# Global Information Assurance Certification Paper

# SSH – 10 Questions

1. What are the advantages of SSH over telnet?
    a. Encrypted communication.
    b. Faster using compression.
    c. Can be used to forward X11 over the established secure channel.
    d. All of the above,

**Correct answer is d.**
*Ref: Page 2*

2. If you fail to connect to the remote SSH daemon what happens next?
    a. Your TCP connection is dropped.
    b. Your TCP connection hangs.
    c. The remote SSH daemon can fall back to rsh.
    d. The remote SSH daemon can fall back to telnet.

**Correct answer is c.**
*Ref: Page 7*

3. What is not one of the SSH authentication methods?
    a. RSA-based user authentication.
    b. Host-based trust files.
    c. PAM (Pluggeable Authentication Module)
    d. Rhosts combined with RSA-based authentication.

**Correct answer is c.**
*Ref: Pages 8, 9, 10*

4. How do you forward X11 traffic via a SSH connection?
    a. You configure SSH to redirect all traffic to port 6000 on your computer.
    b. You configure SSH to redirect all traffic to port 6000 on your computer and place the appropriate statement in /etc/hosts.allow.
    c. You telnet from the remote X11 server, to your computer on port 22.
    d. You do nothing; SSH automatically sets up Xauthority data on the remote host.

**Correct answer is: d.**
*Ref: Page 13*

5. How do you configure SSHD to compile with TCP wrapper support?
    a. ./configure --with-socks
    b. ./configure --with-login
    c. ./configure --with-libwrap
    d. ./configure --with-rsh

**Correct answer is c.**
*Ref: Page 27*

6. What is the most efficient way to run the SSH daemon?
    a. As a standalone daemon.
    b. From /etc/inetd.conf
    c. With the command line argument `sshd --cache-file'.
    d. With the command line arguments `sshd --cache-file –quick-login'.

**Correct answer is a.**

*Ref: Page 24*

7. How do you launch SSHD with a 1024 bit server key?
    a. sshd -k 1024
    b. sshd -p 1024
    c. sshd -b 1024
    d. sshd -h 1024

**Correct answer is c.**
*Ref: Page 32*

8. What is the purpose of the ~/.ssh/authorized_keys file ?
    a. Automatically redirects X11 over the secure channel.
    b. Holds the public keys allowed to access a specified account.
    c. Allows you to upload your public key to a known key server.
    d. Holds the private keys allowed to access a specified account.

**Correct answer is b.**
*Ref: Page 37*

9. What is the purpose of configuring SSHD with the configure option '--with-libwrap' ?
    a. To compile SSHD against the default libraries.
    b. To compile SSHD with library wrappers.
    c. To enable SSHD to run from /etc/inetd.conf.
    d. To compile with support for TCP_Wrappers.

**Correct answer is d.**
*Ref: Page 27*

10. What is the default level of compression with SSH?
    a. 5
    b. 6
    c. 4
    d. 3

**Correct answer is b.**
*Ref: Page 36*

## Linux Practicum - 25 Questions

1. When using Psionic Portsentry what does the line `KILL_ROUTE="/sbin/ipchains -I input -s $TARGET -j DENY -l" accomplish?
    a. Automatically drops the route of the offending host.
    b. Automatically denies all traffic from the offending host.
    c. Automatically denies all traffic from the offending host and emails root of the attack.
    d. Automatically denies all traffic from the offending host and places a log entry in the appropriate log file.

**Correct answer is d.**
*Ref: Page 110*

2. What are the three basic targets when using IPCHAINS?
    a. ACCEPT, DENY/REJCT, FORWARD
    b. ACCEPT, DENY/REJECT, MASQ/REDIRECT

c. ACCEPT, DENY/REJECT, INPUT/OUTPUT
d. ACCEPT, DENY/REJECT, LOG

**Correct answer is b.**
*Ref: Page 91*

3. Which is not one of the three basic chains ?
    a. input
    b. output
    c. masq
    d. forward

**Correct answer is c.**
*Ref: Page 91*

4. On a default RedHat 6.x system, where does the kernel source reside?
    a. /usr/lib
    b. /usr/local/src
    c. /usr/src/linux
    d. /usr/local/src/linux

**Correct answer is c.**
*Ref: Page 43*

5. If your kernel was too big after compiling, what command should you run to compress it?
    a. blilo
    b. clilo
    c. bzlilo
    d. make bzlilo

**Correct answer is d.**
*Ref: Page 47*

6. If you want to limit your users to 3 simultaneous logins and a file size no larger than 20 megabytes, what file would you modify to accomplish this?

    a. /etc/security/login.conf
    b. /etc/pam.d/limits.conf
    c. /etc/security/limits.conf
    d. /etc/security/access.conf

**Correct answer is c.**
*Ref: Page 26*

7. How would you translate all traffic originating from your internal class C network (192.168.1.0) to route over the Internet?
    a. ipchains -A forward -s 192.168.1.0/24 -d 0/0 -j MASQ
    b. ipchains -A forward -s 0/0 -d 192.168.1.0/25 -j MASQ
    c. ipchains -A masq -s 192.168.1.0/24 -d 0/0 -j MASQ
    d. ipchains -A masq -s 0/0 -d 192.168.1.0/24 -j MASQ

**Correct answer is a.**
*Ref: Page 97*

8. How many run levels are present in RedHat linux?
    a. four

b. five
c. six
d. eight

**Correct answer c.**
*Ref: Page 17*

9. If you were in `single user mode', which run level would you be running in?
    a. five
    b. six
    c. three
    d. one

**Correct answer is d.**
*Ref: Page 17*

10. What file would you configure to disable reboots via the Ctrl+Alt+Del key sequence?
    a. /etc/security/login
    b. /etc/services
    c. /etc/inted.conf
    d. /etc/inittab

**Correct answer is d.**
*Ref: Page 18*

11. What file controls log rotation on a RedHat linux system?
    a. /etc/logrotated.conf
    b. /etc/logrotate.conf
    c. /etc/sysconfig.conf
    d. /etc/logconfig.conf

**Correct answer is b.**
*Ref: Page 31*

12. What file controls the exact data to be logged?
    a. /etc/log.conf
    b. /etc/messages.conf
    c. /etc/syslog.conf
    d. /etc/logrotate.d

