



Unix Security Guidelines

This document is a general overview of the security considerations for a Unix based server implementation.

Table of Contents

Password Security.....	1
Account Security.....	1
Software Installations	2
Network Services.....	3
File System Security.....	8
Major Services.....	9

Password Security

Generally speaking, the UNIX passwd program places very few restrictions on what may be used as a password. It is important to follow the MnSCU standard when choosing UNIX password parameters. Some implementations may or may not have the ability follow the MnSCU password standard. In these cases, a third-party software may be available or the system administrators may need to enforce passwords strength through security awareness training and security reminders.

MnSCU Standards

Password Policy	Member Server
Enforce password history	≥ 10
Maximum password age	<ul style="list-style-type: none"> • ≤ 30 days for administrator accounts • ≤ 90 days for Faculty and staff accounts • ≤ 180 days for student accounts
Minimum password age	≥ 1 day
Minimum password length	≥ 8 characters
Password must meet complexity requirements	Require alpha & numeric

Account Security

Administration

- Regularly audit your system for dormant accounts and disable any that have not been used for a specified period of time, in accordance with MnSCU's security standard.
- Verify that all accounts have passwords. Check shadow, NIS, and NIS+ passwords to verify the password field is not empty.

Special Accounts

- Ensure that there are no shared accounts (other than root) on high security systems (in accordance MnSCU standards).



- Disable guest accounts and/or do not create guest accounts. Some systems come preconfigured with guest accounts.
- Use special groups to restrict which users can use `su` to become root.
- Disable all default vendor accounts shipped with the Operating System. This should be checked after each upgrade or installation.
- Disable or delete accounts that have no password which execute a command, for example "sync". Delete or change ownership of any files owned by these accounts. Ensure that these accounts do not have any cron or at jobs.
- Do not assign non-functional shells (such as `/bin/false`) to system accounts such as `bin` and `daemon` and to the `sync` account if it is not needed.

root Account

- Restrict the number of people who know the root password. These should be the same users registered with `groupid 0`.
- Do not log in as root over the network, use `su` instead. This provides greater tracking and accountability.
- Verify that root does not have a `~/.rhosts` file.
- Verify that "." is not in root's search path.

.netrc Files

- DO NOT use `.netrc` files unless it is absolutely necessary.
- If `.netrc` files must be used, do not use them to store password information.

GCOS / GECOS Field

This field is optional and only used for informational purposes. It is recommended to use this field for greater account identification such as the user's full name.

Software Installations

- Retrieve the latest patches for your specific operating system, as well as any applications updates (i.e. web server, DNS, etc...) from the appropriate vendors. Install any security patches not yet installed that are recommended for your system.
- Keep your software and patches up to date. Notifications of patch releases are generally done via mailing lists.
- Subscribe to the vendor's security update mailing list for your particular operating system.
- Subscribe to security advisory mailing lists from an incident response such as www.securityfocus.com.



Network Services

/etc/inetd.conf

Inetd.conf is a configuration file that tells inetd which daemons to start while the system is running. It contains the list of servers that inetd invokes when it receives an Internet request over a socket. Some consideration for inetd.conf are as follows:

- Disable any services which you do not require.
- Verify that you have disabled any unnecessary startup scripts. This may be done by removing the executable bit, or renaming the files so they do not start with K or S under /etc/init.d or startup script directory for your system.
- Enable access controls and logging for inetd if your version supports it.
- Consider alternatives to inetd. Xinetd is claimed to have enhanced access control and logging capabilities as well as resistance to DoS attacks.

A list of common /etc/inetd.conf services are as follows:

Service	Function	Comments
bootps	bootp services to diskless clients	<ul style="list-style-type: none">• Necessary for Network Installation Management (NIM) and remote booting of systems• Works concurrently with tftp• Disable in most cases
chargen	character generator (testing only)	<ul style="list-style-type: none">• Available as a TCP and UDP service• Provides opportunity for Denial of Service attacks• Disable unless you are testing your network
cmsd	calendar service (as used by CDE)	<ul style="list-style-type: none">• Runs as root, therefore a security concern• Disable unless you require this service with CDE• Disable on back room database servers
comsat	Notifies incoming electronic mail	<ul style="list-style-type: none">• Used for incoming mail notification via biff• Disable, unless you rely on biff.
daytime	obsolete time service (testing only)	<ul style="list-style-type: none">• Runs as root• Available as a TCP and UDP service• Provides opportunity for a Denial of Service PING attacks• Service is obsolete and used for testing only• Disable
discard	/dev/null service (testing only)	<ul style="list-style-type: none">• Available as TCP and UDP service• Used in Denial of Service Attacks• Service is obsolete and used for testing only• Disable
dtspc	CDE Subprocess Control	<ul style="list-style-type: none">• This service is started automatically by the inetd daemon in response to a CDE client requesting a process to be started on the daemon's host. This makes it vulnerable to attacks• Disable on back room servers with no CDE• CDE might be able to function without this service• Disable unless absolutely needed



