IPv6

Does size matter?

- "Information systems security" MS degree
- security analyst

Agenda

001. IPv6 Intro

010. Types of IPv6

011. IPv6 at your own environment

100. Network Reconnaissance

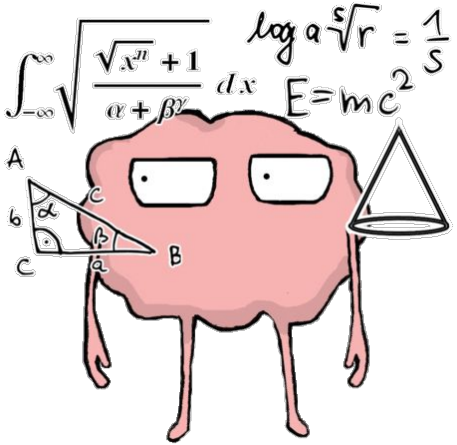
internet communication

IPv6

IPv4

2001:fdb8:1f70:9999:ade8:7648:3a49:16e8

(128-bit addressing scheme)



198.51.100.1

(32-bit addressing scheme)

IPv6 Shortening

1) 2001:0000:0db8:0001:0000:0000:0000:0020
   2001:0000:0db8:0001::0020

2) 2001:0000:0db8:0001::0020
   2001:0:0db8:0001::0020

3) 2001:0:0db8:0001::0020
   2001:0:db8:1::20

expanded addressing capacity

Address Types and Scope

Global Unicast Address --Scope Internet- Routed on Internet

Unique Local -- Scope Internal Network or VPN -Internally routable but Not routed on Internet

Link Local - Scope network link- Not Routed internally or externally.

IPv4

```
10.0.0.0/8
172.16.0.0/12
192.168.0.0/16
169.254.0.0/16
```

A. Link Local

B. Unique Local

IPv6

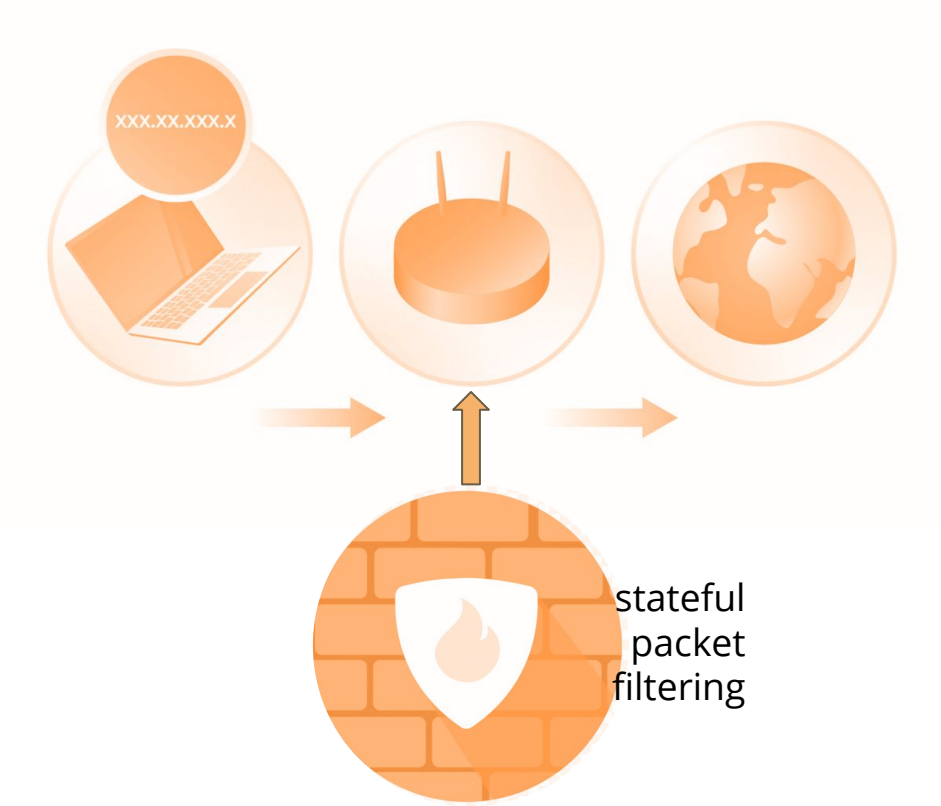
IPv6 Link-Local

- Not routed at all
- Self-assigned
- fe80::/64

IPv6 Unique Local

- Not routed on the Internet
- fc00::/7 - fdff::/7

Won’t my network be less secure without NAT ???