**Correct answer is c.**
*Ref: Page 33*

13. What port does syslogd listen on to receive log messages from remote hosts?
    a. 543
    b. 541
    c. 514
    d. 415

**Correct answer is c.**
*Ref: Page 36*

14. How would you configure syslogd to accept log messages from remote hosts?
    a. modify /etc/rc.d/init.d/syslog ; add daemon syslogd -r ; restart syslogd
    b. modify /etc/rc.d/syslog ; add daemon syslogd -m ; restart syslogd
    c. modify /etc/rc.d/init.d/syslog ; add daemon syslogd -r ; restart syslogd

d. modify /etc/rc.d/rc.local ; add daemon syslogd -r ; restart syslogd

**Correct answer is a.**
*Ref: Page 36*

15. What file would you modify to send log messages to a remote host?
    a. /etc/rc.d/rc.log
    b. /etc/syslogd.conf
    c. /etc/messages.conf
    d. /etc/syslog.conf

**Correct answer is d.**
*Ref: Page 41*

16. What is the purpose of the program `tcpdchk' ?
    a. To ensure your TCP/IP stack is running properly.
    b. To ensure packets are routing properly across your network.
    c. To check the syntax of /etc/inetd.conf /etc/hosts.allow /etc/hosts.deny
    d. To determine what ports are currently open on your machine.

**Correct answer is c.**
*Ref: Page 68*

17. How does RedHat linux implement NFS?
    a. Using module-space NFS.
    b. Using user-space NFS.
    c. Using kernel-space NFS.
    d. Using monolithic NFS.

**Correct answer is c.**
*Ref: Page 75*

18. What file would you modify to mount NFS at boot time?
    a. /etc/mounts
    b. /etc/rc.d/rc.local
    c. /etc/imports
    d. /etc/fstab

**Correct answer is d.**
*Ref: Page 77*

19. What file would you modify to export NFS to specific hosts?
    a. /etc/fstab
    b. /etc/exports
    c. /etc/nfs.conf
    d. /etc/rc.d/rc.local

**Correct answer is b.**
*Ref: Page 79*

20. How would you enable SWAT to run on your RedHat machine?
    a. modify /etc/rc.d/rc.local ; uncomment the SWAT line at the bottom.
    b. modify /etc/sysconfig.conf ; uncomment the SWAT line at the bottom.
    c. modify /etc/inetd.conf
    d. modify /etc/swat.conf

**Correct answer is c.**
*Ref: Page 84*

21. How would you change the default policy to DENY for the chain "input" ?
    a. /sbin/ipchains -P input DENY
    b. /sbin/ipchains - F input DENY
    c. /sbin/ipchains -L input DENY
    d. /sbin/ipchains -X input DENY

**Correct answer is a.**
*Ref: Page 92*

22. How would you expire the current password every 90 days and give a 14 day warning for user netwrkr?
    a. passwd -M 90 -W 14 netwrkr
    b. chage -M 90 -W 14 netwrkr
    c. chage -L 90 -M 14 netwrkr
    d. passwd -W 90 -M 14 netwrkr

**Correct answer is b.**
*Ref: Page 28*

23. To require the root password for single user mode which file(s) would you modify?
    a. /etc/inittab
    b. /etc/fstab ; /etc/inittab
    c. /etc/inittab ; /etc/lilo.conf
    d. /etc/boot.conf ; /etc/inittab

**Correct answer is c.**
*Ref: Page 18*

24. When running Samba, what file(s) would you modify to limit access to specific hosts?
    a. /etc/smb.conf
    b. /etc/samba.conf ; /etc/hosts.default
    c. /etc/hosts.equiv ; /etc/smb.conf
    d. /etc/hosts ; /etc/smb.conf

**Correct answer is a.**
*Ref: Page 85*

25. How would you restart /etc/inetd.conf ?
    a. kill -9 inetd
    b. kill -1 inetd
    c. kill -SIGHUP inetd
    d. kill -HUP inetd

**Correct answer is d.**
*Ref: Page 62*

## Network Time Protocol (NTP) - 10 Questions

1. Where is the default NTP configuration file located?
    a. /etc/ntpd.conmf
    b. /var/run/ntp.conf
    c. /etc/ntp.conf

d. /var/state/ntp/ntp.conf

**Correct answer is c.**
*Ref: Page 27*

2. If you are syncing against 2 Stratum 3 servers and 1 Stratum 2 server, what stratum number is your server ?
    a. 3
    b. 2
    c. 4
    d. 5

**Correct answer is a.**
*Ref: Page 11*

3. What is the purpose of the drift file?
    a. To determine the drift from the stratum 1 to the stratum server.
    b. To determine the drift from your machine to the server you are syncing against.
    c. To keep the system clock accurate in the event of a network partition that causes the host to lose time synch information.
    d. To determine the drift between two or more stratum severs.

**Correct answer is c.**
*Ref: Page 12*

4. Why would you sync against more than one stratum server?
    a. To get the most accurate time available.
    b. To prevent someone from skewing your clocks by impersonating an external NTP server.
    c. To keep your drift file up to date.
    d. To allow machines to use the NTP proxy running on your machine.

**Correct answer is b.**
*Ref: Page 13*

5. What is the purpose of NTP?
    a. To prevent attackers from getting into your system.
    b. To prevent hackers from running distributed denial of service attacks against your network.
    c. To allow networks of machines to keep system clocks in synch.
    d. To prevent a hacker from modifying the time in your log files.

**Correct answer is c.**
*Ref: Page 4*

6. Why is it important to not sync your network against a public stratum one server?
    a. Because there are fewer stratum one servers than stratum two servers.
    b. Because the stratum two servers are as reliable as the stratum one server.
    c. Because the stratum two server allows many thousands of machines to synch without overloading primary servers.
    d. All of the above.

**Correct answer is d.**
*Ref: Page 9*

7. What is the benefit of configuring your NTP server to “broadcast” time info to local clients?
    a. The entire process is faster.
    b. More machines can receive updates simultaneously.
    c. Less network traffic generated.
    d. None of the above.

