# Network Troubleshooting

Charles Edge

# Extrusion Detection

# Toolchains

# Your own little root kit

## Troubleshooting

# Extension Attributes

https://jamfnation.jamfsoftware.com/extensionAttributes.html

No notes needed

# Why?

# Splunk/Logstash

# Get Network Info

Get an IP for

ipconfig getifaddr en0

```
192.168.210.235
```

variabled

ip=`ipconfig getifaddr en0` ; echo $ip

```
192.168.210.235
```

Get

This

ipconfig getoption en0 subnet_mask

```
255.255.255.0
```

Get

This

ipconfig getoption en0 domain_name_server

```
192.168.210.1
```

Get DHCP

ipconfig getpacket en1

```
op = BOOTREPLY
htype = 1
flags = 0
hlen = 6
hops = 0
xid = 656411831
secs = 0
ciaddr = 192.168.210.235
yiaddr = 192.168.210.235
siaddr = 0.0.0.0
giaddr = 0.0.0.0
chaddr = 64:76:ba:b5:f3:28
sname =
file =
options:
Options count is 7
dhcp_message_type (uint8): ACK 0x5
server_identifier (ip): 192.168.210.1
lease_time (uint32): 0x15180
subnet_mask (ip): 255.255.255.0
router (ip_mult): {192.168.210.1}
domain_name_server (ip_mult): {192.168.210.1}
end (none):
```

# Set Network Info

Better

# ifconfig en0

```
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
   ether 64:76:ba:b5:f3:28
   inet6 fe80::6676:baff:feb5:f328%en0 prefixlen 64 scopeid 0x4
   inet 192.168.210.235 netmask 0xffffff00 broadcast 192.168.210.255
   nd6 options=1<PERFORMNUD>
   media: autoselect
   status: active
```

IP

Subnet

ifconfig en4 inet 10.10.10.10 netmask 255.255.255.0

# OS X Locations

Show Locations

networksetup -listlocations

```
Automatic
```

Active Location

networksetup -getcurrentlocation

```
Automatic
```

Create a Location

networksetup -createlocation Work populate

Delete a Location

networksetup -deletelocation Work

Change your Location

networksetup -switchlocation Work

Change your Location

scselect Work

```
CurrentSet updated to A177A2A2-3E7E-4C01-BFF7-D05799346E8F (Work)
```

# OS X network setup

# List the Interfaces

networksetup -listallnetworkservices

```
Bluetooth DUN
USB Ethernet
Wi-Fi
Bluetooth PAN
Thunderbolt Bridge
JAMF VPN
```

Change an Interfaces Name

networksetup -renamenetworkservice Ethernet en1

Disable A Network Service

networksetup -setnetworkserviceenabled off

```
(1) Bluetooth DUN
(Hardware Port: Bluetooth DUN, Device: Bluetooth-Modem)

(2) USB Ethernet
(Hardware Port: USB Ethernet, Device: en3)

(3) Wi-Fi
(Hardware Port: Wi-Fi, Device: en0)

(4) Bluetooth PAN
(Hardware Port: Bluetooth PAN, Device: en2)

(5) Thunderbolt Bridge
(Hardware Port: Thunderbolt Bridge, Device: bridge0)

(6) JAMF VPN
(Hardware Port: IPSec, Device: )
```

## Change Network Interface Order

networksetup -ordernetworkservices “Wi-Fi” “USB Ethernet”

*Must include all

Set an interface to DHCP

networksetup -setdhcp Wi-Fi

## Renew DHCP Lease

ipconfig set en1 BOOTP && ipconfig set en1 DHCP

ifconfig en1 down && ifconfig en1 up

# Renew Leases II

```
echo "add State:/Network/Interface/en0/
RefreshConfiguration temporary" | sudo scutil
```

Configure IP, Subnet & Gateway

networksetup -setmanual Wi-Fi 10.0.0.2
255.255.255.0 10.0.0.1

Configure DNS Servers

networksetup -setdnsservers Wi-Fi 10.0.0.2 10.0.0.3

Get

networksetup -getdnsservers Wi-Fi

alf

hypothesis

bottoms up

troubleshooting

## Stop the Firewall

launchctl unload /System/Library/LaunchAgents/
com.apple.alf.useragent.plist

launchctl unload /System/Library/LaunchDaemons/
com.apple.alf.agent.plist

## Start the Firewall

launchctl load /System/Library/LaunchDaemons/com.apple.alf.agent.plist

launchctl load /System/Library/LaunchAgents/com.apple.alf.useragent.plist

Add an app to alf

socketfilterfw -t
“/Applications/FileMaker Pro/FileMaker Pro.app/
Contents/MacOS/FileMaker Pro”

route

See Routing Table

netstat -nr

For these  Use this

route -n add 10.0.0.0/32 10.0.9.2

bonjour

packet level

sudo killall -USR2 mDNSResponder

## Restart the Service

Stop: launchctl unload -w /System/Library/LaunchDaemons/com.apple.mDNSResponder.plist

