#!/bin/bash

#Weird LIBC6 error fix -required prior to upgrading Kali 2020..

yes Y | sudo apt-get install gcc-9-base libgcc-9-dev libc6-dev;

#Update Kali before starting

echo -e '\e[1;34m'"{::Starting Kali update before installs::}"'\e[0m'

sudo apt update && sudo apt-get -y upgrade && sudo apt-get -y dist-upgrade && sudo apt-get -y autoclean && sudo apt-get -y autoremove

#Build Tools Directories (both in root and OPT depending on user preference)

echo -e '\e[1;34m'"{::Creating linked Tool directories ~/Tools and /OPT/Tools::}"'\e[0m'

mkdir -p /home/$USER/Tools

mkdir -p /opt/Tools

ln -s /home/$USER/Tools /opt/Tools

#Install Sublime Text Editor

echo -e '\e[1;34m'"{::Installing Sublime Text Editor::}"'\e[0m'

wget -qO - <https://download.sublimetext.com/sublimehq-pub.gpg> | sudo apt-key add -

sudo apt-get -y install apt-transport-https

echo -e "deb <https://download.sublimetext.com/> apt/stable/" | sudo tee /etc/apt/sources.list.d/sublime-text.list

sudo apt-get -y update && sudo apt -y install sublime-text

#Install Terminator

echo -e '\e[1;34m'"{::Installing Terminator::}"'\e[0m'

apt-get -y install terminator

# Git Clones of Tools

echo -e '\e[1;34m'"{::Performing GIT clones of tools from GitHub::}"'\e[0m'

cd /opt/Tools

git clone <https://github.com/Tib3rius/AutoRecon.git>

git clone <https://github.com/samratashok/nishang.git>

git clone <https://github.com/3ndG4me/AutoBlue-MS17-010.git>

git clone <https://github.com/BC-SECURITY/Empire.git>

git clone <https://github.com/PowerShellMafia/PowerSploit.git>

git clone <https://github.com/carlospolop/privilege-escalation-awesome-scripts-suite.git>

git clone <https://github.com/rasta-mouse/Sherlock.git>

git clone <https://github.com/rasta-mouse/Watson.git>

git clone <https://github.com/sleventyeleven/linuxprivchecker.git>

git clone <https://github.com/rebootuser/LinEnum.git>

git clone <https://github.com/411Hall/JAWS.git>

git clone <https://github.com/SecureAuthCorp/impacket.git>

git clone <https://github.com/vulnersCom/nmap-vulners>

git clone <https://github.com/swisskyrepo/PayloadsAllTheThings.git>

git clone <https://github.com/BloodHoundAD/BloodHound.git>

git clone <https://github.com/ropnop/kerbrute.git>

git clone <https://github.com/rebootuser/LinEnum.git>

git clone <https://github.com/AonCyberLabs/Windows-Exploit-Suggester.git>

git clone <https://github.com/maurosoria/dirsearch.git>

git clone <https://github.com/D35m0nd142/LFISuite.git>

git clone <https://github.com/mdsecactivebreach/SharpShooter.git>

git clone <https://github.com/nccgroup/demiguise.git>

git clone <https://github.com/vysecurity/morphHTA.git>

git clone <https://github.com/Kevin-Robertson/Inveigh.git>

git clone <https://github.com/noahpowers/nlzr.git>

git clone <https://github.com/noahpowers/ServerSetup.git>

git clone <https://github.com/jasonjfrank/gnmap-parser.git>

git clone <https://github.com/GhostPack/SharpDPAPI.git>

git clone <https://github.com/GhostPack/Seatbelt.git>

git clone <https://github.com/GhostPack/Rubeus.git>

git clone <https://github.com/GhostPack/SharpWMI.git>

git clone <https://github.com/GhostPack/Lockless.git>

git clone <https://github.com/GhostPack/Sharpup.git>

git clone <https://github.com/GhostPack/SafetyKatz.git>

git clone <https://github.com.GhostPack/SharpDump.git>

git clone <https://github.com/GhostPack/SharpRoast.git>

# To Add (temp)

#snmpwalk svwar wkhtmltoimage

# Apt dependency installs

echo -e '\e[1;34m'"{::Installing tools/dependencies avaliable with APT::}"'\e[0m'

echo -e '\e[1;34m'"{:seclists curl bloodhound enum4linux gobuster nbtscan nikto:]\e[0m"

echo -e '\e[1;34m'"{:nmap onesixtyone oscanner smbclient smbmap smtp-user-enum sslscan tnscmd10g whatweb:]\e[0m"

sudo apt-get -y install seclists curl bloodhound enum4linux gobuster nbtscan nikto nmap onesixtyone oscanner smbclient smbmap smtp-user-enum sslscan tnscmd10g whatweb

yes Y | sudo apt install crackmapexec;

yes Y | sudo apt install bless;

yes Y | sudo apt install eyewitness;

