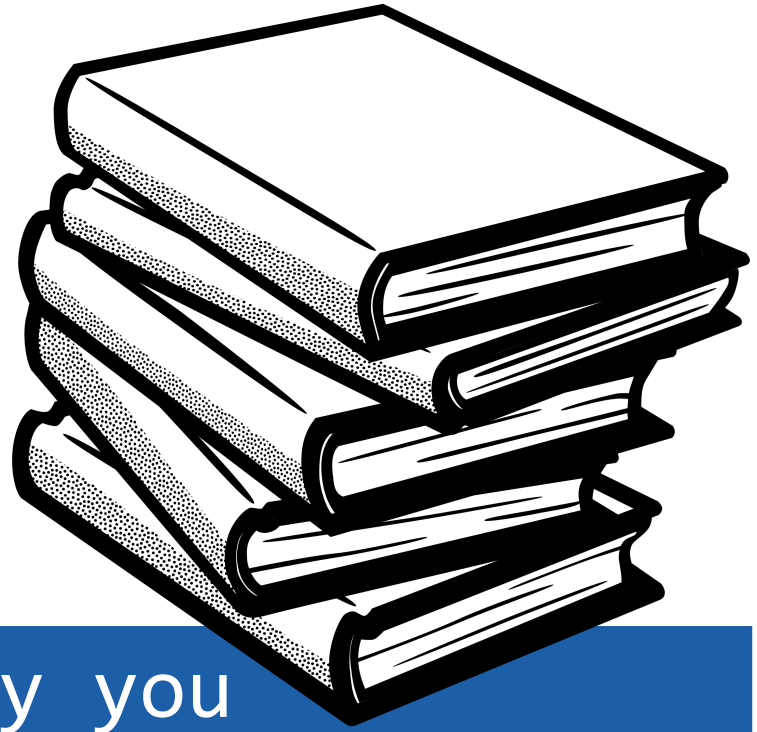
O'REILLY



Why you should not follow textbook examples

A TEXTBOOK ABOUT HOW NOT TO FOLLOW TEXTBOOK EXAMPLES

Gary Steers

DISCLAIMER

- I am not the copyright holder of the original text
- I will not disclose any networks that were found to be ‘vulnerable’
- All instances have been ethically reported and subsequently fixed

Task: Re-Invent the wheel for a new install

- While designing a network for a platform deployment I decided to use the grey matter and not copy and paste boilerplate configs

- I decided to follow the well known ‘RTFM’ method
  (not to be confused with RFC2721)

- Picked an O’REILLEY book for the majority of the reading
  “O’REILLY® - Juniper MX Series”

- This was not for an MX Series device, but All JunOS is equal right?....
  (different talk for a different time)

Chapter 4: Routing Engine Protection and DDoS

- I need to write a firewall to protect the device from the bad guys
- New platform and new feature sets
- Need to validate firewall config will protect the system and still allow operation of new features
- Be a good internet citizen and respond correctly to diagnostic packets *(ICMP/Tracerotue/PMTU etc etc)*

Chapter 4: Routing Engine Protection and DDoS

plex problems have common solutions that have been well tested.

IPv4 RE Protection Filter

This section provides the reader with a current best practice example of an RE protection filter for IPv4 traffic. Protection filters are applied in the input direction to filter traffic arriving on PFE or management ports before it's processed by the RE. Output filters are generally used for CoS marking of locally generated control plane traffic, as opposed to security-related reasons, as you generally trust your own routers and the traffic they originate. Figure 4-1 provides the topology details that surround this case study.

- This is a GREAT place to start right?

Allowing Traceroute...

```
filter accept-traceroute {
    apply-flags omit;
    term accept-traceroute-udp {
        from {
            destination-prefix-list {
                router-ipv4;
                router-ipv4-logical-systems  ;
            }
            protocol udp;
            ttl 1;
            destination-port 33435-33450;
        }
        then {
            policer management-1m;
            count accept-traceroute-udp;
            accept;
        }
    }
    term accept-traceroute-icmp {
        from {
            destination-prefix-list {
                router-ipv4;
                router-ipv4-logical-systems  ;
            }
            protocol icmp;
            ttl 1;
            icmp-type [ echo-request timestamp time-exceeded ];
        }
        then {
            policer management-1m;
            count accept-traceroute-icmp;
            accept;
        }
    }
```

```
    term accept-traceroute-tcp {
        from {
            destination-prefix-list {
                router-ipv4;
                router-ipv4-logical-systems  ;
            }
            protocol tcp;
            ttl 1;
        }
        then {
            policer management-1m;
            count accept-traceroute-tcp;
            accept;
        }
    }
}
```

Looks Good!...

WAIT...

WHAT ON EARTH IS THAT?????

Allowing Traceroute...

Did you spot the problem?

