|  |  |
| --- | --- |
| #!/bin/bash |  |
|  |  |
|  | function main { |
|  | #variable assignment |
|  | now="$(date +'%d/%m/%Y %r')" |
|  | #intro |
|  | echo "running main ($now)" |
|  | echo "run as 'sudo sh harrisburg-linux.sh 2>&1 | tee output.log' to output the console output to a log file." |
|  | #manual config edits |
|  | nano /etc/apt/sources.list #check for malicious sources |
|  | nano /etc/resolv.conf #make sure if safe, use 8.8.8.8 for name server |
|  | nano /etc/hosts #make sure is not redirecting |
|  | nano /etc/rc.local #should be empty except for 'exit 0' |
|  | nano /etc/sysctl.conf #change net.ipv4.tcp\_syncookies entry from 0 to 1 |
|  | nano /etc/lightdm/lightdm.conf #allow\_guest=false, remove autologin |
|  | nano /etc/ssh/sshd\_config #Look for PermitRootLogin and set to no |
|  | #installs |
|  | apt-get -V -y install firefox hardinfo chkrootkit iptables portsentry lynis ufw gufw sysv-rc-conf nessus clamav |
|  | apt-get -V -y install --reinstall coreutils |
|  | apt-get update |
|  | apt-get upgrade |
|  | apt-get dist-upgrade |
|  | #network security |
|  | iptables -A INPUT -p tcp -s 0/0 -d 0/0 --dport 23 -j DROP #Block Telnet |
|  | iptables -A INPUT -p tcp -s 0/0 -d 0/0 --dport 2049 -j DROP #Block NFS |
|  | iptables -A INPUT -p udp -s 0/0 -d 0/0 --dport 2049 -j DROP #Block NFS |
|  | iptables -A INPUT -p tcp -s 0/0 -d 0/0 --dport 6000:6009 -j DROP #Block X-Windows |
|  | iptables -A INPUT -p tcp -s 0/0 -d 0/0 --dport 7100 -j DROP #Block X-Windows font server |
|  | iptables -A INPUT -p tcp -s 0/0 -d 0/0 --dport 515 -j DROP #Block printer port |
|  | iptables -A INPUT -p udp -s 0/0 -d 0/0 --dport 515 -j DROP #Block printer port |
|  | iptables -A INPUT -p tcp -s 0/0 -d 0/0 --dport 111 -j DROP #Block Sun rpc/NFS |
|  | iptables -A INPUT -p udp -s 0/0 -d 0/0 --dport 111 -j DROP #Block Sun rpc/NFS |
|  | iptables -A INPUT -p all -s localhost -i eth0 -j DROP #Deny outside packets from internet which claim to be from your loopback interface. |
|  | ufw enable |
|  | ufw deny 23 |
|  | ufw deny 2049 |
|  | ufw deny 515 |
|  | ufw deny 111 |
|  | lsof -i -n -P |
|  | netstat -tulpn |
|  | #media file deletion |
|  | find / -name '\*.mp3' -type f -delete |
|  | find / -name '\*.mov' -type f -delete |
|  | find / -name '\*.mp4' -type f -delete |
|  | find / -name '\*.avi' -type f -delete |
|  | find / -name '\*.mpg' -type f -delete |
|  | find / -name '\*.mpeg' -type f -delete |
|  | find / -name '\*.flac' -type f -delete |
|  | find / -name '\*.m4a' -type f -delete |
|  | find / -name '\*.flv' -type f -delete |
|  | find / -name '\*.ogg' -type f -delete |
|  | find /home -name '\*.gif' -type f -delete |
|  | find /home -name '\*.png' -type f -delete |
|  | find /home -name '\*.jpg' -type f -delete |
|  | find /home -name '\*.jpeg' -type f -delete |
|  | #information gathering |
|  | hardinfo -r -f html |
|  | chkrootkit |
|  | lynis -c |
|  | freshclam |
|  | clamscan -r / |
|  | echo "remember to do user management, gui related configurations, set automatic updates/security updates, etc." |
