***Names: Syed Mahad Arshad Hussaini & Mahum Shaikh***

***ID’s: 19163 & 16419***

***Course: OS (Lab)***

***Submitted To: Miss Hira Farman***

**PROJECT**

Internet Security Firewall (ISF) is a simple bash shell script to automate the iptables which allows you to whitelist and blacklist a list of IP addresses and allow or block the ports etc. easily without knowing iptables and remembering much commands. You just need to define the rules in config.json file and run the script. The script use iptables to apply the firewall.

**Code:**

WHITELIST=$(cat config.json | jq .whitelist | sed 's/"//g')

BLACKLIST=$(cat config.json | jq .blacklist | sed 's/"//g')

ALLOW\_PORTS=$(cat config.json | jq .allow\_ports | sed 's/"//g')

DENY\_PORTS=$(cat config.json | jq .deny\_ports | sed 's/"//g')

IPTABLES=$(cat config.json | jq .iptables | sed 's/"//g')

IPTABLES\_SAVE=$(cat config.json | jq .iptables\_save | sed 's/"//g')

$IPTABLES\_SAVE > /usr/local/etc/iptables.last

$IPTABLES -P INPUT ACCEPT

echo "[+] Setting default INPUT policy to ACCEPT"

$IPTABLES -F

echo "[~] Clearing Tables..."

$IPTABLES -X

echo "[-] Deleting user defined Chains..."

$IPTABLES -Z

echo "[-] Zero chain counters"

echo "[+] Allowing Localhost"

$IPTABLES -A INPUT -s 127.0.0.1 -j ACCEPT

##The following rule ensures that established connections are not checked.

##It also allows for things that may be related but not part of those connections such as ICMP.

$IPTABLES -A INPUT -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT

# Whitelist

for x in `grep -v ^# $WHITELIST | awk '{print $1}'`; do

echo "[+] Permitting $x..."

$IPTABLES -A INPUT -s $x -j ACCEPT

done

# Blacklist

for x in `grep -v ^# $BLACKLIST | awk '{print $1}'`; do

echo "[-] Denying $x..."

$IPTABLES -A INPUT -s $x -j DROP

done

# Permitted Ports

for port in $ALLOWED; do

echo "[+] Accepting port TCP $port..."

$IPTABLES -A INPUT -p tcp --dport $port -j ACCEPT

done

for port in $ALLOWED; do

echo "[+] Accepting port UDP $port..."

