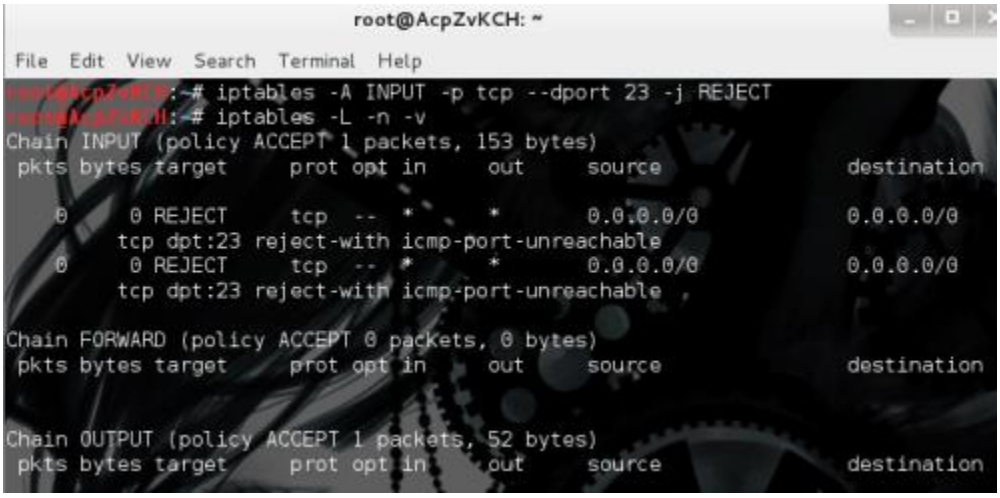
Iptables is a kernel based utility to set up access control based on protocols, services, ports or the actual interface. You will use Zenmap to test the iptables are operational.

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**



******

How to DROP Telnet instead of REJECT

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

*****

iptables -L -n -v

iptables -v -L INPUT

****

Step 2 – To stop TELNET outbound connections

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

iptables -L -n -v

iptables -v -L OUTPUT

DROP vs REJECT

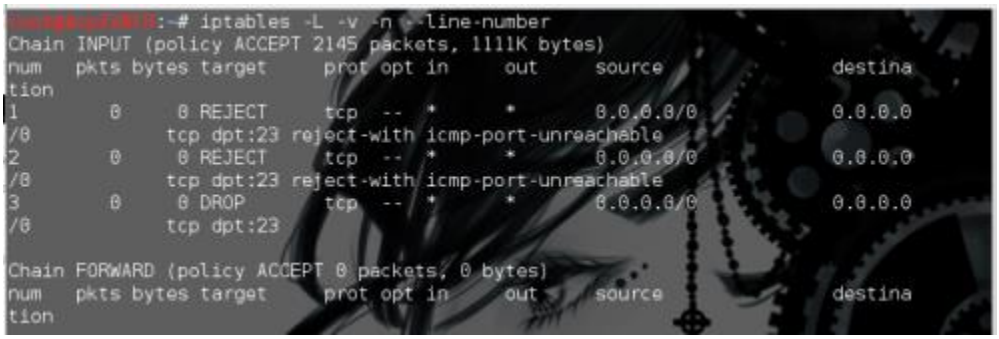
The REJECT target will send a reply icmp packet to the source system telling that system that the packet has been rejected. By default the message will be “port is unreachable”.

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

The REJECT target is vulnerable to DoS attacks.