To start:launchctl load -w /System/Library/LaunchDaemons/com.apple.mDNSResponder.plist

# ping

Wait a little

ping -i 5 192.168.210.1

```
64 bytes from 192.168.210.1: icmp_seq=233 ttl=64 time=2.522 ms
Request timeout for icmp_seq 234
64 bytes from 192.168.210.1: icmp_seq=235 ttl=64 time=3.554 ms
```

Write to logs/files

Number of pings

ping -c 5 google.com

```
64 bytes from 74.125.239.40: icmp_seq=0 ttl=56 time=84.861 ms
64 bytes from 74.125.239.40: icmp_seq=1 ttl=56 time=135.179 ms
```

flood

ping -f localhost

```
.Request timeout for icmp_seq 3690
```

Set Packet Size

ping -s 100 google.com

Set a Source

ping -S 10.10.10.11 google.com

iostat -d disk0

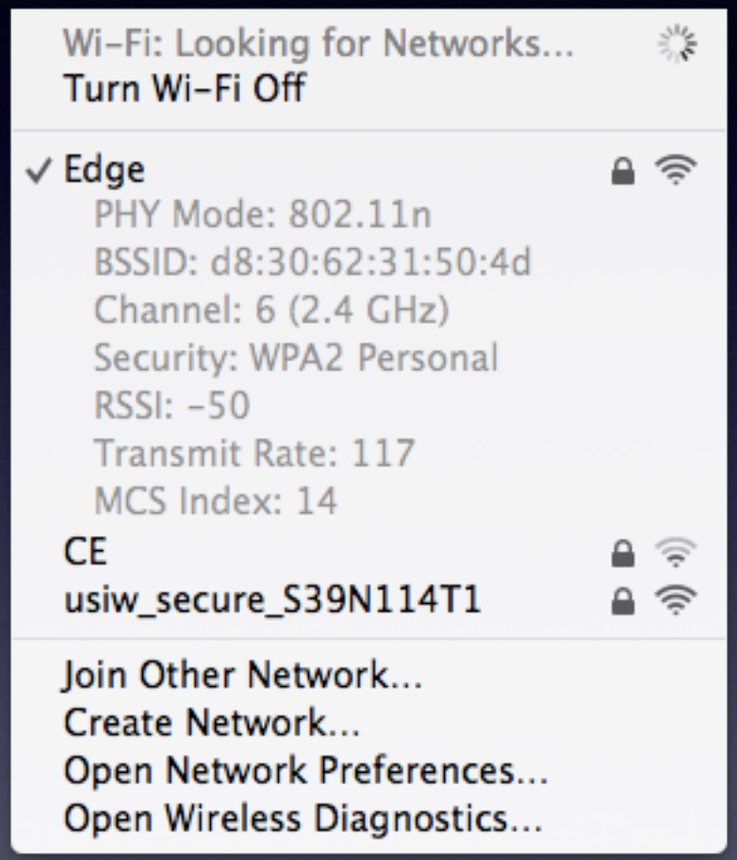
airport

Get Info on wireless network

/System/Library/PrivateFrameworks/

Apple80211.framework/Versions/A/Resources/airport -I

```
     agrCtlRSSI: -47
     agrExtRSSI: 0
    agrCtlNoise: -92
    agrExtNoise: 0
          state: running
        op mode: station
     lastTxRate: 145
        maxRate: 144
lastAssocStatus: 0
    802.11 auth: open
      link auth: wpa2-psk
          BSSID: d8:30:62:31:50:4d
           SSID: Edge
            MCS: 15
        channel: 6
```


Wi-Fi: Looking for Networks...
Turn Wi-Fi Off
✓ Edge
PHY Mode: 802.11n
BSSID: d8:30:62:31:50:4d
Channel: 6 (2.4 GHz)
Security: WPA2 Personal
RSSI: -50
Transmit Rate: 117
MCS Index: 14
CE
usiw_secure_S39N114T1
Join Other Network...
Create Network...
Open Network Preferences...
Open Wireless Diagnostics...