Allowing Traceroute...

```
term accept-traceroute-tcp {
    from {
        destination-prefix-list {
            router-ipv4;
            router-ipv4-logical-systems  ;
        }
        protocol tcp;
        ttl 1;
    }
    then {
        policer management-1m;
        count accept-traceroute-tcp;
        accept;
    }
}
```

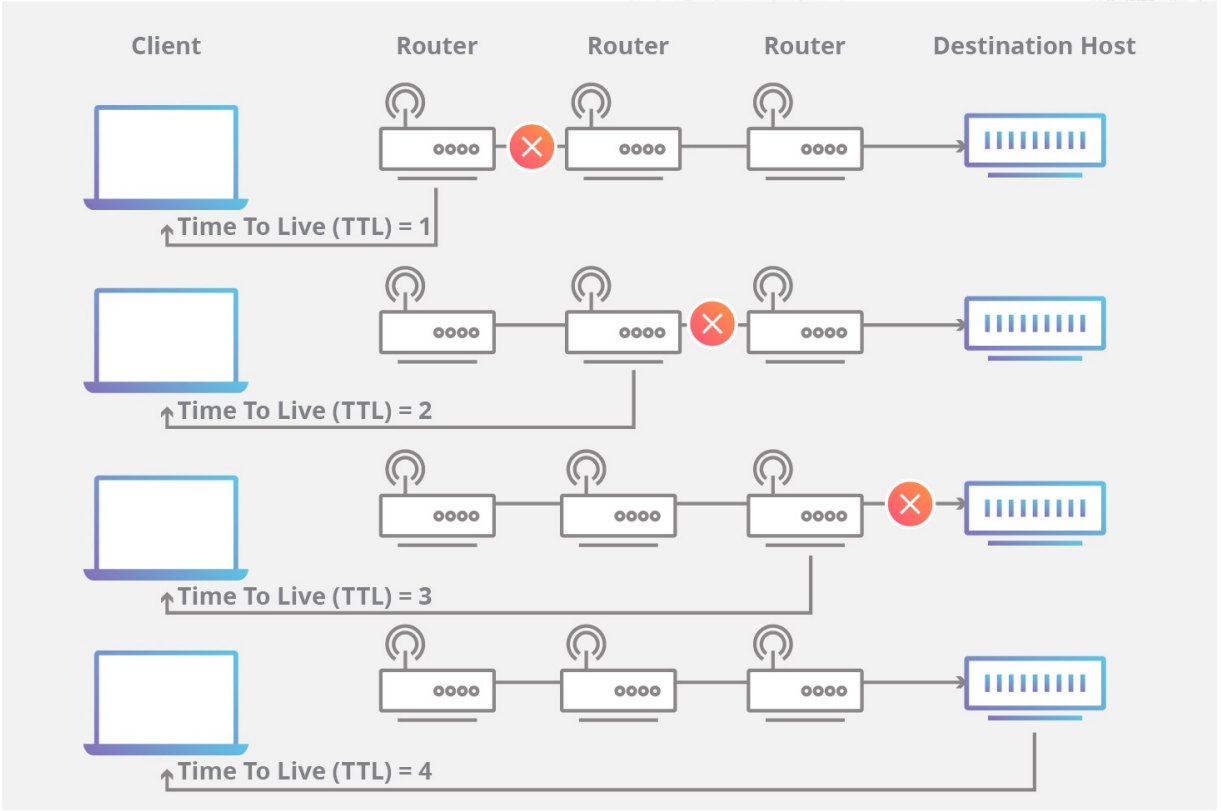
- Where Destination is one of routers IP's
- Where the Protocol is TCP
- Where TTL == 1
- ACCEPT == Let the packet through the firewall so that the kernel can respond with the appropriate response...

That's all fine right?

What is TTL?

WIKIPEDIA
The Free Encyclopedia

Time to live (**TTL**) or **hop limit** is a mechanism that limits the lifespan or lifetime of data in a computer or network.

