Hardening CentOS

**Essentials**

Enter # yum update -y | Updates installed packages to the latest version.

Enter # passwd root | Changes root password.

Enter # useradd sysadmin | Creates system administrator account used to manage system.

Enter # passwd sysadmin | Adds password to sysadmin.

Enter # vi /etc/sudoers | Edit sudoers file and add user who wants sudo privileges.

Graphical user interface, text, application, email

Description automatically generated

**Disable Crons**

Enter # systemctl disable crond | To stop crond from startup on boot.

Enter # systemctl stop crond | To stop crond service.

Enter # crontab -e | to edit/delete crons

**Additional information:**

Enter # crontab -l | Lists crons for current user.

Enter # crontab -u user -l | Lists crons for specific user.

**Check Aliases**

Enter # cat .bashrc | to view aliases

Remove any malicious aliases found. Should look like this by default:

Graphical user interface, text, application, email

Description automatically generated

**Remove Rouge Users**

Enter # vi /etc/passwd | to view all users in system (Newer users should be at the bottom)

Enter # pkill -u username | sudo userdel -r username | To kill session and delete user

**Iptables / Ufw / Open Ports**

Enter # stop firewalld | Stops firewall.

Enter # systemctl disable firewalld | Disables firewall to start on boot.

Enter # systemctl mask --now firewalld |

Enter # yum install iptables-services | Installs iptables (New firewall)

Enter # iptables -F | To flush firewall rules.

Enter # iptables -P FORWARD DROP | To block all forward traffic.

Enter # iptables -A INPUT -p tcp --dport 80 -j ACCEPT |

Enter # iptables -A INPUT -p tcp --dport 443 -j ACCEPT |

Enter # iptables -A INPUT -p tcp --dport 3306 -j ACCEPT |

Enter # iptables -A INPUT -p udp --dport 53 -j ACCEPT |

Enter # iptables -A INPUT -p udp --dport 123 -j ACCEPT |

Enter # iptables -A INPUT -p tcp --sport 80 -j ACCEPT |

Enter # iptables -A OUTPUT -p tcp --sport 80 -j ACCEPT |

Enter # service iptables save |

Enter # systemctl enable iptables |

Enter # systemctl restart iptables |

Enter # iptables -L | less | to view IPtable rules.

Enter # ipt6tables -P FORWARD DROP |

Enter # ipt6tables -P INPUT DROP |

Enter # ipt6tables -P OUTPUT DROP |

**Additional information:**

Enter # nmap localhost | Scans local system for open ports.

Enter # netstat -tulnp | Lists open ports with process ID, protocol, and state.

Enter # iptables -L | less | to view IPtable rules.

Enter # iptables -F | to flush IPtable rules.

Enter # vi /etc/sysconfig/iptables | to view IPtable config file.

Enter # chkconfig iptables | to view if it is enabled.

Enter # sudo iptables -D INPUT -p tcp --dport xxxx -j ACCEPT |

**SSH**

**Disable SSH:**

Enter # systemctl disable sshd | Disables SSH from starting on boot.

Enter # systemctl stop sshd | Stops SSH service.

Enter # reboot | Or follow step in additional information if uptime is an issue.

**Change default port number:**

Enter # vi /etc/ssh/sshd\_config | To edit the SSH config file.

UNCOMMENT PORT AND CHANGE TO 549

Enter # dnf install policycoreutils-python-utils | To install semange if needed.

Enter # semanage port -a -t ssh\_port\_t -p tcp 549 | To add port 549 to selinux rules.

Enter # systemctl restart sshd | To reset SSH.

**Create SSH key gen authentication to allow login without password (Windows to Linux):**

1. Run Puttygen – then generate a key by waving the mouse around.
2. Save the private key to your windows computer.
3. Open ssh conncetion to Linux server and create these files.

Enter # mkdir ~/.ssh | Creates new directory new directory for SSH keys.

Enter # chmod 0700 ~/.ssh | Changes permission to allow read write execute.

Enter # touch ~/.ssh/authorized\_keys | Create SSH key folder.

Enter # chmod 0644 ~/.ssh/authorized\_keys | Change permissions to folder.

THEN PASTE THE PUBLIC KEY FROM Puttygen INTO THIS FILE:

Enter # vi ~/.ssh/authorized\_keys | To edit key file.

Enter # systemctl restart sshd | To reset SSH.

**Lockdown SSH config settings:**

Enter # vi /etc/ssh/sshd\_config | To edit SSH config file.

Text

Description automatically generatedText

Description automatically generated

Enter # systemctl restart sshd | To reset SSH.

