Intro to Bro

Sean Cochran

$whoami

- KCMO #midwestisbest
- 18 Years MOARNG
- RockNSM Contributor
- breaker and builder of things

sean@perched.io @seven62

Brandon DeVault

$whoami

Panama City, FL

10 Years FL Air National Guard

AOC Mission Defense Team

Former JCSE/JCU

Perched

linkedin.com/in/brandondevault

@Oofles

brandon@perched.io

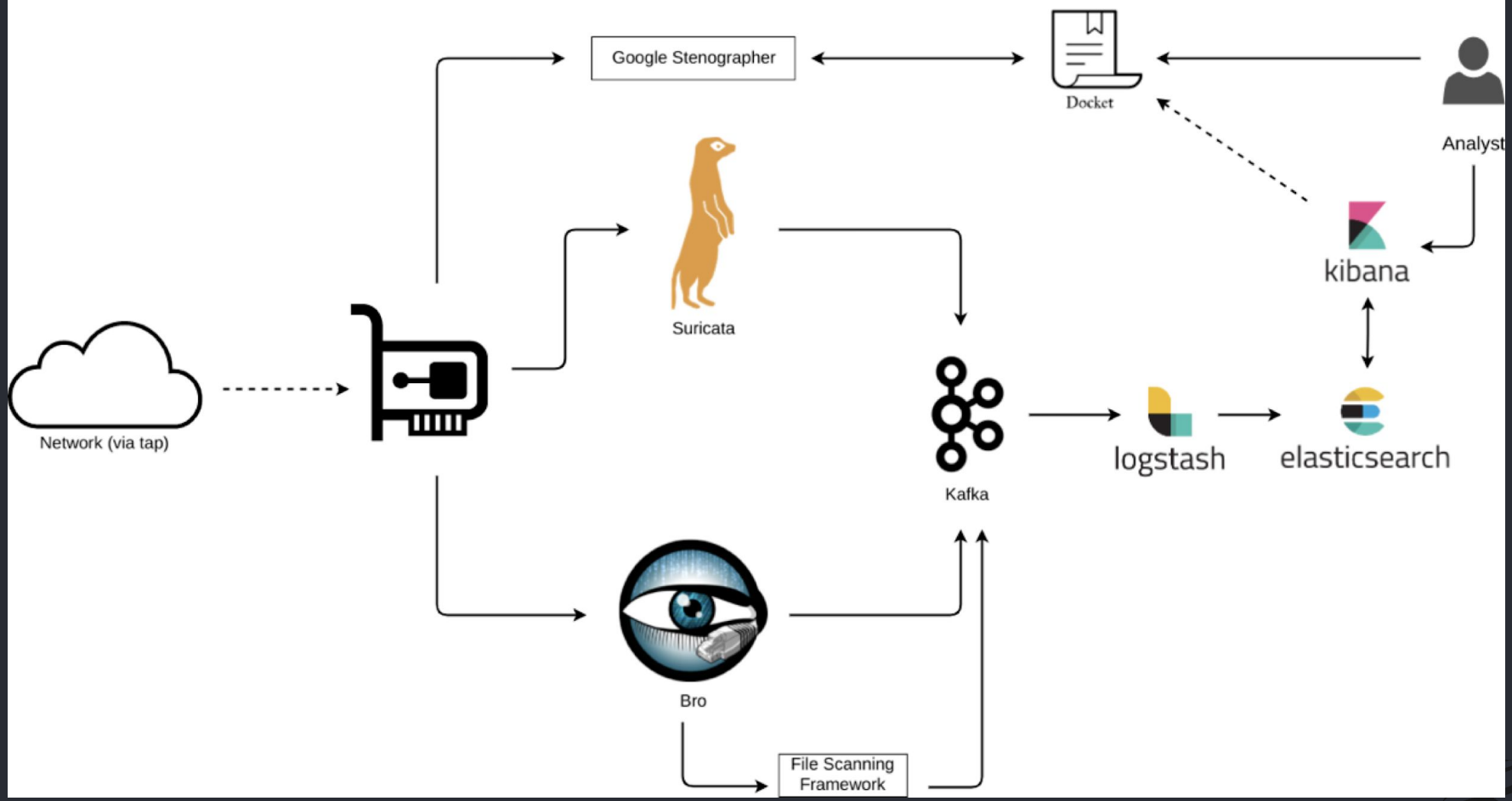
Johnathon Hall

- 7 years active duty Navy
- Creator of the Navy's tactical Kit
- Private sector fortune 200 company
- Self employed consulting
- RockNSM contributor
- Perched


linkedin.com/in/johnathon-hall


@spartan782


johnathon@perched.io



Day 1 Outline

- What is Bro?
- PCAP vs Bro
- ASCII Bro Logs
- IDS, Scripting Language, or Protocol analyzer?
- Bro-Cut