Service	Function	Comments
echo	echo service (testing only)	<ul style="list-style-type: none">• Available as UDP and TCP service• Could be used in Denial of Service or Smurf attacks• Used to echo at someone else to get through a firewall or start a datastorm• Disable
exec	remote execution service	<ul style="list-style-type: none">• Runs as root user• Requires that you enter a user ID and password, which are passed unprotected• This service is highly susceptible to being snooped• Disable
finger	finger peeking at users	<ul style="list-style-type: none">• Considered highly insecure• Gives out information about your systems and users• Disable or using a more secure version such as cfinger
ftp	file transfer protocol	<ul style="list-style-type: none">• User id and password are transferred unprotected, thus allowing them to be snooped• Disable this service and use a secure shell suite
imap	Internet Mail Access Protocol	<ul style="list-style-type: none">• Ensure that you are using the latest version of this server• Only necessary if you are running a mail server. Otherwise, disable• User ID and password are passed unprotected
login	rlogin service	<ul style="list-style-type: none">• Susceptible to IP spoofing, DNS spoofing• Data, including User IDs and passwords, is passed unprotected• Considered highly insecure• Use a secure shell instead of this service
netstat	reporting of current network status	<ul style="list-style-type: none">• Could potentially give network information to hackers if run on your system• Disable
ntalk	Allows users to talk with each other	<ul style="list-style-type: none">• Runs as root user• Not required on production or back room servers• Disable unless absolutely needed
pcnfsd	PC NFS file services	<ul style="list-style-type: none">• Disable service if not currently in use• If you need a service similar to this, consider Samba, as the pcnfsd daemon predates Microsoft's release of SMB specifications
pop3	Post Office Protocol	<ul style="list-style-type: none">• User IDs and passwords are sent unprotected• Only needed if your system is a mail server and you have clients who are using applications that only support POP3• If your clients use IMAP, use that instead, or use the POP3s service. This service has a Secure Socket Layer (SSL) tunnel• Disable if you are not running a mail server or have clients who need POP services
rexid	remote execution	<ul style="list-style-type: none">• Runs as root user• Peers with the on command• Disable service• Use rsh and rshd instead



Service	Function	Comments
quotad	reports of file quotas (for NFS clients)	<ul style="list-style-type: none"> • Only needed if you are running NFS file services • Disable this service unless required to provide an answer for the quota command • If you need to use this service, keep all patches and fixes for this service up to date
rstatd	Kernel Statistics Server	<ul style="list-style-type: none"> • If you need to monitor systems, use SNMP and disable this service • Required for use of the rup command
rusersd	info about user logged in	<ul style="list-style-type: none"> • This is not an essential service. Disable • Runs as root user • Gives out a list of current users on your system and peers with rusers
rwalld	write to all users	<ul style="list-style-type: none"> • Runs as root user • If your systems have interactive users, you might need to keep this service • If your systems are production or database servers, this is not needed • Disable
shell	rsh service	<ul style="list-style-type: none"> • Considered highly insecure • Disable this service if possible. Use Secure Shell instead • If you must use this service, use the TCP Wrapper to stop spoofing and limit exposures
sprayd	RPC spray tests	<ul style="list-style-type: none"> • Runs as root user • Might be required for diagnosis of NFS network problems • Disable if you are not running NFS
systat	"ps -ef" status report	<ul style="list-style-type: none"> • Allows for remote sites to see the process status on your system • This service is disabled by default. You must check periodically to ensure that the service has not been enabled
talk	establish split screen between 2 users on the net	<ul style="list-style-type: none"> • Not a required service • Used with the talk command • Provides UDP service at Port 517 • Disable unless you need multiple interactive chat sessions for UNIX user
ntalk	"new talk" establish split screen between 2 users on the net	<ul style="list-style-type: none"> • Not a required service • Used with the talk command • Provides UDP service at Port 517 • Disable unless you need multiple interactive chat sessions for UNIX user
telnet	telnet service	<ul style="list-style-type: none"> • Supports remote login sessions, but the password and ID are transmitted in clear text • If possible, disable this service and use Secure Shell for remote access instead
tftp	trivial file transfer	<ul style="list-style-type: none"> • Provides UDP service at port 69 • Runs as root user and might be compromised • If required, create a separate partition to store the files to be served by tftp and limit the tftp daemon to the directory where this partition is mounted. • Ensure that the files in the tftp area are not writable



