SECURITY ONION CONFERENCE 2023

October 6, 2023

Augusta, GA

About Me

- Principal Technical Success Manager, FortiNDR Cloud
- Security Onion user since 2014
- 9 years building, deploying, managing lightweight network sensors

WHAT AM I TALKING ABOUT?

- Preparing for conversation
- Only sending one side of traffic
- 73% analogies, 10% fake stats
- I have to make an analogy

A Good Analogy?

A Good Analogy?

A Good Analogy?

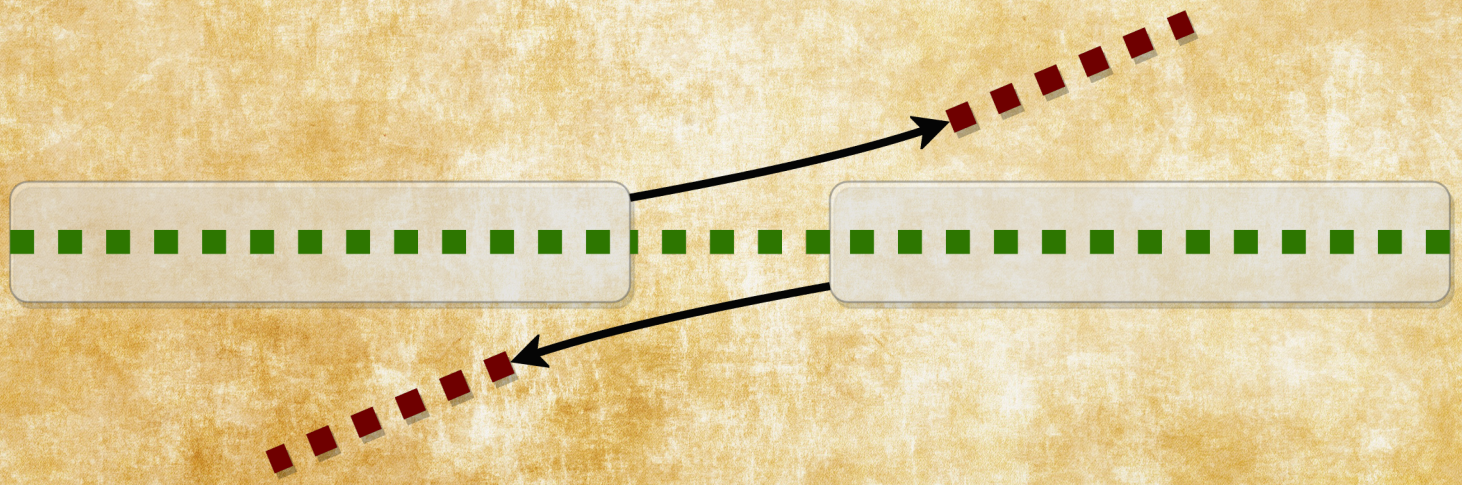
A Good Analogy?

They're Digging in the Wrong Place!

Identifying and dealing with one-sided traffic.