**Correct answer is d.**
*Ref: Page 22*

8. Which program allows you to administer and interrogate running NTP servers for statistical information?
    a. xntpd
    b. xntpdc
    c. ntpd
    d. ntpdc

**Correct answer is b.**
*Ref: Page 25*

9. What is the term to define a person who synchs against a public time server without first obtaining permission from the system administrator?

    a. NTP Looser.
    b. Blacklisted.
    c. Clock Sucker
    d. Cheap

**Correct answer is c.**
*Ref: Page 28*

10. What is a *pseudo clock* ?
    a. Causes your server to synchronize to its own system clock.
    b. A stratum 4 server.
    c. A master/slave server within your organization.
    d. None of the above.

**Correct answer is a.**
*Ref: Page 19.*

## Unix Basics for Security Professionals – 25 Questions

1. What file(s) control crontab access ?
    a. hosts.allow
    b. cron.allow
    c. hosts.allow; hosts.deny
    d. cron.allow ; cron.deny

**Correct answer is d.**
*Ref: Page 119*

2. What command would you execute to view the contents of your crontab file?
    a. crontab –e
    b. crontab –f
    c. crontab –r
    d. crontab –l

**Correct answer is d.**
*Ref: Page 118.*

3. What port does sendmail run on?
    a. 21
    b. 25
    c. 23
    d. 24

**Correct answer is b.**
*Ref: Page 107*

4. What is the purpose of ARP?
    a. Translate hostnames to IP addresses.
    b. Translate hostnames to MAC addresses.
    c. Translate IP addresses to MAC addresses.
    d. Translate hostnames and MAC addresses to IP addresses.

**Correct answer is c.**
*Ref: Page 101 & 102*

5. When you run "netstat –in" what does the MTU define?
    a. The type of network you are running i.e. star, bus, token ring
    b. The largest packet that may be transmitted on a given network.
    c. The speed at which your network is routing packets.
    d. The current SNMP statistics for a given interface.

**Correct answer is b.**
*Ref: Page 86*

6. What does is the purpose of the renice command?
    a. To allow normal users to request more CPU time.
    b. To allow normal users to lower the nice value to speed up a given process.
    c. To control how much CPU time a given process will receive.
    d. To increase the I/O on your system.

**Correct answer is c.**
*Ref: Page 82*

7. If you wanted to see only the user names listed in your /etc/passwd file what command would you run?
    a. cat /etc/passwd | grep users
    b. grep –f2 –d /etc/passwd
    c. cat /etc/passwd | grep id
    d. grep –f2 –d: /etc/passwd

**Correct answer is d.**
*Ref: Page 60*

8. Under Solaris what is the purpose of the /sbin directory?

a. Contains system configuration files.
b. Holds third party software.
c. Contains programs critical for boot sequence.
d. Contains files used to talk to system devices.

**Correct answer is c.**
*Ref: Page 28*

9. What is the longest directory pathname that can be specified in Solaris?

a. 255
b. 512
c. 1024
d. 1120

**Correct answer is c.**
*Ref: Page 25*

10. How many run levels are available in Solaris?

a. 5
b. 6
c. 7
d. 4

**Correct answer is b.**
*Ref: Page 15*

11. When run as the superuser what does the command "init 6" do?
a. Shutdown the system.
b. Send a 10 minute shutdown warning to all users.
c. Reboot the system.
d. Reboot the system with a 10 minute advance warning to all users logged in.

**Correct answer is c.**
*Ref: Page 15*

12. You run the command "ls –la" and see the file sans.html with the file permissions "-rwxr-sr-x"; What does the "s" signify?

a. This is a "special" file that is used by apache web server.
b. This is a "special" file that is used by apache web server for SSL connections.
c. This file has the set group id bit set.
d. This file has the set user id bit set.

**Correct answer is c.**
*Ref: Page 36*

13. What is the purpose of the "sticky bit" ?
a. To allow root to modify that file as necessary.
b. To allow department administrators to perform maintenance on a given directory.
c. Specifies that only the owner may remove file(s).
d. Specifies that only members of the group may remove file(s).

**Correct answer is c.**

*Ref: Page 37*

14. What is the octal notation for -rwxr-xr-x ?
    a. 0600
    b. 0700
    c. 1777
    d. 755

**Correct answer is d.**
*Ref: Page 38*

15. What information is **not** stored in the inodes?
    a. Access and creation time.
    b. Permissions and ownership.
    c. File size and number of blocks used.
    d. Pointer to the data blocks.

**Correct answer is a.**
*Ref: Page 44 (Creation time is not stored in the inode information)*

16. If you wanted to recursively copy an entire directory tree what command would you use?
    a. copy –r
    b. copy –R
    c. copy –d
    d. copy –L

**Correct answer is b.**
*Ref: Page 46*

17. How would you create a symbolic link from the file sans to file org ?

    a. ln –s org sans
    b. ln –S sans org
    c. ln –s sans org
    d. ln –S org sans

**Correct answer is c.**
*Ref: Page 49*

18. How would you terminate an out of control process to include leaving a core file for debugging?
    a. kill –9
    b. kill –1
    c. kill –3
    d. kill –15

**Correct answer is c.**
*Ref: Page 80*

19. What does “pid” stand for ?
    a. Parent ID
    b. Priority ID
    c. Parent Process ID
    d. Process ID

**Correct answer is d.**

*Ref: Page 78*

20. What is the purpose of the "at" command?
    a. To run scheduled jobs on a regular basis.
    b. To run scheduled jobs more securely than crond
    c. To run a job just once at some time in the future.
    d. To replace the insecure crond shipped with Solaris.

**Correct answer is c.**
*Ref: Page 120*

21. At the end of a crontab entry you see "> /dev/null 2>&1"; what does the 2>&1 signify?
    a. Send all output to /dev/null
    b. Send all normal output to /dev/null
    c. Redirect the normal and error output to /dev/null
    d. Redirect /dev/null output to tty1

**Correct answer is c.**
*Ref: Page 116*

22. When running the command "netstat –rn" what does the flag "U" designate?
    a. The route is actively being used or is up.
    b. The route is slower than other available routes.
    c. The route is experiencing receive errors.
    d. The loopback adapter is incorrectly configured.

