#!/bin/bash

#net.ipv4.ip\_forward = 0 is used to tell the system whether it can forward packets or not

echo -e "\e[36m---------ip\_forward---------\e[0m"

if grep "net.ipv4.ip\_forward" /etc/sysctl.conf

then

sed -i "s/net.ipv4.ip\_forward.\*/net.ipv4.ip\_forward=0/g" /etc/sysctl.conf

sysctl -w net.ipv4.ip\_forward=0

sysctl -w net.ipv4.route.flush=1

else

echo "net.ipv4.ip\_forward=0"

sysctl -w net.ipv4.ip\_forward=0

sysctl -w net.ipv4.route.flush=1

fi

#net.ipv4.conf.all.send\_redirects=0

#ICMP redirects used to send routing information to other hosts

#As a host itself does not act as a router, there is no need to send redirects

echo -e "\e[36m---------conf.all.send\_redirects---------\e[0m"

if grep "net.ipv4.conf.all.send\_redirects" /etc/sysctl.conf

then

sed -i "s/net.ipv4.conf.all.send\_redirects.\*/net.ipv4.conf.all.send\_redirects=0/g" /etc/sysctl.conf

sysctl -w net.ipv4.conf.all.send\_redirects=0

sysctl -w net.ipv4.route.flush=1

else

echo "net.ipv4.conf.all.send\_redirects=0"

sysctl -w net.ipv4.conf.all.send\_redirects=0

sysctl -w net.ipv4.route.flush=1

fi

#net.ipv4.conf.default.send\_redirects

echo -e "\e[36m---------conf.default.send\_redirects---------\e[0m"

if grep "net.ipv4.conf.default.send\_redirects" /etc/sysctl.conf

then

sed -i "s/net.ipv4.conf.default.send\_redirects.\*/net.ipv4.conf.default.send\_redirects=0/g" /etc/sysctl.conf

sysctl -w net.ipv4.conf.default.send\_redirects=0

sysctl -w net.ipv4.route.flush=1

else

echo "net.ipv4.conf.default.send\_redirects=0"

sysctl -w net.ipv4.conf.default.send\_redirects=0

sysctl -w net.ipv4.route.flush=1

fi

#net.ipv4.conf.all.accept\_source\_route

#Source routing allows send to partially or fully specify route packets take through a network

echo -e "\e[36m---------conf.all.accept\_source\_route---------\e[0m"

if grep "net.ipv4.conf.all.accept\_source\_route" /etc/sysctl.conf

then

sed -i "s/net.ipv4.conf.all.accept\_source\_route.\*/net.ipv4.conf.all.accept\_source\_route=0/g" /etc/sysctl.conf

sysctl -w net.ipv4.conf.all.accept\_source\_route=0

sysctl -w net.ipv4.route.flush=1

else

echo "net.ipv4.conf.all.accept\_source\_route=0"

sysctl -w net.ipv4.conf.all.accept\_source\_route=0

sysctl -w net.ipv4.route.flush=1

fi

#net.ipv4.conf.default.accept\_source\_route

echo -e "\e[36m---------conf.default.accept\_source\_route---------\e[0m"

if grep "net.ipv4.conf.default.accept\_source\_route" /etc/sysctl.conf

then

sed -i "s/net.ipv4.conf.default.accept\_source\_route.\*/net.ipv4.conf.default.accept\_source\_route=0/g" /etc/sysctl.conf

sysctl -w net.ipv4.conf.default.accept\_source\_route=0

sysctl -w net.ipv4.route.flush=1

else

echo "net.ipv4.conf.default.accept\_source\_route=0"

sysctl -w net.ipv4.conf.default.accept\_source\_route=0

sysctl -w net.ipv4.route.flush=1

fi

#net.ipv4.conf.all.accept\_redirects

#ICMP redirect messages are packets that convey routing information and tell host to send packets by alternative path