Bro

- protocol and metadata analysis
- actually stands for Big Brother

Discussion Time

- what are network logs?
- what are host based logs?
- which is more important?

Discussion Time

- active analysis
- passive analysis
- which one should you use?

Typical Network log data

- packet captures (PCAP)
- alerts
- session and protocol metadata logs

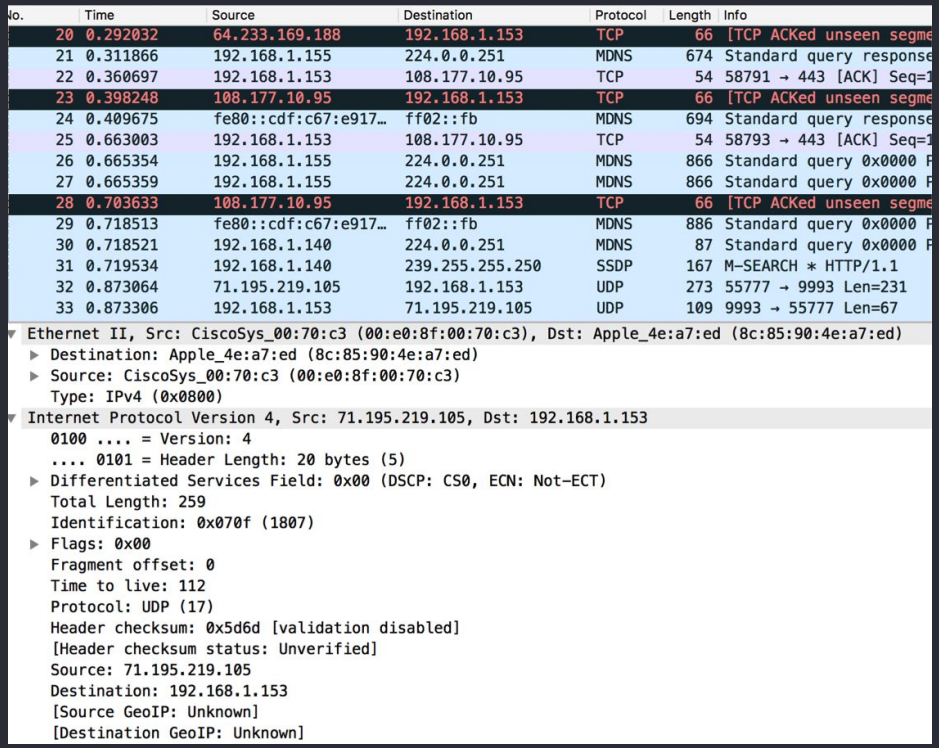
Discussion Time

- what type of data would provide the most value?

PCAP

- obtained via stenographer
- very detailed and verbose
- hard to search through and find anomalies

