result. We will give you a FULLY REFUND of your purchasing fee and send you another same value product for free.

4. Exam4Test SCSA10 310-301 Exam Downloadable.

Our PDF or Testing Engine Preparation Material of SCSA10 310-301 exam provides everything which you need to pass your exam. The SCSA10 Certification details are researched and produced by our Professional Certification Experts who are constantly using industry experience to produce precise, and logical. You may get "310-301 exam" questions from different websites or books, but logic is the key. Our Product will help you not only pass in the first Sun Certified Security Administrator( SCSA10 ) exam try, but also save your valuable time.

Comprehensive questions with complete details about 310-301 exam.

310-301 exam questions accompanied by exhibits. Verified Answers Researched by Industry Experts and almost 100% correct.

Drag and Drop questions as experienced in the Real SCSA10 exam. 310-301 exam questions updated on regular basis.

Like actual SCSA10 Certification exams, 310-301 exam preparation is in multiple-choice questions (MCQs). Tested by many real SCSA10 exams before publishing.

Try free SCSA10 exam demo before you decide to buy it in <http://www.Exam4Test.com>

High quality and Valued for the 310-301 Exam: 100% Guarantee to Pass Your 310-301 exam and get your SCSA10 Certification. Come to <http://www.Exam4Test.com> The easiest and quickest way to get your SCSA10 Certification.

Exam4Test professional provides SCSA10 310-301 the newest Q&A, completely covers 310-301 test original topic. With our completed SCSA10 resources, you will minimize your SCSA10 cost and be ready to pass your 310-301 tes on Your First Try, 100% Money Back Guarantee included!

## 310-301 Exam Study Guide

310-301 exam is regarded as one of the most favourite [SCSA10 Certifications](#). Many IT professionals prefer to add 310-301 exam among their credentials. Exam4Test not only caters you all the information regarding the 310-301 exam but also provides you the excellent 310-301 study guide which makes the certification exam easy for you.

### Exam4Test 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 Exam4Test.com

### Exam4Test Help You Pass Any IT Exam

[Exam4Test.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. 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

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. 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

4. 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

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

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

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. 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

8. 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

9. 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

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 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

12. 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

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 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

15. Which is a public key encryption algorithm?

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

Answer: C

16. 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

17. 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

18. /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

19. 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

20. 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

[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

#### **Other SUN Exams**

[310-230](#)      [310-877](#)      [310-220](#)      [310-016](#)      [310-036](#)      [310-014](#)      [310-045](#)      [310-066](#)

[310-810](#)      [310-303](#)      [310-345](#)      [310-055](#)      [212-055](#)      [310-065](#)      [310-](#)      [310-878](#)

[065Big5](#)      [310-](#)

[055Big5](#)

[311-203](#)      [310-092](#)      [310-301](#)