# AutoRecon Specific install

echo -e '\e[1;34m'"{::Installing AutoRecon python dependencies::}"'\e[0m'

pip install -r /opt/Tools/AutoRecon/requirements.txt

# Installing Empire V3

echo -e '\e[1;34m'"{::Installing Empire V3::}"'\e[0m'

pushd /opt/Tools/Empire

echo -e "password" | bash "./setup/install.sh"

popd

# Installing Evil-WinRM

echo -e '\e[1;34m'"{::Installing Evil-WinRM::}"'\e[0m'

gem install evil-winrm

# Installing Impacket (updated version)

echo -e '\e[1;34m'"{::Installing Impacket::}"'\e[0m'

pip install argparse pyasn1 pycryptodomex pyOpenSSL ldapdomaindump flask ldap3 tox

pip install /opt/Tools/impacket

# Extracting Bloodhound

echo -e '\e[1;34m'"{::Extracting Bloodhound Ingestors::}"'\e[0m'

pushd /opt/Tools/BloodHound/

rm \*.\*

mv ./Ingestors/\*.\* ./

rm -rf Ingestors src BloodHoundExampleDB.graphdb

popd

# Install Veil Evasion

echo -e '\e[1;34m'"{::Installing Veil 3.0::}"'\e[0m'

apt -y install veil

/usr/share/veil/config/setup.sh --force --silent

# Install Nmap Vulners script

echo -e '\e[1;34m'"{::Copying Vulners.nse to Nmap Scripts directory and update db::}"'\e[0m'

cp /opt/Tools/nmap-vulners/vulners.nse /usr/share/nmap/scripts

nmap --script-updatedb

#Extract Rockyou

echo -e '\e[1;34m'"{::Extracting Rockyou::}"'\e[0m'

gzip -d /usr/share/wordlists/rockyou.txt.gz

# Update WPScan and Searchsploit

echo -e '\e[1;34m'"{::Updating WPScan::}"'\e[0m'

wpscan --update

echo -e '\e[1;34m'"{::Updating Searchsploit::}"'\e[0m'

searchsploit --update

#creating pastable file (This generates a file tree map of /usr/share/wordlists for easy

#cutting and pasting into xyz tool for input...

echo "Creating File list pastable";

echo '/usr/share/wordlists/wfuzz/general/common.txt

/usr/share/wordlists/wfuzz/general/mutations\_common.txt

/usr/share/wordlists/wfuzz/general/euskera.txt

/usr/share/wordlists/wfuzz/general/big.txt

/usr/share/wordlists/wfuzz/general/admin-panels.txt

/usr/share/wordlists/wfuzz/general/extensions\_common.txt

/usr/share/wordlists/wfuzz/general/http\_methods.txt

/usr/share/wordlists/wfuzz/general/catala.txt

/usr/share/wordlists/wfuzz/general/megabeast.txt

/usr/share/wordlists/wfuzz/general/spanish.txt

/usr/share/wordlists/wfuzz/general/test.txt

/usr/share/wordlists/wfuzz/general/medium.txt

/usr/share/wordlists/wfuzz/Injections/bad\_chars.txt

/usr/share/wordlists/wfuzz/Injections/XML.txt

/usr/share/wordlists/wfuzz/Injections/All\_attack.txt

/usr/share/wordlists/wfuzz/Injections/Traversal.txt

/usr/share/wordlists/wfuzz/Injections/SQL.txt

/usr/share/wordlists/wfuzz/Injections/XSS.txt

/usr/share/wordlists/wfuzz/others/names.txt

/usr/share/wordlists/wfuzz/others/common\_pass.txt

/usr/share/wordlists/wfuzz/stress/uri\_hex.txt

/usr/share/wordlists/wfuzz/stress/alphanum\_case.txt

/usr/share/wordlists/wfuzz/stress/char.txt

/usr/share/wordlists/wfuzz/stress/doble\_uri\_hex.txt

/usr/share/wordlists/wfuzz/stress/test\_ext.txt

/usr/share/wordlists/wfuzz/stress/alphanum\_case\_extra.txt

/usr/share/wordlists/wfuzz/vulns/sunas.txt

/usr/share/wordlists/wfuzz/vulns/weblogic.txt

/usr/share/wordlists/wfuzz/vulns/sql\_inj.txt

/usr/share/wordlists/wfuzz/vulns/dirTraversal.txt

/usr/share/wordlists/wfuzz/vulns/dirTraversal-win.txt

/usr/share/wordlists/wfuzz/vulns/vignette.txt

/usr/share/wordlists/wfuzz/vulns/fatwire.txt

/usr/share/wordlists/wfuzz/vulns/dirTraversal-nix.txt

/usr/share/wordlists/wfuzz/vulns/fatwire\_pagenames.txt

/usr/share/wordlists/wfuzz/vulns/iis.txt

/usr/share/wordlists/wfuzz/vulns/coldfusion.txt

/usr/share/wordlists/wfuzz/vulns/domino.txt

/usr/share/wordlists/wfuzz/vulns/oracle9i.txt

/usr/share/wordlists/wfuzz/vulns/iplanet.txt

/usr/share/wordlists/wfuzz/vulns/tomcat.txt

/usr/share/wordlists/wfuzz/vulns/cgis.txt

/usr/share/wordlists/wfuzz/vulns/websphere.txt

/usr/share/wordlists/wfuzz/vulns/jrun.txt

/usr/share/wordlists/wfuzz/vulns/tests.txt

/usr/share/wordlists/wfuzz/vulns/sharepoint.txt

/usr/share/wordlists/wfuzz/vulns/frontpage.txt

/usr/share/wordlists/wfuzz/vulns/netware.txt

/usr/share/wordlists/wfuzz/vulns/apache.txt

/usr/share/wordlists/wfuzz/webservices/ws-dirs.txt

/usr/share/wordlists/wfuzz/webservices/ws-files.txt'>>/home/kali/Desktop/Pastable.txt;

#CPT Super User Creation

echo ‘CPT User Creation’;

sudo useradd -p $(openssl passwd -1 1337P@ss) cptuser;

sudo usermod -aG sudo cptuser;

echo ‘/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/‘;

echo ‘CHANGE THE PASSWORD NOW!!!!!!!!!!!’;

echo ‘/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/‘;

sudo passwd cptuser;