Service	Function	Comments
time	obsolete time service	<ul style="list-style-type: none"> • Internal function of inetd that is used by rdate command. • Service is outdated. Use ntpdate instead • Disable this only after you have tested your systems (boot/reboot) with this service disabled and have observed no problems
tttdbserver	tool-talk database server (for CDE)	<ul style="list-style-type: none"> • The rpc.ttdbserverd runs as root user and might be compromised • Stated as a required service for CDE, but CDE is able to work without it • Should not be run on back room servers or any systems where security is a concern
uucp	UUCP network	<ul style="list-style-type: none"> • Disable unless you have an application that uses UUCP • Disable the uucp account, including it's login shell, if it is not used at your site. Remember, uucp may be shipped in a dangerous state. • Remove any .rhosts file at the uucp home directory. • Ensure that you have assigned a different uucp login for each site that needs uucp access to your machine. • Ensure that you have limited the number of commands that each uucp login can execute to a bare minimum. • Consider deleting the whole uucp subsystem if it is not required. • Ensure there are no vendor-supplied uucp or root crontab entries.

TCP/IP Related Services

Service	Function	Comments
autoconf6	IPv6 interfaces	<ul style="list-style-type: none"> • Disable unless you are running IPV6
dhcpcd	Dynamic Host Configure Protocol (client)	<ul style="list-style-type: none"> • Back room servers should not rely on DHCP. Disable this service • If your host is not using DHCP, disable
dhcprd	Dynamic Host Configure Protocol (relay)	<ul style="list-style-type: none"> • Grabs DHCP broadcasts and sends them to a server on another network • Duplicate of a service found on routers • Disable this if you are not using DHCP or rely on passing information between networks
dhcpsd	Dynamic Host Configure Protocol (server)	<ul style="list-style-type: none"> • Answers DHCP requests from clients at boot time; gives client information, such as IP name, number, netmask, router, and broadcast address • Disable this if you are not using DHCP • Disabled on production and back room servers along with hosts not using DHCP
dpid2	outdated SNMP service	<ul style="list-style-type: none"> • Disable unless you need SNMP
gated	gated routing between interfaces	<ul style="list-style-type: none"> • Emulates router function • Disable this service and use RIP or a router instead
mrouted	multi-cast routing	<ul style="list-style-type: none"> • Emulates router function of sending multi-cast packets between network segments • Disable this service. Use a router instead
ndp-host	IPv6 host	<ul style="list-style-type: none"> • Disable unless you use IPV6
ndp-router	IPv6 routing	<ul style="list-style-type: none"> • Disable this unless you use IPV6. Consider using a router instead of IPv6



Service	Function	Comments
portmap	RPC services	<ul style="list-style-type: none">• RPC servers register with portmap daemon. Clients who need to locate RPC services ask the portmap daemon to tell them where a particular service is located• Do not enable the portmap service unless necessary. A machine that doesn't use the sunrpc services (i.e. NFS or NIS) should not need portmap.
routed	RIP routing between interfaces	<ul style="list-style-type: none">• Emulates router function• Disable if you have a router for packets between networks
rwhod	Remote "who" daemon	<ul style="list-style-type: none">• Collects and broadcasts data to peer servers on the same network• Disable this service
sendmail	mail services	<ul style="list-style-type: none">• Runs as root user• Disable this service unless the machine is used as a mail server• If disabled, then do one of the following:• Place an entry in crontab to clear the queue. Use the /usr/lib/sendmail -q command• Configure DNS services so that the mail for your server is delivered to some other system
snmpd	Simple Network Management Protocol	<ul style="list-style-type: none">• Disable if you are not monitoring the system via SNMP tools• SNMP may be required on critical servers
syslogd	system log of events	<ul style="list-style-type: none">• Disabling this service is not recommended• Prone to denial of service attacks• Required in any system

/etc/inittab

The /etc/inittab file plays a crucial role in the boot sequence by controlling what happens at each runlevel. The /etc/inittab file supplies the script to the [init](#) command's role as a general process dispatcher. The process that constitutes the majority of the init command's process dispatching activities is the /etc/getty line process, which initiates individual terminal lines. Other processes typically dispatched by the init command are daemons and the shell.

