Passer - effortless discovery!

Making use of passer knowledge

Bill Stearns

- Passer's author
- Open source software author
  - Contributor, doc author, enthusiast
  - Many thanks for the shoulders!
- Teaching network security for decades

What's Passer?

- **Pas**sive **Ser**vice locator
  - Sniffer that identifies hosts, services, names, ports
  - Passive
  - Hands-off - no configuration
- Network sniffer
  - Interfaces or pcap files
- Non-interactive
  - Collects info for later use

It finds servers...

TS,36.110.185.107,TCP_80,listening,http://p/nginx/ v/1.6.0/ cpe:/a:igor_sysoev:nginx:1.6.0/

TS,37.1.208.56,TCP_80,listening,http://p/Apache httpd/ v/2.4.6/ i/(CentOS) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 PHP/5.4.16/ cpe:/a:apache:http_server:2.4.6/

US,1.255.106.60,UDP_53,open,dns/server

US,2a0a:1c01:0000:0001:0000:0000:0000:0020,UDP_53,open,dns/server

...Routers...

RO,fc00:0000:0000:0000:0000:0000:0000:0001,HostUn,router,

RO,fd80:0000:0000:0000:0000:0000:0afd:fd8e,HostUn,router,

RO,fe80:0000:0000:0000:f60e:83ff:febd:3bdc,NeighborAdvRouterFlag,router,

RO,fe80:0000:0000:0000:f60e:83ff:febd:3bdc,RouterAdv,router,hop_limit=64 net=2601:018c:4200:5998:0000:/64 dns=2001:0558:feed::1 dns=2001:0558:feed::2

RO,62.115.134.6,TTLEx,router,client_ip=172.17.0.29

...Clients...

TC,10.0.0.41,TCP_22,open,ssh/openssh

TC,2601:018c:4200:5998:2dc2:eab4:a9a4:4c92,TCP_80,open,

UC,71.6.199.23,UDP_520,open,rip/client

UC,172.104.30.252,UDP_19,open,chargen/client

...IOT devices...

DN,10.0.0.179,PTR,_printer._tcp.local.,

DN,10.0.0.179,SRV,Brother MFC-J5830DW._printer._tcp.local.,

DN,2601:018c:4200:5998:0000:0000:0000:8be7,AAAA,apple-tv.local.,

...malicious traffic...

IP,1.22.67.8,IP,suspicious,Warnings:malicious

IP,1.22.124.243,IP,suspicious,Warnings:portpolicyviolation

IP,5.79.65.7,IP,suspicious,Warnings:scan

UC,23.95.213.110,UDP_123,open,ntp/client REQ_MON_GETLIST_1: Likely spoofed and DDOSed source IP Warnings:amplification:spoofed

UC,37.49.231.38,UDP_5060,open,sipscanner/client From:100(1.1.1.1) To:100(1.1.1.1) Warnings:scan

...and Misc:

MA,2601:074c:1200:5998:0000:0000:0000:5f23,Ethernet,7C:01:91:A2:FD:6B,Apple

DN,172.217.8.174,A,www-google-analytics.l.google.com.,

DN,17.249.76.30,CNAME,1.courier-push-apple.com.akadns.net.,

DN,fe80:0000:0000:0000:08d9:63a9:1f6f:b248,PTR,Bart's iPad._device-info._tcp.local.,model=J81AP

Passer details

- Runs on Linux and Mac
- Uses python and the python Scapy library
- Read pcap file or listen on an interface
- Currently single process
  - Multiprocessor version in the works
  - Also extracts ASN and geoip info
- Needs a span port to see all traffic
  - Can still capture a lot on a normal port!

Install

- See https://github.com/activecm/passer/
  - Multiple ways to install
  - Docker is probably easiest
- Please get permission to sniff!
  - Home lab time!
    - https://www.youtube.com/watch?v=t7bhnK47Ygo

Passer output

- Comma separated
  - Deliberately basic
  - Easy to import into other tools

Output fields

```
TS,2001:146a:4000:0000:0000:0000:0000:0004,TCP_80,listening,http://p/nginx/ v/1.10.3/
i/Ubuntu/ o/Linux/ cpe:/a:igor_sysoev:nginx:1.10.3/ cpe:/o:linux:linux_kernel/a
```

- 2 character type
- IP address
- Protocol (TCP_*port* , UDP_*port*, or how do we know?)
- State (dead/alive/open/closed/listening/router)
- Description/details
  - Thanks to nmap for extracting many of the details!