PCAP



No.	Time	Source	Destination	Protocol	Length	Info
20	0.292032	64.233.169.188	192.168.1.153	TCP	66	[TCP ACKed unseen segme
21	0.311866	192.168.1.155	224.0.0.251	MDNS	674	Standard query response
22	0.360697	192.168.1.153	108.177.10.95	TCP	54	58791 → 443 [ACK] Seq=1
23	0.398248	108.177.10.95	192.168.1.153	TCP	66	[TCP ACKed unseen segme
24	0.409675	fe80::cdf:c67:e917…	ff02::fb	MDNS	694	Standard query response
25	0.663003	192.168.1.153	108.177.10.95	TCP	54	58793 → 443 [ACK] Seq=1
26	0.665354	192.168.1.155	224.0.0.251	MDNS	866	Standard query 0x0000 P
27	0.665359	192.168.1.155	224.0.0.251	MDNS	866	Standard query 0x0000 P
28	0.703633	108.177.10.95	192.168.1.153	TCP	66	[TCP ACKed unseen segme
29	0.718513	fe80::cdf:c67:e917…	ff02::fb	MDNS	886	Standard query 0x0000 P
30	0.718521	192.168.1.140	224.0.0.251	MDNS	87	Standard query 0x0000 P
31	0.719534	192.168.1.140	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
32	0.873064	71.195.219.105	192.168.1.153	UDP	273	55777 → 9993 Len=231
33	0.873306	192.168.1.153	71.195.219.105	UDP	109	9993 → 55777 Len=67

```
▼ Ethernet II, Src: CiscoSys_00:70:c3 (00:e0:8f:00:70:c3), Dst: Apple_4e:a7:ed (8c:85:90:4e:a7:ed)
  ▶ Destination: Apple_4e:a7:ed (8c:85:90:4e:a7:ed)
  ▶ Source: CiscoSys_00:70:c3 (00:e0:8f:00:70:c3)
    Type: IPv4 (0x0800)
▼ Internet Protocol Version 4, Src: 71.195.219.105, Dst: 192.168.1.153
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 259
    Identification: 0x070f (1807)
  ▶ Flags: 0x00
    Fragment offset: 0
    Time to live: 112
    Protocol: UDP (17)
    Header checksum: 0x5d6d [validation disabled]
    [Header checksum status: Unverified]
    Source: 71.195.219.105
    Destination: 192.168.1.153
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
```

Alerts

- obtained via Suricata or Snort (interchangeable)
- very small portion of the actual network traffic
- may cause false positives
- ideal for already ”known bad” traffic

Suricata Alert

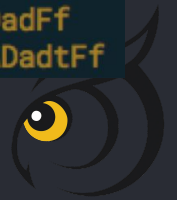
```
Count:1 Event#3.13546 2016-04-15 23:34:01
ETPRO CURRENT_EVENTS Successful Paypal Phish Dec 8 M2
172.16.155.149 -> 91.194.91.203
IPVer=4 hlen=5 tos=0 dlen=634 ID=0 flags=0 offset=0 ttl=0 chksum=47435
Protocol: 6 sport=49273 -> dport=80

Seq=0 Ack=0 Off=5 Res=0 Flags=******** Win=0 urp=3 chksum=0
--------------------------------------------------------------------------
Count:1 Event#3.13547 2016-04-15 23:34:01
ETPRO CURRENT_EVENTS Successful Paypal Phish Mar 14
172.16.155.149 -> 91.194.91.203
IPVer=4 hlen=5 tos=0 dlen=634 ID=0 flags=0 offset=0 ttl=0 chksum=47435
Protocol: 6 sport=49273 -> dport=80

Seq=0 Ack=0 Off=5 Res=0 Flags=******** Win=0 urp=3 chksum=0
--------------------------------------------------------------------------
Count:1 Event#3.13550 2016-04-15 23:34:44
ETPRO CURRENT_EVENTS Successful Paypal Phish Dec 8 M3
172.16.155.149 -> 91.194.91.203
IPVer=4 hlen=5 tos=0 dlen=806 ID=0 flags=0 offset=0 ttl=0 chksum=47263
Protocol: 6 sport=49279 -> dport=80

Seq=0 Ack=0 Off=5 Res=0 Flags=******** Win=0 urp=9886 chksum=0
--------------------------------------------------------------------------
Count:1 Event#3.13552 2016-04-15 23:36:14
ETPRO CURRENT_EVENTS Successful Paypal Phish Dec 8 M4
172.16.155.149 -> 91.194.91.203
IPVer=4 hlen=5 tos=0 dlen=1005 ID=0 flags=0 offset=0 ttl=0 chksum=47064
Protocol: 6 sport=49280 -> dport=80

Seq=0 Ack=0 Off=5 Res=0 Flags=******** Win=0 urp=40687 chksum=0
--------------------------------------------------------------------------
Count:1 Event#3.13554 2016-04-15 23:37:47
ETPRO CURRENT_EVENTS Successful Paypal Phish Dec 8 M4
172.16.155.149 -> 91.194.91.203
IPVer=4 hlen=5 tos=0 dlen=909 ID=0 flags=0 offset=0 ttl=0 chksum=47160
Protocol: 6 sport=49282 -> dport=80

Seq=0 Ack=0 Off=5 Res=0 Flags=******** Win=0 urp=7451 chksum=0
```