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

iptables -L -v -n –line-number



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

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

******

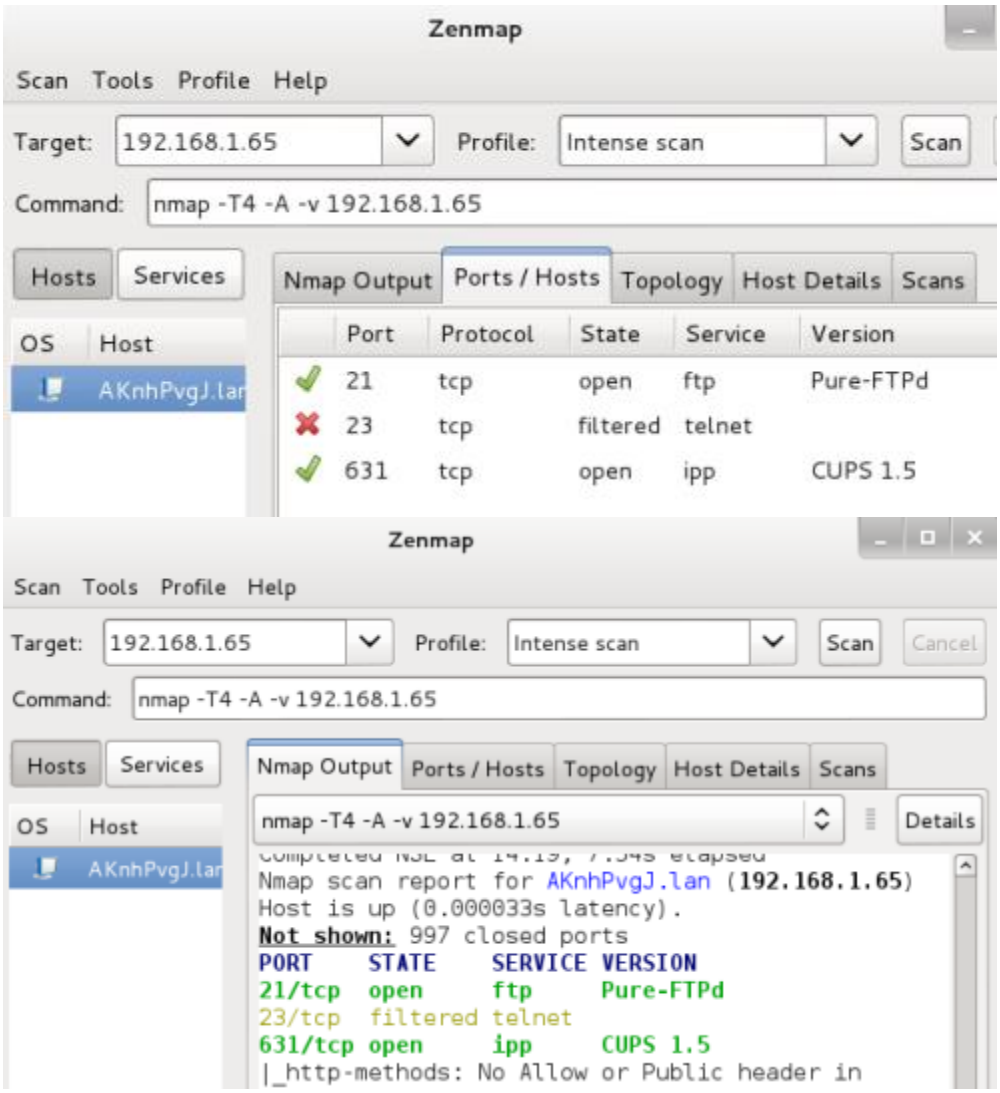
Step 5 – Test the rules with ZENMAP

Applications > Kali > Vulnerability > Misc Scanners < Zenmap

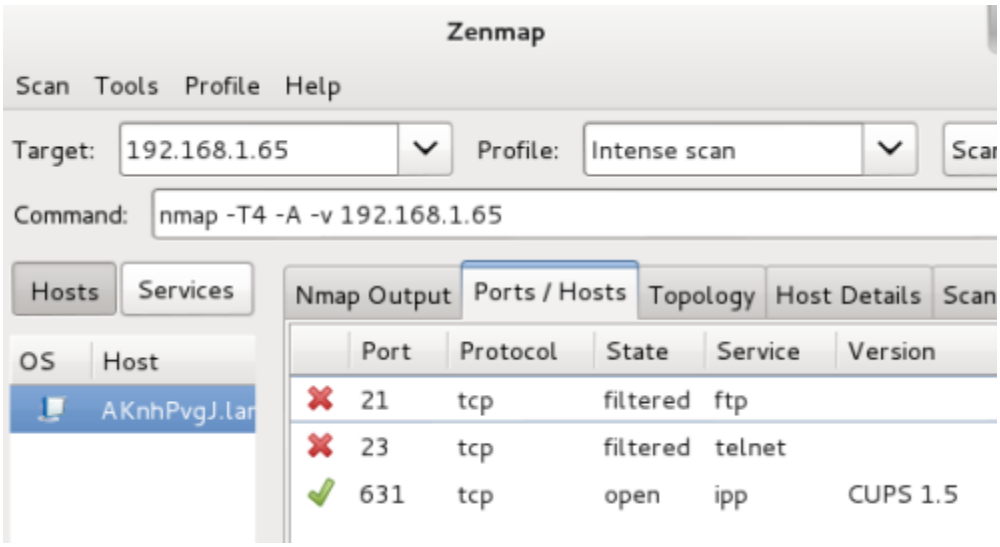
Type the IP address of your machine into Target > Scan

****

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