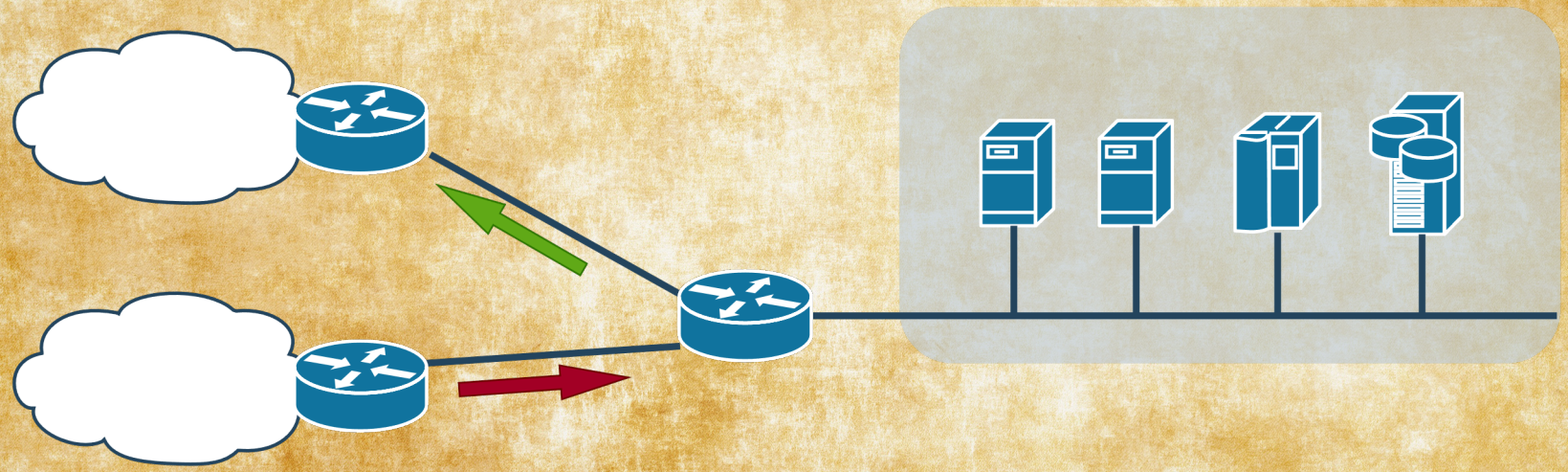
What's the cause?

- Packet loss



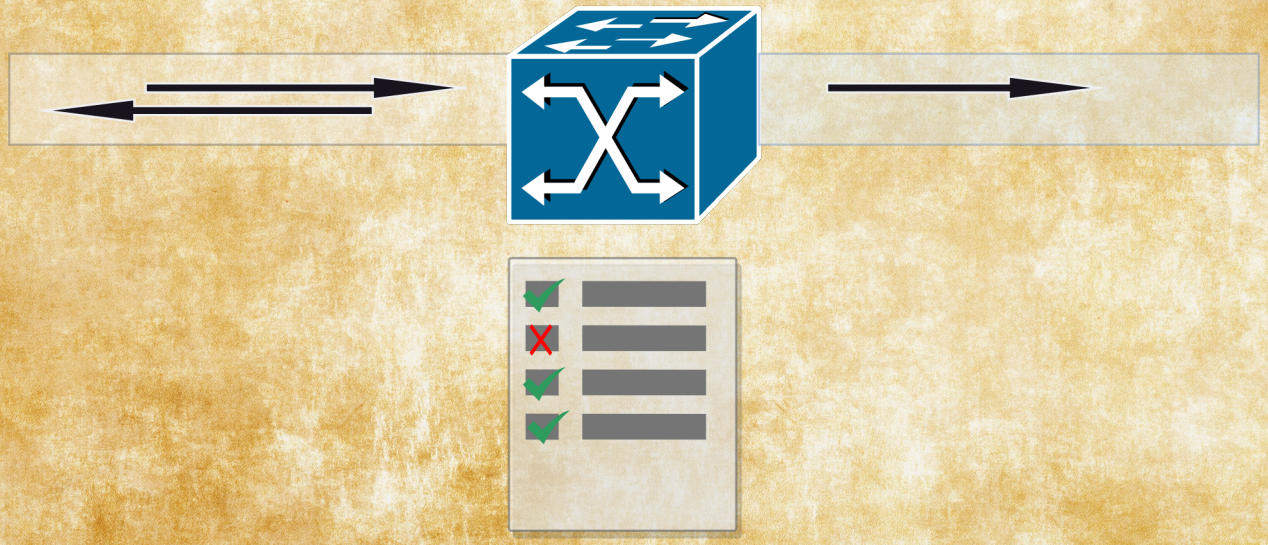
What's the cause?