$IPTABLES -A INPUT -p udp --dport $port -j ACCEPT

done

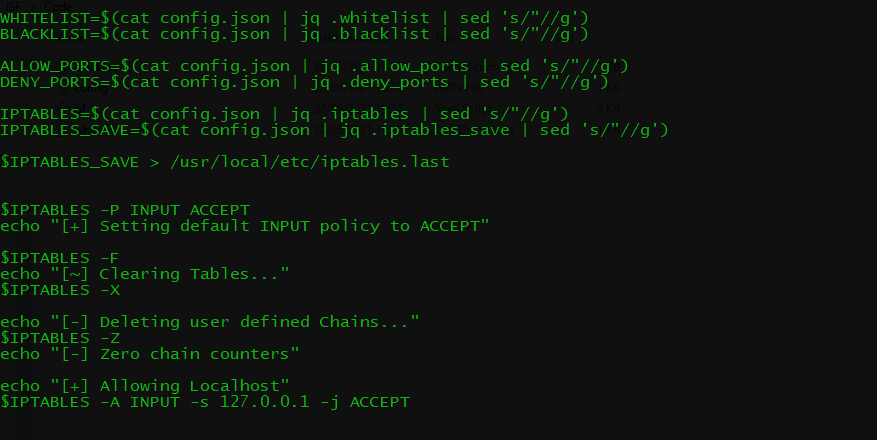
$IPTABLES -A INPUT -p udp -j DROP

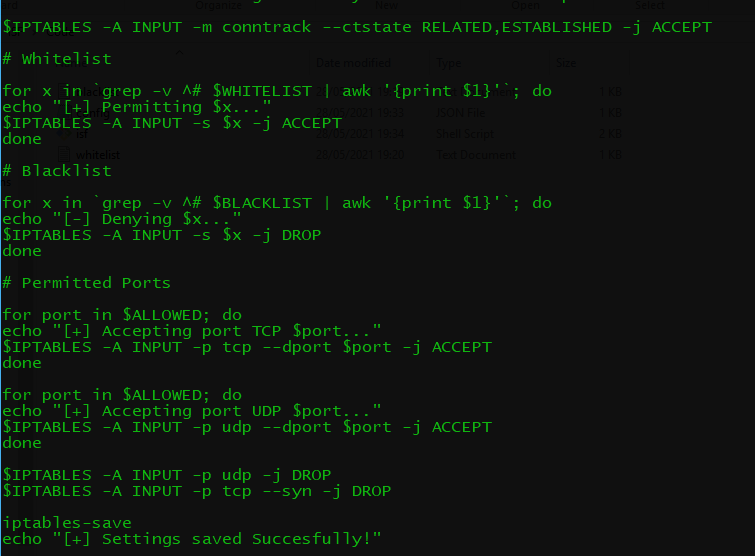
$IPTABLES -A INPUT -p tcp --syn -j DROP

iptables-save

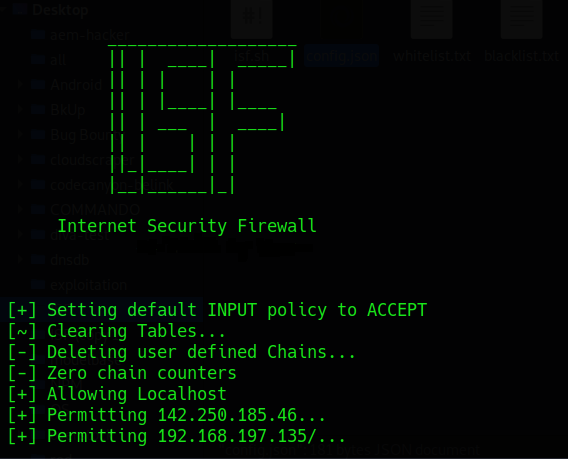
echo "[+] Settings saved Succesfully!"

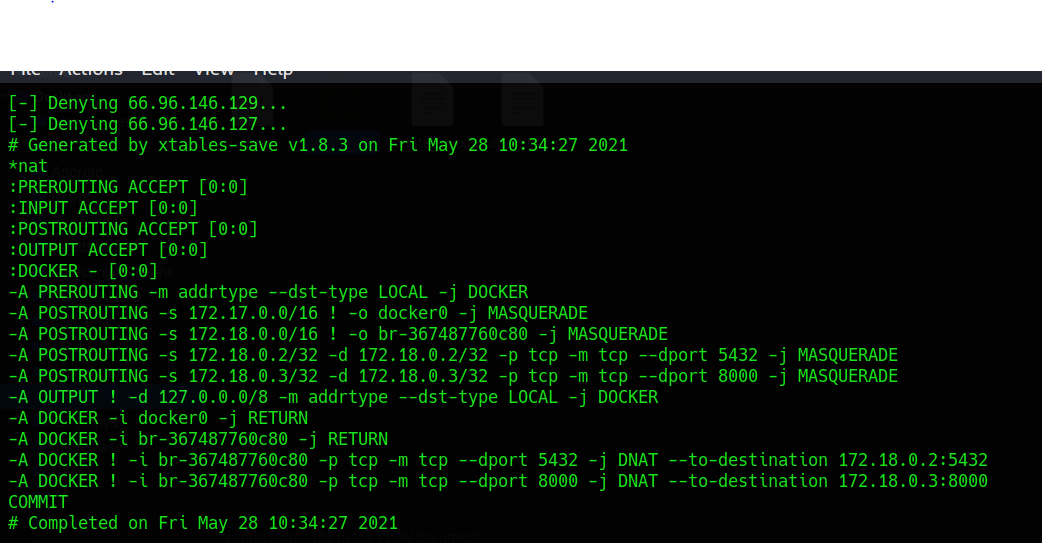
**Code Screen Shots:**

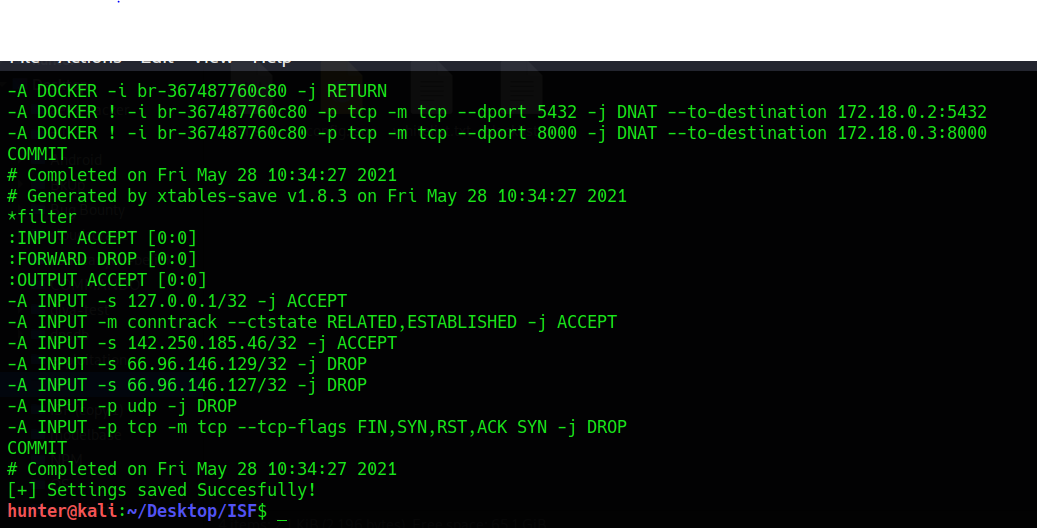
****

****

**OUTPUT:**







**# CODED BY MAHAD & MAHUM**

**THE END**