Bro Logs - session & protocol metadata

- analyzes Network data and creates a session log
- uses the terms Originator and Responder
  - Originator ≠ Source
  - Responder ≠ Destination
- used to construct full timeline of events
- see the bigger picture

Bro Logs

```
#ts  uid  id_orig_h  id_orig_p  id_resp_h  id_resp_p  proto  service  history
#time  string  addr  port  addr  port  enum  string  string
1492901992.641214  CfnJ3D1TjbmomafHWf  192.168.10.15  58501  172.217.12.69  443  tcp  ssl  ShADadtFf
1492901993.626358  C6ngJt36P8ulIXXIVc  192.168.10.15  58504  172.217.9.129  443  tcp  ssl  ShADadtFf
1492901937.837590  CJPFeg24plNQrUlEi1  192.168.10.4  8  192.168.10.1  0  icmp  -  -
1492901993.228698  CeIbOK2uGV2fpmHiJ1  192.168.10.15  58503  31.13.66.3  443  tcp  ssl  ShADadtFfr
1492901994.578721  C9t5ko1PGKHXXovSf5  192.168.10.16  50770  216.58.218.202  443  tcp  -  ShR
1492901992.662988  CNneTb3T8J9g4BT2o1  192.168.10.15  58502  172.217.2.226  443  tcp  ssl  ShADadtFf
1492901994.022743  CsUC8A40dFXzxZCYle  192.168.10.15  58508  172.217.9.129  443  tcp  ssl  ShADadtFf
1492901993.627272  CGy2HW1ohX1zIItba9  192.168.10.15  58506  172.217.9.129  443  tcp  ssl  ShADadtFf
1492901994.022621  C7JAhy4U9oNsLCkgF1  192.168.10.15  58507  172.217.9.129  443  tcp  ssl  ShADadtFf
1492901994.022837  CaTMSVpBOSd4GcYIk  192.168.10.15  58509  172.217.9.129  443  tcp  ssl  ShADadtFf
1492901993.626748  CslW3o2Xm1AlcL1lp8  192.168.10.15  58505  172.217.9.129  443  tcp  ssl  ShADadtFf
1492901994.270606  Cw7Ixr4V0EiEmcC6K3  192.168.10.16  50766  172.217.12.69  443  tcp  ssl  ShADadtFf
1492901996.873916  C97Zwv1BYFIz5UBsz  192.168.10.16  50684  31.13.66.1  443  tcp  -  F
1492901940.875572  CATL4y2DhCw7urQxI2  192.168.10.160  45855  172.217.9.131  443  udp  -  Dd
1492901994.466849  C4CWHd3vn9skNg3cVk  192.168.10.16  50767  216.58.218.170  443  tcp  ssl  ShADadtFf
1492901994.022889  CjUg2t1cAAkIyWtg1i  192.168.10.15  58510  172.217.9.129  443  tcp  ssl  ShADadtFf
1492901994.466942  CRq1J71ieSMvVzOnj  192.168.10.16  50768  216.58.218.170  443  tcp  ssl  ShADadtFf
1492901995.793617  C0RN102WlbKFNHDn66  192.168.10.16  50771  216.58.218.138  443  tcp  ssl  ShADadtFf
```

PCAP vs Session vs Alerts

PCAP

BRO/METADATA

ALERTS

Exercise 1 - discussion

- **Where do you begin?**
  - out of date network maps
  - unknown infrastructure
  - more unknowns...