- Packet loss
- Asymmetric routing



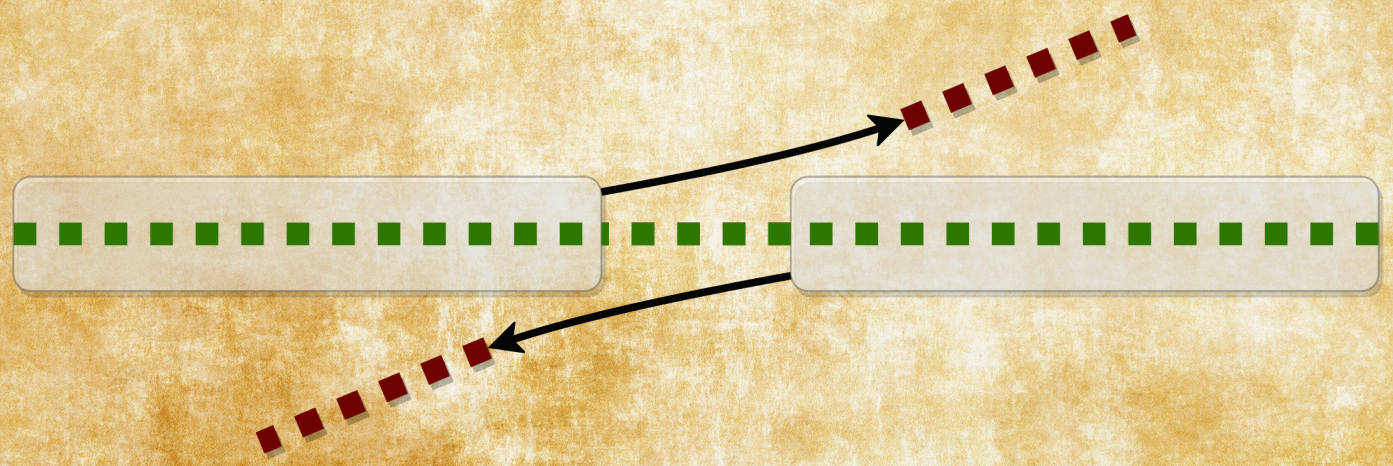
What's the cause?

- Packet loss
- Asymmetric routing
- Misconfiguration



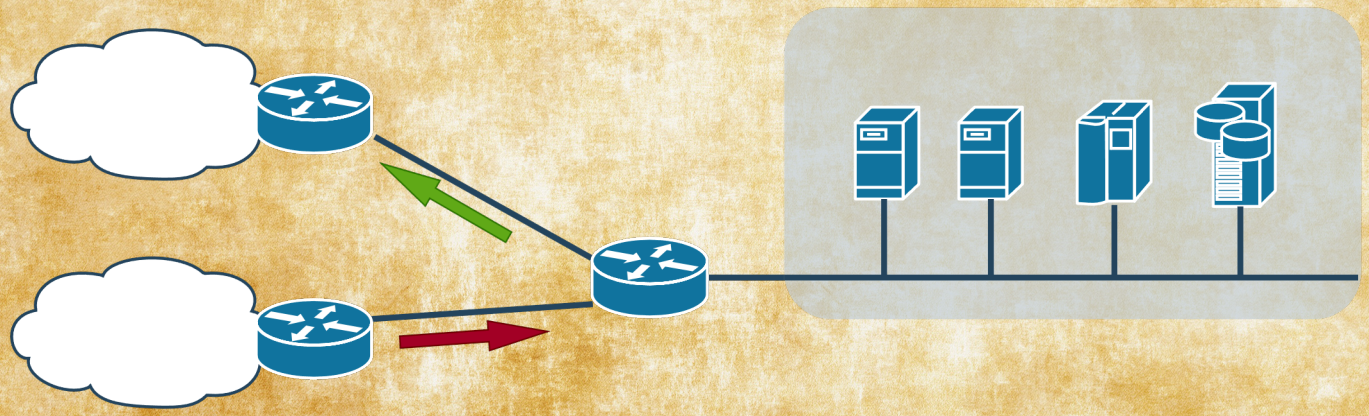
Packet Loss

- Imperfect world
- Loss is not drops
- Could be overloaded switch
- Could be to more traffic than pipe