Scan

/System/Library/PrivateFrameworks/Apple80211.framework/Versions/A/Resources/airport -s

```
                            SSID BSSID             RSSI CHANNEL HT CC SECURITY (auth/unicast/group)
                      EliteWifi 6c:f3:7f:80:59:90 -84  6       Y  -- NONE
                      EliteWifi 6c:f3:7f:80:54:30 -89  11      Y  -- NONE
                            NJG d8:c7:c8:13:30:98 -76  140     N  -- NONE
                     EliteAdmin 6c:f3:7f:80:54:39 -92  100,+1  Y  -- WPA2(PSK/AES/AES)
                      EliteWifi 6c:f3:7f:80:54:38 -89  100,+1  Y  -- NONE
                     EliteAdmin 24:de:c6:53:69:19 -76  100,+1  Y  -- WPA2(PSK/AES/AES)
                      EliteWifi 24:de:c6:53:69:18 -75  100,+1  Y  -- NONE
                            NJG d8:c7:c8:13:2f:18 -89  60      N  -- NONE
                            NJG d8:c7:c8:13:2d:b8 -85  52      N  -- NONE
                            NJG d8:c7:c8:13:30:68 -87  44      N  -- NONE
                  staden!guest b8:62:1f:ac:49:bf -91  40      Y  SE NONE
                           ubnt 00:27:22:78:a3:7e -91  40,-1   Y  -- WPA2(PSK/AES,TKIP/TKIP)
                            NJG d8:c7:c8:13:30:c8 -82  40      N  -- NONE
                Bestseller Guest 00:27:0d:0b:8f:3f -84  36      Y  DK NONE
                            NJG 9c:1c:12:29:61:38 -74  36      N  -- NONE
```

# traceroute

Follow a packet

traceroute google.com

```
traceroute: Warning: google.com has multiple addresses; using 74.125.225.40
traceroute to google.com (74.125.225.40), 64 hops max, 52 byte packets
 1  my.meraki.net (192.168.210.1)  3.670 ms  3.584 ms  5.392 ms
 2  192.168.0.1 (192.168.0.1)  3.685 ms  4.551 ms  2.654 ms
 3  mpls-dsl-gw59.mpls.qwest.net (207.225.140.59)  27.482 ms  23.386 ms  25.172 ms
 4  mpls-agw1.inet.qwest.net (75.168.229.209)  26.737 ms  27.121 ms  24.119 ms
 5  cer-edge-18.inet.qwest.net (67.14.122.10)  38.196 ms  41.479 ms  34.211 ms
 6  208.47.121.146 (208.47.121.146)  34.515 ms * *
 7  * 209.85.255.26 (209.85.255.26)  43.698 ms *
 8  209.85.250.28 (209.85.250.28)  40.666 ms  37.084 ms  36.150 ms
 9  ord08s06-in-f8.1e100.net (74.125.225.40)  37.846 ms  34.610 ms  35.192 ms
```

Don’t worry about names

traceroute -n google.com

```
traceroute to google.com (74.125.228.38), 64 hops max, 52 byte packets
 1  192.168.210.1  3.283 ms  15.190 ms  7.438 ms
 2  192.168.0.1  4.153 ms  3.461 ms  6.043 ms
 3  207.225.140.59  53.902 ms  28.369 ms  57.029 ms
 4  75.168.229.209  52.066 ms  50.941 ms  53.188 ms
 5  67.14.122.10  45.733 ms  35.629 ms  36.975 ms
 6  * * *
 7  209.85.255.26  37.034 ms
    209.85.255.132  41.356 ms  36.471 ms
 8  72.14.237.133  38.175 ms
    72.14.237.130  36.642 ms
    72.14.237.133  35.128 ms
 9  209.85.246.82  56.368 ms  56.933 ms  54.827 ms
10  72.14.236.147  61.698 ms
```

write lines to syslog

traceroute -n google.com | logger -is

```
traceroute to google.com (74.125.228.38), 64 hops max, 52 byte packets
 1  192.168.210.1  3.283 ms  15.190 ms  7.438 ms
 2  192.168.0.1  4.153 ms  3.461 ms  6.043 ms
 3  207.225.140.59  53.902 ms  28.369 ms  57.029 ms
 4  75.168.229.209  52.066 ms  50.941 ms  53.188 ms
 5  67.14.122.10  45.733 ms  35.629 ms  36.975 ms
 6  * * *
 7  209.85.255.26  37.034 ms
    209.85.255.132  41.356 ms  36.471 ms
 8  72.14.237.133  38.175 ms
    72.14.237.130  36.642 ms
    72.14.237.133  35.128 ms
 9  209.85.246.82  56.368 ms  56.933 ms  54.827 ms
10  72.14.236.147  61.698 ms
```

Debug

traceroute -d google.com

# netstat

All Sockets

# netstat -at

```
963418e019e78549 dgram       0      0                0 963418e019e78611 963418e019e78611
963418e018905351 dgram       0      0                0 963418e018905289 963418e018905289
963418e018905289 dgram       0      0                0 963418e018905351 963418e018905351
963418e018906ea9 dgram       0      0 963418e0190820d1                0 963418e0209255a9
run/syslog
```

