Iptables Essentials - Common Firewall Rules And Commands

5:18 PM | POST SPONSORED BY FARADAYSEC | MULTIUSER PENTEST ENVIRONMENT

ZION3R

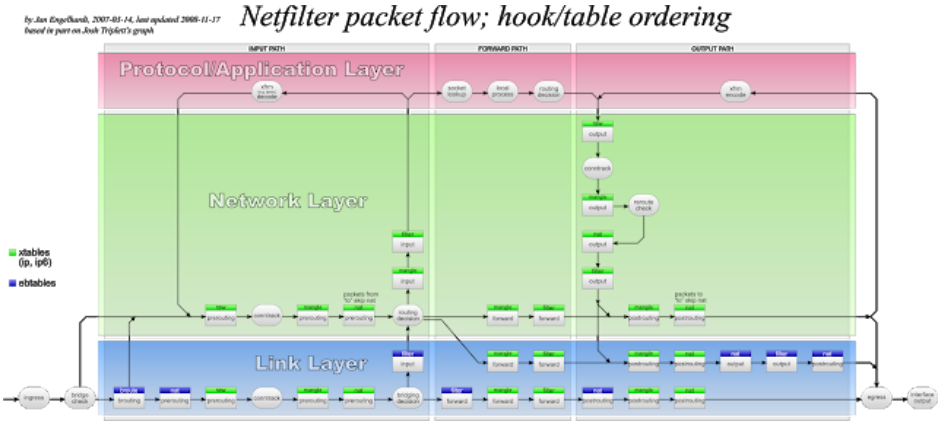
Tools to help you configure Iptables

Shorewall - advanced gateway/firewall configuration tool for GNU/Linux.
Firewalld - provides a dynamically managed firewall.
UFW - default firewall configuration tool for Ubuntu.
FireHOL - offer simple and powerful configuration for all Linux firewall and traffic shaping requirements.

Manuals/Howtos/Tutorials

Best practices: iptables - by Major Hayden
An In-Depth Guide to Iptables, the Linux Firewall
Advanced Features of netfilter/iptables
Linux Firewalls Using iptables
Debugging iptables and common firewall pitfalls?
Netfilter Hacking HOWTO
Per-IP rate limiting with iptables

How it works?



Iptables Rules

Saving Rules

Debian Based

```
netfilter-persistent save
```

RedHat Based

```
service iptables save
```

List out all of the active iptables rules with verbose

```
iptables -n -L -v
```

List out all of the active iptables rules with numeric lines and verbose

```
iptables -n -L -v --line-numbers
```

Print out all of the active iptables rules

```
iptables -S
```

List Rules as Tables for INPUT chain

```
iptables -L INPUT
```

Print all of the rule specifications in the INPUT chain

```
iptables -S INPUT
```

Show Packet Counts and Aggregate Size

```
iptables -L INPUT -v
```

To display INPUT or OUTPUT chain rules with numeric lines and verbose

```
iptables -L INPUT -n -v
iptables -L OUTPUT -n -v --line-numbers
```

Delete Rule by Chain and Number

```
iptables -D INPUT 10
```

Delete Rule by Specification

```
iptables -D INPUT -m conntrack --ctstate INVALID -j DROP
```

Flush All Rules, Delete All Chains, and Accept All

```
iptables -P INPUT ACCEPT
iptables -P FORWARD ACCEPT
iptables -P OUTPUT ACCEPT

iptables -t nat -F
iptables -t mangle -F
iptables -F
iptables -X
```

Flush All Chains

```
iptables -F
```

Flush a Single Chain

```
iptables -F INPUT
```

Insert Firewall Rules

In many past internal penetration tests I often had problems with the existing Powershell Recon / Exploitation scripts due to missing pr...

Wireshark Cheatsheet

Wireshark, whose old name is Ethereal; It is a program that can run in many operating systems such as Windows, Linux, MacOS or Solaris ...

FFM (Freedom Fighting Mode) - Open Source Hacking Harness

FFM is a hacking harness that you can use during the post-exploitation phase of a red-teaming engagement. The idea of the tool was deri...

Mimikatz v2.2.0 - A Post-Exploitation Tool to Extract Plaintexts Passwords, Hash, PIN Code from Memory

mimikatz is a tool I've made to learn C and make somes experiments with Windows security. It's now well known to extract plai...