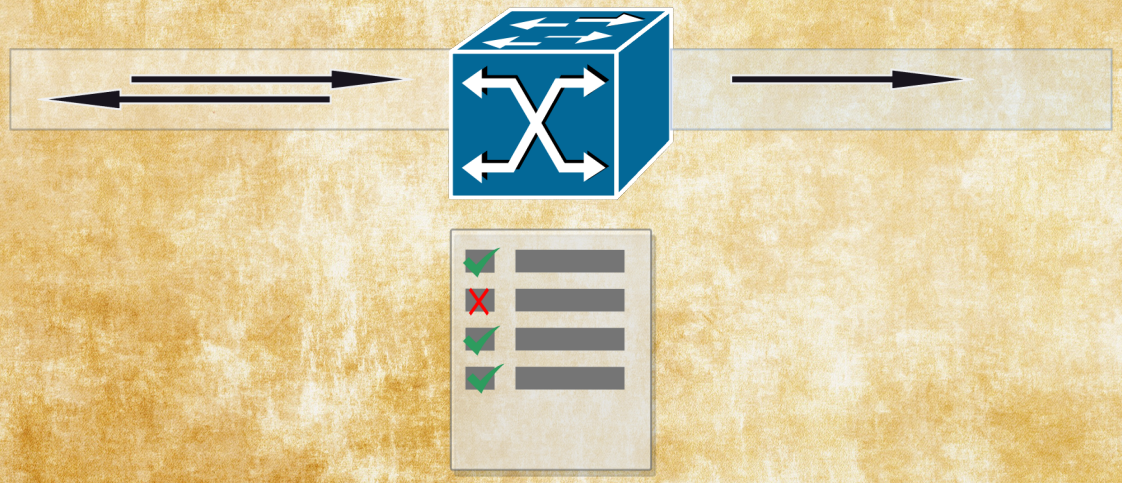
Routing

- MPLS Networks
- Asymmetric routing
- Systemic
- Capture point might not be ideal



Configuration

- More advanced active TAPs
- TAPs with bad TX/RX links
- Switch mirror/monitor ports
- Load balancers



Spanning the Globe

- SPAN port fault 79.3% of time
- Sporadic loss? How busy is switch?
- Are you mirroring more than monitor?
- Configured for bi-directional?

WHAT DOES IT LOOK LIKE?

wget http://voxpop.freeshell.org/plink.exe

HTTP WITH PE DOWNLOAD

DNS

Full Duplex

wget http://voxpop.freeshell.org/plink.exe

dns.answers.name	"205.166.94.9"
dns.authoritative	false
dns.highest_registered_domain	freeshell.org
dns.id	40400
dns.parent_domain	freeshell
dns.parent_domain_length	9
dns.query.class	1
dns.query.class_name	C_INTERNET
dns.query.length	20
dns.query.name	voxpop.freeshell.org
dns.query.rejected	false
dns.query.type	1

dns.query.type_name	A
dns.recursion.available	true
dns.recursion.desired	true
dns.reserved	0
dns.response.code	0
dns.response.code_name	NOERROR
dns.subdomain	voxpop
dns.subdomain_length	6
dns.top_level_domain	org
dns.truncated	false
dns.ttls	15624

DNS

TX Only

wget http://voxpop.freeshell.org/plink.exe

dns.answers.name	"205.166.94.9"
dns.authoritative	false
dns.highest_registered_domain	freeshell.org
dns.id	40400
dns.parent_domain	freeshell
dns.parent_domain_length	9
dns.query.class	[redacted]
dns.query.class_name	[redacted]
dns.query.length	20
dns.query.name	voxpop.freeshell.org
dns.query.rejected	false
dns.query.type	[redacted]

dns.query.type_name	[redacted]
dns.recursion.available	true
dns.recursion.desired	true
dns.reserved	0
dns.response.code	0
dns.response.code_name	NOERROR
dns.subdomain	voxpop
dns.subdomain_length	6
dns.top_level_domain	org
dns.truncated	false
dns.ttls	15624

