Create_initial_process_list_to_be_diff_d_throughout_comp.sh

```
ps >> ./records/ps_list_short
ps all >> ./records/ps_list_all
```

find_immutable_files.sh

```
find . | xargs -I file lsattr -a file 2>/dev/null | grep '^....
i'
```

IPTABLE_Stuff

```
systemctl enable netfilter-persistent
sysctl -w net.ipv6.conf.all.disable_ipv6=1
sysctl -w net.ipv6.conf.default.disable_ipv6=1
iptables -A INPUT -p tcp --tcp-flags ALL NONE -j DROP
iptables -A INPUT -p tcp --tcp-flags ALL ALL -j DROP
iptables -A INPUT -i lo -j ACCEPT
iptables -A INPUT -p tcp -m tcp --dport <SERVICE 1> -j ACCEPT
iptables -A INPUT -p tcp -m tcp --dport <SERVICE 2> -j ACCEPT
iptables -A INPUT -p tcp -m tcp --dport <SERVICE 3> -j ACCEPT
iptables -I INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -P OUTPUT ACCEPT
iptables -P INPUT DROP
iptables-save > /etc/iptables/rules.v4
```

File_Stuff.txt

```
sed -i "s/UMASK.*022/UMASK   077/" /etc/login.defs
sed -i "s/#.*umask.*022/umask 077/" /root/.bashrc
chown root:root /etc/passwd
chmod 644 /etc/passwd
chown root:shadow /etc/shadow
chmod 640 /etc/shadow
chown root:root /etc/group
chmod 644 /etc/group
chown root:shadow /etc/gshadow
chmod 640 /etc/group
chown root:root /etc/security/opasswd
chmod 600 /etc/security/opasswd
chown root:root /etc/passwd-
chmod 600 /etc/passwd-
chown root:root /etc/shadow-
chmod 600 /etc/shadow-
chown root:root /etc/group-
chmod 600 /etc/group-
chown root:root /etc/gshadow-
chmod 600 /etc/gshadow-
```

Known_Ubuntu_users.txt

```
root
daemon
bin
sys
sync
games
man
lp
mail
news
uucp
proxy
www-data
backup
list
irc
gnats
nobody
systemd-network
systemd-resolve
syslog
messagebus
_apt
uuidd
avahi-autoipd
usbmux
dnsmasq
rtkit
cups-pk-helper
speech-dispatcher
whoopsie
kernoops
saned
pulse
avahi
colord
hplip
geoclue
gnome-initial-setup
gdm
```

list_user_crons.sh

```
for user in $(cut -f1 -d: /etc/passwd); do crontab -u $user -l; done;
```

SSH_Lockdown.sh

```
#!/bin/bash

# Set /etc/ssh/sshd_config ownership and access permissions
chown root:root /etc/ssh/sshd_config
chmod 600 /etc/ssh/sshd_config

# Change Port
sed -i "s/#Port 22/Port 10101/g" /etc/ssh/sshd_config

# Protocol 2
echo "Protocol 2" >> /etc/ssh/sshd_config

# Set SSH LogLevel to INFO
sed -i "/LogLevel.*/s/^#//g" /etc/ssh/sshd_config

# Set SSH MaxAuthTries to 3
sed -i "s/#MaxAuthTries 6/MaxAuthTries 3/g" /etc/ssh/sshd_config

# Enable SSH IgnoreRhosts
sed -i "/IgnoreRhosts.*/s/^#//g" /etc/ssh/sshd_config

# Disable SSH HostbasedAuthentication
sed -i "/HostbasedAuthentication.*no/s/^#//g" /etc/ssh/sshd_config

# Disable SSH root login
sed -i "s/#PermitRootLogin prohibit-password/PermitRootLogin no/g" /etc/ssh/sshd_config

# Deny Empty Passwords
sed -i "/PermitEmptyPasswords.*no/s/^#//g" /etc/ssh/sshd_config

# Deny Users to set environment options through the SSH daemon
sed -i "/PermitUserEnvironment.*no/s/^#//g" /etc/ssh/sshd_config

# Allow only approved ciphers
echo "Ciphers aes256-ctr" >> /etc/ssh/sshd_config

# Configure SSH Idle Timeout Interval
sed -i "s/#ClientAliveInterval 0/ClientAliveInterval 300/g" /etc/ssh/sshd_config
sed -i "s/#ClientAliveCountMax 3/ClientAliveCountMax 0/g" /etc/ssh/sshd_config

# Set Banner
sed -i "s/#Banner none/Banner \/etc\/issue\.net/g" /etc/ssh/sshd_config
echo "Text me memes @ 814-470-5192" > /etc/issue.net

# Disable X11 forwarding
sed -i "s/X11Forwarding yes/#X11Forwarding yes/g" /etc/ssh/sshd_config

service sshd restart
```