

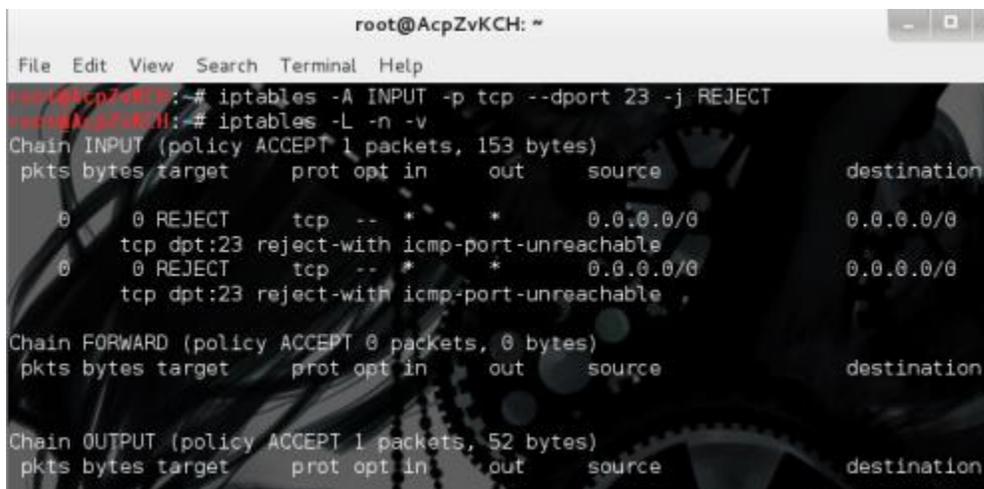
Iptables is a kernel based utility to set up access control based on protocols, services, ports or the actual interface. You will use Zenmap to test the iptables are operational.

Step 1 – Root Terminal – To reject Telnet incoming connections

iptables -A INPUT -p tcp --dport 23 -j REJECT

iptables -L -n -v

****Your rules will be displayed**

A terminal window titled 'root@AcpZvKCH: ~' showing the execution of iptables commands. The first command is 'iptables -A INPUT -p tcp --dport 23 -j REJECT' and the second is 'iptables -L -n -v'. The output shows the configuration of the INPUT, FORWARD, and OUTPUT chains. The INPUT chain has two rules: one for rejecting all TCP traffic from 0.0.0.0/0, and another for rejecting TCP traffic on port 23 with an ICMP unreachable message.

```
root@AcpZvKCH: ~
File Edit View Search Terminal Help
root@AcpZvKCH:~# iptables -A INPUT -p tcp --dport 23 -j REJECT
root@AcpZvKCH:~# iptables -L -n -v
Chain INPUT (policy ACCEPT 1 packets, 153 bytes)
 pkts bytes target    prot opt in     out   source            destination
    0     0 REJECT    tcp  --  *     *     0.0.0.0/0         0.0.0.0/0
    0     0 REJECT    tcp  --  *     *     0.0.0.0/0         0.0.0.0/0
    tcp dpt:23 reject-with icmp-port-unreachable
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out   source            destination
Chain OUTPUT (policy ACCEPT 1 packets, 52 bytes)
 pkts bytes target    prot opt in     out   source            destination
```

How to DROP Telnet instead of REJECT

iptables -A INPUT -p tcp --dport 23 -j DROP

iptables -L -n -v

iptables -v -L INPUT

```
Chain OUTPUT (policy ACCEPT 7591 packets, 1579K bytes)
 pkts bytes target    prot opt in     out     source         destination
root@kali:~# iptables -A INPUT -p tcp --dport 23 -j DROP
root@kali:~# iptables -L -n -v
Chain INPUT (policy ACCEPT 10 packets, 2939 bytes)
 pkts bytes target    prot opt in     out     source         destination
    0     0 REJECT    tcp  --  *      *      0.0.0.0/0      0.0.0.0/0
    0     0 REJECT    tcp  --  *      *      0.0.0.0/0      0.0.0.0/0
    0     0 REJECT    tcp  --  *      *      0.0.0.0/0      0.0.0.0/0
    0     0 DROP     tcp  --  *      *      0.0.0.0/0      0.0.0.0/0
    0     0          tcp  --  *      *      0.0.0.0/0      0.0.0.0/0
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source         destination
```

Step 2 – To stop TELNET outbound connections

iptables -A OUTPUT -p tcp --sport 23 -j DROP

iptables -L -n -v

iptables -v -L OUTPUT

```
root@kali:~# iptables -A OUTPUT -p tcp --sport 23 -j DROP
root@kali:~# iptables -L -n -v
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source         destination
    0     0 DROP     tcp  --  *      *      0.0.0.0/0      0.0.0.0/0
    0     0          tcp  --  *      *      0.0.0.0/0      0.0.0.0/0
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source         destination
Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target    prot opt in     out     source         destination
    0     0 DROP     tcp  --  *      *      0.0.0.0/0      0.0.0.0/0
    0     0          tcp  --  *      *      0.0.0.0/0      0.0.0.0/0
root@kali:~#
```

DROP vs REJECT

The REJECT target will send a reply icmp packet to the source system telling that system that the packet has been rejected. By default the message will be “port is unreachable”.