DNS

RX Only

wget http://voxpop.freeshell.org/plink.exe

dns.answers.name	[redacted]
dns.authoritative	false
dns.highest_registered_domain	freeshell.org
dns.id	40400
dns.parent_domain	freeshell
dns.parent_domain_length	9
dns.query.class	1
dns.query.class_name	C_INTERNET
dns.query.length	20
dns.query.name	voxpop.freeshell.org
dns.query.rejected	false
dns.query.type	1

dns.query.type_name	A
dns.recursion.available	true
dns.recursion.desired	true
dns.reserved	0
dns.response.code	[redacted]
dns.response.code_name	[redacted]
dns.subdomain	voxpop
dns.subdomain_length	6
dns.top_level_domain	org
dns.truncated	false
dns.ttls	[redacted]

CONN

Full Duplex

wget http://voxpop.freeshell.org/plink.exe

client_bytes	144
client.ip_bytes	29948
client.packets	573
connection.bytes.missed	0
connection.history	ShADdFaf
connection.state	SF
network.bytes	839945
network.protocol	http
server.bytes	839801
server.ip_bytes	870281
server.packets	586

CONN

TX Only

wget http://voxpop.freeshell.org/plink.exe

client_bytes	0
client.ip_bytes	0
client.packets	0
connection.bytes.missed	0
connection.history	^hdttaf
connection.state	SHR
network.bytes	839801
network.protocol	
server.bytes	839801
server.ip_bytes	870281
server.packets	586

CONN

RX Only

wget http://voxpop.freeshell.org/plink.exe

client_bytes	144
client.ip_bytes	29948
client.packets	573
connection.bytes.missed	0
connection.history	SADF
connection.state	SH
network.bytes	144
network.protocol	http
server.bytes	0
server.ip_bytes	0
server.packets	0

HTTP

Full Duplex

wget http://voxpop.freeshell.org/plink.exe

file.resp_mime_types	“application/x-dosexec”
http.method	GET
http.request.body.length	0
http.response.body.length	839472
http.status_code	200
http.status_message	OK
http.trans_depth	1
http.uri	/plink.exe
http.useragent	Wget/1.21.1
http.version	1.1
http.virtual_host	voxpop.freeshell.org

HTTP

TX Only

wget http://voxpop.freeshell.org/plink.exe

file.resp_mime_types	“application/x-dosexec”
http.method	[redacted]
http.request.body.length	0
http.response.body.length	221591
http.status_code	200
http.status_message	OK
http.trans_depth	1
http.uri	[redacted]
http.useragent	[redacted]
http.version	1.1
http.virtual_host	[redacted]

HTTP

RX Only

wget http://voxpop.freeshell.org/plink.exe

file.resp_mime_types	
http.method	GET
http.request.body.length	0
http.response.body.length	0
http.status_code	
http.status_message	
http.trans_depth	1
http.uri	/plink.exe
http.useragent	Wget/1.21.1
http.version	
http.virtual_host	voxpop.freeshell.org

FILE

Full Duplex

wget http://voxpop.freeshell.org/plink.exe

file.analyzer	“PE”,”SHA1”,”EXTRACT”,”MD5”
file.bytes.missing	0
file.bytes.overflow	0
file.bytes.seen	839472
file.bytes.total	839472
file.depth	0
file.is_orig	false
file.mime_type	application/x-dosexec
file.source	HTTP
file.timed_out	false
hash.md5	75f5df9679c340cfd299dd3d
hash.sha1	641ea9689b96c441d3da4b5da8a461

FILE

TX Only

wget http://voxpop.freeshell.org/plink.exe

file.analyzer	“PE”,”SHA1”,”EXTRACT”,”MD5”
file.bytes.missing	0
file.bytes.overflow	0
file.bytes.seen	221591
file.bytes.total	839472
file.depth	0
file.is_orig	false
file.mime_type	application/x-dosexec
file.source	HTTP
file.timed_out	false
hash.md5	8c152e0f10272c294e20da
hash.sha1	abfd8a4e7a0037e689ca9ec97df1e