IPv6

# netstat -lt

```
963418e019e78549 dgram       0      0                0 963418e019e78611 963418e019e78611
963418e018905351 dgram       0      0                0 963418e018905289 963418e018905289
963418e018905289 dgram       0      0                0 963418e018905351 963418e018905351
963418e018906ea9 dgram       0      0 963418e0190820d1                0 963418e0209255a9
run/syslog
```

## Per Protocol Stats

## netstat -s

```
tcp:
  55445720 packets sent
     44946257 data packets (679561584 bytes)
     48361 data packets (26644924 bytes) retransmitted
     0 resends initiated by MTU discovery
     8513407 ack-only packets (45500 delayed)
     0 URG only packets
     6614 window probe packets
     1730411 window update packets
     203196 control packets
     0 data packets sent after flow control
     52548455 checksummed in software
```

One Protocol

netstat -p igmp

Show the Interfaces

# netstat -i

```
Name  Mtu   Network       Address            Ipkts Ierrs    Opkts Oerrs  Coll
lo0   16384 <Link#1>                        3595751     0  3595751     0     0
lo0   16384 localhost   ::1                 3595751     -  3595751     -     -
lo0   16384 127           localhost         3595751     -  3595751     -     -
lo0   16384 localhost   fe80:1::1           3595751     -  3595751     -     -
gif0* 1280  <Link#2>                              0     0        0     0     0
stf0* 1280  <Link#3>                              0     0        0     0     0
en0   1500  <Link#4>    64:76:ba:b5:f3:28 37706820     0 55168500     0     0
en0   1500  charless-ma fe80:4::6676:baff 37706820     - 55168500     -     -
en0   1500  192.168.210   192.168.210.235 37706820     - 55168500     -     -
en1   1500  <Link#5>    32:00:1a:34:e0:00        0     0        0     0     0
bridg 1500  <Link#6>    66:76:ba:5b:17:00        0     0        1     0     0
p2p0  2304  <Link#7>    06:76:ba:b5:f3:28        0     0        0     0     0
```

# ntop

stroke

/System/Library/CoreServices/Applications/Network\
Utility.app/Contents/Resources/stroke
www.google.com 80 80

```
Port Scanning host: 74.125.192.103

   Open TCP Port:   80          http
```

# nmap

nmap -sS -O krypted.com/24

# nc (netcat)

# nc -v www.apple.com 80

```
found 0 associations
found 1 connections:
     1:  flags=82<CONNECTED,PREFERRED>
  outif en0
  src 192.168.210.235 port 55997
  dst 23.7.151.44 port 80
  rank info not available
  TCP aux info available

Connection to www.apple.com port 80 [tcp/http] succeeded!
```

Timeout

/usr/bin/nc -v -w 15 gateway.push.apple.com 2195

```
found 0 associations
found 1 connections:
     1:  flags=82<CONNECTED,PREFERRED>
  outif en0
  src 192.168.210.235 port 55998
  dst 17.110.226.98 port 2195
  rank info not available
  TCP aux info available

Connection to gateway.push.apple.com port 2195 [tcp/*] succeeded!
```

IPv4

/usr/bin/nc -v -4 feedback.push.apple.com 2196

```
found 0 associations
found 1 connections:
     1: flags=82<CONNECTED,PREFERRED>
  outif en0
  src 192.168.210.235 port 56005
  dst 17.172.233.38 port 2196
  rank info not available
  TCP aux info available
```

