Exam : **310-301**

Title : Sun Certified Security Administrator

Version : DEMO

1.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
Correct:A
2.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
Correct:D
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.
Correct:D
4.Which two types of host keys are supported by Solaris Secure Shell? (Choose two.)
A.AES
B.RSA
C.DSA
D.DES
E.3DES
Correct:B C
5.Which is a public key encryption algorithm?
A.AH
B.AES
C.RSA
D.PGP
E.IDEA
Correct:C
6.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 **Correct:C**
7.Click the Exhibit button. Which connection demonstrates that telnet has been denied using TCP Wrappers?

Connection 1

```
$ telnet foo.com
Trying 10.100.0.24...
Connected to foo.com.
Escape character is '^]'
Connection to foo.com closed by foreign host.
```

Connection 2

```
$ telnet foo.com
Trying 10.100.0.24...
telnet: Unable to connect to remote host: Connection refused
```

Connection 3

```
$ telnet foo.com
foo.com: Unknown host
```

Connection 4

```
$ telnet foo.com
Trying 10.100.0.24...
Connected to foo.com.
Escape character is '^]'.


SunOS 5.9

login: foo
Password:
Login incorrect
```

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

Correct: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

Correct:C

9.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

Correct:A E

10.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
Correct:B

11.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.
Correct:A

12.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
Correct:A

13.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.
Correct:A

14.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
Correct:C D

15.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.
Correct:A

16.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`

Correct:B

17.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

Correct:C

18.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.

Correct:A

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

A.dmesg

B.logger

C.logadm

D.syslog

E.syslogd

Correct:C

20.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

Correct:D

Trying our product !

★ **100%** Guaranteed Success

★ **100%** Money Back Guarantee

★ **365 Days** Free Update

★ **Instant Download** After Purchase

★ **24x7** Customer Support

★ Average **99.9%** Success Rate

★ More than **69,000** Satisfied Customers Worldwide

★ Multi-Platform capabilities - **Windows, Mac, Android, iPhone, iPod, iPad, Kindle**

Need Help

Please provide as much detail as possible so we can best assist you.
To update a previously submitted ticket:

Guarantee & Policy | Privacy & Policy | Terms & Conditions

Any charges made through this site will appear as Global Simulators Limited.
All trademarks are the property of their respective owners.