**Correct answer is a.**
*Ref: Page 100*

23. How would you display partition information for every available file system?

    a. du
    b. cat /etc/fstab
    c. df
    d. df –m ntfs ufs ffs

**Correct answer is c.**
*Ref: Page 43*

24. What is the longest filename that can be created under Solaris?

    a. 1024
    b. 1023
    c. 255
    d. 256

**Correct answer is c.**
*Ref: Page 25*

25. How would you turn off chargen services on your Solaris machine?
    a. edit /etc/rcX.d
    b. edit /etc/services
    c. edit /etc/inetd.conf ; kill –HUP inetd
    d. edit /etc/inetd.conf

**Correct answer is c.**

*Ref: Page 17, 142*

## Kerberos Basics – 10 Questions

1. What does Kerberos not provide?
    a. Secure communications via Telnet.
    b. Strong authentication under proper operation.
    c. Ability to run in conjunction with other authentication schemes.
    d. Secure authentication.

**Correct answer is a.**
*Ref: Page 39*

2. What is the KDC?
    a. System where all authentication takes place.
    b. Any entity that gets a service ticket for a Kerberized service.
    c. Publically accessable database that holds all public Kerberos keys.
    d. The client which obtains the secure key.

**Correct answer is a.**
*Ref: Page 5*

3. How would a user initially authenticate using Kerberos?
    a. Login to the KDC.
    b. Request a ticket via email.
    c. Type kinit.
    d. SSH in to the preauth server with the correct username / password.

**Correct answer is c.**
*Ref: Page 18, 19*

4. When a user is authenticated, what data is not contained within the ticket?
    a. The users public key.
    b. Session Key.
    c. Server Principal.
    d. Client Principal.

**Correct answer is a.**
*Ref: Page 11,12,13*

5. What is a known weakness in Kerberos?
    a. The initial user authentication password is sent in clear text.
    b. The users private key is sent in clear text.
    c. The request for the ticket is sent in clear text.
    d. The user must login to the Key Server.

**Correct answer is c.**
*Ref: Page 18*

6. What is an “application server”?
    a. The primary Key Distribution Center.
    b. The main Kerberos server.
    c. Any Kerberized program that clients communicate with using Kerberos tickets.
    d. Any entity that gets a service ticket for a Kerberized service.

**Correct answer is c.**
*Ref: Page 5*

7. What is a system requirement of Kerberos?
    a. NTP server.
    b. DNS Server.
    c. Authentication Server.
    d. All of the above.

**Correct answer is d.**
*Ref: Page 7*

8. What is the default encryption scheme for Kerberos?
    a. Blowfish
    b. Triple DES.
    c. MD5
    d. 56-bit DES.

**Correct answer is d.**
*Ref: Page 9*

9. How many tickets are generated to authenticate a user?
    a. One
    b. Two
    c. Three
    d. Four

**Correct answer is b.**
*Ref: Page 12*

10. What is the second ticket encrypted with?
    a. The users public key.
    b. The users principal key.
    c. The key of the server principal.
    d. The server principal's public key.

**Correct answer is c.**
*Ref: Page 12*

## Common Issues and Vulnerabilities in Unix Security - 25 Questions

1. In your shadow file you see "root:$1$cmCn291b$4Ei5EqDHLUGYB03/:11118:0:99999:-7:-1:-1:134540356". What is the salt that is being used to permute the encryption algorithm?

    a. $4E
    b. 11118
    c. $1
    d. DHLUG

**Correct answer is c.**
*Ref: Page 18*

2. While viewing /etc/profile you see “ulimit –c 0”. What does this mean?
    a. The user may create files of unlimited size.
    b. The administrator has eliminated core files.
    c. The administrator is giving all users unlimited cpu time.
    d. The administrator has removed the session time limit.

**Correct answer is b.**
*Ref: Page 30*

3. What are some of the common attacks again set-UID scripts?
    a. Environment attacks.
    b. Race conditions.
    c. Symlink tricks.
    d. All of the above.

**Correct answer is d.**
*Ref: Page 51*

4. What is an alternative to set-UID scripts?
    a. Writing programs in perl and using suidperl.
    b. Properly configure /etc/security/limits.conf
    c. Properly configure /etc/profile.
    d. Properly configure /etc/security/access.conf

**Correct answer is a.**
*Ref: Page 58*

5. What is the definition of “chroot”?
    a. Writing a set-UID program in a C or Perl wrapper.
    b. Change your current login to that of the root user.
    c. A Unix system call that allows a process to give up access to all but a small portion of the file system.
    d. A Unix system call that moves all set-UID programs to a special file system that runs without root privileges.

**Correct answer is c.**
*Ref: Page 59*

6. How would an attacker hide his presence on your system?
    a. Replace ps.
    b. Hide files in /dev
    c. Replace syslogd.
    d. All of the above.

**Correct answer is d.**
*Ref: Page 78, 79*

7. Why would someone put files in the /dev directory?
    a. To modify your device drivers.
    b. To link binaries against older version of libc.
    c. To have those files get lost in the noise from all the device files located within the directory.
    d. To install a sniffer.

**Correct answer is c.**

*Ref: Page 76*

8. What octal notation should all .rhosts files on your system be?
    a. 0700
    b. 0400
    c. 0444
    d. 0600

**Correct answer is d.**
*Ref: Page 87*

9. What is a more secure way to run X ?
    a. Disable the xhost command.
    b. Use Kerberos authentication.
    c. Tunnel your X session through SSH.
    d. All of the above.

**Correct answer is d.**
*Ref: Page 94*

10. How can you implement cabling security within your network?
    a. Use coaxial cable.
    b. Use two-layer pressurized conduit.
    c. Install devices to detect voltage drops from sniffers being used.
    d. Use thick steel conduit.

**Correct answer is b.**
*Ref: Page 132*

11. What are some common steps you can use to prevent session hijacking?
    a. Configure your firewall(s) to block spoofed packets at all ingress points.
    b. Configure your firewall(s) to block source-routed packets at all ingress points.
    c. Require all users to use some form of encrypted communication i.e. SSH, Secure Copy.
    d. All of the above.

**Correct answer is d.**
*Ref: Page 100*

12. What are some of the common exploits against a machine running X windows?
    a. Buffer overflow attacks
    b. Denial of service attacks
    c. Session Hijacking
    d. All of the above.

**Correct answer is d.**
*Ref: Page 92*

13. What are some of the common mistakes made when securing a computer space?
    a. Doors with exterior accessible hinges.
    b. Drop down ceilings.
    c. Both a & b.
    d. None of the above.