|  | echo "thank you for using harrisburg-linux.sh ($now)" |
|  | now="$(date +'%d/%m/%Y %r')" #update date/time |
|  | } |
|  |  |
|  | if [ "$(id -u)" != "0" ]; then |
|  | echo "harrisburg-linux.sh is not being run as root" |
|  | echo "run as 'sudo sh harrisburg-linux.sh 2>&1 | tee output.log' to output the console output to a log file." |
|  | exit |
|  | else |
|  | main |
|  | fi |

|  |  |
| --- | --- |
| #!/bin/bash |  |
|  | #MIT Licence |
|  | #Copyright (c) Ethan Perry, Andy Lyu |
|  | unalias -a #Get rid of aliases |
|  | echo "unalias -a" >> ~/.bashrc |
|  | echo "unalias -a" >> /root/.bashrc |
|  | PWDthi=$(pwd) |
|  | if [ ! -d $PWDthi/referenceFiles ]; then |
|  | echo "Please Cd into this script's directory" |
|  | exit |
|  | fi |
|  | if [ "$EUID" -ne 0 ] ; |
|  | then echo "Run as Root" |
|  | exit |
|  | fi |
|  | #List of Functions: |
|  | #PasswdFun |
|  | #zeroUidFun |
|  | #rootCronFun |
|  | #apacheSecFun |
|  | #fileSecFun |
|  | #netSecFun |
|  | #aptUpFun |
|  | #aptInstFun |
|  | #deleteFileFun |
|  | #firewallFun |
|  | #sysCtlFun |
|  | #scanFun |
|  | startFun() |
|  | { |
|  | clear |
|  |  |
|  | PasswdFun |
|  | zeroUidFun |
|  | rootCronFun |
|  | apacheSecFun |
|  | fileSecFun |
|  | netSecFun |
|  | aptUpFun |
|  | aptInstFun |
|  | deleteFileFun |
|  | firewallFun |
|  | sysCtlFun |
|  | scanFun |
|  | printf "\033[1;31mDone!\033[0m\n" |
|  | } |
|  | cont(){ |
|  | printf "\033[1;31mI have finished this task. Continue to next Task? (Y/N)\033[0m\n" |
|  | read contyn |
|  | if [ "$contyn" = "N" ] || [ "$contyn" = "n" ]; then |
|  | printf "\033[1;31mAborted\033[0m\n" |
|  | exit |
|  | fi |
|  | clear |
|  | } |
|  | PasswdFun(){ |
|  | printf "\033[1;31mChanging Root's Password..\033[0m\n" |
|  | #--------- Change Root Password ---------------- |
|  | passwd |
|  | echo "Please change other user's passwords too" |
|  | cont |
|  | } |
|  | zeroUidFun(){ |
|  | printf "\033[1;31mChecking for 0 UID users...\033[0m\n" |
|  | #--------- Check and Change UID's of 0 not Owned by Root ---------------- |
|  | touch /zerouidusers |
|  | touch /uidusers |
|  |  |
|  | cut -d: -f1,3 /etc/passwd | egrep ':0$' | cut -d: -f1 | grep -v root > /zerouidusers |
|  |  |
|  | if [ -s /zerouidusers ] |
|  | then |
|  | echo "There are Zero UID Users! I'm fixing it now!" |
|  |  |
|  | while IFS='' read -r line || [[ -n "$line" ]]; do |
|  | thing=1 |
|  | while true; do |
|  | rand=$(( ( RANDOM % 999 ) + 1000)) |
|  | cut -d: -f1,3 /etc/passwd | egrep ":$rand$" | cut -d: -f1 > /uidusers |
|  | if [ -s /uidusers ] |
|  | then |
|  | echo "Couldn't find unused UID. Trying Again... " |
|  | else |
|  | break |
|  | fi |
|  | done |
|  | usermod -u $rand -g $rand -o $line |
|  | touch /tmp/oldstring |
|  | old=$(grep "$line" /etc/passwd) |
|  | echo $old > /tmp/oldstring |
|  | sed -i "s~0:0~$rand:$rand~" /tmp/oldstring |
|  | new=$(cat /tmp/oldstring) |
|  | sed -i "s~$old~$new~" /etc/passwd |
|  | echo "ZeroUID User: $line" |
|  | echo "Assigned UID: $rand" |
|  | done < "/zerouidusers" |
|  | update-passwd |