IPv6 for personal use

www.worldipv6launch.org

HURRICANE ELECTRIC
INTERNET SERVICES

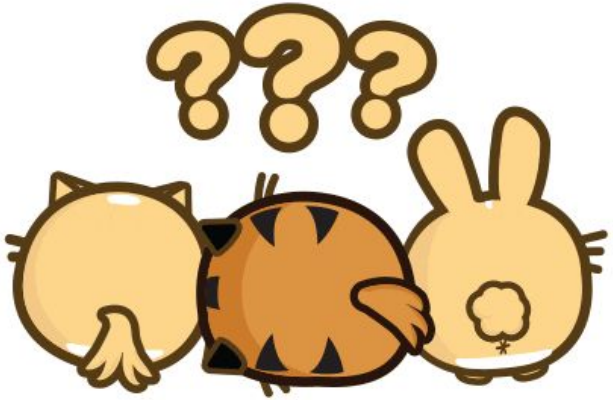
www.tunnelbroker.net

/64

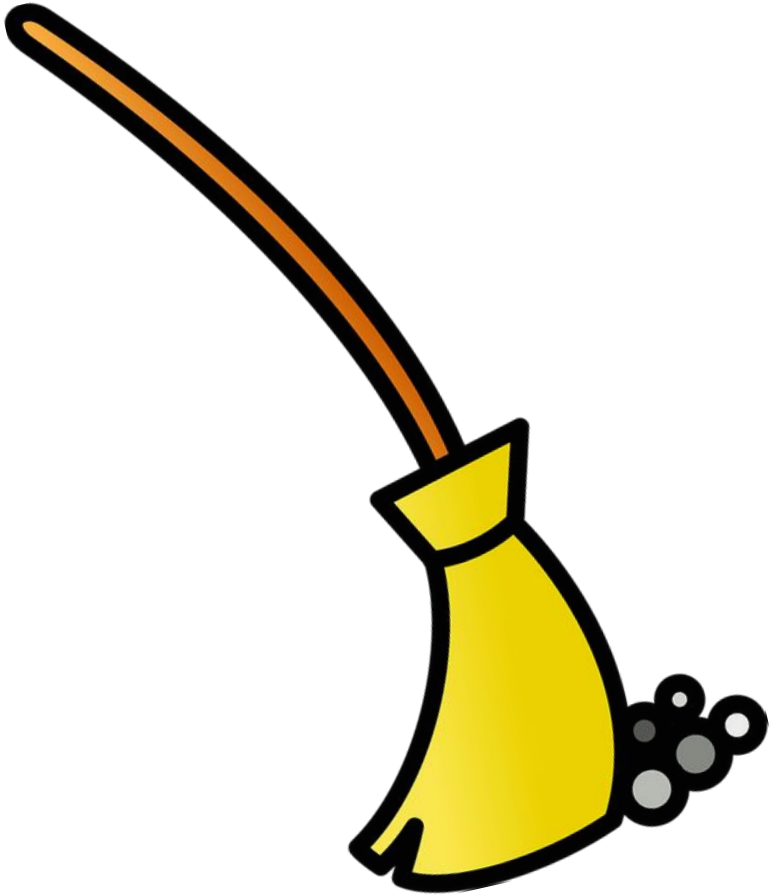
2001:db8:cafe::1/64

18 446 744 073 709 551 616

Network Reconnaissance???