#way of allowing outside routing device to update system routing tables

echo -e "\e[36m---------conf.all.accept\_redirects---------\e[0m"

if grep "net.ipv4.conf.all.accept\_redirects" /etc/sysctl.conf

then

sed -i "s/net.ipv4.conf.all.accept\_redirects.\*/net.ipv4.conf.all.accept\_redirects=0/g" /etc/sysctl.conf

sysctl -w net.ipv4.conf.all.accept\_redirects=0

sysctl -w net.ipv4.route.flush=1

else

echo "net.ipv4.conf.all.accept\_redirects=0"

sysctl -w net.ipv4.conf.all.accept\_redirects=0

sysctl -w net.ipv4.route.flush=1

fi

#net.ipv4.conf.default.accept\_redirects

echo -e "\e[36m---------conf.default.accept\_redirects---------\e[0m"

if grep "net.ipv4.conf.default.accept\_redirects" /etc/sysctl.conf

then

sed -i "s/net.ipv4.conf.default.accept\_redirects.\*/net.ipv4.conf.default.accept\_redirects=0/g" /etc/sysctl.conf

sysctl -w net.ipv4.conf.default.accept\_redirects=0

sysctl -w net.ipv4.route.flush=1

else

echo "net.ipv4.conf.default.accept\_redirects=0"

sysctl -w net.ipv4.conf.default.accept\_redirects=0

sysctl -w net.ipv4.route.flush=1

fi

#net.ipv4.conf.all.secure\_redirects

#Same as regular ICMP redirects, but come from gateways listed on default gateway list

#Assumed that gateways are known to your system, likely secure

echo -e "\e[36m---------conf.all.secure\_redirects---------\e[0m"

if grep "net.ipv4.conf.all.secure\_redirects" /etc/sysctl.conf

then

sed -i "s/net.ipv4.conf.all.secure\_redirects.\*/net.ipv4.conf.all.secure\_redirects=0/g" /etc/sysctl.conf

sysctl -w net.ipv4.conf.all.secure\_redirects=0

sysctl -w net.ipv4.route.flush=1

else

echo "net.ipv4.conf.all.secure\_redirects=0"

sysctl -w net.ipv4.conf.all.secure\_redirects=0

sysctl -w net.ipv4.route.flush=1

fi

#net.ipv4.conf.default.secure\_redirects

echo -e "\e[36m---------conf.default.secure\_redirects---------\e[0m"

if grep "net.ipv4.conf.default.secure\_redirects" /etc/sysctl.conf

then

sed -i "s/net.ipv4.conf.default.secure\_redirects.\*/net.ipv4.conf.default.secure\_redirects=0/g" /etc/sysctl.conf

sysctl -w net.ipv4.conf.default.secure\_redirects=0

sysctl -w net.ipv4.route.flush=1

else

echo "net.ipv4.conf.default.secure\_redirects=0"

sysctl -w net.ipv4.conf.default.secure\_redirects=0

sysctl -w net.ipv4.route.flush=1

fi

#net.ipv4.conf.all.log\_martians=1

#logs packets with un-routable source addresses to the kernel log

echo -e "\e[36m---------conf.all.log\_martians---------\e[0m"

if grep "net.ipv4.conf.all.log\_martians" /etc/sysctl.conf

then

sed -i "s/net.ipv4.conf.all.log\_martians.\*/net.ipv4.conf.all.log\_martians=1/g" /etc/sysctl.conf

sysctl -w net.ipv4.conf.all.log\_martians=1

sysctl -w net.ipv4.route.flush=1

else

echo "net.ipv4.conf.all.log\_martians=1"

sysctl -w net.ipv4.conf.all.log\_martians=1

sysctl -w net.ipv4.route.flush=1

fi

#net.ipv4.conf.default.log\_martians=1

echo -e "\e[36m---------conf.default.log\_martians---------\e[0m"

if grep "net.ipv4.conf.default.log\_martians" /etc/sysctl.conf

then

sed -i "s/net.ipv4.conf.default.log\_martians.\*/net.ipv4.conf.default.log\_martians=1/g" /etc/sysctl.conf

sysctl -w net.ipv4.conf.default.log\_martians=1

sysctl -w net.ipv4.route.flush=1

else

echo "net.ipv4.conf.default.log\_martians=1"

sysctl -w net.ipv4.conf.default.log\_martians=1

sysctl -w net.ipv4.route.flush=1

fi

#net.ipv4.icmp\_echo\_ignore\_broadcasts=1

#will cause system to ignore all ICMP echo and timestamp requests to broadcast and multicast addresses

