Linux Configuration

Tools and General Information

Install

- ☐ apt-get install nmap
- ☐ apt-get install htop
- ☐ apt-get install bastille

Information

- /var/log/message – Where whole system logs or current activity logs are available.
- /var/log/auth.log – Authentication logs.
- /var/log/kern.log – Kernel logs.
- /var/log/cron.log – Crond logs (cron job).
- /var/log/maillog – Mail server logs.
- /var/log/boot.log – System boot log.
- /var/log/mysqld.log – MySQL database server log file.
- /var/log/secure – Authentication log.
- /var/log/utmp or /var/log/wtmp : Login records file.
- Port 135/TCP - used by smbd
- Port 137/UDP - used by nmbd
- Port 138/UDP - used by nmbd
- Port 139/TCP - used by smbd
- Port 445/TCP - used by smbd

Emergency Plan

- Ensure that the network adapter on VSphere is set NOT to startup on boot.
- In case of lockout restart from most recent backup, change passwords, and turn the network adapter on.
- In the case of a service going down, uninstall the service then reinstall it while the network adapter is off
- In case of a power failure, attempt to reboot, restart from recent backup in the event of failure to reboot.

Quick Defenses (First 10 mins)

Firewall

- ☐ ufw enable
- ☐ ufw logging on
- ☐ ufw logging high
- ☐ gedit /etc/ufw/before.rules
  - Comment all lines containing icmp, save
- ☐ gedit /etc/ufw/before6.rules
  - Comment all lines containing icmp, save
- ☐ ufw disable
- ☐ ufw enable
- ☐ ufw default deny ~~outgoing~~ to
- ☐ ufw default deny ~~incoming~~ from
- ☐ ufw allow http ~~outgoing~~
- ☐ ufw allow <port number/protocol>

User Accounts and Groups

- ☐ sudo gedit users
  - add all users to this file and save
- ☐ sudo gedit users1
  - Enter the following into this file:

```
#!/bin/bash
for i in $(cat <PATH TO USERS>); do
        echo -e "123QWEASDzxc!@#\n123QWEASDzxc!@#" | passwd $i
done
```

- ☐ chmod -R 744 ~
- ☐ ./users1
- ☐ grep ':0:' /etc/passwd, users with UID of 0
- ☐ sudo gedit /etc/passwd
  - Fix ID's as needed, save
- ☐ sudo gedit /etc/group
  - Add and remove users from groups as needed, save
- ☐ echo "" /var/log/auth.log, will clear auth file → how to copy to /home/desktop
  - make backup first then clear the auth file
- ☐ sudo visudo
  - comment users that don't belong, save

Permissions

- ☐ chmod -R 444 /var/log
- ☐ chmod 440 /etc/passwd
- ☐ chmod 440 /etc/shadow
- ☐ chmod 440 /etc/group

Services

- ☐ service sshd stop
- ☐ service telnet stop
- ☐ service vsftpd stop
- ☐ service snmp stop
- ☐ service pop3 stop
- ☐ service icmp stop
- ☐ service sendmail stop
- ☐ service dovecot stop
- ☐ service --status-all | grep "+"
- ☐ service <service name> stop, for services that do not need to be enabled

Host File DNS

- ☐ Check /etc/hosts file for unauthorized users

Save/Backup apt-get update upgrade & update

- ☐ Save machine configuration in VSphere for later reboot

Quick Defenses(ASAP)

- ☐ sestatus
- ☐ gedit /etc/selinux/config
  - to turn on or off
- ☐ setenforce enforcing
- ☐ echo ALL >>/etc/cron.deny , sets to ALL users cannot use cron jobs
- ☐ gedit /etc/passwd
  - change root shell from "/bin/root" to "/sbin/nologin"
- ☐ gedit /etc/pam.d/common-password
  - add " minlen=12 sha512" to "password [success=1 default=ignore] pam_unix.so"
- ☐ sudo chown root:admin /bin/su sudo
- ☐ chmod 04750 /bin/su
- ☐ gedit /etc/fstab
  - add LABEL=/boot /boot ext2 defaults,ro 1 2 ,
- ☐ gedit etc/pam.d/passwd
  - change the password line to say "required pam_cracklib.so retry=3 minlen=8 minclass=4 maxsequence=4 maxrepeat=3"
- ☐ gedit /etc/pam.d/common-auth
  - change auth line from "pam_permit.so" to "pam_tally.so onerr =fail deny=3 unlock_time=108000"
- ☐ gedit /etc/fstab
  - add "tmpfs /dev/shm tmpfs defaults,noexec,nosuid 0 0"
- ☐ Use graphical update manager. Check for updates daily.
- ☐ gedit /etc/sysctl.conf
  - add
    - "net.ipv4.tcp_syncookies = 1", "net.ipv4.tcp_max_syn_backlog = 2048"
    - "net.ipv4.tcp_synack_retries = 2", "net.ipv4.tcp_syn_retries = 5"
    - "net.ipv4.icmp_echo_ignore_all = 1", "net.ipv4.conf.all.rp_filter = 1"
    - "net.ipv4.conf.default.rp_filter = 1"
    - "net.ipv4.icmp_echo_ignore_broadcasts = 1"
    - "net.ipv4.conf.all.redirects = 0"
    - "net.ipv4.conf.default.accept_redirects = 0", reload file with sysctl -p
- ☐ Repeat for ipv6
- ☐ gedit /etc/rc.d ls run level 0-6
  - look for processes that run on startup
  - Remove any processes that do not need to run on startup.
- ☐ echo 0 > /proc/sys/net/ipv4/conf/all/arp_accept, gratuitous arp