**Additional information:**

Enter # w | To display list of active SSH sessions (Note the PID)

Enter # kill PID | To kill the SSH session.

Enter # w | To verify it is no longer active.

**SELinux**

Enter # sestatus | To see if its enabled or not.

Enter # vi /etc/selinux/config | To view the SELinux config file.

This is the default configuration (Make sure it is enforcing):

Text

Description automatically generated

**Setting a SELinux Boolean (with example):**

Enter # yum install setroubleshoot -y | To install the troubleshooting tool for SELinux.

Enter # sealert -a /var/log/audit/audit.log | To view the error causing blocked access.

Look at example provided for solution:

Graphical user interface, text, application, email

Description automatically generated

Enter # setsebool -P httpd\_read\_user\_content 1 | To create the Boolean.

**Apache**

**Disallow Apache from showing directories:**

Enter # vi /httpd.conf | To edit the http config file.

Edit the following (ADD PICTURE):

ServerTokens Prod

ServerSignature Off

TraceEnable Off

Option all -Indexes

**Change the admin folder name:**

**Additional information:**

Enter # sed -i "s/Options Indexes FollowSymLinks/Options FollowSymLinks/" /etc/httpd/conf/httpd.conf

**PHP**

**Backups**

**Iptables backup and restore:**

Enter # iptables-save > tab.txt | Saves configured settings to tab.txt.

Enter # iptables-restore < tab.txt | Imports configured settings from tab.txt into iptables.

**Iptables override configured settings to start on boot (Layered security):**

Enter # iptables-save > /root/iptables | Saves iptables settings to /root/iptables.

Enter # chmod 700 /etc/rc.local | To change the permissions to rc.local.

Enter # vi /etc/rc.local | To edit the rc.local file.

INPUT THE FOLLOWING:

/sbin/iptables-restore < /root/iptables | Iptables starts with configured settings on boot.

**MySQL backup:**

Enter # mysqldump -u root -p prestashop > prestashop.sql | To create a backup of a database

**Additional information:**

Enter # mysqldump -u username -p --all -databases >> name.sql | To export a database.

Enter # mysql -u username -p < nameofdatabasebackup | To import a database.

**Tools For Malware / Rootkits / Vulnerabilities / Exploits**

**ClamAV**

Description: Clam Antivirus is a free, open-source, cross-platform antimalware toolkit able to detect many types of malware, including viruses. (Test virus: wget -P ~/ http://www.eicar.org/download/eicar.com)

INSTALL:

Enter # yum install clamav clamav-update -y | Installs ClamAV.

Enter # freshclam | Get the newest update of malware searches.

Enter # mkdir scanresult | Create directory to house the results from scan.

USAGE:

Enter # clamscan -r --move=/home/user1/scanresult /home | Move malware into scanresult.

Enter # cd scanresult | Change directory to scanresult.

Enter # ls | List all files found from scan.

**Lynis**

**rkhunter**

**General Security Concepts**

**Disable IPv6 through the system (Also do through firewall for layered security):**

Enter # vi /etc/sysctl.conf | To edit the IPv6 file.

Add the following lines (REPLACE WITH PICTURE)

net.ipv6.conf.all.disable\_ipv6 = 1

net.ipv6.conf.default.disable\_ipv6 = 1

Enter # systemctl restart network | To restart the network settings.

Enter # Ip -6 addr | To verify if IPv6 is down.

**Create a banner for SSH logins:**

Enter # vi /etc/sshbanner.txt | To create the file for the banner.

INPUT THE FOLLOWING:



Enter # vi /etc/ssh/sshd\_config | To edit the SSH config file.

INPUT THE FOLLOWING (Add picture):

/etc/sshbanner.txt into the login spot

Enter # systemctl restart sshd | To reset the settings for SSH.

**Lock down files:**

Enter # chattr +I /etc/passwd |

Enter # chattr +I /etc/shadow |

**Make sure essential services are enabled:**

Enter # systemctl enable httpd mariadb | Allows services to start on boot.

**Remove useless programs:**

Enter # yum remove xinetd telnet-server rsh-server \ telnet rsh ypbind ypserv tfsp-server bind \ vsfptd dovecot squid net-snmpd talk-server talk

**fail2ban**

**List of CVEs**

**Red Team Activity**

**Finding specific users files:**

Enter # find / -user john | Finds all files owned by the user john.

Enter # cat /home/john/.bash\_history | Finds users previously typed commands.

**Managing processes:**

**Checking connections / ports:**

Ps aux

W

Kill 1234

Ps ax | grep nc

ON DEBIAN:

Identify quickly if firewall is installed then check the status of it afterwards

dpkg -l | grep -E '(iptables|ufw|nftables|firewall)'