Making use of the output

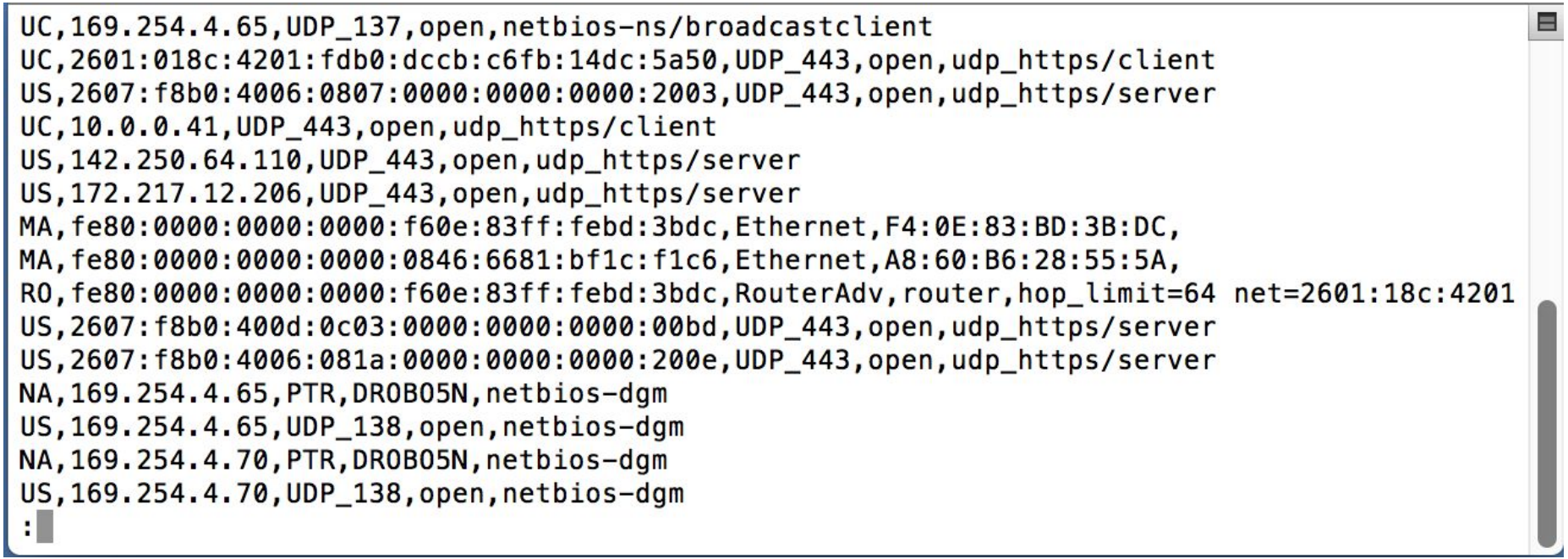
- Read from the command line
  - Group by IP
  - Only see certain record types
- Load into a spreadsheet
- Load into a database

Seeing a log file

```
wlsmacpro:sample-logs wstearns$ cat passer.log | head
UC,169.254.4.65,UDP_137,open,netbios-ns/broadcastclient
UC,2601:018c:4201:fdb0:dccb:c6fb:14dc:5a50,UDP_443,open,udp_https/client
US,2607:f8b0:4006:0807:0000:0000:0000:2003,UDP_443,open,udp_https/server
UC,10.0.0.41,UDP_443,open,udp_https/client
US,142.250.64.110,UDP_443,open,udp_https/server
US,172.217.12.206,UDP_443,open,udp_https/server
MA,fe80:0000:0000:0000:f60e:83ff:febd:3bdc,Ethernet,F4:0E:83:BD:3B:DC,
MA,fe80:0000:0000:0000:0846:6681:bf1c:f1c6,Ethernet,A8:60:B6:28:55:5A,
RO,fe80:0000:0000:0000:f60e:83ff:febd:3bdc,RouterAdv,router,hop_limit=64 net=2601:18c:4201
:fdb0::/64 dns=2001:558:feed::1 dns=2001:558:feed::2
US,2607:f8b0:400d:0c03:0000:0000:0000:00bd,UDP_443,open,udp_https/server
wlsmacpro:sample-logs wstearns$
```

