Please start your VMs and replay honc-baseline.pcap

```
sudo tcpreplay -i eth1 –M20 honc-baseline.pcap
```

CHIRON
TRAINING

Hands on Network Characterization

@hashtagcyber
BSides Jackson – 12NOV16

DISCOVERY AND COUNTER-INFILTRATION PROFESSIONAL™ (DCIP)™

Hands on Network Characterization

Please start your VMs and replay Baseline.pcap

```
sudo tcpreplay -i eth1 –M10 Baseline.pcap
```

About Me

- Keep it short
  - Infosec Instructor
  - Motorcycle Enthusiast
  - <3 Blue Team
- Thanks to
  - My Ginger
  - @Killswitch_GUI
  - @Chirontech
  - Attendees and Organizers

Do This

```
sudo tcpreplay -i eth1 -M10 Baseline.pcap
```

TLDR; What’s in it for me?

10 minutes	What’s a network baseline?
5 minutes	Scenario Network
10 minutes	SecurityOnion Basics
***10 minutes**	**ELSA, Bro, and Bro Scripts**
***30 minutes**	**Building the baseline “database”**
***10 minutes**	**Installing baselinereport.bro**
***30 minutes**	**Analyze honc-malicious.pcap**
10 minutes	Review Attacker actions
10 minutes	Questions

*denotes lab time
or watch me demo if you don’t have a laptop

Why I'm Here

- "Bad Guys" are clever
- Blacklisting doesn't catch everything
- SNORT rules only work if a signature exists

What else can I do?

Whitelisting!

- But…
  - Services can't go down "because security"
  - "I'm undermanned in <insert> department"
  - Baselines are hard to write

Baselines are hard

- What can go in a baseline?
  - Operating System version
  - Authorized Software
    - Software Versions
    - File Hashes
  - Authorized Users
  - Operating hours
  - Bandwidth utilization
  - Processor/Disk/Memory usage
  - Incoming Ports/Protocols
  - Source/Destination addresses
  - Application utilizing sockets
  - Outgoing connections
- Soooo much data, let's focus on networking

My Goals for a Network Baseline

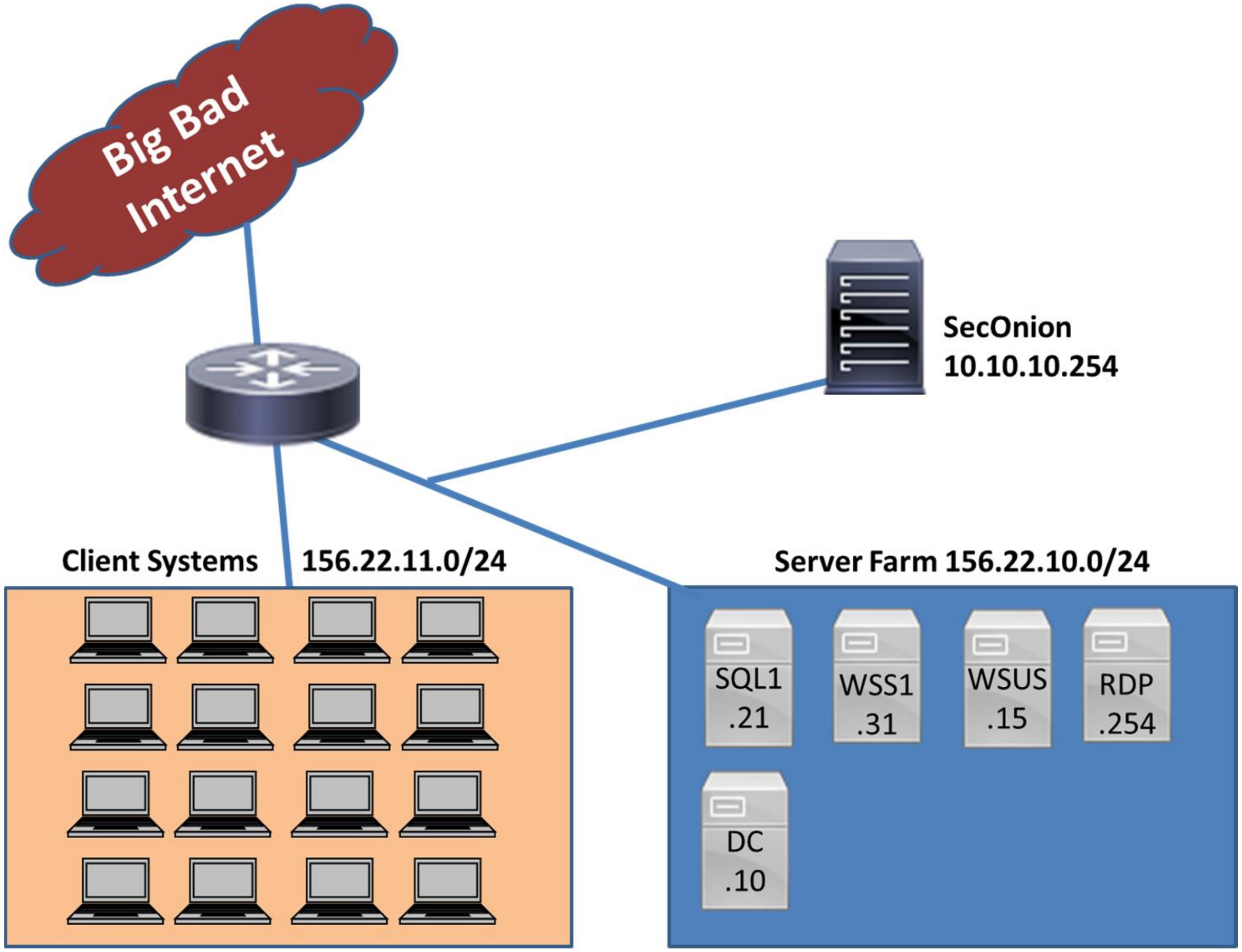
- Focus on key business assets
- Focus on high risk areas
- Start with one segment/subnet and grow