YES
NO
MAYBE



sweeping impossible

Patterns

- low-byte addresses: 2001:db8::1, 2001:db8::d
- IPv4-based addresses: 2001:db8::192.0.2.1
- service port addresses: 2001:db8::80, 2001:db8::25
- wordy addresses: 2001:db8::bad:cafe

Techniques

Local Network

- **Local Address Scanning**
- **Obtaining Network Information via Traffic Snooping**
- **Leveraging Local Name Resolution**
- **Service Discovery Services Gleaning Information from Routing Protocols**

Remote Network

- Remote Address Scanning
- DNS Brute Forcing
- DNS Advertised Hosts
- DNS Zone Transfers
- DNS Reverse Mappings
- Public Archives
- Application Participation
- Inspection of the IPv6 Neighbor Cache and Routing Table
- Inspecting System Configuration and Log Files
- Gleaning Information from IP Flow Information Export
- Obtaining Network Information with traceroute6
- Gleaning Information from Network Devices Using SNMP

DNS Brute Forcing

1) nmap dns-brute

looking for DNS AAAA records against commonly used host names

```
$nmap --script dns-brute google.com
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-15 17:30 EDT
Nmap scan report for google.com (216.58.214.238)
Host is up (0.028s latency).
Other addresses for google.com (not scanned): 2a00:1450:400d:803::200e
rDNS record for 216.58.214.238: bud02s24-in-f14.1e100.net
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Host script results:
| dns-brute:
|   DNS Brute-force hostnames:
|     admin.google.com - 172.217.16.110
|     admin.google.com - 2a00:1450:400d:808::200e
|     ads.google.com - 172.217.19.110
|     id.google.com - 172.217.19.99
|     ads.google.com - 2a00:1450:400d:804::200e
|     id.google.com - 2a00:1450:400d:809::2003
|     images.google.com - 172.217.19.110
|     images.google.com - 2a00:1450:400d:804::200e
|     alerts.google.com - 172.217.19.110
|     news.google.com - 216.58.214.206
|     alerts.google.com - 2a00:1450:400d:804::200e
|     news.google.com - 2a00:1450:400d:802::200e
```

DNS Reverse Mappings

ip6.arpa zone - "0.8.0.0.8.b.d.0.1.0.0.2.ip6.arpa." for "2001:db8:80::/48"

looking up PTR records -

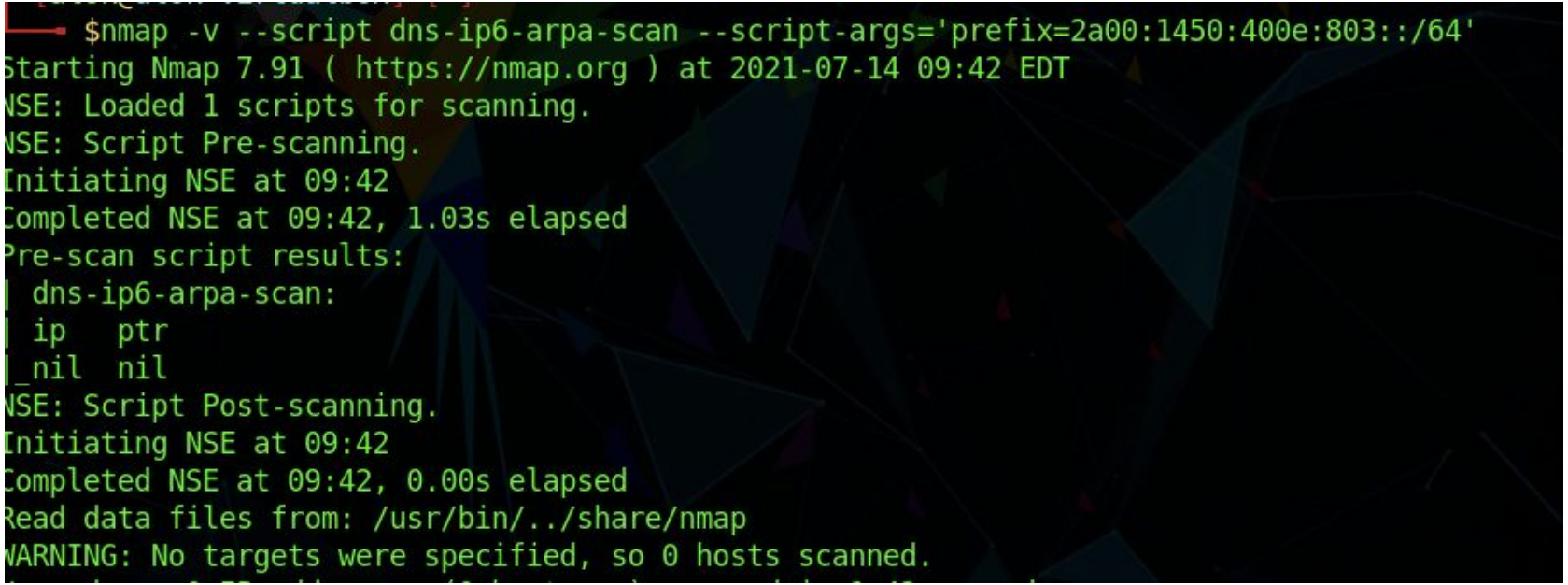
"0.0.8.0.0.8.b.d.0.1.0.0.2.ip6.arpa."