echo -e "\e[36m---------icmp\_echo\_ignore\_broadcasts---------\e[0m"

if grep "net.ipv4.icmp\_echo\_ignore\_broadcasts" /etc/sysctl.conf

then

sed -i "s/net.ipv4.icmp\_echo\_ignore\_broadcasts.\*/net.ipv4.icmp\_echo\_ignore\_broadcasts=1/g" /etc/sysctl.conf

sysctl -w net.ipv4.icmp\_echo\_ignore\_broadcasts=1

sysctl -w net.ipv4.route.flush=1

else

echo "net.ipv4.icmp\_echo\_ignore\_broadcasts=1"

sysctl -w net.ipv4.icmp\_echo\_ignore\_broadcasts=1

sysctl -w net.ipv4.route.flush=1

fi

#net.ipv4.icmp\_ignore\_bogus\_error\_responses=1

#prevents kernel from logging bogus responses (RFC-1122 non-compliant) from broadcast reframes

echo -e "\e[36m---------icmp\_ignore\_bogus\_error\_responses---------\e[0m"

if grep "net.ipv4.icmp\_ignore\_bogus\_error\_responses" /etc/sysctl.conf

then

sed -i "s/net.ipv4.icmp\_ignore\_bogus\_error\_responses.\*/net.ipv4.icmp\_ignore\_bogus\_error\_responses=1/g" /etc/sysctl.conf

sysctl -w net.ipv4.icmp\_ignore\_bogus\_error\_responses=1

sysctl -w net.ipv4.route.flush=1

else

echo "net.ipv4.icmp\_ignore\_bogus\_error\_responses=1"

sysctl -w net.ipv4.icmp\_ignore\_bogus\_error\_responses=1

sysctl -w net.ipv4.route.flush=1

fi

#net.ipv4.conf.all.rp\_filter=1

#forces kernel to utilize reverse path filtering on received packet to determine if packet is valid

#if return packet does not go out the same interface that corresponding source packet came from, packet is dropped

echo -e "\e[36m---------conf.all.rp\_filter---------\e[0m"

if grep "net.ipv4.conf.all.rp\_filter" /etc/sysctl.conf

then

sed -i "s/net.ipv4.conf.all.rp\_filter.\*/net.ipv4.conf.all.rp\_filter=1/g" /etc/sysctl.conf

sysctl -w net.ipv4.conf.all.rp\_filter=1

sysctl -w net.ipv4.route.flush=1

else

echo "net.ipv4.conf.all.rp\_filter=1"

sysctl -w net.ipv4.conf.all.rp\_filter=1

sysctl -w net.ipv4.route.flush=1

fi

#net.ipv6.conf.all.accept\_ra

#disables system ability to accept v6 router advertisements

echo -e "\e[36m---------v6.conf.all.accept\_ra---------\e[0m"

if grep "net.ipv6.conf.all.accept\_ra" /etc/sysctl.conf

then

sed -i "s/net.ipv6.conf.all.accept\_ra.\*/net.ipv6.conf.all.accept\_ra=0/g" /etc/sysctl.conf

sysctl -w net.ipv6.conf.all.accept\_ra=0

sysctl -w net.ipv6.route.flush=1

else

echo "net.ipv6.conf.all.accept\_ra=0"

sysctl -w net.ipv6.conf.all.accept\_ra=0

sysctl -w net.ipv6.route.flush=1

fi

#net.ipv6.conf.all.accept\_redirects

#prevents system from accepting ICMP redirects

echo -e "\e[36m---------v6.conf.all.accept\_redirects---------\e[0m"

if grep "net.ipv6.conf.all.accept\_redirects" /etc/sysctl.conf

then

sed -i "s/net.ipv6.conf.all.accept\_redirects.\*/net.ipv6.conf.all.accept\_redirects=0/g" /etc/sysctl.conf

sysctl -w net.ipv6.conf.all.accept\_redirects=0

sysctl -w net.ipv6.route.flush=1

else

echo "net.ipv6.conf.all.accept\_redirects=0"

sysctl -w net.ipv6.conf.all.accept\_redirects=0

sysctl -w net.ipv6.route.flush=1

fi