The DROP target simply drops the packet without sending any reply packets back.

The REJECT target is vulnerable to DoS attacks.

```
Chain OUTPUT (policy ACCEPT 7591 packets, 1579K bytes)
pkts bytes target      prot opt in      out     source      destination
root@kali:~# iptables -A INPUT -p tcp --dport 23 -j DROP
root@kali:~# iptables -L -n -v
Chain INPUT (policy ACCEPT 10 packets, 2939 bytes)
pkts bytes target      prot opt in      out     source      destination
 0      0 REJECT      tcp  --  *      *      0.0.0.0/0    0.0.0.0/0
    tcp dpt:23 reject-with icmp-port-unreachable
 0      0 REJECT      tcp  --  *      *      0.0.0.0/0    0.0.0.0/0
    tcp dpt:23 reject-with icmp-port-unreachable
 0      0 DROP       tcp  --  *      *      0.0.0.0/0    0.0.0.0/0
    tcp dpt:23
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target      prot opt in      out     source      destination
```

Step 3 – Want to see Line numbers on the rules?

iptables -L -v -n --line-number

```
root@kali:~# iptables -L -v -n --line-number
Chain INPUT (policy ACCEPT 2145 packets, 1111K bytes)
num  pkts bytes target      prot opt in      out     source      destination
 1      0      0 REJECT      tcp  --  *      *      0.0.0.0/0    0.0.0.0/0
    /0      tcp dpt:23 reject-with icmp-port-unreachable
 2      0      0 REJECT      tcp  --  *      *      0.0.0.0/0    0.0.0.0/0
    /0      tcp dpt:23 reject-with icmp-port-unreachable
 3      0      0 DROP       tcp  --  *      *      0.0.0.0/0    0.0.0.0/0
    /0      tcp dpt:23
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
num  pkts bytes target      prot opt in      out     source      destination
```

Step 4 – Made a mistake and need to delete a rule?

List by line numbers – then delete the rule by it's line number

iptables -D INPUT 2

-D = Delete

INPUT rule 2

```
root@kali:~# iptables -D INPUT 2
root@kali:~# iptables -L -v -n --line-number
Chain INPUT (policy ACCEPT 9 packets, 982 bytes)
num  pkts bytes target    prot opt in     out     source         destination
 1     0     0 REJECT    tcp  --  *     *     0.0.0.0/0      0.0.0.0/0
    tcp opt:23 reject-with icmp-port-unreachable
 2     0     0 DROP     tcp  --  *     *     0.0.0.0/0      0.0.0.0/0
    tcp opt:23
```