Without line wrap

cat passer.log | less -S



Grouped by IP address

cat passer.log | sort -t, -k2 -u -V | less -S

```
DN,2a03:2880:f04f:000f:face:b00c:0000:0003,AAAA,scontent-bos3-1.xx.fbcdn.net.,
DN,2a03:2880:f04f:000f:face:b00c:0000:0003,AAAA,scontent.xx.fbcdn.net.,
DN,2a03:2880:f04f:000f:face:b00c:0000:0003,CNAME,connect.facebook.net.,
DN,2a03:2880:f04f:000f:face:b00c:0000:0003,CNAME,external-bos3-1.xx.fbcdn.net.,
DN,2a03:2880:f04f:000f:face:b00c:0000:0003,CNAME,static.xx.fbcdn.net.,
DN,2a03:2880:f04f:000f:face:b00c:0000:0003,PTR,xx-fbcdn6-shv-01-bos3.fbcdn.net.,
TS,2a03:2880:f04f:000f:face:b00c:0000:0003,TCP_443,listening,
TS,2a03:2880:f04f:000f:face:b00c:0000:0003,TCP_443,listening,ssl://p/TLSv1.2/
DN,2a03:2880:f04f:0009:face:b00c:0000:1823,AAAA,video-bos3-1.xx.fbcdn.net.,
DN,2a03:2880:f04f:0009:face:b00c:0000:1823,PTR,edge-video6-shv-01-bos3.fbcdn.net.,
TS,2a03:2880:f04f:0009:face:b00c:0000:1823,TCP_443,listening,
TS,2a03:2880:f04f:0009:face:b00c:0000:1823,TCP_443,listening,ssl://p/TLSv1.2/
DN,2a03:2880:f04f:0011:face:b00c:0000:0002,AAAA,star.c10r.facebook.com.,
DN,2a03:2880:f04f:0011:face:b00c:0000:0002,CNAME,api.facebook.com.,
DN,2a03:2880:f04f:0011:face:b00c:0000:0002,CNAME,edge-chat.facebook.com.,
:
```

Only a few IP addresses

cat passer.log | sort -t, -k2 -u -V | grep ',10.0.0.17' | less -S

```
UC,10.0.0.176,UDP_5353,open,mdns/client
DN,10.0.0.179,A,brwf8da0c339ce8.local.,
DN,10.0.0.179,PTR,Brother MFC-J5830DW._ipp._tcp.local.,['txtvers=1'  'qtotal=1'  'pdl=appl
DN,10.0.0.179,PTR,Brother MFC-J5830DW._pdl-datastream._tcp.local.,['txtvers=1'  'qtotal=1'
DN,10.0.0.179,PTR,Brother MFC-J5830DW._printer._tcp.local.,['txtvers=1'  'qtotal=1'  'pdl=
DN,10.0.0.179,PTR,Brother MFC-J5830DW._privet._tcp.local.,['txtvers=1'  'ty=Brother MFC-J5
DN,10.0.0.179,PTR,Brother MFC-J5830DW._scanner._tcp.local.,['txtvers=1'  'note='  'adminur
DN,10.0.0.179,PTR,_ipp._tcp.local.,brother mfc-j5830dw._ipp._tcp.local.
DN,10.0.0.179,PTR,_pdl-datastream._tcp.local.,brother mfc-j5830dw._pdl-datastream._tcp.loc
DN,10.0.0.179,PTR,_printer._tcp.local.,brother mfc-j5830dw._printer._tcp.local.
DN,10.0.0.179,PTR,_privet._tcp.local.,brother mfc-j5830dw._privet._tcp.local.
DN,10.0.0.179,PTR,_scanner._tcp.local.,brother mfc-j5830dw._scanner._tcp.local.
DN,10.0.0.179,PTR,_uscan._tcp.local.,brother mfc-j5830dw._uscan._tcp.local.
US,10.0.0.179,UDP_5353,open,mdns/server
(END)
```