**Correct answer is c.**

*Ref: Page 128 & 129*

14. How is dynamic memory implemented in a Unix process?
    a. Subroutine.
    b. Frame.
    c. Stack Frame.
    d. Frame pointer.

**Correct answer is c.**
*Ref: Page 37, 38, 39*

15. How does a buffer overflow work?
    a. Attempts to write past the end of the allocated string buffer and clobber the return execution address.
    b. Attempts to write past the end of the allocated string buffer and clobber the Stack Frame.
    c. Attempts to overwrite the Stack Frame and write past the data for the main program.
    d. Attempts to overwrite the subroutine buffer and write past the data for the Stack Frame.

**Correct answer is a.**
*Ref: Page 39*

16. What is the purpose of the /etc/shadow file?
    a. To allow users to view only their password.
    b. To allow administrators the ability to force strong passwords.
    c. To fool hackers with bogus passwords.
    d. To allow only the root user the ability to view users encrypted passwords.

**Correct answer is d.**
*Ref: Page 23*

17. What are some of the RPC based program(s) that are commonly attacked/exploited?
    a. NIS
    b. NFS
    c. Both a & b.
    d. Httpd

**Correct answer is c.**
*Ref: Page 3*

18. What program compares the cryptographic checksum of a binary against a known good database of checksum values?
    a. Shaft
    b. Tripwire
    c. Abacus Checksum
    d. RPM

**Correct answer is b.**
*Ref: Page 80*

19. What happens if someone steals your .Xauthority file?
    a. Nothing, the file is encrypted.
    b. They have access to your X display.
    c. Nothing since the person doesn't know your password.

d. Both a & c.

**Correct answer is b.**
*Ref: Page 90*

20. What are some of the drawbacks to using .Xauthority?
    a. Users end up reverting to using xhost.
    b. Attackers can launch buffer overflow attacks against your X server.
    c. Attackers can create symlinks to your .Xauthority file and hijack your X session.
    d. Both b & c.

**Correct answer is a.**
*Ref: Page 91*

21. What is "expreserve" ?
    a. A utility which helps httpd serve commonly accessed web pages faster.
    b. A utility which caches commonly used information for faster access.
    c. A utility which is used by emacs to automatically recover your current buffer in the event the system crashes while a user is editing a file.
    d. A utility which is used by vi to automatically recover vi buffers in the event the system crashed while the user is editing a file.

**Correct answer is d.**
*Ref: Page 48*

22. What are some daemon(s)s that chroot naturally?
    a. Ftpd & named
    b. Tftpd & httpd
    c. Tftpd & sshd
    d. Ftpd & sshd

**Correct answer is a.**
*Ref: Page 62*

23. What are some considerations you should make when running critical systems that depend on backup power?
    a. Ensure you schedule frequent tests of your backup system(s).
    b. Ensure all critical systems are plugged into your backup power source(s).
    c. Always get electrical work done by a reliable vendor.
    d. All of the above.

**Correct answer is d.**
*Ref: Page 133*

24. What are some of the most common programs contained in a root kit?
    a. trojaned login & ftp
    b. trojaned sshd
    c. trojaned ping
    d. Both a & b.

**Correct answer is d.**
*Ref: Page 74*

25. How can you prevent your users from reading and cracking your password file?
    a. Remove world readable permissions from /etc/passwd.
    b. Install password shadowing.

c. Remove world readable permissions from /etc.
d. None of the above.

**Correct answer is b.**
*Ref: Page 23.*

## One time passwords – 10 Questions

1. What are some of the problems with Unix passwords?
    a. They are sent over the network in clear text.
    b. They are limited to 9 characters.
    c. Attackers can easily break encrypted string used on the Unix imposed 9 character limit.
    d. Both b & c.

**Correct answer is a.**
*Ref: Page 4*

2. What are the different types of two-factor devices?
    a. Challenge/Response & Synchronous.
    b. Synchronous & Private Key.
    c. Challenge/Response & Public Key.
    d. Opie & PGP.

**Correct answer is a.**
*Ref: Page 8*

3. Where is a users private key stored in Public Key Authentication?
    a. On the main key server.
    b. On the OTP server.
    c. One the main Kerebos server.
    d. None of the above.

**Correct answer is d.**
*Ref: Page 9*

4. Where is the opieaccess file normally located?
    a. /etc/
    b. /usr/bin
    c. /usr/local/bin
    d. /opt/

**Correct answer is a.**
*Ref: Page 18*

5. Commercial OTP solutions generally user an open source, non-relational database back-end?
    a. True
    b. False

**Correct answer is b.**
*Ref: Page 33*

6. What are some of the common files which will be replaced when installing and using OPIE?
    a. login
    b. ftp
    c. su
    d. All of the above.

**Correct answer is d.**
*Ref: Page 18*

7. What octal notation should be placed upon /etc/opiekeys ?
    a. 0444
    b. 0400
    c. 0600
    d. 0100

**Correct answer is b.**
*Ref: Page 21*

8. What information is located in /etc/opiekeys ?
    a. All users public / private keys.
    b. Encrypted OPIE secrets.
    c. Both A & B.
    d. None of the above.

**Correct answer is b.**
*Ref: Page 21*

9. What are some of the freely available OTP solutions?
    a. Security ID
    b. Defender
    c. OPIE & S/Key
    d. SafeWord

**Correct answer is c.**
*Ref: Page 11*

10. What is some of the user resistance associate with using OTP?
    a. Too difficult for the average user to master.
    b. Too many passwords to remember.
    c. Lots of hand-holding required.
    d. Both a & c.

**Correct answer is d.**
*Ref: Page 13*

## Solaris Practicum – 25 Questions

1. What is a frequent problem associated with backing up data?
    a. Using the wrong type of backup media.
    b. Failing to test the integrity of the backup.
    c. Failing to backup critical file systems.
    d. Backing up too often.

**Correct answer is b**.

*Ref: Page 97*

2. How would you prevent a user for logging in on a serial port?
    a. Edit the appropriate line in /etc/inetd.conf.
    b. Edit the appropriate line in /etc/serial.conf
    c. Edit the appropriate line in /etc/inittab.
    d. Kill the serial daemon.

**Correct answer is c.**
*Ref: Page 36*

3. What file dictates the file systems that will be mounted at boot time?
    a. /etc/fstab
    b. /etc/vfstab
    c. /etc/mount.conf
    d. None of the above.