Many of the services configured in /etc/inittab can be safely removed in their entirety. Some may require more work. A list of common /etc/inittab services are as follows:

Service	Function	Comments
inittab/dt	desktop login to CDE environment	<ul style="list-style-type: none">• Starts the X11 server on the console• Supports the X11 Display Manager Control Protocol (xdcmp) so that other X11 stations can log into the same machine• Service should be used on personal workstations only. Avoid using it for back room systems
inittab/dt_nogb	desktop login to CDE environment (NO graphic boot)	<ul style="list-style-type: none">• No graphical display until the system is up fully• Same concerns as inittab/dt
inittab/httpd-lite	web server for the docsearch command	<ul style="list-style-type: none">• Default web server for the docsearch engine• Disable unless your machine is a documentation server
inittab/i4ls	license manager	<ul style="list-style-type: none">• Enable for development machines



Service	Function	Comments
	servers	<ul style="list-style-type: none"> • Disable for production machines • Enable for back room database machines that have license requirements • Provides support for compilers, database software, or any other licensed products
inittab/imqss	search engine for "docsearch"	<ul style="list-style-type: none"> • Part of the default web server for the docsearch engine • Disable unless your machine is a documentation server
inittab/lpd	BSD line printer interface	<ul style="list-style-type: none"> • Accepts print jobs from other systems • You can disable this service and still send jobs to the print server • Disable this after you confirm that printing is not affected
inittab/nfs	Network File System/Net Information Services	<ul style="list-style-type: none"> • NFS and NIS services based which were built on UDP/RPC • Authentication is minimal • Disable this for back room machines
inittab/piobe	printer IO Back End (for printing)	<ul style="list-style-type: none"> • Handles the scheduling, spooling and printing of jobs submitted by the qdaemon • Disable if you are not printing from your system because you are sending print job to a server
inittab/qdaemon	queue daemon (for printing)	<ul style="list-style-type: none"> • Submits print jobs to the piobe daemon • If you are not printing from your system, then disable
inittab/uprintfd	kernel messages	<ul style="list-style-type: none"> • Generally not required • Disable
inittab/writesrv	writing notes to ttys	<ul style="list-style-type: none"> • Only used by interactive UNIX workstation users • Disable this service for servers, back room databases, and development machines • Enable this service for workstations
inittab/xdm	traditional X11 Display Management	<ul style="list-style-type: none"> • Do not run on back room production or database servers • Do not run on development systems unless X11 display management is needed • Acceptable to run on workstations if graphics are needed

File System Security

Files	Comments
World Writable Files and Directories	<p>World-writable files, particularly system files, can be a security hole if a cracker gains access to your system and modifies them. Additionally, world-writable directories are dangerous, since they allow a cracker to add or delete files as he wishes. Ensure that there are no unexpected world writable files or directories on your system. To do this, execute the following command:</p> <pre># /bin/find / -type f \(-perm -2 -o -perm -20 \) -exec ls -lg {} \; # /bin/find / -type d \(-perm -2 -o -perm -20 \) -exec ls -ldg {} \;</pre>
SUID or SGID bit	This describes set-user-id permissions on the file. When the set user ID access mode is set in the owner permissions, and the file is executable, processes which



Files	Comments
	<p>run it are granted access to system resources based on user who owns the file, as opposed to the user who created the process. This is the cause of many "buffer overflow" exploits. Ensure that files which have the SUID or SGID bit set, need to have it that way.</p> <pre># /bin/find / -type f \(-perm -004000 -o -perm -002000 \) \ -exec ls -lg {} \;</pre> <p>Remove this bit from programs that do not require elevated privileges to function successfully.</p>
Umask Settings	<p>The <code>umask</code> command can be used to determine the default file creation mode on your system. If files are created without any regard to their permissions settings, the user could inadvertently give read or write permission to someone that should not have this permission. Typical <code>umask</code> settings include 022, 027, and 077 (which is the most restrictive). Normally the <code>umask</code> is set in <code>/etc/profile</code>, so it applies to all users on the system. Use the following script to ensure that <code>umask</code> settings are configured appropriately.</p> <pre>#!/bin/sh PATH=/bin:/usr/bin:/usr/etc:/usr/ucb HOMEDIRS=`cat /etc/passwd awk -F":" 'length(\$6) > 0 {print \$6}' sort -u` FILES=".cshrc .login .profile" for dir in \$HOMEDIRS do for file in \$FILES do grep -s umask /dev/null \$dir/\$file done done</pre>
Home Directories	<p>There should never be a reason for users' home directories to allow SUID/SGID programs to be run from there. Use the <code>nosuid</code> option in <code>/etc/fstab</code> for partitions that are writable by others than root. You may also wish to use <code>nODEV</code> and <code>noexec</code> on users' home partitions, as well as <code>/var</code>, thus prohibiting execution of programs, and creation of character or block devices.</p>
Require root ownership	<p>Ensure that <code>/etc /usr/etc /bin /usr/bin /sbin /usr/sbin /tmp</code> and <code>/var/tmp</code> are owned by root.</p>
Sticky-bit	<p>Ensure the sticky-bit is set on <code>/tmp</code> and on <code>/var/tmp</code>. If the sticky bit is set on a directory, a user may only delete files that he owns or for which he has explicit write permission granted, even when he has write access to the directory.</p>