|  | cut -d: -f1,3 /etc/passwd | egrep ':0$' | cut -d: -f1 | grep -v root > /zerouidusers |
|  |  |
|  | if [ -s /zerouidusers ] |
|  | then |
|  | echo "WARNING: UID CHANGE UNSUCCESSFUL!" |
|  | else |
|  | echo "Successfully Changed Zero UIDs!" |
|  | fi |
|  | else |
|  | echo "No Zero UID Users" |
|  | fi |
|  | cont |
|  | } |
|  | rootCronFun(){ |
|  | printf "\033[1;31mChanging cron to only allow root access...\033[0m\n" |
|  |  |
|  | #--------- Allow Only Root Cron ---------------- |
|  | #reset crontab |
|  | crontab -r |
|  | cd /etc/ |
|  | /bin/rm -f cron.deny at.deny |
|  | echo root >cron.allow |
|  | echo root >at.allow |
|  | /bin/chown root:root cron.allow at.allow |
|  | /bin/chmod 644 cron.allow at.allow |
|  | cont |
|  | } |
|  | apacheSecFun(){ |
|  | printf "\033[1;31mSecuring Apache...\033[0m\n" |
|  | #--------- Securing Apache ---------------- |
|  | a2enmod userdir |
|  |  |
|  | chown -R root:root /etc/apache2 |
|  | chown -R root:root /etc/apache |
|  |  |
|  | if [ -e /etc/apache2/apache2.conf ]; then |
|  | echo "<Directory />" >> /etc/apache2/apache2.conf |
|  | echo " AllowOverride None" >> /etc/apache2/apache2.conf |
|  | echo " Order Deny,Allow" >> /etc/apache2/apache2.conf |
|  | echo " Deny from all" >> /etc/apache2/apache2.conf |
|  | echo "</Directory>" >> /etc/apache2/apache2.conf |
|  | echo "UserDir disabled root" >> /etc/apache2/apache2.conf |
|  | fi |
|  |  |
|  | systemctl restart apache2.service |
|  | cont |
|  | } |
|  | fileSecFun(){ |
|  | printf "\033[1;31mSome automatic file inspection...\033[0m\n" |
|  | #--------- Manual File Inspection ---------------- |
|  | cut -d: -f1,3 /etc/passwd | egrep ':[0-9]{4}$' | cut -d: -f1 > /tmp/listofusers |
|  | echo root >> /tmp/listofusers |
|  |  |
|  | #Replace sources.list with safe reference file (For Ubuntu 14 Only) |
|  | cat $PWDthi/referenceFiles/sources.list > /etc/apt/sources.list |
|  | apt-get update |
|  |  |
|  | #Replace lightdm.conf with safe reference file |
|  | cat $PWDthi/referenceFiles/lightdm.conf > /etc/lightdm/lightdm.conf |
|  |  |
|  | #Replace sshd\_config with safe reference file |
|  | cat $PWDthi/referenceFiles/sshd\_config > /etc/ssh/sshd\_config |
|  | /usr/sbin/sshd -t |
|  | systemctl restart sshd.service |
|  |  |
|  | #/etc/rc.local should be empty except for 'exit 0' |
|  | echo 'exit 0' > /etc/rc.local |
|  |  |
|  | printf "\033[1;31mFinished automatic file inspection. Continue to manual file inspection? (Y/N)\033[0m\n" |
|  | read contyn |
|  | if [ "$contyn" = "N" ] || [ "$contyn" = "n" ]; then |
|  | exit |
|  | fi |
|  | clear |
|  |  |
|  | printf "\033[1;31mSome manual file inspection...\033[0m\n" |
|  |  |
|  | #Manual File Inspection |
|  | nano /etc/resolv.conf #make sure if safe, use 8.8.8.8 for name server |
|  | nano /etc/hosts #make sure is not redirecting |
|  | visudo #make sure sudoers file is clean. There should be no "NOPASSWD" |
|  | nano /tmp/listofusers #No unauthorized users |
|  |  |
|  | cont |
|  | } |
|  | netSecFun(){ |
|  | printf "\033[1;31mSome manual network inspection...\033[0m\n" |
