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