Listen

/usr/bin/nc -l 2196

# tcpdump

Capture

# tcpdump -nS

```
21:47:55.558172 IP 192.168.210.140.5353 > 224.0.0.251.5353: 0*- [0q] 26/0/2 (Cache flush) TXT "deviceid=58:55:CA:2B:17
"features=0x4A7FFFF7,0xE" "flags=0x44" "model=AppleTV2,1" "pk=2e8e654efd5fd2833240785094cc8bcc11f2e00efc4bf3db666e609f
"srcvers=190.9" "vv=2", PTR _airplay._tcp.local., PTR Office Apple TV._airplay._tcp.local., TXT "model=K66AP", (Cache
"cn=0,1,2,3" "da=true" "et=0,3,5" "ft=0x4A7FFFF7,0xE" "md=0,1,2" "am=AppleTV2,1"
"pk=2e8e654efd5fd2833240785094cc8bcc11f2e00efc4bf3db666e609ffef9a4dc" "sf=0x44" "tp=UDP" "vn=65537" "vs=190.9" "vv=2",
_raop._tcp.local., PTR 5855CA2B17F3@Office Apple TV._raop._tcp.local., (Cache flush) SRV Office-Apple-TV-10.local.:700
(Cache flush) SRV Office-Apple-TV-10.local.:5000 0 0, (Cache flush) TXT "txtvers=1" "atSV=65539" "RmSV=65536"
"DbId=16B6AA4F17E80878" "CtlN=Office Apple TV" "DvTy=AppleTV" "DvSv=1536" "Ver=131075", PTR _touch-able._tcp.local., P
243E8F2E38F3FCBE._touch-able._tcp.local., (Cache flush) TXT "txtvers=1" "atSV=65539" "hG=00000000-05c5-ea14-9ad7-8ec25
"MniT=167845888" "fs=2" "Name=Office Apple TV" "PrVs=65538" "DFID=2" "EiTS=1" "MiTPV=196611", PTR _appletv-v2._tcp.loc
243E8F2E38F3FCBE._appletv-v2._tcp.local., PTR 243E8F2E38F3FCBE._appletv-v2._tcp.local., (Cache flush) SRV Office-Apple
TV-10.local.:3689 0 0, (Cache flush) SRV Office-Apple-TV-10.local.:3689 0 0, (Cache flush) PTR Office-Apple-TV-10.loca
flush) AAAA fe80::44f:21df:dd3c:b5d1, (Cache flush) PTR Office-Apple-TV-10.local., (Cache flush) A 192.168.210.140, (C
TXT "", PTR _sleep-proxy._udp.local., PTR 70-35-60-63.1 Office Apple TV._sleep-proxy._udp.local., (Cache flush) SRV Of
TV-10.local.:56188 0 0 (1436)
```

Verbose with data

# tcpdump -nnvvXS

```
21:50:14.273950 IP (tos 0x40, ttl 114, id 6972, offset 0, flags [DF], proto TCP (6), length 1492)
    139.218.201.51.53043 > 192.168.210.235.52189: Flags [.], cksum 0x7ace (correct), seq
3116828193:3116829633, ack 3101844790, win 255, options [nop,nop,TS val 5463774 ecr 1633904510],
1440
   0x0000:  6476 bab5 f328 0018 0a17 2fa0 0800 4540  dv...(..../...E@
   0x0010:  05d4 1b3c 4000 7206 ff05 8bda c933 c0a8  ...<@.r......3..
   0x0020:  d2eb cf33 cbdd b9c7 0621 b8e2 6536 8010  ...3.....!..e6..
   0x0030:  00ff 7ace 0000 0101 080a 0053 5ede 6163  ..z........S^.ac
   0x0040:  677e 86b1 984a 6457 4af5 8dbf 4f22 b2ed  g~...JdWJ...O"..
   0x0050:  9a94 606f ee5e aaba 8897 ea3c 9968 e93d  ..`o.^.....<.h.=
   0x0060:  ecf8 d389 97b8 9274 4a33 1bec ca93 95bd  .......tJ3......
   0x0070:  4dbf e670 6b8b 6100 e067 b542 1000 6cd8  M..pk.a..g.B..l.
   0x0080:  e67a 2bdb 73f5 bc72 d202 3091 e5d7 4955  .z+.s..r..0...IU
   0x0090:  a7d0 a5ab 2e1f 4198 164e 6fd9 ec8c 38b4  ......A..No...8.
   0x00a0:  6029 d0b8 302b 9b91 ad9b 4b35 ddbc a612  `)..0+....K5....
   0x00b0:  0c21 d8ad 6f3d 6f4a 8497 876e 654c eaf3  .!..o=oJ...neL..
```

A Port

tcpdump -nnvvXs 548

```
21:51:28.143400 IP (tos 0x0, ttl 64, id 31894, offset 0, flags [DF], proto TCP (6
length 52)
    192.168.210.235.52189 > 139.218.201.51.53043: Flags [.], cksum 0x4439 (correc
3101846291, ack 3118157129, win 8192, options [nop,nop,TS val 1633977911 ecr 5471
length 0
  0x0000:  0018 0a17 2fa0 6476 bab5 f328 0800 4500  ..../.dv...(..E.
  0x0010:  0034 7c96 4000 4006 d58b c0a8 d2eb 8bda  .4|.@.@.........
  0x0020:  c933 cbdd cf33 b8e2 6b13 b9db 4d49 8010  .3...3..k...MI..
  0x0030:  2000 4439 0000 0101 080a 6164 8637 0053  ..D9......ad.7.S
  0x0040:  7bc6                                     {.
```

Destination

tcpdump -nnvvXs 548 dst 10.0.0.48

To a file

```
tcpdump -nnvvXs 548 dst 10.0.0.48 -w /tmp/myfile.pcap
```

NOT

tcpdump -nnvvXs dst 10.0.0.48 -w /tmp/myfile and not dst port 548

Read from a file

tcpdump -qns 0 -A -r /var/tmp/capture.pcap

```
....alIAHTTP/1.1 200 OK
Cache-Control: no-cache, no-store, must-revalidate
Content-Type: image/gif
Expires: 0
Pragma: no-cache
Content-Length: 43
Connection: keep-alive
```