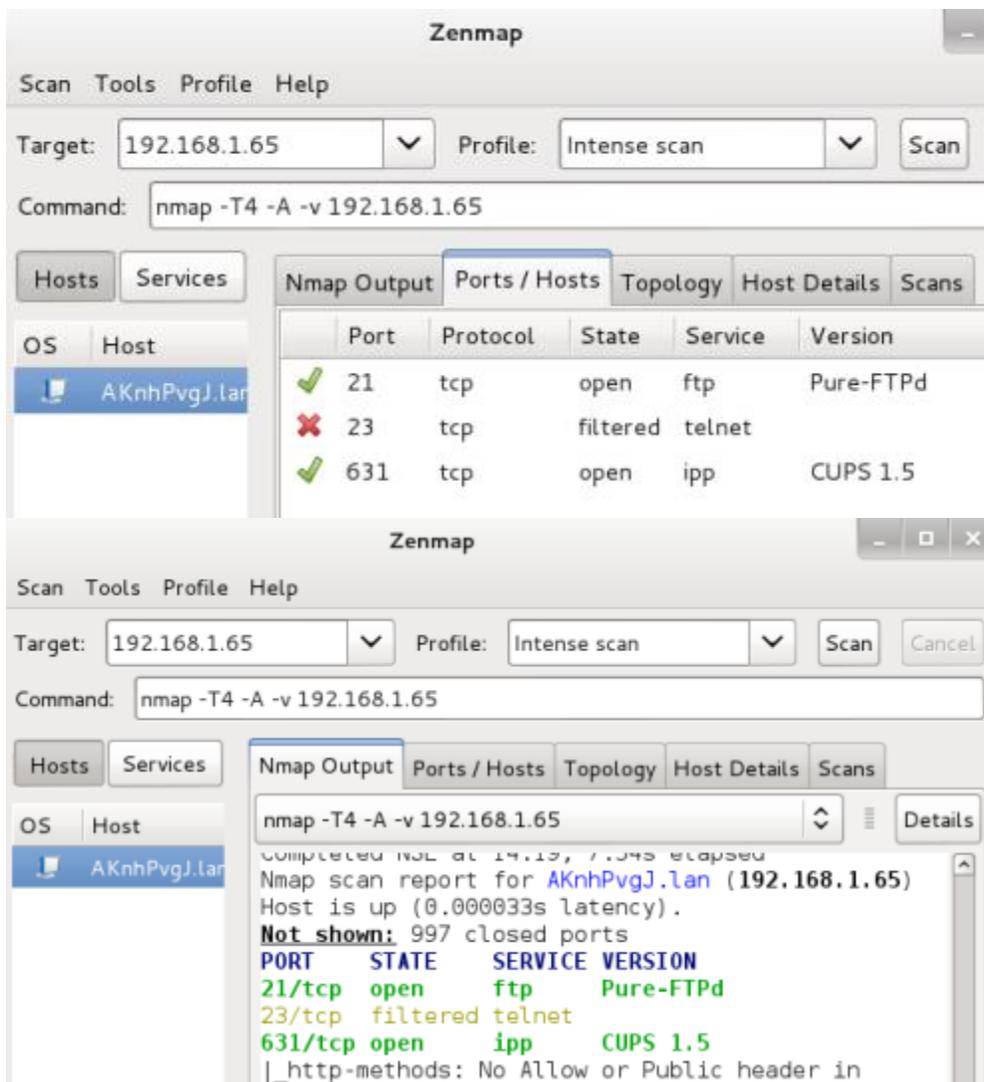
The rules are temporary... so after a reboot they'll be cleared

Step 5 – Test the rules with ZENMAP

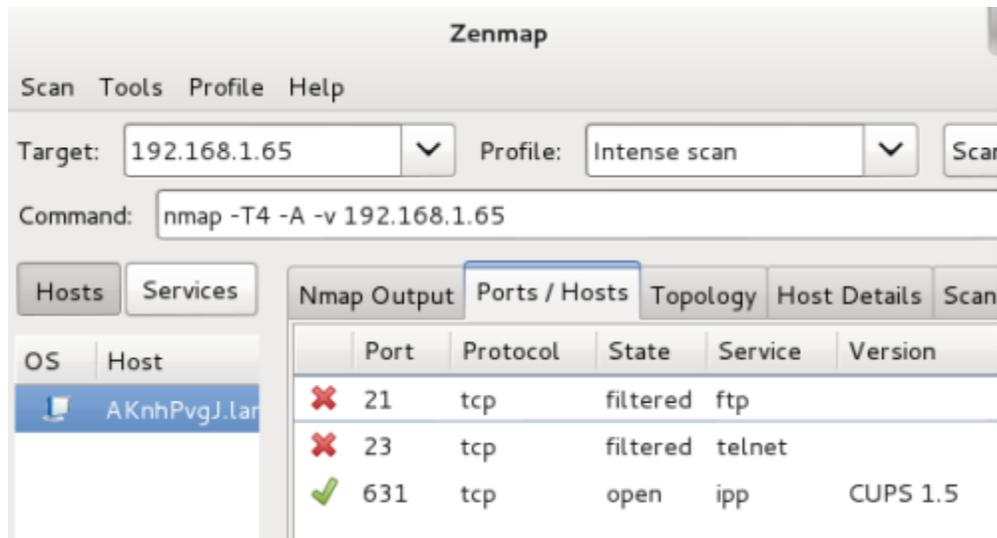
**Applications > Kali > Vulnerability > Misc Scanners <
Zenmap**

Type the IP address of your machine into Target > Scan

The iptables blocking telnet gave these results when tested:



When both FTP and Telnet are blocked, Zenmap results were:



That's it. You've blocked Telnet incoming and outgoing, and doublechecked your work using Zenmap. Easy right?

So what is Iptables?

Iptables is a user space utility

Designed to configure the 3 network layer kernel filtering chains

INPUT, OUTPUT, FORWARD

-i = Incoming interface (INPUT and FORWARD Chains)

-o = Outgoing interface

-A = Append or Add to a chain

-P = Default policy eg deny all or allow all