TCP services on your net

cat passer.log | grep '^TS,' | grep ',10\.' | less

```
TS,10.0.0.41,TCP_49167,listening,
TS,10.0.0.179,TCP_515,listening,printer/server not confirmed
TS,10.0.0.179,TCP_9100,listening,pdl-datastream/server not confirmed
TS,10.0.0.179,TCP_80,listening,http/server not confirmed
TS,10.0.0.179,TCP_9100,listening,hp-pdl-datastr/server not confirmed
TS,10.0.0.179,TCP_631,listening,ipp/server not confirmed
(END)
```

Open UDP services on your net

cat passer.log | grep '^US,' | grep ',10\.' | grep ,open, | less

```
US,10.0.0.179,UDP_5353,open,mdns/server
US,10.0.0.235,UDP_138,open,netbios-dgm
US,10.0.0.234,UDP_138,open,netbios-dgm
US,10.0.0.18,UDP_5353,open,mdns/server
US,10.0.0.41,UDP_5353,open,mdns/server
US,10.0.0.1,UDP_67,open,bootpordhcp/server
US,10.0.0.176,UDP_5353,open,mdns/server
US,10.0.0.41,UDP_123,open,ntp/server stratum=2 reference=17.253.14.253
US,10.0.0.41,UDP_123,open,ntp/server stratum=0
US,10.0.0.239,UDP_5353,open,mdns/server
US,10.0.0.41,UDP_1194,open,openvpn/server Warnings:tunnel
(END)
```

Netbios hosts

```
wlsmacpro:sample-logs wstearns$ grep '^NA,' passer.log | sort -t, -k2 -u -V
NA,10.0.0.41,DHCP,wlsmacpro,dhcp
NA,10.0.0.234,PTR,SECONDARY,netbios-dgm
NA,10.0.0.235,PTR,SECONDARY,netbios-dgm
NA,169.254.4.65,PTR,DROBO5N,netbios-dgm
NA,169.254.4.70,PTR,DROBO5N,netbios-dgm
NA,169.254.5.153,PTR,SECONDARY,netbios-dgm
NA,169.254.5.158,PTR,SECONDARY,netbios-dgm
wlsmacpro:sample-logs wstearns$
```

DNS records galore

grep -hai '^DN,' *.log | sort -t, -k2 -u -V | less

```
DN,17.125.250.130,PTR,umc-tempo-api.apple.com.,
DN,17.125.250.130,PTR,wohgzwksqbabyymatmpppqyxxldoovqk.apple.com.,
DN,17.137.160.100,A,supportmetrics.apple-support.akadns.net.,
DN,17.137.160.100,CNAME,supportmetrics.apple.com.,
DN,17.137.166.35,A,gsas.apple.com.akadns.net.,
DN,17.137.166.35,CNAME,gsas.apple.com.,
DN,17.142.160.59,A,appleid.org.,
DN,17.142.160.59,A,apple.com.,
DN,17.142.160.59,A,pv-apple-com.apple.com.,
DN,17.142.160.59,PTR,appleid.org.,
DN,17.142.160.59,PTR,apple.by.,
DN,17.142.160.59,PTR,apple.com.,
DN,17.142.160.59,PTR,ipad.host.,
DN,17.142.160.59,PTR,pv-apple-com.apple.com.,
DN,17.151.240.53,A,gsa.apple.com.akadns.net.,
:
```

Routers

grep -hai '^RO,' passer.log | sort -t, -k2 -u -V | less

```
RO,10.0.0.1,RouterAdv,router,
RO,10.0.0.1,TTLEx,router,client_ip=10.0.0.41
RO,10.250.3.77,TTLEx,router,client_ip=10.0.0.41
RO,12.11.59.18,TTLEx,router,client_ip=10.0.0.41
RO,12.16.164.180,HostUn,router,client_ip=10.0.0.41
RO,12.83.170.17,TTLEx,router,client_ip=10.0.0.41
RO,12.83.179.193,TTLEx,router,client_ip=10.0.0.41
RO,12.83.185.166,TTLEx,router,client_ip=10.0.0.41
RO,12.83.186.189,TTLEx,router,client_ip=10.0.0.41
RO,12.83.188.241,TTLEx,router,client_ip=10.0.0.41
RO,12.86.131.54,TTLEx,router,client_ip=10.0.0.41
RO,12.89.72.82,TTLEx,router,client_ip=10.0.0.41
RO,12.89.88.70,TTLEx,router,client_ip=10.0.0.41
RO,12.90.96.26,TTLEx,router,client_ip=10.0.0.41
RO,12.90.125.194,TTLEx,router,client_ip=10.0.0.41
:
```