- Data I need to start:
  - Host address
  - Host purpose
    - DC, Exchange MB, Web, SQL, etc.

- Data I can generate:
  - Listening Ports
  - Expected Client Addresses
  - Destination Addresses
  - Destination Ports

CHIRON TRAINING

Scenario Network



Scenario Goals

- Perform a network baseline of all hosts within the server farm.
- Key Business Assets:
  - Sharepoint Farm (SQL1, WSS1)
  - Domain Controller (DC)
- Give SOC the ability to react to unexpected incoming connections to Key Assets
- How?
  - Enter SecurityOnion

Security Onion

- TLDR; SecurityOnion is awesome
  - Thanks Doug Burks and everyone else that works on the project
  - Lot’s of built in network monitoring tools that JUST WORK
    - BRO – Tracks/Logs connections, alerts over time, packet string
    - SNORT – Signature based IDS
    - ELSA – Ingests alerts/logs for searching
    - SGUIL – GUI for accessing SNORT Alerts
    - Many many more

Last Chance

Start VMs!

- In Security Onion:
  - Open a shell
  - Run TCPReplay against honc-baseline.pcap and your monitoring interface

```
sudo tcpreplay –i eth1 –M30 honc-baseline.pcap
```

ELSA Demo

- Useful search terms:
  - Show all notice’s generated by baselinereport
    - class=BRO_NOTICE "-" notice_type="TrafficBaselineException“
  - Show all connections to an IP, grouped by destination port
    - BRO_CONN.dstip=156.22.10.10 groupby:dstport
  - Show all connection to an IP/Port pair grouped by source IP
    - *BRO_CONN.dstip=156.22.10.10 BRO_CONN.dstport=445 groupby:srcip*