|  | #--------- Manual Network Inspection ---------------- |
|  | lsof -i -n -P |
|  | netstat -tulpn |
|  | cont |
|  | } |
|  | aptUpFun(){ |
|  | printf "\033[1;31mUpdating computer...\033[0m\n" |
|  | #--------- Update Using Apt-Get ---------------- |
|  | #apt-get update --no-allow-insecure-repositories |
|  | apt-get update |
|  | apt-get dist-upgrade -y |
|  | apt-get install -f -y |
|  | apt-get autoremove -y |
|  | apt-get autoclean -y |
|  | apt-get check |
|  | cont |
|  | } |
|  | aptInstFun(){ |
|  | printf "\033[1;31mInstalling programs...\033[0m\n" |
|  | #--------- Download programs ---------------- |
|  | apt-get install -y chkrootkit clamav rkhunter apparmor apparmor-profiles |
|  |  |
|  | #This will download lynis 2.4.0, which may be out of date |
|  | wget https://cisofy.com/files/lynis-2.5.5.tar.gz -O /lynis.tar.gz |
|  | tar -xzf /lynis.tar.gz --directory /usr/share/ |
|  | cont |
|  | } |
|  | deleteFileFun(){ |
|  | printf "\033[1;31mDeleting dangerous files...\033[0m\n" |
|  | #--------- Delete Dangerous Files ---------------- |
|  | find / -name '\*.mp3' -type f -delete |
|  | find / -name '\*.mov' -type f -delete |
|  | find / -name '\*.mp4' -type f -delete |
|  | find / -name '\*.avi' -type f -delete |
|  | find / -name '\*.mpg' -type f -delete |
|  | find / -name '\*.mpeg' -type f -delete |
|  | find / -name '\*.flac' -type f -delete |
|  | find / -name '\*.m4a' -type f -delete |
|  | find / -name '\*.flv' -type f -delete |
|  | find / -name '\*.ogg' -type f -delete |
|  | find /home -name '\*.gif' -type f -delete |
|  | find /home -name '\*.png' -type f -delete |
|  | find /home -name '\*.jpg' -type f -delete |
|  | find /home -name '\*.jpeg' -type f -delete |
|  | cd / && ls -laR 2> /dev/null | grep rwxrwxrwx | grep -v "lrwx" &> /tmp/777s |
|  | cont |
|  |  |
|  | printf "\033[1;31m777 (Full Permission) Files : \033[0m\n" |
|  | printf "\033[1;31mConsider changing the permissions of these files\033[0m\n" |
|  | cat /tmp/777s |
|  | cont |
|  | } |
|  | firewallFun(){ |
|  | printf "\033[1;31mSetting up firewall...\033[0m\n" |
|  | #--------- Setup Firewall ---------------- |
|  | #Please verify that the firewall wont block any services, such as an Email server, when defaulted. |
|  | #I will back up iptables for you in and put it in /iptables/rules.v4.bak and /iptables/rules.v6.bak |
|  | #Uninstall UFW and install iptables |
|  | apt-get remove -y ufw |
|  | apt-get install -y iptables |
|  | apt-get install -y iptables-persistent |
|  | #Backup |
|  | mkdir /iptables/ |
|  | touch /iptables/rules.v4.bak |
|  | touch /iptables/rules.v6.bak |
|  | iptables-save > /iptables/rules.v4.bak |
|  | ip6tables-save > /iptables/rules.v6.bak |
|  | #Clear out and default iptables |
|  | iptables -t nat -F |
|  | iptables -t mangle -F |
|  | iptables -t nat -X |
|  | iptables -t mangle -X |
|  | iptables -F |
|  | iptables -X |
|  | iptables -P INPUT DROP |
|  | iptables -P FORWARD DROP |
|  | iptables -P OUTPUT ACCEPT |
|  | ip6tables -t nat -F |
|  | ip6tables -t mangle -F |
|  | ip6tables -t nat -X |
|  | ip6tables -t mangle -X |