FILE

RX Only

wget http://voxpop.freeshell.org/plink.exe

file.analyzer

file.bytes.missing

file.bytes.overflow

file.bytes.seen

file.bytes.total

file.depth

file.is_orig

file.mime_type

file.source

file.timed_out

hash.md5

hash.sha1

PE

Full Duplex

wget http://voxpop.freeshell.org/plink.exe

file.code_integrity	false
file.compile_timestamp	1693035956
file.debug_data	false
file.is_64bit	false
file.is_exe	true
file.machine	I386
file.os	Windows XP
file.section_names	“.text”,”.rdata”,”.data”,…
file.subsystem	WINDOWS_CUI
file.table.cert	true
file.table.export	false
file.table.import	true

PE

TX Only

wget http://voxpop.freeshell.org/plink.exe

file.code_integrity	false
file.compile_timestamp	1693035956
file.debug_data	false
file.is_64bit	false
file.is_exe	true
file.machine	I386
file.os	Windows XP
file.section_names	“.text”,”.rdata”,”.data”,…
file.subsystem	WINDOWS_CUI
file.table.cert	true
file.table.export	false
file.table.import	true

PE

TX Only

wget http://voxpop.freeshell.org/plink.exe

file.code_integrity

file.compile_timestamp

file.debug_data

file.is_64bit

file.is_exe

file.machine

file.os

file.section_names

file.subsystem

file.table.cert

file.table.export

file.table.import

SURICATA

Full Duplex

wget http://voxpop.freeshell.org/plink.exe

rule.category	Potentially Bad Traffic
rule.metadata.affected_product	Windows_XP_Vista_7_8_10_Server
rule.metadata.attack_target	Client_Endpoint
rule.metadata.created_at	2019_03_12
rule.metadata.former_category	INFO
rule.metadata.signature_severity	Minor
rule.metadata.updated_at	2020_11_11
rule.name	ET INFO Wget Request for Executable
rule.reference	https://doc.emergingthreats.net/...
rule.rev	4
rule.ruleset	Emerging Threats
rule.uuid	2027076

SURICATA

TX Only

wget http://voxpop.freeshell.org/plink.exe

rule.category

rule.metadata.affected_product

rule.metadata.attack_target

rule.metadata.created_at

rule.metadata.former_category

rule.metadata.signature_severity

rule.metadata.updated_at

rule.name

rule.reference

rule.rev

rule.ruleset

rule.uuid

SURICATA

RX Only

wget http://voxpop.freeshell.org/plink.exe

rule.category

rule.metadata.affected_product

rule.metadata.attack_target

rule.metadata.created_at

rule.metadata.former_category

rule.metadata.signature_severity

rule.metadata.updated_at

rule.name

rule.reference

rule.rev

rule.ruleset

rule.uuid

smb://10.1.1.36/foo/secret/plink.exe

SMB FILE TRANSFER

CONN

Full Duplex

smb://10.1.1.36/foo/secret/plink.exe

client_bytes	849264
client.ip_bytes	884052
client.packets	669
connection.bytes.missed	0
connection.history	DdAa
connection.state	OTH
network.bytes	861796
network.protocol	smb
server.bytes	12532
server.ip_bytes	17836
server.packets	102

CONN

TX Only

smb://10.1.1.36/foo/secret/plink.exe

client_bytes	0
client.ip_bytes	0
client.packets	0
connection.bytes.missed	0
connection.history	^da
connection.state	OTH
network.bytes	12996
network.protocol	
server.bytes	12996
server.ip_bytes	18352
server.packets	103

CONN

RX Only

smb://10.1.1.36/foo/secret/plink.exe

client_bytes	850926
client.ip_bytes	8886442
client.packets	683
connection.bytes.missed	0
connection.history	DA
connection.state	OTH
network.bytes	850926
network.protocol	smb
server.bytes	0
server.ip_bytes	0
server.packets	0