"1.0.8.0.0.8.b.d.0.1.0.0.2.ip6.arpa."

Responses : RCODE of 0 (no error);

otherwise, RCODE of 4 (NXDOMAIN).

1) nmap dns-ip6-arpa-scan



2) reverse-dns (web tool)

network-tools.webwiz.net/reverse-dns.htm

Reverse DNS to 2a00:1450:400e:803::200e

IP address:	2a00:1450:400e:803::200e
Reverse DNS:	ams15s42-in-x0e.1e100.net [IP: 2a00:1450:400e:803::200e]
Reverse DNS Authenticity:	Verified
Country:	Ireland
Link to IP Information:	IP Information for 2a00:1450:400e:803::200e
Direct Link to Reverse DNS:	Reverse DNS for 2a00:1450:400e:803::200e

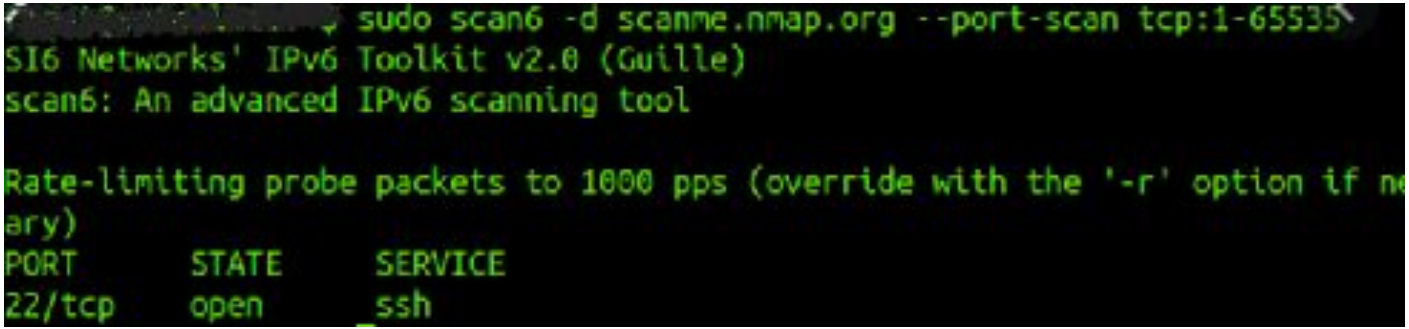
Remote Address Scanning

First - Reduce

RFC5375

- **Run from low number upwards**
  2001:db8:0::/64, 2001:db8:1::/64, etc.
- **Use building numbers**
- **Use Virtual Local Area Network (VLAN) numbers.**

scan6 tool from IPv6-Toolkit



Obtaining Network Information via Traffic Snooping

MUST. SNIFF. EVERYTHING.