Reconerator - C# Targeted Attack Reconnaissance Tools

This is a custom .NET assembly which will perform a number of situational awareness activities. There are a number of current featuresets...

```
iptables -I INPUT 2 -s 202.54.1.2 -j DROP
```

Allow Loopback Connections

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

Allow Established and Related Incoming Connections

```
iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
```

Allow Established Outgoing Connections

```
iptables -A OUTPUT -m conntrack --ctstate ESTABLISHED -j ACCEPT
```

Internal to External

```
iptables -A FORWARD -i eth1 -o eth0 -j ACCEPT
```

Drop Invalid Packets

```
iptables -A INPUT -m conntrack --ctstate INVALID -j DROP
```

Block an IP Address

```
iptables -A INPUT -s 192.168.252.10 -j DROP
```

Block and IP Address and Reject

```
iptables -A INPUT -s 192.168.252.10 -j REJECT
```

Block Connections to a Network Interface

```
iptables -A INPUT -i eth0 -s 192.168.252.10 -j DROP
```

Allow All Incoming SSH

```
iptables -A INPUT -p tcp --dport 22 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -p tcp --sport 22 -m conntrack --ctstate ESTABLISHED -j ACCEPT
```

Allow Incoming SSH from Specific IP address or subnet

```
iptables -A INPUT -p tcp -s 192.168.240.0/24 --dport 22 -m conntrack --ctstate NEW,E
iptables -A OUTPUT -p tcp --sport 22 -m conntrack --ctstate ESTABLISHED -j ACCEPT
```

Allow Outgoing SSH

```
iptables -A OUTPUT -p tcp --dport 22 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEP
iptables -A INPUT -p tcp --sport 22 -m conntrack --ctstate ESTABLISHED -j ACCEPT
```

Allow Incoming Rsync from Specific IP Address or Subnet

```
iptables -A INPUT -p tcp -s 192.168.240.0/24 --dport 873 -m conntrack --ctstate NEW,
iptables -A OUTPUT -p tcp --sport 873 -m conntrack --ctstate ESTABLISHED -j ACCEPT
```

Allow All Incoming HTTP

```
iptables -A INPUT -p tcp --dport 80 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -p tcp --sport 80 -m conntrack --ctstate ESTABLISHED -j ACCEPT
```

Allow All Incoming HTTPS

```
iptables -A INPUT -p tcp --dport 443 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -p tcp --sport 443 -m conntrack --ctstate ESTABLISHED -j ACCEPT
```

Allow All Incoming HTTP and HTTPS

```
iptables -A INPUT -p tcp -m multiport --dports 80,443 -m conntrack --ctstate NEW,EST
iptables -A OUTPUT -p tcp -m multiport --dports 80,443 -m conntrack --ctstate ESTABL
```

Allow MySQL from Specific IP Address or Subnet

```
iptables -A INPUT -p tcp -s 192.168.240.0/24 --dport 3306 -m conntrack --ctstate NEW
iptables -A OUTPUT -p tcp --sport 3306 -m conntrack --ctstate ESTABLISHED -j ACCEPT
```

Allow MySQL to Specific Network Interface

```
iptables -A INPUT -i eth1 -p tcp --dport 3306 -m conntrack --ctstate NEW,ESTABLISHED
iptables -A OUTPUT -o eth1 -p tcp --sport 3306 -m conntrack --ctstate ESTABLISHED -j
```

PostgreSQL from Specific IP Address or Subnet

```
iptables -A INPUT -p tcp -s 192.168.240.0/24 --dport 5432 -m conntrack --ctstate NEW
iptables -A OUTPUT -p tcp --sport 5432 -m conntrack --ctstate ESTABLISHED -j ACCEPT
```

Allow PostgreSQL to Specific Network Interface

```
iptables -A INPUT -i eth1 -p tcp --dport 5432 -m conntrack --ctstate NEW,ESTABLISHED
iptables -A OUTPUT -o eth1 -p tcp --sport 5432 -m conntrack --ctstate ESTABLISHED -j
```

Block Outgoing SMTP Mail

```
iptables -A OUTPUT -p tcp --dport 25 -j REJECT
```

Allow All Incoming SMTP

```
iptables -A INPUT -p tcp --dport 25 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -p tcp --sport 25 -m conntrack --ctstate ESTABLISHED -j ACCEPT
```

Allow All Incoming IMAP

```
iptables -A INPUT -p tcp --dport 143 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -p tcp --sport 143 -m conntrack --ctstate ESTABLISHED -j ACCEPT
```

Allow All Incoming IMAPS

```
iptables -A INPUT -p tcp --dport 993 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -p tcp --sport 993 -m conntrack --ctstate ESTABLISHED -j ACCEPT
```

Allow All Incoming POP3

```
iptables -A INPUT -p tcp --dport 110 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -p tcp --sport 110 -m conntrack --ctstate ESTABLISHED -j ACCEPT
```

Allow All Incoming POP3S

```
iptables -A INPUT -p tcp --dport 995 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEP
iptables -A OUTPUT -p tcp --sport 995 -m conntrack --ctstate ESTABLISHED -j ACCEPT
```