Bro Demo

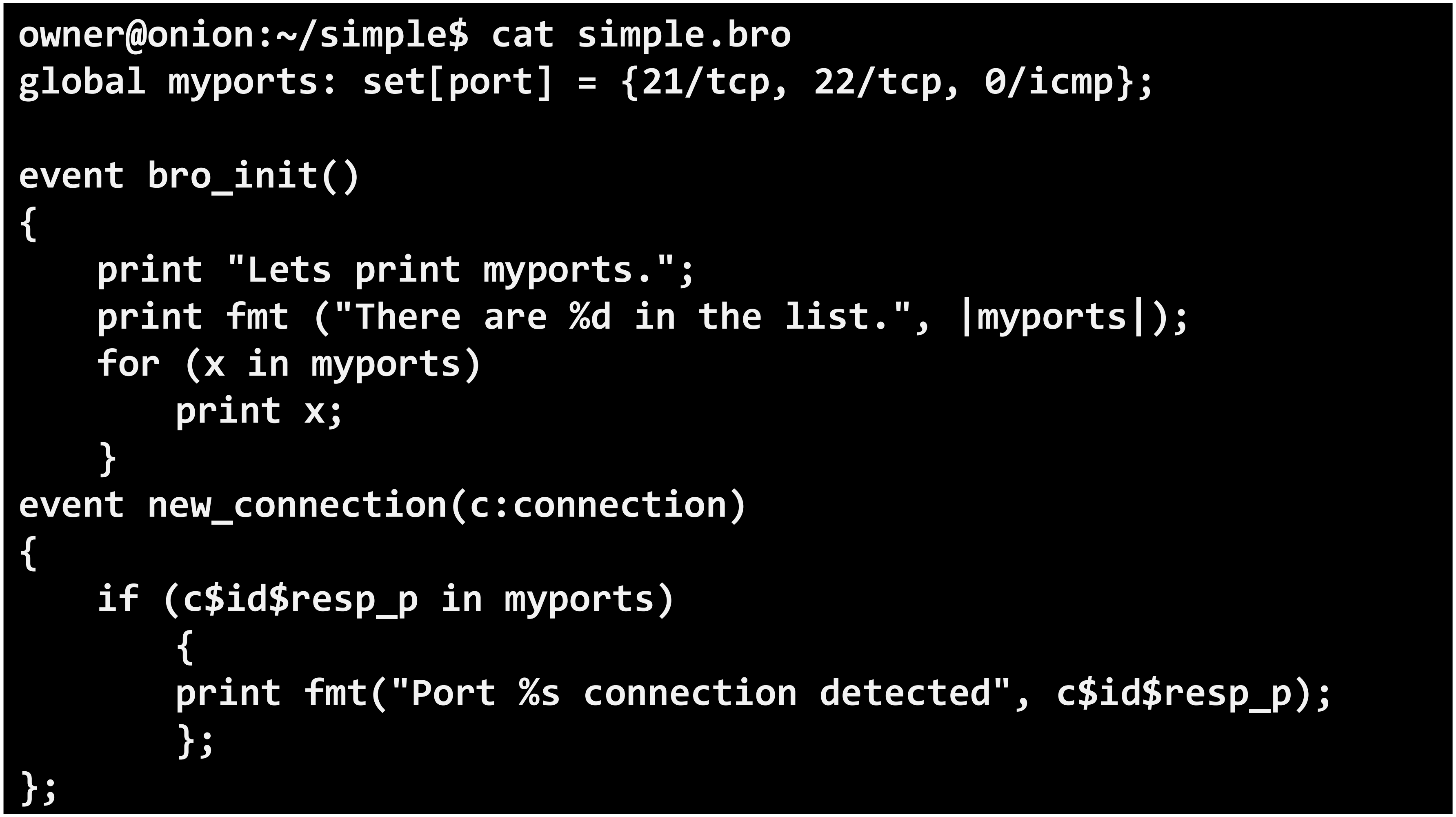
- Key Directories:
  - /nsm/bro/logs/current
    - notices.log
    - conn.log
    - weird.log
  - /opt/bro/share/bro/policy
    - Contains scripts loaded by Bro
  - /opt/bro/share/bro/site/local.bro
    - Add path to custom scripts to this file to load when bro starts

Bro Scripts

"The best way to learn to write Bro scripts, is to write Bro scripts"