Monitoring

Shares

- ☐ gedit/mnt directory
- ☐ gedit/media directory

Other

- ☐ netstat -tulpn, l
  - list connections that have PIDs
- ☐ htop, F5
  - to see process tree
- ☐ cat /var/log/auth.log,
  - check occasionally
- ☐ faillog –a
  - failed login attempts
- ☐ echo "" ~/.bash_history
  - use occasionally to keep commands used secret
- ☐ ~~gedit /etc/rc.d~~
  - for startup services
- ☐ ~~gedit /etc/init.d~~ cd/etc/init.d -a
  - for services and delete unnecessary Ex. MongoDB
- ☐ tcpdump -i eth0 -tttt dst <IP ADDRESS> and not net 192.168.1.0/24
  - show connections to specific IP addresses
- ☐ sestatus
  - Check the status of SELinux make sure it is on and not set to permissive
- ☐ ifconfig,
  - ensure that there is only one interface
- ☐ ls /lib
- ☐ ls /var/lib

Software

- ☐ dpkg -l | grep "<name of software>" THEN find -name / "<name of software>"
  - Medusa
  - hydra
  - truecrack
  - ophcrack
  - Kismet
  - John
  - Nikto
  - cryptcat
  - nc
- ☐ dpkg -P <name of software>
  - to remove

FTP Server

Modify config file

- ☐ gedit /etc/vsftpd.conf
  - Anonymous_enable set to no
  - local_enable most likely set to yes
  - write_enable set to no
  - local_umask set to 022
  - anon_upload_enable set to no
  - anon_mkdir_write_enable set to no
  - dirmessage_enable set to yes
  - xferlog_enable set to yes
  - connect_from_port_20 set to yes
  - Chown_uploads set to yes, chown_username needs to be set to unprivileged user
  - idle_session_timeout set to 30
  - data_connection_timeout set to 30
  - ascii_upload_enable set to no
  - ascii_download_enable set to no
  - chroot_local_user set to yes, need to add users who cannot chroot to /etc/vsftpd.chroot_list
  - chroot_list_file, change owner of file to root
  - chroot_list_enable set to yes
  - listen needs to be set to yes if people will be remotely accessing the server or not
  - listen_ipv6 set to no
- ☐ chmod 444 /etc/vsftpd.conf
- ☐ gedit /etc/ftpusers
  - needs to changed so that certain users cannot access ftp

SSH Server

- ☐ Change permissions and owner of all "~/.ssh/" so private key is unobtainable
- ☐ In /etc/ssh/sshd_config change "PermitRootLogin" to "no"
- ☐ In /etc/ssh/sshd_config change "PermitEmptyPasswords" to "no"
- ☐ In /etc/ssh/sshd_config set to Protocol 2
- ☐ chmod –R 444 /etc/ssh

Apache2 Server

- ☐ gedit /etc/apache2/apache2.conf
  - Comment out the following modules:
    - mod_imap
    - mod_include
    - mod_info
    - mod_userdir
    - mod_autoindex
- ☐ timeout needs to be set to 15
- ☐ KeepAlive needs to be set to off
- ☐ ServerSignature needs to be set to off
- ☐ ServerTokens needs to be set to prod
- ☐ Add the following for any directory that does not need to be accessed by external visitors
  For example:
  - <Directory / >
  - Options None
  - Order deny, allow
  - Deny from all
  - </ Directory>
- ☐ Add the following:
  - <Directory /var/www/html>
  - Options –Indexes
  - </Directory>
- ☐ /etc/apache2/ports.conf
  - ensure that listen 0.0.0.0:80
  - ensure that <IfModule mod_ssl.c>
  - Listen 0.0.0.0:443
  - </IfModule>
- ☐ HostnameLookups set to on
- ☐ Disable autocomplete and caching on webpage where sensitive data needs to be input
- ☐ Ensure that apache has a separate user and group to run itself in
- ☐ chmod –R 444 /var/www

Samba Server

- Gedit /etc/pam.d
  - Change the max_smbd_processes option to 1
  - Check the hosts allow and hosts deny options to ensure that only specific IP ranges are able to access the server.
  - Set hosts deny to 0.0.0.0 will deny all connections that are not specified to be allowed
  - Ensure the valid users option only allows users specified in the readme file
  - Change the bind interfaces only option to yes
  - Set the interfaces option to eth*, lo
  - In the homes share, set the valid users option to %S
    - %S refers to the name of the share
    - users will only be able to access their own home directories
  - Add the following:

    [IPC$]

    hosts allow = <Your IP range>
    127.0.0.1

    hosts deny = 0.0.0.0/0

- chmod –R 444 <share location>