*4 interfaces [Wireshark 1.12.0 (v1.12.0-0-g4fab41a from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

| No. | Time | Source | Destination | Protocol | Length | Info |
|---|---|---|---|---|---|---|
| 715 | 3.042760000 | 10.0.3.186 | 173.194.32.37 | TCP | 54 | [TCP Dup ACK 714#1] 55335→443 [ACK] Seq=55 Ack=2 Win=16384 Len=0 |
| 716 | 3.043344000 | 23.78.52.171 | 10.0.3.186 | TCP | 78 | [TCP Dup ACK 658#1] 443→55300 [ACK] Seq=55 Ack=55 Win=557 Len=0 TS |
| 717 | 3.043386000 | 10.0.3.186 | 23.78.52.171 | TCP | 54 | 55300→443 [RST] Seq=55 Win=0 Len=0 |
| 718 | 3.044891000 | 173.194.32.56 | 10.0.3.186 | TCP | 60 | 443→55338 [FIN, ACK] Seq=1 Ack=55 Win=670 Len=0 |
| 719 | 3.044959000 | 10.0.3.186 | 173.194.32.56 | TCP | 54 | 55338→443 [ACK] Seq=55 Ack=2 Win=16384 Len=0 |
| 720 | 3.045478000 | 93.184.220.101 | 10.0.3.186 | TCP | 60 | 80→55290 [RST] Seq=1 Win=0 Len=0 |
| 721 | 3.045729000 | 23.78.47.139 | 10.0.3.186 | TCP | 66 | 80→55316 [FIN, ACK] Seq=1 Ack=2 Win=486 Len=0 TSval=447362447 TSec |
| 722 | 3.045731000 | 93.184.220.101 | 10.0.3.186 | TCP | 60 | 80→55289 [RST] Seq=1 Win=0 Len=0 |

```
Frame 717: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
Ethernet II, Src: 64:76:ba:b5:f3:28 (64:76:ba:b5:f3:28), Dst: 00:1a:1e:20:02:70 (00:1a:1e:20:02:70)
Internet Protocol Version 4, Src: 10.0.3.186 (10.0.3.186), Dst: 23.78.52.171 (23.78.52.171)
Transmission Control Protocol, Src Port: 55300 (55300), Dst Port: 443 (443), Seq: 55, Len: 0
```

```
0000  00 1a 1e 20 02 70 64 76  ba b5 f3 28 08 00 45 00   ... .pdv ...(..E.
0010  00 28 c9 84 40 00 40 06  17 99 0a 00 03 ba 17 4e   .(..@.@. .......N
0020  34 ab d8 04 01 bb b5 33  fb e3 00 00 00 00 50 04   4......3 ......P.
0030  00 00 cb 56 00 00                                 ...V..
```

File: "/var/folders/yl/cbc7dr... Packets: 844 · Displayed: 844 (100.0%) · Dropped: 0 (0.0%) Profile: Default

# lsof

Get an IP for

# lsof -n -i4TCP

```
COMMAND     PID        USER   FD   TYPE             DEVICE SIZE/OFF NODE NAME
netsessio   807 charlesedge    7u  IPv4 0x8ec0cbe037424fe5      0t0  TCP 127.0.0.1:49494->127.0.0.1:9421 (CLOSED)
netsessio   807 charlesedge    9u  IPv4 0x8ec0cbe0374267cd      0t0  TCP 127.0.0.1:9421 (LISTEN)
CrashPlan   811 charlesedge    8u  IPv4 0x8ec0cbe02b0dc7cd      0t0  TCP 127.0.0.1:50990->127.0.0.1:4243 (ESTABLISHED)
CrashPlan   811 charlesedge   14u  IPv4 0x8ec0cbe02b0dc7cd      0t0  TCP 127.0.0.1:50990->127.0.0.1:4243 (ESTABLISHED)
Box\x20Sy   846 charlesedge   24u  IPv4 0x8ec0cbe0375d7fe5      0t0  TCP 192.168.210.235:49549->74.112.184.96:https (C
Keynote    5413 charlesedge    8u  IPv4 0x8ec0cbe02e8b07cd      0t0  TCP *:49583 (LISTEN)
Keynote    5413 charlesedge   12u  IPv6 0x8ec0cbe027bb1e45      0t0  TCP *:49584 (LISTEN)
idea      98581 charlesedge  141u  IPv4 0x8ec0cbe0375d87cd      0t0  TCP 127.0.0.1:6942 (LISTEN)
idea      98581 charlesedge  142u  IPv4 0x8ec0cbe02e4d4fe5      0t0  TCP 127.0.0.1:50928->127.0.0.1:50927 (CLOSED)
idea      98581 charlesedge  308u  IPv4 0x8ec0cbe03c097fe5      0t0  TCP 127.0.0.1:63342 (LISTEN)
idea      98581 charlesedge  399u  IPv4 0x8ec0cbe0375d4fe5      0t0  TCP *:50932 (LISTEN)
```