Major Services

[BIND](#)

BIND (Berkeley Internet Name Domain) server is distributed with most UNIX variants and provides name services to countless networks. However, the BIND server is not without certain vulnerabilities, and is often a choice target for hackers. These hackers utilize BIND vulnerabilities



to gain root access to the host or to turn the host into a launching platform for DDOS attacks. An improper or insufficiently robust BIND configuration can also "leak" information about the hosts and addressing within the intranet. Here are some guidelines for securing your configuration of BIND.

1. Use the latest version of BIND available. The latest version of BIND and a list of BIND vulnerabilities can be found at: <http://www.isc.org/products/BIND>.
2. Use multiple authoritative BIND servers for each zone in order to avoid a single point of failure. If feasible, logically place your BIND servers within different segments.
3. Place your BIND servers behind a firewall and restrict TCP ports access from anonymous entities.
4. Run BIND in a chroot(ed) environment. When you run BIND (or any other process) in a chroot environment, the process is simply unable to see any part of the file system outside the chrooted environment. For example, if BIND is running chrooted to the directory `/chroot/named`, to BIND, the contents of this directory will appear to be `/`, its root directory.
5. Restrict queries; depending on the function of your BIND server, it should not accept and respond to queries from any IP address.
 - a. A caching-only name server should only accept queries from the IP addresses of resolvers it serves.
 - b. An authoritative-only name server must accept queries from any IP address, but should not accept recursive queries.
6. Restrict zone transfers to slave name servers and other required systems. A zone transfer will reveal an entire authoritative zone. By restricting zone transfers you ensure that the only information available to people is that which they ask for directly - no one can just ask for all the details about your set-up.
7. Restrict dynamic updates as much as possible. A dynamic DNS updater can delete every record in the zone except for the SOA record and on NS record and replace the contents with entirely different records. Dynamic updates should be restricted by IP addresses, consider using TSIG or SIG(0) to further protect dynamic updates.
8. Use "split service" name servers to protect private and public authoritative zones. The public servers should be configured to provide Authoritative Only responses and no caching or no recursive queries.

APACHE Web Server

1. The first step in securing Apache web server is to keep apprised of updates to the Apache software. It is recommended to subscribe to the Apache HTTP Server Announcements List (<http://httpd.apache.org/lists.html#http-announce>) where you can keep informed of new releases and security updates.
2. The second step in securing an Apache web server is to keep apprised updates to related HTTP components such as add-on code, CGI scripts, or the underlying Operating System.
3. Consider running the web server machine solely for the purpose of being a web server (e.g. - do not run any other services such as mail, DNS etc).
4. Run Apache in a chroot(ed) environment. When you run Apache (or any other process) in a chroot environment, the process is simply unable to see any part of the file system outside the chrooted environment. For example, if Apache is running chrooted to the



- directory `/chroot/named`, to Apache, the contents of this directory will appear to be `/`, its root directory.
5. Ensure the server is configured to execute only those CGI scripts which reside in the CGI binary directory, e.g., `/cgi-bin`. Set the ownership and permissions on this directory to 755 or 751.
 6. Ensure that all default or example CGI scripts are removed if not needed or thoroughly tested for signs of bad programming practices.
 7. Server Side Includes (SSI) present several potential security risks, consider disabling the ability to run scripts and programs from Server Side Includes pages. To do this, replace `Includes` with `IncludesNOEXEC` in the Options directive. Note that users may still use `<--#include virtual="..." -->` to execute CGI scripts if these scripts are in directories designated by a `ScriptAlias` directive.
 8. Consider preventing users from setting up `.htaccess` files which can override security features. This can be done by putting the following text in the server Apache configuration file.

```
<Directory />
AllowOverride None
</Directory>
```