FILE

Full Duplex

smb://10.1.1.36/foo/secret/plink.exe

file.analyzer	“PE”,”SHA1”,”EXTRACT”,”MD5”
file.bytes.missing	0
file.bytes.overflow	0
file.bytes.seen	839472
file.bytes.total	839472
file.name	foo\secret\plink.exe
file.is_orig	true
file.mime_type	application/x-dosexec
file.source	SMB
file.timed_out	false
hash.md5	75f5df9679c340cfd299dd3d
hash.sha1	641ea9689b96c441d3da4b5da8a461

FILE

TX Only

smb://10.1.1.36/foo/secret/plink.exe

file.analyzer

file.bytes.missing

file.bytes.overflow

file.bytes.seen

file.bytes.total

file.depth

file.is_orig

file.mime_type

file.source

file.timed_out

hash.md5

hash.sha1

FILE

RX Only

smb://10.1.1.36/foo/secret/plink.exe

file.analyzer

file.bytes.missing

file.bytes.overflow

file.bytes.seen

file.bytes.total

file.depth

file.is_orig

file.mime_type

file.source

file.timed_out

hash.md5

hash.sha1

SMB_FILES

Full Duplex

smb://10.1.1.36/foo/secret/plink.exe

file.action	SMB::FILE_OPEN
file.name	foo\secret\plink.exe
file.size	839472
file.times_accessed	1693838811
file.times_changed	1693862938.8395452
file.times_created	1693862938.7926378
file.times_modified	1693838811

SMB_FILES

TX Only

smb://10.1.1.36/foo/secret/plink.exe

file.action
file.name
file.size
file.times_accessed
file.times_changed
file.times_created
file.times_modified

SMB_FILES

RX Only

smb://10.1.1.36/foo/secret/plink.exe

file.action

file.name

file.size

file.times_accessed

file.times_changed

file.times_created

file.times_modified

How do we know?

TRUST ZEEK

- Check your informational events
- Weird logs
- Good at identifying sporadic loss

Example Weird Log

- data_before_established


```
{"ts":1693839132.452792,"uid":"CJ1ObaKhYLpw9TR","id.orig_h":"10.1.1.36","id.orig_p":51428,"id.resp_h":"204.79.197.203","id.resp_p":443,"name":"data_before_established","notice":false,"peer":"zeek","source":"TCP"}
```

Example Weird Log

- data_before_established
- possible_split_routing


```
{"ts":1693839134.341365,"uid":"CQuH7B1J2vjfDhiNVk","id.orig_h":"10.1.1.36","id.orig_p":51437,"id.resp_h":"20.189.173.5","id.resp_p":443,"name":"possible_split_routing","notice":false,"peer":"zeek"}
```

Example Weird Log

- data_before_established
- possible_split_routing
- inappropriate_FIN


```
{"ts":1693839135.667021,"uid":"CV6GDD1ABWeSxiCgy7","id.orig_h":"10.1.1.76","id.orig_p":61158,"id.resp_h":"17.253.7.205","id.resp_p":80,"name":"inappropriate_FIN","notice":false,"peer":"zeek","source":"TCP"}
```

Go looking for it

- State of the connection?
- Stack on connection.state
- Narrow your query to one sensor

GO LOOKING FOR IT

Security Onion

- Overview
- Alerts
- Dashboards
- Hunt
- Cases
- PCAP
- Grid
- Downloads
- Administration

Tools

- Kibana
- Elastic Fleet
- Osquery Manager
- InfluxDB
- CyberChef
- Navigator

Overview

Getting Started

New to Security Onion 2? Click the menu in the upper-right corner and you'll find links for Help and a Cheatsheet that will help you best utilize Security Onion to hunt for evil! In addition, check out our free Security Onion 2 Essentials online course, available on our Training website.

If you're ready to dive in, take a look at the Alerts interface to see what Security Onion has detected so far. Then go to the Dashboards interface for a general overview of all logs collected or go to the Hunt interface for more focused threat hunting. Once you've found something of interest, escalate it to Cases to then collect evidence and analyze observables as you work towards closing the case.

What's New

To see all the latest features and fixes in this version of Security Onion, click the upper-right menu and then click the What's New link.