**Correct answer is b.**
*Ref: Page 43*

4. What file can you edit to help prevent buffer overflow attacks?
    a. /etc/security/limits.conf
    b. /etc/inetd.conf
    c. /etc/system
    d. /etc/limits.conf

**Correct answer is c.**
*Ref: Page 85*

5. What program would you use to gather data on system resource usage on an ongoing basis?
    a. ps
    b. top
    c. sar
    d. vmstat

**Correct answer is c.**
*Ref: 70*

6. What program would you use to gather system resource usage in real time?
    a. sar
    b. ps
    c. top
    d. vmstat

**Correct answer is d.**
*Ref: Page 70*

7. How would you enable process accounting?
    a. accton
    b. pact
    c. accton /var/adm/pacct
    d. acct

**Correct answer is c.**

*Ref: Page 75*

8. How would you disable process accounting?
    a. acctoff
    b. accton
    c. sar
    d. acctoff /var/adm/pact

**Correct answer is b.**
*Ref: Page 75*

9. Why is running process accounting on a heavily loaded system unwise?
    a. Performance degradation.
    b. Alerts hackers that you are watching the system.
    c. Can cause processes to stop running.
    d. Both b & c.

**Correct answer is a.**
*Ref: Page 76*

10. By default sshd is configure with TCP wrapper support.
    a. True
    b. False

**Correct answer is b.**
*Ref: Page 53*

11. What is the benefit of mounting the root filesystem read only and nosuid?
    a. Prevents attackers from running buffer overflows.
    b. Easier than placing daemons in a chrooted environment.
    c. Both a & b.
    d. None of the above.

**Correct answer is d.**
*Ref: Page 45*

12. How should you remotely login to perform administrative tasks requiring root access?
    a. SSH in as root and perform the work necessary.
    b. SSH into your normal account and su to root.
    c. Telnet into your normal account and su to root.
    d. Either b or c.

**Correct answer is b.**
*Ref: Page 62*

13. What is the purpose of the /etc/ftpusers file?
    a. To allow certain users ftp access.
    b. To list users not allowed ftp access.
    c. To log the activities of certain users logging in and transferring files.
    d. Both a & b.

**Correct answer is b.**
*Ref: Page 64*

14. Where would you set the default UMASK and PATH for your users?
    a. /etc/default/.login

b. /etc/profile
c. /etc/skel
d. Both a & b.

**Correct answer is d.**
*Ref: Page 81*

15. Where would you set the max file descriptors allowed per user?
    a. /etc/security/limits.conf
    b. /etc/shadow
    c. /etc/passwd
    d. /etc/system

**Correct answer is d.**
*Ref: Page 85*

16. What program modifies file permissions under Solaris in an effort to make things more secure?
    a. YASSP
    b. Secure-mode
    c. Fix-modes
    d. Bastille

**Correct answer is c.**
*Ref: Page 102*

17. How would you configure /etc/hosts.allow to accept all traffic from 192.168.1.0/29?
    a. ALL: 192.168.1.0/255.255.255.248
    b. ALL: 192.168.1.0/29
    c. ALL: 192.168.1.0/29 255.255.255.248
    d. None of the above.

**Correct answer is a.**
*Ref: Page 56*

18. How would you prevent remote root logins via SSH ?
    a. Modify /etc/hosts.allow
    b. Modify /etc/pam.d/login
    c. Modify sshd_config
    d. Modify ssh_config

**Correct answer is c.**
*Ref: Page 54*

19. What are some of the benefits of SSH?
    a. Drop in secure replacement for rsh/rcp/rlogin.
    b. Allows tunneling of other protocols.
    c. Host-to-host encryption solution.
    d. All of the above.

**Correct answer is d.**
*Ref: Page 49*

20. What is the function of TCP Wrappers?
    a. Controls access based on hostname / destination port.
    b. Controls access based on IP address / destination port.

c. Controls access based on IP address / source port.
d. Controls access based on hostname / source port.

**Correct answer *is b.***
*Ref: Page 50*

21. What file lists all the files that have been installed on your system?
    a. /var/sadm/contents
    b. /var/sadm/contents/install
    c. /var/sadm/install/contents
    d. /var/log/install/contents

**Correct answer is c**.
*Ref: Page 20*

22. When first setting up a Solaris machine, you should ensure the network connection is active to correctly configure all interfaces.
    a. True
    b. False

**Correct answer is b.**
*Ref: 13, 16*

23. When installing a patch, what does "Return code 2" indicate?
    a. You are missing Core system files.
    b. The patch applies to a package that is not installed on the system.
    c. The patch has already been applied from the OS CD.
    d. The MD5 checksum isn't correct.

**Correct answer is c.**
*Ref: Page 24*

24. Your users report they are unable to start up Netscape Communicator; what is the solution?
    a. Re-install the latest version of Communicator.
    b. Start nscd.
    c. Install the Communicator package to /usr/local
    d. Modify /etc/init.d to enable the Netscape daemon.

**Correct answer is b.**
*Ref: Page 27*

25. How could you securely mount the /usr filesystem?
    a. nosuid
    b. read-only
    c. noguid
    d. Both a & b.

**Correct answer is b**.
*Ref: Page 46*

# Unix Forensics – 10 Questions

1. What file keeps a snapshot of all users currently logged in?

    a. wtmp
    b. utmp
    c. syslog
    d. secure

**Correct answer is b.**
*Ref: Page 77*

2. Why are SUID root files dangerous?
    a. When executed, the effective UID is that of the program, not the user.
    b. Allows unprivileged users to assume the superuser role.
    c. Targets for hackers to attack to gain uid 0 privileges.
    d. All of the above.

**Correct answer is d.**
*Ref: Page 86, 87*

3. What program can list all open network connection and those programs that are using those connections?
    a. netstat
    b. ps aux
    c. lsof
    d. vmstat

**Correct answer is c.**
*Ref: Page 45, 46*

4. What command could indicate your NIC is in promiscuous mode?
    a. netstat
    b. lsof
    c. ifconfig
    d. vmstat

**Correct answer is c.**
*Ref: Page 46*

5. An incident handling toolkit should contain dynamically linked executables?
    a. True.
    b. False.

**Correct answer is b.**
*Ref: Page 25*

6. What is the most volatile during evidence collection?
    a. Memory
    b. Network connections.
    c. File System
    d. Disk Blocks

**Correct answer is a.**

*Ref: Page 36*

7. What does a file integrity assessment tell you?
    a. Details which files have been altered.
    b. Indicates a possible compromise.
    c. Details which lines of a file have been altered.
    d. Both a & b.