|  | ip6tables -F |
|  | ip6tables -X |
|  | ip6tables -P INPUT DROP |
|  | ip6tables -P FORWARD DROP |
|  | ip6tables -P OUTPUT DROP |
|  | #Block Bogons |
|  | printf "\033[1;31mEnter primary internet interface: \033[0m\n" |
|  | read interface |
|  | #Blocks bogons going into the computer |
|  | iptables -A INPUT -s 127.0.0.0/8 -i $interface -j DROP |
|  | iptables -A INPUT -s 0.0.0.0/8 -j DROP |
|  | iptables -A INPUT -s 100.64.0.0/10 -j DROP |
|  | iptables -A INPUT -s 169.254.0.0/16 -j DROP |
|  | iptables -A INPUT -s 192.0.0.0/24 -j DROP |
|  | iptables -A INPUT -s 192.0.2.0/24 -j DROP |
|  | iptables -A INPUT -s 198.18.0.0/15 -j DROP |
|  | iptables -A INPUT -s 198.51.100.0/24 -j DROP |
|  | iptables -A INPUT -s 203.0.113.0/24 -j DROP |
|  | iptables -A INPUT -s 224.0.0.0/3 -j DROP |
|  | #Blocks bogons from leaving the computer |
|  | iptables -A OUTPUT -d 127.0.0.0/8 -o $interface -j DROP |
|  | iptables -A OUTPUT -d 0.0.0.0/8 -j DROP |
|  | iptables -A OUTPUT -d 100.64.0.0/10 -j DROP |
|  | iptables -A OUTPUT -d 169.254.0.0/16 -j DROP |
|  | iptables -A OUTPUT -d 192.0.0.0/24 -j DROP |
|  | iptables -A OUTPUT -d 192.0.2.0/24 -j DROP |
|  | iptables -A OUTPUT -d 198.18.0.0/15 -j DROP |
|  | iptables -A OUTPUT -d 198.51.100.0/24 -j DROP |
|  | iptables -A OUTPUT -d 203.0.113.0/24 -j DROP |
|  | iptables -A OUTPUT -d 224.0.0.0/3 -j DROP |
|  | #Blocks outbound from source bogons - A bit overkill |
|  | iptables -A OUTPUT -s 127.0.0.0/8 -o $interface -j DROP |
|  | iptables -A OUTPUT -s 0.0.0.0/8 -j DROP |
|  | iptables -A OUTPUT -s 100.64.0.0/10 -j DROP |
|  | iptables -A OUTPUT -s 169.254.0.0/16 -j DROP |
|  | iptables -A OUTPUT -s 192.0.0.0/24 -j DROP |
|  | iptables -A OUTPUT -s 192.0.2.0/24 -j DROP |
|  | iptables -A OUTPUT -s 198.18.0.0/15 -j DROP |
|  | iptables -A OUTPUT -s 198.51.100.0/24 -j DROP |
|  | iptables -A OUTPUT -s 203.0.113.0/24 -j DROP |
|  | iptables -A OUTPUT -s 224.0.0.0/3 -j DROP |
|  | #Block receiving bogons intended for bogons - Super overkill |
|  | iptables -A INPUT -d 127.0.0.0/8 -i $interface -j DROP |
|  | iptables -A INPUT -d 0.0.0.0/8 -j DROP |
|  | iptables -A INPUT -d 100.64.0.0/10 -j DROP |
|  | iptables -A INPUT -d 169.254.0.0/16 -j DROP |
|  | iptables -A INPUT -d 192.0.0.0/24 -j DROP |
|  | iptables -A INPUT -d 192.0.2.0/24 -j DROP |
|  | iptables -A INPUT -d 198.18.0.0/15 -j DROP |
|  | iptables -A INPUT -d 198.51.100.0/24 -j DROP |
|  | iptables -A INPUT -d 203.0.113.0/24 -j DROP |
|  | iptables -A INPUT -d 224.0.0.0/3 -j DROP |
|  | iptables -A INPUT -i lo -j ACCEPT |
|  | #Least Strict Rules |
|  | #iptables -A INPUT -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT |
|  | #Strict Rules -- Only allow well known ports (1-1022) |
|  | #iptables -A INPUT -p tcp --match multiport --sports 1:1022 -m conntrack --ctstate ESTABLISHED -j ACCEPT |
|  | #iptables -A INPUT -p udp --match multiport --sports 1:1022 -m conntrack --ctstate ESTABLISHED -j ACCEPT |
|  | #iptables -A OUTPUT -p tcp --match multiport --dports 1:1022 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT |
