



SUN 310-301

Exam Name: Sun Certified Security Administrator

Q & A : 240 Q&As

Pdf Demo

Quality and Value for the 310-301 Exam

[Just4Exams Practice Exams](#) for SUN SCSA10 310-301 are written to the highest standards of technical accuracy, using only certified subject matter experts and published authors for development.

100% Guarantee to Pass Your 310-301 Exam

If you do not pass the SCSA10 310-301 exam on your first attempt using our Just4Exams **310-301 testing engine and pdf study guide**, we will give you a FULL REFUND of your purchasing fee.

Downloadable, Interactive 310-301 Testing engines and PDF Version

Our Exam Preparation Material provides you everything you will need to take a [SCSA10 certification](#) examination. Details are researched and produced by [SUN Certification](#) Experts who are constantly using industry experience to produce precise, and logical.

Free 310-301 Exams:

This is demo only, this pdf do not include the questions and answers picture

Exam : SUN 310-301

Title : Sun Certified Security Administrator Solaris 9

1. 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

2. 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

3. /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

4. 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

5. 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

6. 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

7. 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

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

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

Answer: C

9. 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

10. 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

11. 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

12. 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

13. 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

14. 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

15. 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

16. 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

17. 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

18. Which is a public key encryption algorithm?

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

Answer: C

19. 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

20. 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

More [310-301 Braindumps](#) Information

Related 310-301 Exams

310-200	310-202	310-302	310-303	310-301
212-200	212-202			

Other SUN Exams

212-056	310-019	310-230	310-051	310-100
310-035	310-065Big5	212-811	310-814	310-502
		212-814	310-877	310-811
310-083	310-150	310-400	412-600	310-013
310-813	310-231			