SLOTHILDA.COM

ipv6

No.	Time	Source	Destination	Protocol	Length	Info
2	0.000240400	fe80::3f…	ff02::1	ICMPv6	118	Echo (ping) request id=0x920e, s
3	0.000941079	fe80::cf…	fe80::3f…	ICMPv6	118	Echo (ping) reply id=0x920e, seq
4	1.003891482	fe80::3f…	ff02::1	ICMPv6	118	Echo (ping) request id=0x920e, s
5	1.004858465	fe80::3f…	ff02::1	ICMPv6	118	Echo (ping) request id=0x920e, s
6	1.004858584	fe80::cf…	fe80::3f…	ICMPv6	118	Echo (ping) reply id=0x920e, seq
7	5.052817101	fe80::cf…	fe80::3f…	ICMPv6	86	Neighbor Solicitation for fe80:::
8	5.052846585	fe80::3f…	fe80::cf…	ICMPv6	78	Neighbor Advertisement fe80::3f8

```
▸ Frame 4: 118 bytes on wire (944 bits), 118 bytes captured (944 bits) on interface eth0, id 0
▸ Ethernet II, Src: PcsCompu_b1:ba:80 (08:00:27:b1:ba:80), Dst: IPv6mcast_01 (33:33:00:00:00:01)
▸ Internet Protocol Version 6, Src: fe80::3f89:ea82:e0ac:55f4, Dst: ff02::1
▾ Internet Control Message Protocol v6
    Type: Echo (ping) request (128)
    Code: 0
    Checksum: 0xa77c [correct]
    [Checksum Status: Good]
    Identifier: 0x920e
    Sequence: 2
  ▸ Data (56 bytes)
```

```
0000  33 33 00 00 00 01 08 00  27 b1 ba 80 86 dd 60 0b   33······ '·····`·
0010  6b 07 00 40 3a 01 fe 80  00 00 00 00 00 00 3f 89   k··@:··· ······?
0020  ea 82 e0 ac 55 f4 ff 02  00 00 00 00 00 00 00 00   ····U··· ········
0030  00 00 00 00 00 01 80 00  a7 7c 92 0e 00 02 60 d3   ········ ·|····`·
0040  78 60 00 00 00 00 41 bf  0e 00 00 00 00 00 10 11   x`····A· ········
0050  12 13 14 15 16 17 18 19  1a 1b 1c 1d 1e 1f 20 21   ········ ····· !
0060  22 23 24 25 26 27 28 29  2a 2b 2c 2d 2e 2f 30 31   "#$%&'() *+,-./01
```

