

Example IPTables Firewall Script

```
#!/bin/sh

## This flushes/clears any and all previously cached tables
echo "[+] Flushing existing iptables rules and tables..."
iptables -F
iptables -X
iptables -F -t nat

## This sets the default policy for the iptables chains
echo "[+] Changing default chain policy..."
iptables -P INPUT DROP
iptables -P FORWARD DROP
iptables -P OUTPUT ACCEPT

## This defines our Log-N-Drop policy and what information we collect and send to syslog
echo "[+] Creating and activating the Log-N-Drop chain and policy..."
iptables -N Log-N-Drop

## Check for different types of attack scans, Drop all invalid TCP state combinations
## First list of TCP state flags lists the bits to be tested, Second list of TCP state flags lists the bits that must be set to match test
iptables -A Log-N-Drop -p tcp -m tcp --tcp-flags FIN,SYN,RST,PSH,ACK,URG FIN,PSH,URG -j LOG --log-prefix "Denied XMAS SCAN: "
iptables -A Log-N-Drop -p tcp -m tcp --tcp-flags FIN,SYN,RST,PSH,ACK,URG NONE -j LOG --log-prefix "Denied NULL SCAN: "
iptables -A Log-N-Drop -p tcp -m tcp --tcp-flags FIN,SYN,RST,PSH,ACK,URG FIN,SYN -j LOG --log-prefix "Denied SYNFIN SCAN: "
iptables -A Log-N-Drop -p tcp -m tcp --tcp-flags SYN,RST SYN,RST -j LOG --log-prefix "Denied SYN_RST SCAN: "
iptables -A Log-N-Drop -p tcp -m tcp --tcp-flags FIN,RST FIN,RST -j LOG --log-prefix "Denied FIN_RST SCAN: "
iptables -A Log-N-Drop -p tcp -m tcp --tcp-flags FIN,ACK FIN -j LOG --log-prefix "Denied FIN SCAN: "
iptables -A Log-N-Drop -p tcp -m tcp --tcp-flags ACK,URG URG -j LOG --log-prefix "Denied URG SCAN: "

# All of the bits are cleared
iptables -A Log-N-Drop -p tcp -m tcp --tcp-flags ALL NONE -j DROP
```

```
# SYN and FIN are both set
iptables -A Log-N-Drop -p tcp -m tcp --tcp-flags SYN,FIN SYN,FIN -j DROP
```

```
# FIN is set without the expected accompanying ACK
iptables -A Log-N-Drop -p tcp -m tcp --tcp-flags ACK,FIN FIN -j DROP
```

```
# PSH is set without the expected accompanying ACK
iptables -A Log-N-Drop -p tcp -m tcp --tcp-flags ACK,PSH PSH -j DROP
```

```
## Check for invalid packets and drop them ##
iptables -A Log-N-Drop -m state --state INVALID -j LOG --log-prefix "Denied Invalid Packet: " --log-level debug
```

```
## Check for and drop everything else that is not permitted ##
iptables -A Log-N-Drop -p TCP -m limit --limit 5/min -j LOG --log-prefix "Denied TCP: " --log-ip-options --log-tcp-options --log-level 7
iptables -A Log-N-Drop -p UDP -m limit --limit 5/min -j LOG --log-prefix "Denied UDP: " --log-level 7
iptables -A Log-N-Drop -p ICMP -m limit --limit 5/min -j LOG --log-prefix "Denied ICMP: " --log-level 7
```

```
iptables -A Log-N-Drop -j DROP
```

```
#####
```

```
##### INPUT CHAIN #####
```

```
#####
```

```
echo "[+] Setting up INPUT chain..."
```

```
## Accepts all connections from localhost (lo0) and drops traffic to 127/8 that does not use lo0
```

```
iptables -A INPUT -i lo -j ACCEPT
```

```
iptables -A INPUT -i ! lo -d 127.0.0.0/8 -j Log-N-Drop
```

```
## Accepts all previously established and related inbound connections
```

```
iptables -A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
```

```
## Allows local SSL webserver traffic to be accessed from KSU address space only
```

```
iptables -A INPUT -p TCP --dport 443 -s 129.130.0.0/255.255.0.0 -j ACCEPT
```

```
## Allows local webserver traffic to be accessed from KSU address space only
```

```
iptables -A INPUT -p TCP --dport 80 -s 129.130.0.0/255.255.0.0 -j ACCEPT
```

```
#iptables -A INPUT -p TCP --dport 80 -j ACCEPT
```

```
## Allows SSH to be accessible from any IP address
```

```
iptables -A INPUT -p TCP -m state --state NEW --dport 22 -j ACCEPT
```

```
## Allows pings
```

```
iptables -A INPUT -p icmp -m icmp --icmp-type 8 -j ACCEPT
```

```
## Drops all other incoming connections on TCP and UDP ports
```

```
iptables -A INPUT -p TCP --dport 1:65535 -j Log-N-Drop
```

```
iptables -A INPUT -p UDP --dport 1:65535 -j Log-N-Drop
```

```
iptables -A INPUT -p ICMP -j Log-N-Drop
```

```
#####
```

```
##### OUTPUT CHAIN #####
```

```
#####
```

```
# echo "[+] Setting up OUTPUT chain..."
```

```
iptables -A OUTPUT -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT
```

```
#####
```

```
##### FILTER CHAIN #####
```

```
#####
```

```
# echo "[+] Setting up FILTER chain..."
```