|  | #iptables -A OUTPUT -p udp --match multiport --dports 1:1022 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT |
|  | #iptables -A OUTPUT -o lo -j ACCEPT |
|  | #iptables -P OUTPUT DROP |
|  | #Very Strict Rules - Only allow HTTP/HTTPS, NTP and DNS |
|  | iptables -A INPUT -p tcp --sport 80 -m conntrack --ctstate ESTABLISHED -j ACCEPT |
|  | iptables -A INPUT -p tcp --sport 443 -m conntrack --ctstate ESTABLISHED -j ACCEPT |
|  | iptables -A INPUT -p tcp --sport 53 -m conntrack --ctstate ESTABLISHED -j ACCEPT |
|  | iptables -A INPUT -p udp --sport 53 -m conntrack --ctstate ESTABLISHED -j ACCEPT |
|  | iptables -A OUTPUT -p tcp --dport 80 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT |
|  | iptables -A OUTPUT -p tcp --dport 443 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT |
|  | iptables -A OUTPUT -p tcp --dport 53 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT |
|  | iptables -A OUTPUT -p udp --dport 53 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT |
|  | iptables -A OUTPUT -o lo -j ACCEPT |
|  | iptables -P OUTPUT DROP |
|  | mkdir /etc/iptables/ |
|  | touch /etc/iptables/rules.v4 |
|  | touch /etc/iptables/rules.v6 |
|  | iptables-save > /etc/iptables/rules.v4 |
|  | ip6tables-save > /etc/iptables/rules.v6 |
|  | cont |
|  | } |
|  | sysCtlFun(){ |
|  | printf "\033[1;31mMaking Sysctl Secure...\033[0m\n" |
|  | #--------- Secure /etc/sysctl.conf ---------------- |
|  | sysctl -w net.ipv4.tcp\_syncookies=1 |
|  | sysctl -w net.ipv4.ip\_forward=0 |
|  | sysctl -w net.ipv4.conf.all.send\_redirects=0 |
|  | sysctl -w net.ipv4.conf.default.send\_redirects=0 |
|  | sysctl -w net.ipv4.conf.all.accept\_redirects=0 |
|  | sysctl -w net.ipv4.conf.default.accept\_redirects=0 |
|  | sysctl -w net.ipv4.conf.all.secure\_redirects=0 |
|  | sysctl -w net.ipv4.conf.default.secure\_redirects=0 |
|  | sysctl -p |
|  | cont |
|  | } |
|  | scanFun(){ |
|  | printf "\033[1;31mScanning for Viruses...\033[0m\n" |
|  | #--------- Scan For Vulnerabilities and viruses ---------------- |
|  |  |
|  | #chkrootkit |
|  | printf "\033[1;31mStarting CHKROOTKIT scan...\033[0m\n" |
|  | chkrootkit -q |
|  | cont |
|  |  |
|  | #Rkhunter |
|  | printf "\033[1;31mStarting RKHUNTER scan...\033[0m\n" |
|  | rkhunter --update |
|  | rkhunter --propupd #Run this once at install |
|  | rkhunter -c --enable all --disable none |
|  | cont |
|  |  |
|  | #Lynis |
|  | printf "\033[1;31mStarting LYNIS scan...\033[0m\n" |
|  | cd /usr/share/lynis/ |
|  | /usr/share/lynis/lynis update info |
|  | /usr/share/lynis/lynis audit system |
|  | cont |
|  |  |
|  | #ClamAV |
|  | printf "\033[1;31mStarting CLAMAV scan...\033[0m\n" |
|  | systemctl stop clamav-freshclam |
|  | freshclam --stdout |
|  | systemctl start clamav-freshclam |
|  | clamscan -r -i --stdout --exclude-dir="^/sys" / |
|  | cont |
|  | } |
|  |  |
|  | repoFun(){ |
|  | read -p "Please check the repo for any issues [Press any key to continue...]" -n1 -s |
|  | nano /etc/apt/sources.list |
|  | gpg /etc/apt/trusted.gpg > /tmp/trustedGPG |