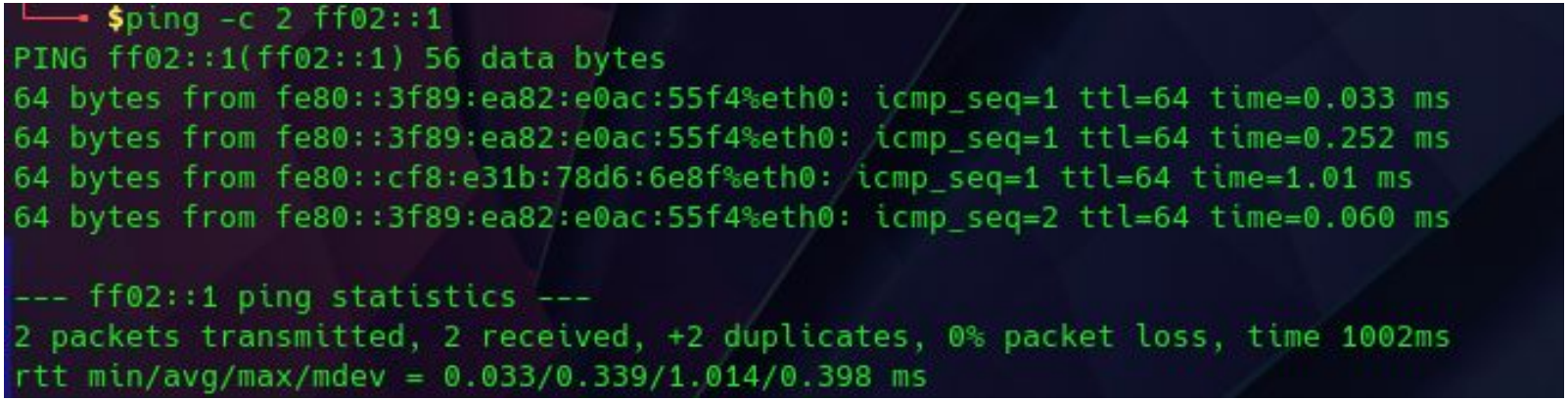
Local Address Scanning

Completely different problem:

link-local multicast addresses can relieve the attacker of searching for unicast addresses in a large IPv6 address space

PING

link-local multicast address (ff02::1)



nmap and THC-IPV6 (alive6)

```
root@kali:~# alive6 eth0 -l
Alive: fe80::21a:a0ff:fea4:4ae9 [ICMP echo-reply]
Alive: fe80::21a:a0ff:fe4e:34f0 [ICMP echo-reply]
Alive: fe80::215:f9ff:fef7:5949 [ICMP echo-reply]
```

```
└─$ sudo nmap -6 fe80::80a4:11ec:e45f:7d19/128 -Pn
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2021-07-14 09:53 EDT
Nmap scan report for fe80::80a4:11ec:e45f:7d19
Host is up (0.0000080s latency).
All 1000 scanned ports on fe80::80a4:11ec:e45f:7d19 are closed

Nmap done: 1 IP address (1 host up) scanned in 0.26 seconds
```

github: ArcStatic
twitter: @gl4cierBlue

README.md

IPv6 Scanning Project

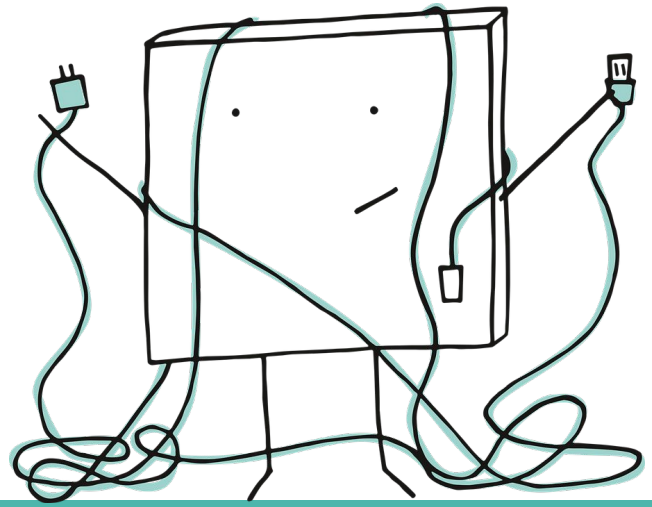
This is an early-stage PhD project to investigate strategies which could be used to scan the IPv6 address space.

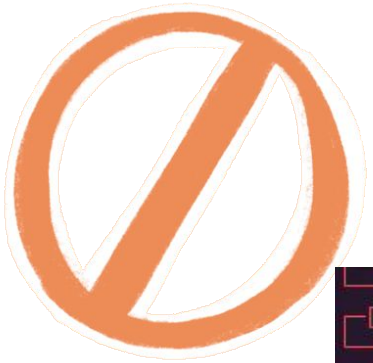
Research Question

How would malware perform scans for automated host recruitment on IPv6-only networks?