– Seth Hall, SecurityOnion Conference 2015

A Simple Bro Script



```
owner@onion:~/simple$ cat simple.bro
global myports: set[port] = {21/tcp, 22/tcp, 0/icmp};

event bro_init()
{
    print "Lets print myports.";
    print fmt ("There are %d in the list.", |myports|);
    for (x in myports)
        print x;
    }
event new_connection(c:connection)
{
    if (c$id$resp_p in myports)
        {
        print fmt("Port %s connection detected", c$id$resp_p);
        };
};
```

baselinereport.bro

- Create a list of hosts that are baselined:

```
global protected: set[subnet] = {156.22.10.0/24,10.246.50.0/24};
```

- Import a table containing the baseline from a file:

```
    Input::add_table([$source="baseline.data", $name="hosts", $idx=Idx,
$val=Val, $destination=hosts]);
```

- Check if the destination host is baselined:

```
if ([c$id$resp_h] in protected)
```

- If it is, check the table to see if the source is authorized on that port:

```
if (c$id$orig_h !in hosts[c$id$resp_h,c$id$resp_p]$ips)
```

“Installing” the script

- Copy the script and baseline.data file to the scripts dir

```
# cp baseline* /opt/bro/share/bro/policy/misc/
```

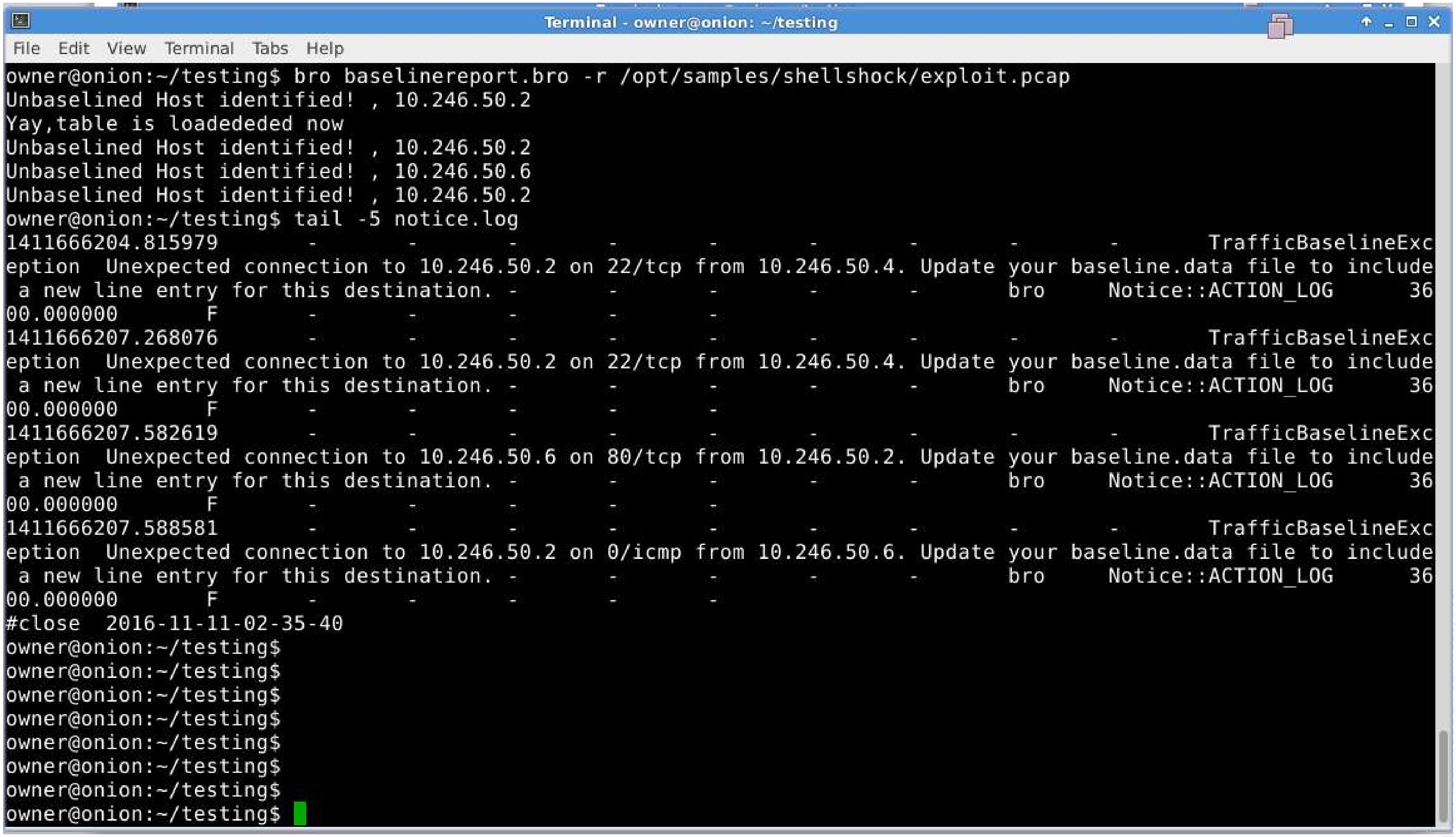
- Add the script name to local.bro to ensure it gets loaded

```
# vi /opt/bro/share/bro/site/local.bro
@load misc/baselinereport.bro
```