Drop Private Network Address On Public Interface

```
iptables -A INPUT -i eth1 -s 192.168.0.0/24 -j DROP
iptables -A INPUT -i eth1 -s 10.0.0.0/8 -j DROP
```

Drop All Outgoing to Facebook Networks

Get Facebook AS:

```
whois -h v4.whois.cymru.com " -v $(host facebook.com | grep "has address" | cut -d "
```

Drop:

```
for i in $(whois -h whois.radb.net -- '-i origin AS32934' | grep "^route:" | cut -d '

  iptables -A OUTPUT -s "$i" -j REJECT

done
```

Log and Drop Packets

```
iptables -A INPUT -i eth1 -s 10.0.0.0/8 -j LOG --log-prefix "IP_SPOOF A: "
iptables -A INPUT -i eth1 -s 10.0.0.0/8 -j DROP
```

By default everything is logged to `/var/log/messages` file:

```
tail -f /var/log/messages
grep --color 'IP SPOOF' /var/log/messages
```

Log and Drop Packets with Limited Number of Log Entries

```
iptables -A INPUT -i eth1 -s 10.0.0.0/8 -m limit --limit 5/m --limit-burst 7 -j LOG
iptables -A INPUT -i eth1 -s 10.0.0.0/8 -j DROP
```

Drop or Accept Traffic From Mac Address

```
iptables -A INPUT -m mac --mac-source 00:0F:EA:91:04:08 -j DROP
iptables -A INPUT -p tcp --destination-port 22 -m mac --mac-source 00:0F:EA:91:04:07
```

Block or Allow ICMP Ping Request

```
iptables -A INPUT -p icmp --icmp-type echo-request -j DROP
iptables -A INPUT -i eth1 -p icmp --icmp-type echo-request -j DROP
```

Specifying Multiple Ports with `multiport`

```
iptables -A INPUT -i eth0 -p tcp -m state --state NEW -m multiport --dports ssh,smtp
```

Load Balancing with `random*` or `nth*`

```
_ips=("172.31.250.10" "172.31.250.11" "172.31.250.12" "172.31.250.13")

for ip in "${_ips[@]}" ; do
  iptables -A PREROUTING -i eth0 -p tcp --dport 80 -m state --state NEW -m nth --cou
    -j DNAT --to-destination ${ip}:80
done
```

or

```
_ips=("172.31.250.10" "172.31.250.11" "172.31.250.12" "172.31.250.13")

for ip in "${_ips[@]}" ; do
  iptables -A PREROUTING -i eth0 -p tcp --dport 80 -m state --state NEW -m random --
    -j DNAT --to-destination ${ip}:80
done
```

Restricting the Number of Connections with `limit` and `iplimit*`

```
iptables -A FORWARD -m state --state NEW -p tcp -m multiport --dport http,https -o e
    -m limit --limit 20/hour --limit-burst 5 -j ACCEPT
```

or

```
iptables -A INPUT -p tcp -m state --state NEW --dport http -m iplimit --iplimit-above
```

Maintaining a List of recent Connections to Match Against

```
iptables -A FORWARD -m recent --name portscan --rcheck --seconds 100 -j DROP
iptables -A FORWARD -p tcp -i eth0 --dport 443 -m recent --name portscan --set -j DR
```

Matching Against a `string*` in a Packet's Data Payload

```
iptables -A FORWARD -m string --string '.com' -j DROP
iptables -A FORWARD -m string --string '.exe' -j DROP
```

Time-based Rules with `time*`

```
iptables -A FORWARD -p tcp -m multiport --dport http,https -o eth0 -i eth1 \
    -m time --timestart 21:30 --timestop 22:30 --days Mon,Tue,Wed,Thu,Fri -j ACCEPT
```

Packet Matching Based on TTL Values

```
iptables -A INPUT -s 1.2.3.4 -m ttl --ttl-lt 40 -j REJECT
```

Protection against port scanning

```
iptables -N port-scanning
iptables -A port-scanning -p tcp --tcp-flags SYN,ACK,FIN,RST RST -m limit --limit 1/
iptables -A port-scanning -j DROP
```

SSH brute-force protection

```
iptables -A INPUT -p tcp --dport ssh -m conntrack --ctstate NEW -m recent --set
iptables -A INPUT -p tcp --dport ssh -m conntrack --ctstate NEW -m recent --update -
```