**Correct answer is d.**
*Ref: Page 56, 59*

8. How can you detect files that have a link count of zero?
    a. lsof +L0
    b. lsof +L1
    c. find
    d. None of the above.

**Correct answer is b.**
*Ref: Page 90*

9. What command lists bad login attempts.
    a. last
    b. lastbad
    c. lastb
    d. btmp

**Correct answer is c.**
*Ref: Page 81*

10. What is the benefit of using dd over tar during evidence collection?
    a. dd includes blocks of data marked as “deleted.
    b. Dd is ideal for backing up a particular directory tree.
    c. Dd has the ability to ability to swap byte pairs.
    d. Both a & c.

**Correct answer is d.**
*Ref: Page 48, 49.*

## Running Unix Applications Securely – 25 Questions

1. Why would you run BIND in a chroot () ed environment?
    a. To prevent someone from compromising your zone files.
    b. To help protect against someone gaining root privileges on your name server.
    c. To prevent attackers from executing zone transfers.
    d. Both a & b.

**Correct answer is b.**
*Ref: Page 94*

2. What does the file module mod_access provide?

a. Enables basic authentication with the username/passwords stored in Berkeley DB files.
b. Handles HTTP basic authentication.
c. Handles the basic allow/deny access control.
d. Handles the anonymous username/password authentication.

**Correct answer is c.**
*Ref: Page 29*

3. Which file module(s) is/are not included by default with Apache?
    a. mod_access
    b. mod_auth
    c. mod_auth_db
    d. Both b & c.

**Correct answer is c.**
*Ref: Page 29*

4. When running Apache what file or files would you modify to deny access to all directories and files?
    a. httpd.conf
    b. srm.conf
    c. access.conf
    d. .htaccess

**Correct answer is c.**
*Ref: Page 33*

5. Where would be the best place(s) to enable Sendmails' anti-spam functionally?
    a. All mail servers that receive email from the outside world.
    b. All mail servers in your organization.
    c. All internal mail servers.
    d. Any server acting as a smart host.

**Correct answer is a.**
*Ref: Page 118*

6. How would you limit your web server to serve requests made solely by your local workstation?
    a. edit httpd.conf to "Listen 192.168.1.0:80"
    b. edit access.conf to "Listen 192.168.1.0:80"
    c. edit httpd.conf to "Listen 127.0.0.1:80"
    d. edit access to conf to "Listen 127.0.0.1:80"

**Correct answer is c.**
*Ref: Page 47*

7. What type(s) of authentication does Apache support?
    a. MD5
    b. Basic
    c. Digest
    d. Both b & c.

**Correct answer id d.**
*Ref: Page 43*

8. What feature in Apache allows HTML pages with the execute permission bit set, to be parsed for server-side includes?
    a. shtml_mod
    b. html_mod
    c. XBitHack
    d. Exec_mod

**Correct answer is c.**
*Ref: Page 39*

9. If you have FollowSymLinks turned on, this will affect the performance of your server.
    a. True
    b. False

**Correct answer is b.**
*Ref: Page 38*

10. What port does a mail server listen on?
    a. 23
    b. 22
    c. 24
    d. 25

**Correct answer is d.**
*Ref: Page 107*

11. Sendmail is a _____
    a. MTP
    b. MTA
    c. MHA
    d. MUA

**Correct answer is b.**
*Ref: Page 104, 105*

12. You are assessing a clients name server and see file "named.boot". What version of BIND is this client likely running?
    a. BIND V8
    b. BIND V6
    c. BIND V4
    d. BIND V5

**Correct answer is c.**
*Ref: Page 80 (Written in; put out in class)*

13. Why would someone attempt to perform a zone-transfer against your organization?
    a. To update DNS information.
    b. To gain knowledge about your internal hosts and network.
    c. To ensure they have the most up to date DNS information available.
    d. To attempt to poison your cache file.

**Correct answer is b.**
*Ref: Page 68*

14. SSL uses _____ encryption.
    a. Private Key

b. Public Key
c. One time
d. Network Socket.

**Correct answer is b.**
*Ref: Page 55*

15. What file defines the permitted file operations for FTP users?
    a. /etc/ftpusers
    b. /etc/ftpaccess
    c. /etc/ftpconversions
    d. /etc/ftphosts

**Correct answer is b.**
*Ref: Page 10*

16. When running WU FTPD , how would you deny all traffic from 192.168.1.3 ?
    a. Modify /etc/ftpusers
    b. Modify /etc/ftphosts
    c. Modify /etc/ftpaccess
    d. Modify /etc/hosts.deny

**Correct answer is d.**
*Ref: Page 16*

17. What file defines which ftp users can login from a given IP address.
    a. /etc/ftpusers
    b. /etc/ftphosts
    c. /etc/ftpaccess
    d. /etc/ftpgroups

**Correct answer is b.**
*Ref: Page 10*

18. What function does the Indexes Option perform?
    a. Lists files and directories that might otherwise be hidden.
    b. Assists the webmaster by indexing all web pages on a server.
    c. Prints a directory listing if there is no index.html.
    d. Both a & c.

**Correct answer is d.**
*Ref: Page 40*

19. What file contains directives that can override settings for a directory?
    a. .htpaccess
    b. .htaccess
    c. .access_conf
    d. mod_conf

**Correct answer is b.**
*Ref: Page 41*

20. What are some common security issues when running BIND?
    a. Buffer overflows.
    b. Cache Poisoning.
    c. Giving the public too much information about your internal network.

d. All of the above.

**Correct answer is d.**
*Ref: Page 65, 66*

21. What is IP-Based authentication?
    a. Reversing the IP address to a hostname.
    b. Looking up the hostname to check against the IP address.
    c. Denying access to spoofed IP addresses.
    d. All of the above.

**Correct answer is d.**
*Ref: Page 72*

22. What is a CNAME ?
    a. An alias.
    b. A way to associate functional names with specific machines.
    c. A Canonical Name.
    d. All of the above.