- Restart Bro (I’m lazy)

```
# nsm_sensor_ps-restart
```

Testing and Results


Terminal - owner@onion: ~/testing
File Edit View Terminal Tabs Help

```
owner@onion:~/testing$ bro baselinereport.bro -r /opt/samples/shellshock/exploit.pcap
Unbaselined Host identified! , 10.246.50.2
Yay,table is loadededed now
Unbaselined Host identified! , 10.246.50.2
Unbaselined Host identified! , 10.246.50.6
Unbaselined Host identified! , 10.246.50.2
owner@onion:~/testing$ tail -5 notice.log
1411666204.815979       -       -       -       -       -       -       -       -       -       TrafficBaselineExc
eption  Unexpected connection to 10.246.50.2 on 22/tcp from 10.246.50.4. Update your baseline.data file to include
 a new line entry for this destination. -       -       -       -       -       bro     Notice::ACTION_LOG      36
00.000000       F       -       -       -       -       -
1411666207.268076       -       -       -       -       -       -       -       -       -       TrafficBaselineExc
eption  Unexpected connection to 10.246.50.2 on 22/tcp from 10.246.50.4. Update your baseline.data file to include
 a new line entry for this destination. -       -       -       -       -       bro     Notice::ACTION_LOG      36
00.000000       F       -       -       -       -       -
1411666207.582619       -       -       -       -       -       -       -       -       -       TrafficBaselineExc
eption  Unexpected connection to 10.246.50.6 on 80/tcp from 10.246.50.2. Update your baseline.data file to include
 a new line entry for this destination. -       -       -       -       -       bro     Notice::ACTION_LOG      36
00.000000       F       -       -       -       -       -
1411666207.588581       -       -       -       -       -       -       -       -       -       TrafficBaselineExc
eption  Unexpected connection to 10.246.50.2 on 0/icmp from 10.246.50.6. Update your baseline.data file to include
 a new line entry for this destination. -       -       -       -       -       bro     Notice::ACTION_LOG      36
00.000000       F       -       -       -       -       -
#close  2016-11-11-02-35-40
owner@onion:~/testing$
owner@onion:~/testing$
owner@onion:~/testing$
owner@onion:~/testing$
owner@onion:~/testing$
owner@onion:~/testing$
owner@onion:~/testing$
owner@onion:~/testing$
```

Lab Time : Complete the Baseline

- Complete the baseline
  - DC is already done

Lab Review: My Complete Baseline

Fun Times : What happened?

- Extract honc-malicious.zip
  - Zip Password: bsides
- TCPReplay

```
sudo tcpreplay -i eth1 -M20 honc-malicious.pcap
```

- Write down the story
  - Yes, you can use other tools, but try sticking to Bro and ELSA

Lab Review: Attacker Actions

- Successfully exploited web browser of an admin that was logged in and browsing the internet
- Dumped passwords
- Identified local webserver that may be of some use…
- Gained access to webserver using stolen creds
- Configured bind shell on webserver for easy access
- Profit?

Lab Review: Evidence in PCAP

CHIRON TRAINING

Questions?