Bro Configuration

- binaries
- config
- data
- scripts

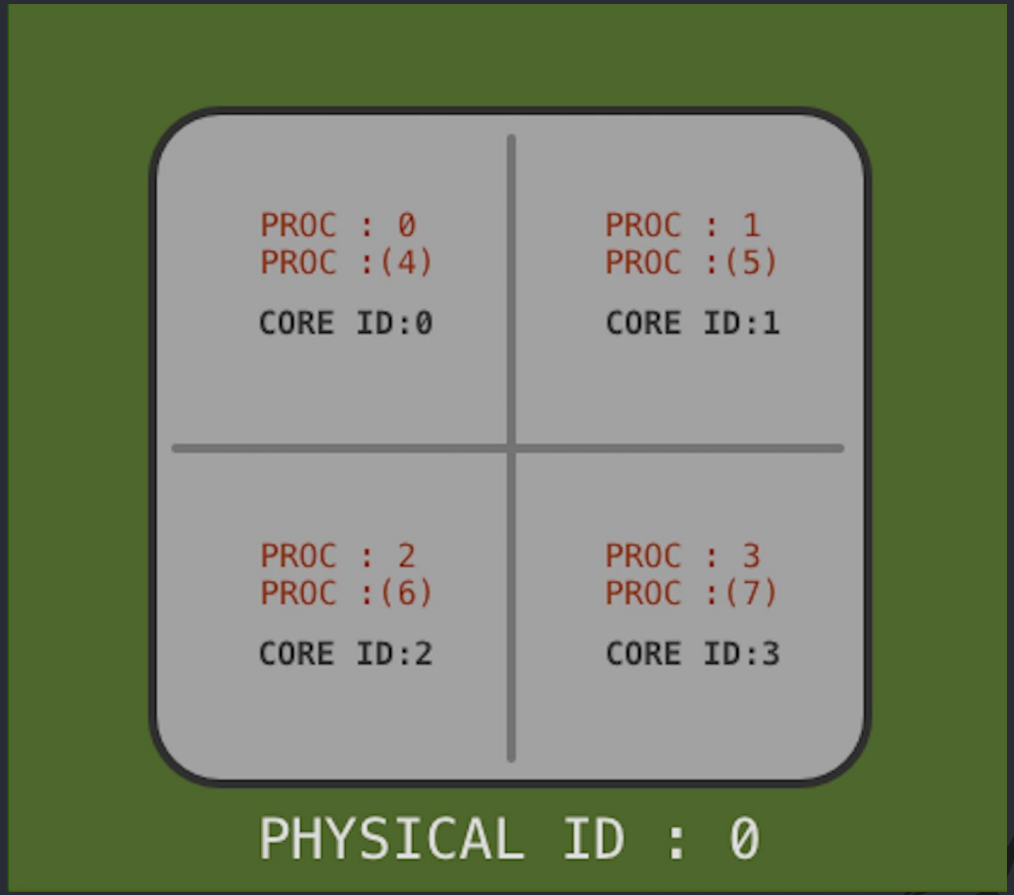
Bro Configuration

config path: /etc/bro

- nodes.cfg
- broctl.cfg
- networks.cfg

Bro Workers

- workers need to be assigned a physical CPU core



Bro CLI - command options

- bro --help
- bro -Cr [pcap file]

ASCII Bro Logs - functions check

- use linux CLI to view Bro logs
- create and navigate to a new directory
  - mkdir -p ~/bro/test
  - cd ~/bro/test
- replay the supplied PCAP into new path
  - bro -Cr /mnt/pcap/pe2.pcap
  - ls -la

Bro- log structure

```
ls -lah /data/bro/logs
```

- active logs are current for one hour
- then rolled out of "current" and into archive

Bro CLI - displaying logs

```
cat dns.log | bro-cut query | sort | uniq -c | sort -n
```


Bro CLI - displaying logs

use commands of your choice to view logs

- cat
- less
- sort
- uniq
- cut
- head

CONN - you've got the conn(_log)!

- bro logs start with a connection, or conn.log
- other logs refer to the Conn UUID
- this anchors other events together

CONN cont.

- conn log is written and *closed* when:
- conn log is NETFLOW and connection metadata
- key fields:
  - duration, number of bytes seen, originator, responder
  - ports, UUID, more

CONN exercise

- enable SMB analyzer
- enable rock scripts
- enable local network monitoring

CONN exercise

- make a new exercise directory to work in
  - mkdir -p ~/bro/pe2
- move to that directory
  - cd ~/bro/pe2
- replay the pe2.pcap using bro
  - bro -Cr /mnt/pcap/pe2.pcap local

CONN exercise

- how many connections are over http?
- how many of those are over non-standard http ports?
- how many connections are over 100 seconds in duration?
- how many connections are over ssl?

CONN exercise

- how many of those are over non-standard ssl ports?
- how many hosts originated bytes over 10000
- what protocols and services did they use in the above?

