ZEEK ON A RASPBERRY PI

My experiences

THANKS FOR THE IDEA

- I got the idea from Bill Stearns. The original talk is found here: https://www.youtube.com/watch?v=vja_H59fh1I&feature=youtu.be
- After the talk they setup a Q&A site which can be found at
- https://www.activecountermeasures.com/raspberry-pi-network-sensor-webinar-qa/
- Shopping list for parts:
- https://www.activecountermeasures.com/raspberry_pi_sensor/Raspberry%20Pi%20network%20sensor%20shopping%20list.pdf

WHY?

GAIN KNOWLEDGE OF RASPBERRY PI

GAIN INSIGHT AS TO WHAT IS TRAVERSING MY NETWORK

GAIN KNOWLEDGE OF ZEEK

NETWORK TAP

- The network tap is a netgear 5 port managed switch (GS305E) about $25 dollars on amazon.
- Configure port mirror so all data that arrives on Port 1 is sent out Port 5

LOCATION TO PLACE THE TAP

- Varies depending on what you want to look at.
- Generally you will want to find a "choke point" on the network to put this.
- I placed mine between the cable modem and my Wifi access point. All network traffic from all devices must pass through this.

SETUP RASPBERRY PI

- Originally purchased the 4GB Raspberry Pi
- Updated to the 8GB Raspberry Pi
- Purchased the canakit that comes with SD card, case fan and heatsinks
- Assembled the kit and installed OS

INSTALL ZEEK

- After installing and updating OS install zeek.
- Sudo apt install bro broctl

CONFIGURE NIC

- Configure network port to listen in promiscuous mode
- Place the following lines in /etc/network/interfaces
- auto eth0
- iface eth0 inet manual
- up ifconfig 0.0.0.0 up
- up ip link set eth0 promisc on
- down ip link set eth0 promisc off
- down ip link set eth0 down

CONFIGURE NIC

- Add the following to not get an IP address for sniffing NIC
- This is added in /etc/dhcpcd.conf
- denyinterfaces eth0

CONFIGURE TO START AT BOOT

- These need to be added in /etc/rc.local
- screen -S capture -t capture -d -m bash -c "nice -n 15 tcpdump -i eth0 -G 3600 -w '/opt/bro/pcaps/'`hostname -s`'.%Y%m%d%H%M%S.pcap' -z bzip2 '((tcp[13] & 0x17 != 0x10) or not tcp) and (port 53 or not ((src net 10.0.0.0/8 or src net 172.16.0.0/12 or src net 192.168.0.0/16 or src net 169.254.0.0/16) and (dst net 10.0.0.0/8 or dst net 172.16.0.0/12 or dst net 192.168.0.0/16 or dst net 169.254.0.0/16)))'"

- /usr/bin/broctl deploy

SETUP THE EASY WAY

- Run the scripts found in the zip found at https://www.activecountermeasures.com/raspberry_pi_sensor/

ZEEK LOG FILES

Zeek creates various log files ones I have found useful

DNS.log

File.log

Conn.log

X509.log

DNS.LOG

- #fields ts uid id.orig_h id.orig_p id.resp_h id.resp_p proto trans_id rtt query qclass qclass_name qtype qtype_name rcode rcode_name AA TC RD RA Z answers TTLs rejected

- Useful fields
- Id.orig_h - Host that made the request
- Query – Dns request
- Qtype – type of query
- Answers – the response to the query

DNS.LOG

- Useful queries
- bro-cut -d query qtype_name rcode_name answers

```
104 thind-gke-usc.prd.data.corp.unity3d.com AAAA    NOERROR -
107 time-ios.g.aaplimg.com  AAAA    NOERROR -
109 logsink.devices.nest.com        A       NOERROR 35.190.54.210
116 cdn01.x-plarium.com     AAAA    NOERROR cs523.wac.zetacdn.net,2606:2800:220:26c6:9f4:104b:1f83:10e7
116 cdn01.x-plarium.com     A       NOERROR cs523.wac.zetacdn.net,192.229.163.97
126 cdp.cloud.unity3d.com   AAAA    NOERROR prd-lender.cdp.internal.unity3d.com,thind-prd-knob.data.ie.unity3d.com,thind-gke-usc.prd.data.corp.unity3d.com
126 cdp.cloud.unity3d.com   A       NOERROR prd-lender.cdp.internal.unity3d.com,thind-prd-knob.data.ie.unity3d.com,thind-gke-usc.prd.data.corp.unity3d.com,35.241.52.229
137 rdint1s04.plrm.zone     A       NOERROR 173.244.180.74
142 www-cdn.icloud.com.akadns.net   AAAA    NOERROR www.icloud.com.edgekey.net,e4478.a.akamaiedge.net
144 weave-logsink.nest.com  A       NOERROR 35.188.154.186
```

CONN.LOG

- #fields ts uid id.orig_h id.orig_p id.resp_h id.resp_p proto service duration orig_bytes resp_bytes conn_state local_orig local_resp missed_bytes history orig_pkts orig_ip_bytes resp_pkts resp_ip_bytes tunnel_parents

- Useful fields
- Id.orig_h
- Id.orig_p
- Id.resp_h
- Id.resp_p
- Proto
- service
- duration

CONN.LOG

- Useful Query
- bro-cut id.orig_h id.resp_h id.resp_p proto service
- Screen shot is missing id.orig_h

ISSUES I RAN INTO

- Don't put your hard drive over the fan opening on the raspberry PI.
- Make sure you know how to connect to the raspberry pi after it is installed.

WHERE TO GO FROM HERE?

- Import the data that zeek captures into something for analysis
- Elastic search
- Rita (find beacons in the data)

QUESTIONS?

- A pdf of this can be found on my github at