Syn-flood protection

```
iptables -N syn_flood

iptables -A INPUT -p tcp --syn -j syn_flood
iptables -A syn_flood -m limit --limit 1/s --limit-burst 3 -j RETURN
iptables -A syn_flood -j DROP

iptables -A INPUT -p icmp -m limit --limit  1/s --limit-burst 1 -j ACCEPT

iptables -A INPUT -p icmp -m limit --limit 1/s --limit-burst 1 -j LOG --log-prefix P
iptables -A INPUT -p icmp -j DROP

iptables -A OUTPUT -p icmp -j ACCEPT
```

Mitigating SYN Floods With SYNPROXY

```
iptables -t raw -A PREROUTING -p tcp -m tcp --syn -j CT --notrack
iptables -A INPUT -p tcp -m tcp -m conntrack --ctstate INVALID,UNTRACKED -j SYNPROXY
iptables -A INPUT -m conntrack --ctstate INVALID -j DROP
```

Block New Packets That Are Not SYN

```
iptables -A INPUT -p tcp ! --syn -m state --state NEW -j DROP
```

or

```
iptables -t mangle -A PREROUTING -p tcp ! --syn -m conntrack --ctstate NEW -j DROP
```

Force Fragments packets check

```
iptables -A INPUT -f -j DROP
```

XMAS packets

```
iptables -A INPUT -p tcp --tcp-flags ALL ALL -j DROP
```

Drop all NULL packets

```
iptables -A INPUT -p tcp --tcp-flags ALL NONE -j DROP
```

Block Uncommon MSS Values

```
iptables -t mangle -A PREROUTING -p tcp -m conntrack --ctstate NEW -m tcpmss ! --mss
```

Block Packets With Bogus TCP Flags

```
iptables -t mangle -A PREROUTING -p tcp --tcp-flags FIN,SYN,RST,PSH,ACK,URG NONE -j
iptables -t mangle -A PREROUTING -p tcp --tcp-flags FIN,SYN FIN,SYN -j DROP
iptables -t mangle -A PREROUTING -p tcp --tcp-flags SYN,RST SYN,RST -j DROP
iptables -t mangle -A PREROUTING -p tcp --tcp-flags FIN,RST FIN,RST -j DROP
iptables -t mangle -A PREROUTING -p tcp --tcp-flags FIN,ACK FIN -j DROP
iptables -t mangle -A PREROUTING -p tcp --tcp-flags ACK,URG URG -j DROP
iptables -t mangle -A PREROUTING -p tcp --tcp-flags ACK,FIN FIN -j DROP
iptables -t mangle -A PREROUTING -p tcp --tcp-flags ACK,PSH PSH -j DROP
iptables -t mangle -A PREROUTING -p tcp --tcp-flags ALL ALL -j DROP
iptables -t mangle -A PREROUTING -p tcp --tcp-flags ALL NONE -j DROP
iptables -t mangle -A PREROUTING -p tcp --tcp-flags ALL FIN,PSH,URG -j DROP
iptables -t mangle -A PREROUTING -p tcp --tcp-flags ALL SYN,FIN,PSH,URG -j DROP
iptables -t mangle -A PREROUTING -p tcp --tcp-flags ALL SYN,RST,ACK,FIN,URG -j DROP
```

Block Packets From Private Subnets (Spoofing)

```
_subnets=("224.0.0.0/3" "169.254.0.0/16" "172.16.0.0/12" "192.0.2.0/24" "192.168.0.0

for _sub in "${_subnets[@]}" ; do
  iptables -t mangle -A PREROUTING -s "$_sub" -j DROP
done
iptables -t mangle -A PREROUTING -s 127.0.0.0/8 ! -i lo -j DROP
```

Iptables Essentials

TAGS

FIREWALL X FIREWALL CONFIGURATION X FIREWALL RULES X FIREWALLS X IPTABLES X IPTABLES CONFIGURATIONS X IPTABLES ESSENTIALS X IPTABLES FIREWALL X IPTABLES RULES X LINUX X MAC

Wireshark Cheatsheet

WPScan v3.4.5 - Black Box WordPress Vulnerability Scanner

Androwarn - Yet Another Static Code Analyzer For Malicious Android Applications

PREVIOUS
HexRaysCodeXplorer - Hex-Rays Decompiler Plugin For Better Code Navigation

NEXT
Reko - A General Purpose Binary Decompiler

0 Comments Sort by **Oldest**

Add a comment...

Facebook Comments Plugin

BLOG ARCHIVE

Blog Archive

SOCIAL

Your Email

Subscribe to our Newsletter

BY FEEDBURNER

RECOMMENDED

1. Dreamhost: Best WordPress Hosting
2. SSD cloud server on DigitalOcean
3. HackIsOn
4. Exploit Collector
5. BlackPloit
6. Hacking Reviews
7. Hacking Land
8. Daily Picture

CONTACT FORM

Name

Email *

Message *

Send

BACK TO TOP