**Correct answer is d.**
*Ref: Page 87*

23. What file contains all files that are uploaded and downloaded?
    a. ftplog
    b. xferlog
    c. ftpdlog
    d. messages

**Correct answer is b.**
*Ref: Page 16*

24. How would you prevent files from being uploaded that started with "." ?
    a. Modify /etc/ftpacess
    b. Modify /etc/ftpusers to include a path-filter
    c. Modify /etc/ftpaccess to include a path-filter
    d. None of the above.

**Correct answer is c.**
*Ref: Page 20*

25. Why should you use the allow-transfer option?
    a. To control access to your name server.
    b. To restrict zone transfers.
    c. To prevent recursive queries from outside hosts.
    d. Both b & c.

**Correct answer is b.**
*Ref: Page 82*

## Unix Security Tools and Their Uses – 25 Questions

1. What mode under Satan probes UDP ports from 32767 to 33500 ?

a. Heavy
b. Normal
c. Exhaustive
d. Light

**Correct answer is a.**
*Ref: Slide 237*

2. What option helps you understand your output format string when using Watcher?
    a. –f
    b. –h
    c. –V
    d. –v

**Correct answer is d.**
*Ref: Slide 193*

3. How do you list your users passwords when using nessusd?
    a. nessusd –passwd
    b. nessusd –L
    c. nessusd –l
    d. nessus –v

**Correct answer is b.**
*Ref: Slide 285*

4. What percentage of passwords can be guessed in an hour?
    a. 10%
    b. 5%
    c. 20%
    d. 15%

**Correct answer is b.**
*Ref: Slide 405*

5. What program forces a user to pick a good password?
    a. crack
    b. password +
    c. npassword
    d. passwd+

**Correct answer is d.**
*Ref: Slide 404*

6. What form of authentication does NTPv3 use?
    a. DES-CBC
    b. Blowfish
    c. MD5
    d. Triple DES

**Correct answer is a.**
*Ref: Slide 391*

7. What command would you use to view all keys on your PGP key ring?
    a. pgp –ka
    b. pgp –kvv

c. pgp –kc
d. pgp –esa

**Correct answer is b.**
*Ref: Slide 375*

8. What compile time option defines who to send mail to for unauthorized user who tries to use sudo?
    a. --with-alerter
    b. --with-altermail
    c. --with-logging
    d. --with-syslog

**Correct answer is b.**
*Ref: Slide 337*

9. What type of nmap scan would you execute to see if a firewall is stateful or packet filter based?
    a. TCP SYN/FIN
    b. TCP SYN
    c. TCP FIN
    d. ACK/WIN

**Correct answer is d.**
*Ref: Slide 272*

10. What option would you use to limit scans to ports in a given range?
    a. nmap –P
    b. nmap –sT
    c. nmap –sU
    d. nmap –p

**Correct answer is d.**
*Ref: Slide 276*

11. What does "nmap –b" do?
    a. Scans for open broadcast addresses.
    b. Scans using half open TCP connections.
    c. FTP bounce attack.
    d. Dictates what interface to send and receive packets on.

**Correct answer is c.**
*Ref: NMAP man page (3).*

12. Why would sudo quit with an exit value of 1?
    a. There is a problem with the checksum of the sudo binary.
    b. There is a permission problem.
    c. The command you are trying to execute is not safe.
    d. sudo has detected an attempt to spoof a command.

**Correct answer is b.**
*Ref: SUDO man page (1)*

13. How would you change the log file to one of your choosing when running ISS?
    a. iss –d
    b. iss –m

c. iss –o
d. iss –l

**Correct answer is c.**
*Ref: ISS Man page (1)*

14. What command option directs LSOF to list the PPID number in PPID column?
    a. lsof –P
    b. lsof –p
    c. lsof –R
    d. lsof –S

**Correct answer is c.**
*Ref: LSOF Man page (8)*

15. What command option directs suid.chk to not follow NFS mounted partitions.
    a. –m
    b. –n
    c. –N
    d. –s

**Correct answer is b.**
*Ref: MAN Page (1)*

16. What program checks to see if your device files have write permissions turned on?
    a. dev.sh
    b. dev.chk
    c. swat
    d. device.chk

**Correct answer is b.**
*Ref: Man Page (1)*

17. How often does sudo re-prompt for a password?
    a. 10 minutes
    b. 5 minutes
    c. 15 minutes
    d. None of the above.

**Correct answer is b.**
*Ref: Slide 329*

18. What program is used to test access control rules?
    a. access-control
    b. tcpdchk
    c. tcpdmatch
    d. tcpd

**Correct answer is c.**
*Ref: Slide 299*

19. What facility will tcpd use by default?
    a. Syslog
    b. Messages
    c. Info
    d. auth.adm

**Correct answer is a.**
*Ref: Slide 302*

20. Ident works on _____ .
    a. tcp-based connections
    b. udp-based connections
    c. All TCP/IP protocols.
    d. Both a & b.

**Correct answer is a.**
*Ref: Slide 307*

21. What program provides locking when modifying system configuration files?
    a. vi
    b. emacs
    c. RCS
    d. pico

**Correct answer is c.**
*Ref: Slide 395, 396*

22. Crack is a _____ program.
    a. proactive
    b. reactive
    c. preventative
    d. Both a & c.

**Correct answer is b.**
*Ref: Slide 435*

23. Those words that are more likely to be chosen should be put in _____ dictionary groups.
    a. sorted
    b. lower-numbered
    c. higher-numbered
    d. Alphabetized

**Correct answer is b.**
*Ref: Slide 417*

24. What configuration language does Log check use?
    a. egrep
    b. grep
    c. pattern matching
    d. None of the above.

**Correct answer is b.**
*Ref: Slide 162*

25. What program can detect several known bugs in NFS implementations?
    a. nfschk
    b. nfsbug
    c. rcpchk
    d. rcpcheck

**Correct answer is b.**

*Ref: Slide 217*

Last Updated: October 18th, 2017

# Upcoming Training


| | | | |
|---|---|---|---|
| **SANS 2018** | **Orlando, FL** | **Apr 03, 2018 - Apr 10, 2018** | **Live Event** |
| **SANS OnDemand** | **Online** | **Anytime** | **Self Paced** |
| **SANS SelfStudy** | **Books & MP3s Only** | **Anytime** | **Self Paced** |