9. Protect server files from default access by adding the following block to your server's configuration:

```
<Directory />
    Order Deny,Allow
    Deny from all
</Directory>
```

This will forbid default access to file system locations. Add appropriate `<Directory>` blocks to allow access only in those areas that are required.

```
<Directory /usr/users/*/public_html>
    Order Deny,Allow
    Allow from all
</Directory>
<Directory /usr/local/httpd>
    Order Deny,Allow
    Allow from all
</Directory>
```

10. Use SSL (Secure Socket Layer) to encrypt the transmission of server authentication, client authentication, and sensitive information such as ISRS data.
11. ENSURE that the directory of the documents served by the web server is not also available via anonymous FTP. Any restrictions to access to the documents set by the web server would be circumvented by anonymous FTP.



Sendmail

Sendmail is the de facto standard Mail Transfer Agent (MTA) for Unix systems. The daemon on a machine is only responsible for two things:

- Listening on port 25/tcp for incoming messages from outside of the machine
- Flushing the local queue of unsent messages on a periodic basis

Even though a site typically requires only a handful of mail servers (for relaying mail and receiving external mail, it is quite common that a client only mail server will be running sendmail. The first step in securing a sendmail configuration is to determine the role of the mail server (mail client or smtp server).

1. Be sure to use the latest version of sendmail available. The latest version of sendmail and a list of sendmail vulnerabilities can be found at: <http://www.sendmail.org>.
2. If the server is mail client only, disable the daemon mode. This will still allow clients to use sendmail for mail delivery. If this is implemented, Consider adding `sendmail -q` to your crontab to ensure delayed messages are delivered.
3. Ensure sendmail is configured to deny relaying from unknown hosts. This helps to prevent your mail server from being used inappropriately.
4. Use smrsh if you require progmailer functionality to limit sendmail's scope of program execution to programs in smrsh configuration only. smrsh is a restricted shell utility that may be configured to execute a specific list of programs. smrsh is included with recent versions of sendmail.
5. If you do not require progmailer functionality then disable mail to programs by setting this field to `/bin/false` in the sendmail configuration file.

FTP

- Be sure to using the most recent version of the FTP daemon of your choice.
- Ensure that your FTP server does not have the SITE EXEC command enabled
- Ensure that you have set up a file `/etc/ftpusers` which specifies those users that are not allowed to connect to your ftpd. This should include, as a minimum, the entries: root, bin, uucp, ingres, daemon, news, nobody and all vendor supplied accounts.
- Ensure that you do not include a command interpreter (such as a shell or tools like perl) in `~ftp/bin`, `~ftp/usr/bin`, `~ftp/sbin` or similar directory configurations that can be executed by SITE EXEC.
- Do not keep system commands in `~ftp/bin`, `~ftp/usr/bin`, `~ftp/sbin` or similar directory configurations that can be executed by SITE EXEC. It may be necessary to keep some commands, such as `uncompress`, in these locations.
- Keep an invalid password and user shell for the ftp entry in the system password file and the shadow password file (if you have one). It should look something like:

```
ftp:*:400:400:Anonymous FTP:/home/ftp:/bin/false
```

where `/home/ftp` is the anonymous FTP area.



- Ensure that the permissions of the FTP home directory `~ftp/` are set to 555 (read nowrite execute), owner set to root (not ftp).
- Ensure that you do not have a copy of your real `/etc/passwd` file as `~ftp/etc/passwd`. Create one from scratch with permissions 444, owned by root. It should not contain the names of any accounts in your real password file. It should contain only root and ftp. These should be dummy entries with disabled passwords e.g.:

```
root:*:0:0:Ftp maintainer::  
ftp:*:400:400:Anonymous ftp::
```

The password file is used only to provide uid to username mapping for `ls(1)` listings.

- Ensure that you DO NOT have a copy of your real `/etc/group` file as `~ftp/etc/group`. Create one from scratch with permissions 444, owned by root.
- Ensure the files `~ftp/.rhosts` and `~ftp/.forward` do not exist.
- Do set the login shell of the ftp account to a non-functional shell such as `/bin/false`.
- Ensure files or directories are owned by the ftp account or have the same group as the ftp account. If they are, it may be possible for an intruder to replace them with a trojan version.
- Ensure no files or directories in the FTP area are world writable.
- Ensure that the anonymous ftp user cannot create files or directories in ANY directory unless required. Ensure that the anonymous ftp user can only read information in public areas.