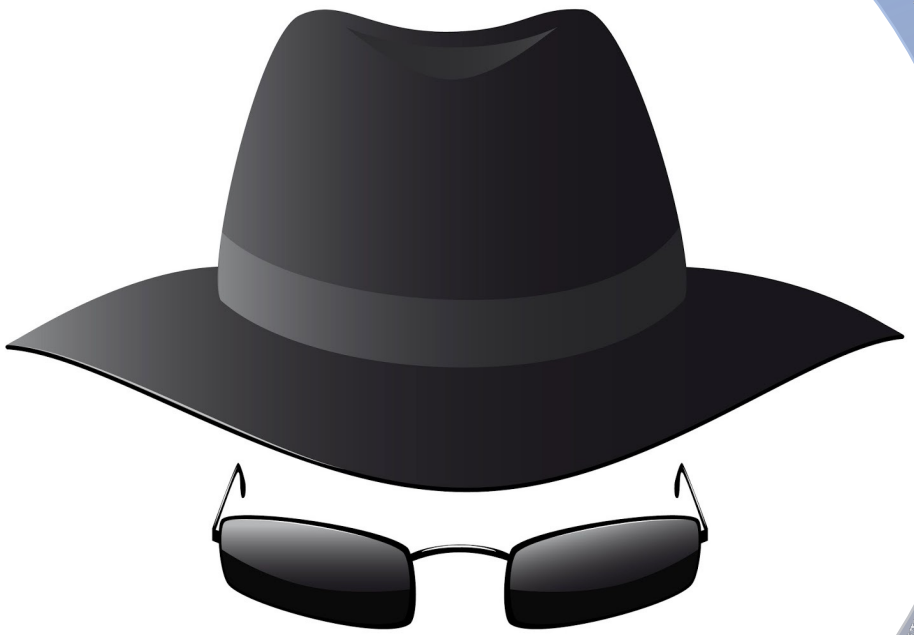


What's the relevance?

```
term accept-traceroute-tcp {
    from {
        destination-prefix-list {
            router-ipv4;
            router-ipv4-logical-systems  ;
        }
        protocol tcp;
        ttl 1;
    }
    then {
        policer management-1m;
        count accept-traceroute-tcp;
        accept;
    }
}
```

- Where Destination is one of routers IP's
- Where the Protocol is TCP
- Where TTL == 1
- ACCEPT == Let the packet through the firewall so that the kernel can respond with the appropriate response...

ANY TCP PACKET WITH TTL == 1 gets through the firewall



DANGER!!!

The internet is **FULL** of bad guys

What's the relevance?

ANY TCP PACKET WITH TTL == 1 gets through the firewall

Q: How do you manage a router?

- Telnet?
- SSH?
- Some AaaS*

- **ALL OF THESE USE TCP**

*Automation As A Service TM pending

IT'S OK, NO ONE FOLLOWS TEXTBOOKS

OR DO THEY?

- Junipers are common on the internet
- Some ISPs have previously referenced this book for their firewall config
- Juniper even recommend this book as good reference material
- It's co-authored by people at Juniper!
- But it's just an example right!

DISCLAIMER

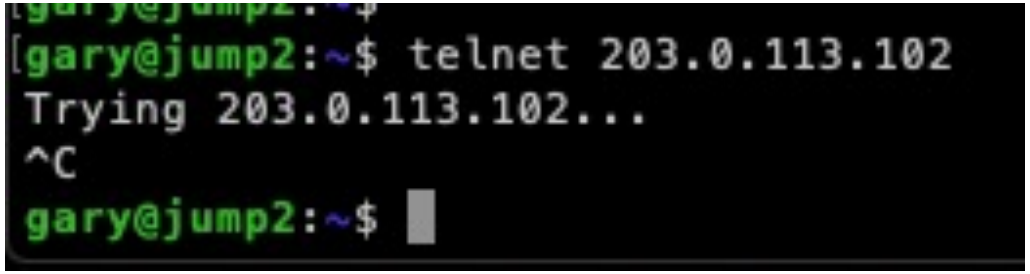
- I will not disclose any networks that were found to be ‘vulnerable’
- All instances have been ethically reported and subsequently fixed
- **Don’t try this at home**

(at least without permission from the owner)

Let’s try this out

- Use a device that would not normally have access to the host

- Verify it can’t access the host



Let’s try this out

- Work out distance
- Access the host

```
gary@jump2:~$ traceroute 203.0.113.102
traceroute to 203.0.113.102 (203.0.113.102), 30 hops max, 60 byte packets
 1  router2-lon.somevpsprovider.example.net (192.0.2.230)  2.968 ms  2.955 ms  2.981 ms
 2  192.0.2.4  0.419 ms  0.372 ms  0.376 ms
 3  203.0.113.102 (199.245.16.69)  2.294 ms  0.347 ms  2.322 ms
```

```
gary@jump2:~$ # Some IPTABLES Command.....
```

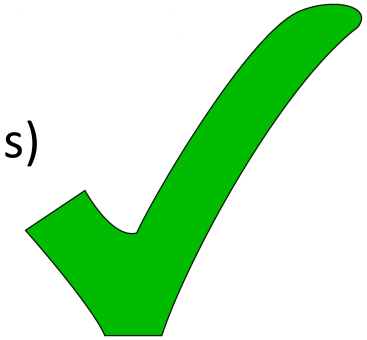
```
gary@jump2:~$ telnet 203.0.113.102
Trying 203.0.113.102...
Connnected to 203.0.113.102.
Escape character is '^]'.
**************************************************************************
*                                                                        *
* This system is for the use of authorized users only.  Usage of         *
* this system may be monitored and recorded by system personnel.         *
*                                                                        *
* Anyone using this system expressly consents to such monitoring         *
* and is advised that if such monitoring reveals possible                *
* evidence of criminal activity, system personnel may provide the        *
* evidence from such monitoring to law enforcement officials.            *
*                                                                        *
**************************************************************************

somerouter.someotherisp.example.net-re0 (ttyp0)

login:
telner> quit
Connection closed.
```

What next?

- Report to the affected network(s)



- Report to the vendor and the publisher

Questions?