# Misc

Read from a file

alias ports='lsof -n -i4TCP | grep LISTEN'

```
netsessio   807 charlesedge    9u  IPv4 0x8ec0cbe0374267cd      0t0  TCP 127.0.0.1:9421 (LISTEN)
Keynote    5413 charlesedge    8u  IPv4 0x8ec0cbe02e8b07cd      0t0  TCP *:49583 (LISTEN)
Keynote    5413 charlesedge   12u  IPv6 0x8ec0cbe027bb1e45      0t0  TCP *:49584 (LISTEN)
idea      98581 charlesedge  141u  IPv4 0x8ec0cbe0375d87cd      0t0  TCP 127.0.0.1:6942 (LISTEN)
idea      98581 charlesedge  308u  IPv4 0x8ec0cbe03c097fe5      0t0  TCP 127.0.0.1:63342 (LISTEN)
idea      98581 charlesedge  399u  IPv4 0x8ec0cbe0375d4fe5      0t0  TCP *:50932 (LISTEN)
```

Get an IP for

```
export SN=`netstat -nr| grep -m 1 -iE 'default|0.0.0.0' |
awk '{print \$2}' | sed 's/\.[0-9]*$//' `
```

```
ping $SN.1
```

```
nmap -p 80 $SN.*
```

Ping the default gateway

```
alias pr="ping \`netstat -nr| grep -m 1 -iE 'default|
0.0.0.0' | awk '{print \$2}'\`"
```

```
alias 3389='ssh -vp 443 krypted@home.krypted.com
-L 10000:ts2.318.com:3389 -N'
```

# Names

# hostname

# scutil

host

dig

dscacheutil -flushcache

# arp

arp -ad

# Server

# serveradmin settings network

```
network:interfaces:_array_index:1:portName = "USB Ethernet"
network:interfaces:_array_index:1:router = ""
network:interfaces:_array_index:1:type = "Ethernet"
network:interfaces:_array_index:1:ipv4SubnetMasks = _empty_array
network:interfaces:_array_index:1:ipv4Addresses = _empty_array
network:interfaces:_array_index:1:orderIndex = 1
network:interfaces:_array_index:1:configMethod = "DHCP"
network:interfaces:_array_index:1:descriptiveName = "USB Ethernet"
network:interfaces:_array_index:1:name = "en3"
network:interfaces:_array_index:1:isActive = yes
network:interfaces:_array_index:2:portName = "Wi-Fi"
network:interfaces:_array_index:2:router = "10.0.0.1"
network:interfaces:_array_index:2:type = "IEEE80211"
network:interfaces:_array_index:2:ipv4SubnetMasks:_array_index:0 = "255.255.252.0"
network:interfaces:_array_index:2:ipv4Addresses:_array_index:0 = "10.0.3.186"
network:interfaces:_array_index:2:orderIndex = 2
network:interfaces:_array_index:2:configMethod = "DHCP"
network:interfaces:_array_index:2:descriptiveName = "Wi-Fi"
```