Mitigations

1) Limit "pattern" addresses
2) Intrusion Prevention Systems (IPSs)
3) IPv6 packet filtering
4) Avoiding use of sequential addresses when using DHCPv6
5) "Default" /64 size IPv6 subnet prefixes
6) Avoiding being predictable





Block Listing

```
└─# ip6tables -A INPUT -j DROP -s 2001:db8::bad:cafe/64 -m comment --comment "MALWARE"
┌─[root@alok-virtualbox]─[/home/alok]
└─# ip6tables -A INPUT -j DROP -s 2001:db8::bad:cafe/56 -m comment --comment "MALWARE"
┌─[root@alok-virtualbox]─[/home/alok]
└─# ip6tables -A INPUT -j DROP -s 2001:db8::bad:cafe/50 -m comment --comment "MALWARE"
┌─[root@alok-virtualbox]─[/home/alok]
└─# ip6tables -A INPUT -j DROP -s 2001:db8::bad:cafe/48 -m comment --comment "MALWARE"
┌─[root@alok-virtualbox]─[/home/alok]
└─# ip6tables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       all      2001:db8::/64        anywhere             /* MALWARE */
DROP       all      2001:db8::/64        anywhere             /* MALWARE */
DROP       all      2001:db8::/56        anywhere             /* MALWARE */
DROP       all      2001:db8::/50        anywhere             /* MALWARE */
DROP       all      2001:db8::/48        anywhere             /* MALWARE */

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

SECURING YOURSELF

1) IPv6 syntax

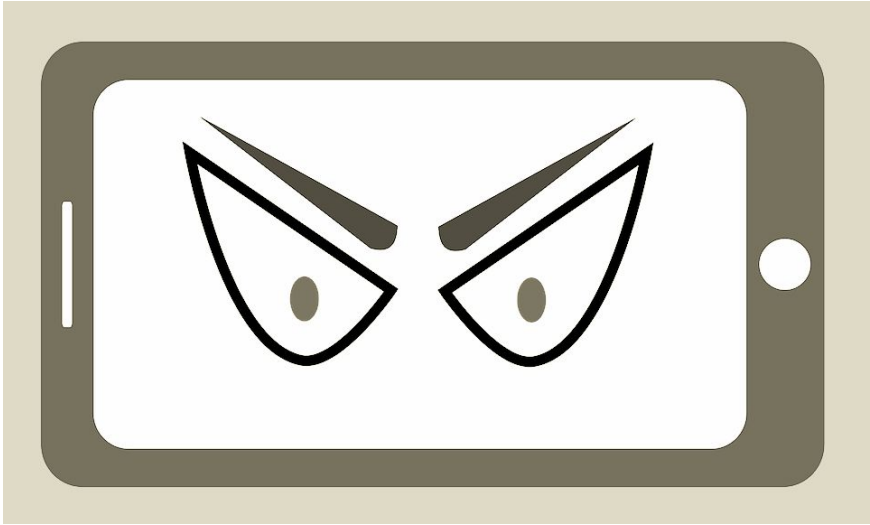
```
2001:0:db8:1111::200
                                2001:db8:ef01:2345:678:910:aaaa:bbbb

fe80::101:1111
                                                fe80::6678:9101:0:34ab

bb2b:ef12:bff3:9125:1111:101:1111:101
                                                        ::1

1031:1976:1:2:3:4::101
                                        2001:db8::1234:5678:9101:1112:1113
```

2) Hit the “off” button



```
sudo ifconfig gif0 down
```

3) How to “kill”

organizations should know how to kill it before it can infect others

What continued IPv6 adoption means for internet security

As IPv6 adoption becomes more prevalent, threat actors are increasingly using its addresses as an attack vector

The ability to monitor anomalous web traffic is the key to detecting a breach

The amount of internet-connected IoT devices grows exponentially

IPv6 may have been a long time coming, but it's too late in the game to ignore.

Links:

www.worldipv6launch.org
www.tunnelbroker.net
network-tools.webwiz.net/reverse-dns.htm

Stacy#0720

Tools:

nmap dns-brute
nmap dns-ip6-arpa-scan
IPv6-Toolkit
THC-IPV6

@stasya7z

Credits

Special thanks to Margaret Fero, Sarthak , Vi, Digital Overdose community,

GRIMMcon