Sample malicious traffic lines

```
UC,5.180.211.73,UDP_53,open,dns/client ANY domains requested:isc.org. Warnings:amplificati
UC,45.79.106.170,UDP_4500,open,esp/client Warnings:scan:tunnel
TC,47.92.55.104,TCP_22,open,TCP SYN/FIN flag scanner Warnings:noncompliant:scan
TC,61.191.50.227,TCP_445,open,TCP SYN/RST flag scanner Warnings:noncompliant:scan
UC,71.6.146.186,UDP_69,open,tftp/client Warnings:plaintext:portpolicyviolation
UC,83.97.20.164,UDP_53,open,dns/client ANY domains requested:census.gov. Warnings:amplific
IP,87.251.74.18,IP,suspicious,Scanned TCP closed ports. Warnings:scan
TC,107.172.197.123,TCP_23,open,Warnings:portpolicyviolation
UC,167.71.110.14,UDP_4500,open,esp/client Warnings:tunnel
UC,172.105.6.55,UDP_53,open,dns/client ANY domains requested:mz.gov.pl. Warnings:amplifica
UC,185.200.118.38,UDP_1194,open,openvpn/client Warnings:tunnel
UC,185.232.64.121,UDP_53,open,dns/client ANY domains requested:cpsc.gov. Warnings:amplific
TC,218.161.106.8,TCP_50533,open,TCP Null flag scanner Warnings:noncompliant:scan
(END)
```

Importing into a spreadsheet

- Use "Import CSV file"
  - Specify comma as field separator
  - May require a .csv extension
- Live example of import
  - Sample search
  - Sample sort
- Should work with any spreadsheet

Importing into a database

- Should work fine
  - Again, import as CSV
  - Specify comma as separator
  - Each line is an individual record

Additional output

- Malicious IP pcap
  - --suspicious *suspicious.pcap*
  - *After* host is flagged, capture all traffic
- Show timestamp
  - --timestamp
  - 2 columns added

Performance

- Can be slow
  - Mitigate with BPF for the data you need
    - See github site for examples
  - Multiprocessor version in progress
  - Can post-process pcaps
- Losing packets isn't fatal

Chew through a pcap!

- Grab a pcap from an incident
- passer.py -r *incident1*.pcap -l *incident1*.csv
  - Review the output
  - Open ports on the system in question?
  - Incoming scans and malicious probes?

System inventory

- Live machines
- Open services
  - And versions
- Great for a quick reference

Passer_ng

- Multiprocess
  - Spread out the load
- ASN data
- Geoip data
- Optional active mode
  - Multiple traceroute processes
  - Active DNS lookups
- Still missing some plumbing!

Passer's history

- Sniff.py
  - Jan 22, 2008: 132 bytes
  - What's the goal?

```
#!/usr/bin/python


import dpkt, pcap
pc = pcap.pcap()
pc.setfilter('icmp')
for ts,pkt in pc:
        print `dpkt.ethernet.Ethernet(pkt)`

sniff.py.080122.\~2\~ (END)
```

Found a goal

- Network security class with a pcap file
  - Student labs
    - What machine is a mail server?
    - Who's port scanning?
  - Could we do these automatically?
  - Of course we can. :-)
- Final goal:
  - What can we learn from network packets?

Thanks!

- Chris, Ethan, Shelby, KC, Jason, Keith
- All the passer contributors and users!

Where to find it

- https://github.com/activecm/passer
- http://www.stearns.org/passer/
- william.l.stearns@gmail.com
- **Threat Hunter Community Discord**
  - **https://discord.gg/FXdKdu**
  - **#passer channel**