|  | printf "\033[1;31mPlease check /tmp/trustedGPG for trusted GPG keys\033[0m\n" |
|  | cont |
|  | } |
|  |  |
|  | startFun |

|  |  |
| --- | --- |
| #!/bin/bash |  |
|  |  |
|  | # Ubuntu Security Script |
|  | # Brian Strauch |
|  |  |
|  | if [[ $EUID -ne 0 ]] |
|  | then |
|  | echo "You must be root to run this script." |
|  | exit 1 |
|  | fi |
|  |  |
|  | # Firewall |
|  | sudo ufw enable |
|  |  |
|  | # Updates |
|  | sudo apt-get -y upgrade |
|  | sudo apt-get -y update |
|  |  |
|  | # Lock Out Root User |
|  | sudo passwd -l root |
|  |  |
|  | # Disable Guest Account |
|  | echo "allow-guest=false" >> /etc/lightdm/lightdm.conf |
|  |  |
|  | # Configure Password Aging Controls |
|  | sudo sed -i '/^PASS\_MAX\_DAYS/ c\PASS\_MAX\_DAYS 90' /etc/login.defs |
|  | sudo sed -i '/^PASS\_MIN\_DAYS/ c\PASS\_MIN\_DAYS 10' /etc/login.defs |
|  | sudo sed -i '/^PASS\_WARN\_AGE/ c\PASS\_WARN\_AGE 7' /etc/login.defs |
|  |  |
|  | # Password Authentication |
|  | sudo sed -i '1 s/^/auth optional pam\_tally.so deny=5 unlock\_time=900 onerr=fail audit even\_deny\_root\_account silent\n/' /etc/pam.d/common-auth |
|  |  |
|  | # Force Strong Passwords |
|  | sudo apt-get -y install libpam-cracklib |
|  | sudo sed -i '1 s/^/password requisite pam\_cracklib.so retry=3 minlen=8 difok=3 reject\_username minclass=3 maxrepeat=2 dcredit=1 ucredit=1 lcredit=1 ocredit=1\n/' /etc/pam.d/common-password |
|  |  |
|  | # MySQL |
|  | echo -n "MySQL [Y/n] " |
|  | read option |
|  | if [[ $option =~ ^[Yy]$ ]] |
|  | then |
|  | sudo apt-get -y install mysql-server |
|  | # Disable remote access |
|  | sudo sed -i '/bind-address/ c\bind-address = 127.0.0.1' /etc/mysql/my.cnf |
|  | sudo service mysql restart |
|  | else |
|  | sudo apt-get -y purge mysql\* |
|  | fi |
|  |  |
|  | # OpenSSH Server |
|  | echo -n "OpenSSH Server [Y/n] " |
|  | read option |
|  | if [[ $option =~ ^[Yy]$ ]] |
|  | then |
|  | sudo apt-get -y install openssh-server |
|  | # Disable root login |
|  | sudo sed -i '/^PermitRootLogin/ c\PermitRootLogin no' /etc/ssh/sshd\_config |
|  | sudo service ssh restart |
|  | else |
|  | sudo apt-get -y purge openssh-server\* |
|  | fi |
|  |  |
|  | # VSFTPD |
|  | echo -n "VSFTP [Y/n] " |
|  | read option |
|  | if [[ $option =~ ^[Yy]$ ]] |
|  | then |
|  | sudo apt-get -y install vsftpd |
|  | # Disable anonymous uploads |
|  | sudo sed -i '/^anon\_upload\_enable/ c\anon\_upload\_enable no' /etc/vsftpd.conf |
|  | sudo sed -i '/^anonymous\_enable/ c\anonymous\_enable=NO' /etc/vsftpd.conf |
|  | # FTP user directories use chroot |
|  | sudo sed -i '/^chroot\_local\_user/ c\chroot\_local\_user=YES' /etc/vsftpd.conf |
|  | sudo service vsftpd restart |
|  | else |
|  | sudo apt-get -y purge vsftpd\* |
|  | fi |
|  |  |
|  | # Malware |
|  | sudo apt-get -y purge hydra\* |
|  | sudo apt-get -y purge john\* |
|  | sudo apt-get -y purge nikto\* |
|  | sudo apt-get -y purge netcat\* |
|  |  |
|  | # Media Files |
|  | for suffix in mp3 txt wav wma aac mp4 mov avi gif jpg png bmp img exe msi bat sh |
|  | do |
|  | sudo find /home -name \*.$suffix |
|  | done |