/Applications/Server.app/Contents/ServerRoot/usr/libexec/afctl -w 10.10.10.2

Whitelist

# InfoSec

# metasploit

# nessus


TOM ROBBINS
Another Roadside Attraction
Maggie: A Girl of the Streets and Other Short Fiction · Stephen Crane
OUGHING IT
MARK TWAIN
IVINE COMEDY VOL. I: INFERNO
OW COUNTRY
YASUNARI KA
ST OF EDEN · JOHN STE
Robert A. Heinlein
ONED FUTURE
COVERIES
eet thursday | john stein
THAT HIDEOUS TRENGTH
KLEY
BRAVE NEW WOR
RAY
DBURY
ONE MORE FOR THE ROAD

```
#!/usr/bin/perl -w
# TODO: find more than one ip in a single line
$debug = "off";

if ($ARGV[0] && -f $ARGV[0]){
  debug("The file exists");
}
else { usage(); }

open (IPFILE, "< $ARGV[0]") or die debug("Couldn't open file: $ARGV[0]");

foreach $line (<IPFILE>) {
  if ($line =~ m/((\d+)\.(\d+)\.(\d+)\.(\d+))/) {
    debug("Condition1 Match: $1") ;}
    if ((($2 && $3 && $4 && $5) ge 0) && (($2 && $3 && $4 && $5) lt 256)) {
      debug("4 Valid Octets: $1");
      print "$1\n";
    }
    else { debug("Invalid Octet: $1"); }
}


sub debug {
  if ($debug eq "on") {
    print "Debug: $_[0]\n";
  }
}
sub usage {
  print "Usage: ipgrep [OPTION]... [FILE]...\n";
  exit;
}
```

```
#!/bin/bash
SUBNET=`netstat -nr| grep -m 1 -iE 'default|0.0.0.0' | awk '{print \$2}' | sed 's/\.[0-9]*$//' `
for n in $(seq 1 254); do
  ADDR=${SUBNET}.${n}
  echo -e "${ADDR}"
done
```

```
#! /usr/bin/perl -w
# $Id: urlgrep.pl,v 1.5 1998/02/10 19:56:56 user Exp $
#
# list all embedded URLs in plaintext, being
# careful of trailing punctuation, like in this line:
# Visit http://www.xor.com/. Maybe http://internet-plaza.net/?

require 5.002;  # not imperative

# cannot use IO::Handle
use FileHandle;
ARGV->input_record_separator('');  # for paragraph reads

$urls = '('
      . join('|', qw{
    http
    ftp
    file
    telnet
    gopher
    mailto
    about
    wais
      } )
      . ')';

$ltrs = '\w';
$gunk = '/#~:.?+=&%@!\-';
$punc = '.:?\-';
$any  = "$ltrs$gunk$punc";

while ($_ = ARGV->getline()) {
 while (m{
 \b          # start at word boundary
 (           # beginning of $1 catch buffer
  $urls     :             # need resource and a literal colon
  [$any] +?         # followed by one or more
          #    of any valid character, but
          #    be conservative and take only
          #    what you need to using +?
 )          # end of $1 catch buffer
 (?=         # look-ahead non-consumptive assertion (?=
  [$punc]*       # either 0 or more punctuation
  [^$any]       #   followed by a non-url char
    |          # or else
  $             #   then end of the string
 )
  }igox)
          # /i means case-insensitive
          # /g means do the substitute globally
          # /o is a hack to avoid extra regcomps
          #    for the interpolated variables
          # /x is for embedded comments and whitespc
          #
          # other cool switches include
          #  /s  make . also match newlines
          #  /m  make ^ and $ multiline match
          #  /e  RHS now full expr, not string:
          #        s/([0-9]+)/3 * $1 + 1/eg;
 { print "$1\n"; }
}

exit 0;
```

```
#!/usr/bin/env python

import re
import sys
import socket

IGNORE = ( "127.0.0.1", "200.206.134.238" )

# Added reserved IANA space (tip by Andrew Lawson) - see
# http://www.iana.org/assignments/ipv4-address-space
RESERVED = (  0,   1,   2,   5,   7,  23,  27,  31,  36,  37,  39, 41,  42,  58,
              59,  60,  70,  71,  72,  73,  74,  75,  76,  77,  78, 79,  83,  84,
              85,  86,  87,  88,  89,  90,  91,  92,  93,  94,  95, 96,  97,  98,
              99, 100, 101, 102, 103, 104, 105, 106, 107, 108, 109, 110, 111, 112,
             113, 114, 115, 116, 117, 118, 119, 120, 121, 122, 123, 124, 125, 126,
             197, 222, 223, 224, 225, 226, 227, 228, 229, 230, 231, 232, 233, 234,
             235, 236, 237, 238, 239, 240, 241, 242, 243, 244, 245, 246, 247, 248,
             249, 250, 251, 252, 253, 254, 255)

if len(sys.argv) > 1:
    data = open(sys.argv[1]).read()
else:
    data = sys.stdin.read()

res = re.findall("\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}", data)

# Counters
bad = 0
ignored = 0
reserved = 0

# # Uniq addresses found
# res2 = {}
# for addr in res:
#     res2[addr] = addr
# res = res2.keys()

verified = []
for addr in res:
    if addr in IGNORE:
        ignored += 1
        continue
    if addr[0] == "0":
        bad += 1
        continue
    parts = map(int, addr.split("."))
    if parts[0] in RESERVED:
        reserved += 1
        continue
    if (parts[:2] == (192, 168) or
         parts[0] in (127, 10) or
         (parts[0] == 172 and parts[1] >= 16 and parts[1] <= 31)):
        reserved += 1
        continue
    for part in parts:
        if part > 255 or part < 0:
            bad += 1
            break
    else:
        verified.append(addr)

for addr in verified:
    print addr

# print "Bad", bad
# print "Ignored", ignored
# print "Reserved", reserved
```