Linux Academy: Host Security – Course Notes
http://linuxacademy.com

Video One – /etc/passwd, /etc/shadow and /usr/sbin/nologin

- /etc/passwd
    - user and/or system accounts are contained in the file
    - path to home directory
    - fields, username:passwd encryption,uid, gid, comment, home, command shell
    - no password is contained in this file in modern Linux systems
- /etc/shadow
    - user along with their encrypted password
    - associated during login with the user and the SHA2 encrypted password hash
    - command 'passwd' will write a new password to the shadow file
- unshadow
    - combines the passwd and shadow file and creates a text file that contains both
    - content will match Unix based systems (System V) /etc/passwd files
- /usr/sbin/nologin
    - replace the command shell at the end of the password file to prevent shell login
    - attempts to do so will indicate on the command line during login

Video Two – /etc/inet.d and /etc/inetd.conf

- /etc/inet.d
    - super daemon or daemon of daemons
    - replaced in modern distributions by more secure xinet.d
- /etc/inetd.conf
    - simple configuration file
    - single line, describes service control and startup parameters as needed
        - i.e. `ftp  stream tcp nowait root  /usr/sbin/ftpd  in.ftpd -el`
            - ftp service, streaming, tcp, don't wait to start, root permissions, location of file, startup script, command line parameters to pass

Video Three – /etc/xinet.d and /etc/xinetd.conf

- /etc/xinet.d
    - super daemon or daemon of daemons
    - directory contains default services that are started with the daemon on system start
- /etc/xinetd.conf
    - sectional, paramterized configuration file that sets up daemons that will be controlled by the superdaemon
        - example of telnet section in file:
            - service telnet
            - {
            - flags = REUSE
            - socket_type = stream
            - wait = no
            - user = root
            - server = /usr/sbin/in.telnetd
            - log_on_failure += USERID
            - disable = yes
            - }
    - configuration files are more flexible and self-explanatory
    - once installed, starts with system and controls only those daemons configured in the configuration file, does not automatically take over service management

Video Four – /etc/hosts.allow and /etc/hosts.deny

- /etc/hosts.allow
    - legacy method of defining hosts that are allowed to use any number of services on the host
    - example:
        - ALL: .domain.com
        - this would allow ALL services to be accessed by anyone connecting from the 'domain.com' domain
- /etc/hosts.deny
    - legacy method of defining hosts that are not allowed to use any number of services on the host
    - example:
        - ALL: ALL
        - this would deny all users from anywhere from using or accessing this system or any of its services
- this will ONLY work if the application providing the service properly implements the TCPWRAPPERS network function and thus knows to check these access control lists
- NOTE: order of implementation (accept will be read before deny and overwrite deny lists when conflicting)
- modern methods of access control are through firewalls
    - firewalls operate at a packet level on all incoming and outgoing connections and do not have the higher level reliance of an application's implementation of the TCPWRAPPER, thus it does not have the limitations of this method

Video Five – /etc/init.d and /etc/inittab

- RPM distributions (those that still use the SysV runlevel script directories in /etc/rc.d)
    - /etc/inittab
        - sets the default runlevel that the system boots into
            - sample: id:3:initdefault (which would boot into full multiuser but no GUI)
    - runlevels:
        - 0: Halt/Shutdown
        - 1: Single User/Repair (no services, no network)
        - 2: Multiuser, no networking
        - 3: Full multiuser, network, all services, no GUI
        - 4: Unused
        - 5: Same as runlevel 3 with X11/GUI
        - 6: Reboot
- Debian distributions (those that have moved to the upstart daemon for service and runlevel management)
    - /etc/init/rc-sysinit.conf
        - env DEFAULT_RUNLEVEL=2 (default runlevel for Debian)
    - /etc/inittab can be created, but will only have the affect of booting to Debian defined runlevels
    - runlevels:
        - 0: Halt/Shutdown
        - 1: Single User/Repair (no services, no network)
        - 2: Full multiuser, networking all services, GUI
        - 3: Full multiuser, networking all services, GUI
        - 4: Full multiuser, networking all services, GUI
        - 5: Full multiuser, networking all services, GUI
        - 6: Reboot
    - all scripts and start up configurations are kept in the upstart directories (not /etc/rc.d) but rather /etc/init, /etc/init.d/ and /lib/upstart