Bro-cut

- reads ASCII Bro logs and more easily displays it by the column names
- can display ASCII Bro log data according to column names provided by user
- demo

Bro-cut examples

- bro-cut id_orig_h id_orig_p id_resp_h id_resp_p < conn.log
- cat conn.log | bro-cut proto service id_resp_p
- cat conn.log | bro-cut | cut -f10 | sort | uniq -c | sort -rn
- cat conn.log | bro-cut proto | sort | uniq -c | sort -rn

Bro-cut exercise

- how many connections are over http?
- how many of those are over non-standard http ports?
- how many connections are over 100 seconds in duration?
- how many connections are over ssl?
- how many of those are over non-standard ssl ports?
- how many hosts originated bytes over 10000
- what protocols and services did they use in the above?

Other Bro logs

- network logs
- file logs
- netControl
- detection
- observations
- miscellaneous
- diagnostic

DNS Log

Key Fields:

- protocol
- query
- answers

- AA
- RD
- RA

DNS exercise

Use the same pe2.pcap to explore dns logs.

DNS exercise

- what are the top 5 requested domains?
- what are the top 5 answers?
- how many connections are over UDP?
- are there any connection not over UDP?
- who is the top 5 originators?
- who is the top 5 responder?
- was there any traffic over non DNS ports?

FTP Log

Key fields:

- user
- password
- command
- arg
- file_size
- reply_code
- reply_msg

FTP exercise

- make a new exercise directory to work in
  - mkdir -p ~/bro/ftp
- move to that directory
  - cd ~/bro/ftp
- replay the ftp.pcap using bro
  - bro -Cr /mnt/pcap/ftp.pcap local

FTP exercise

- how many files were downloaded?
- were there any unsuccessful attempts?
- if yes how many?
- what user was used to download the file?

HTTP Log - key fields

- method
- host
- uri
- status_code
- status_message
- user_agent
- request_body_len
- response_body_len

HTTP exercise

Use the pe2.pcap folder for this exercise.

HTTP exercise

- what methods were used?
- what are the top 5 user-agents?
- what status codes and status messages exist?
- are any of the status code/messages miss matched?
- what are the top 5 visited websites?
- what are the domains of the non-standard http logs?
- what IP’s are associated with the non-standard http logs?

Kerberos Log - key fields

- cipher
- request_type
- client
- success
- error_msg
- from
- till

Kerberos exercise

Use the ftp.pcap folder for this exercise:

Kerberos exercise

- what clients are requesting LDAP services?
- when do these tickets expire?
- which host is requesting a Ticket?
- which hosts are authenticating?

Modbus

- what is ICS?
- is there a problem?
- what is modbus?

Modbus exercise

- make a new exercise directory to work in
  - mkdir -p ~/bro/ics
- move to that directory
  - cd ~/bro/ics
- replay the ics.pcap using bro
  - bro -Cr /mnt/pcap/ics.pcap local

SMB_CMD Log - key fields

- command
- argument
- status
- version

SMB_FILES Log - key fields

- action
- path
- name
- size
- prev_name

SMB_FILES exercise

- make a new exercise directory to work in
  - mkdir -p ~/bro/smb
- move to that directory
  - cd ~/bro/smb
- replay the smb.pcap using bro
  - bro -Cr /mnt/pcap/smb.pcap local

SMB_FILES exercise

- how many unique file names were seen?
- what were the top 3 files opened?
- how many hosts opened a file?
- list each originating host with the files it opened.

SMTP Log - key fields

- mailfrom
- rcptto
- from
- to
- subject
- user_agent

SMTP exercise

- make a new exercise directory to work in
  - mkdir -p ~/bro/smtp
- move to that directory
  - cd ~/bro/smtp
- replay the smtp.pcap using bro
  - bro -Cr /mnt/pcap/smtp.pcap local

SSL Log - key fields

- version
- cipher
- curve
- server_name
- subject
- issuer

SSL exercise

Use the pe2.pcap folder for this exercise.

SSL exercise

- how many different ciphers are used?
- what are the top ciphers?
- what are the top versions
- how many connections are utilizing curve?
- how many are not using curve?
- what are the top 5 https servers?
- is there any servers not ending in “.com, .net, or .org”?

Questions?


Johnathon Hall
johnathon-hall
johnathon@perched.io


Nate Guagenti
nathanguagenti
nate@perched.io