Enterprise Appliances

Want the best hardware for your enterprise deployment? Check out our enterprise appliances!

Customize This Space

Make this area your own by customizing the content in the Config interface.

Brought to you by:

Security Onion SOLUTIONS

Version: 2.4.10

© 2023 Security Onion Solutions, LLC

License: ELv2

GO LOOKING FOR IT

```
event.dataset:"zeek.conn"
```

We only need conn records

GO LOOKING FOR IT

```
event.dataset:"zeek.conn" AND ((source.ip:"10.0.0.0/8" OR
source.ip:"172.16.0.0/12" OR source.ip:"192.168.0.0/16")
AND NOT (destination.ip:"10.0.0.0/8" OR
destination.ip:"172.16.0.0/12" OR
destination.ip:"192.168.0.0/16" ))
```

Internal to external traffic

GO LOOKING FOR IT

```
event.dataset:"zeek.conn" AND ((source.ip:"10.0.0.0/8" OR
source.ip:"172.16.0.0/12" OR source.ip:"192.168.0.0/16")
AND NOT (destination.ip:"10.0.0.0/8" OR
destination.ip:"172.16.0.0/12" OR
destination.ip:"192.168.0.0/16" )) OR
((destination.ip:"10.0.0.0/8" OR
destination.ip:"172.16.0.0/12" OR
destination.ip:"192.168.0.0/16" ) AND NOT
(source.ip:"10.0.0.0/8" OR source.ip:"172.16.0.0/12" OR
source.ip:"192.168.0.0/16"))
```

External to internal traffic

GO LOOKING FOR IT

```
event.dataset:"zeek.conn" AND ((source.ip:"10.0.0.0/8" OR
source.ip:"172.16.0.0/12" OR source.ip:"192.168.0.0/16")
AND NOT (destination.ip:"10.0.0.0/8" OR
destination.ip:"172.16.0.0/12" OR
destination.ip:"192.168.0.0/16" )) OR
((destination.ip:"10.0.0.0/8" OR
destination.ip:"172.16.0.0/12" OR
destination.ip:"192.168.0.0/16" ) AND NOT
(source.ip:"10.0.0.0/8" OR source.ip:"172.16.0.0/12" OR
source.ip:"192.168.0.0/16")) | groupby observer.name
```

Stack on sensors

GO LOOKING FOR IT

```
event.dataset:"zeek.conn" AND ((source.ip:"10.0.0.0/8" OR
source.ip:"172.16.0.0/12" OR source.ip:"192.168.0.0/16")
AND NOT (destination.ip:"10.0.0.0/8" OR
destination.ip:"172.16.0.0/12" OR
destination.ip:"192.168.0.0/16" )) OR
((destination.ip:"10.0.0.0/8" OR
destination.ip:"172.16.0.0/12" OR
destination.ip:"192.168.0.0/16" ) AND NOT
(source.ip:"10.0.0.0/8" OR source.ip:"172.16.0.0/12" OR
source.ip:"192.168.0.0/16")) | groupby observer.name |
groupby network.transport, connection.state_description
```

Stack on transport and state

GO LOOKING FOR IT

```
event.dataset:"zeek.conn" AND ((source.ip:"10.0.0.0/8" OR
source.ip:"172.16.0.0/12" OR source.ip:"192.168.0.0/16")
AND NOT (destination.ip:"10.0.0.0/8" OR
destination.ip:"172.16.0.0/12" OR
destination.ip:"192.168.0.0/16" )) OR
((destination.ip:"10.0.0.0/8" OR
destination.ip:"172.16.0.0/12" OR
destination.ip:"192.168.0.0/16" ) AND NOT
(source.ip:"10.0.0.0/8" OR source.ip:"172.16.0.0/12" OR
source.ip:"192.168.0.0/16")) | groupby observer.name |
groupby network.transport, connection.state_description |
groupby -pie connection.state, connection.history
```

Stack on state and history

GO LOOKING FOR IT

```
event.dataset:"zeek.conn"
```

We only need conn records

GO LOOKING FOR IT

```
event.dataset:"zeek.conn" AND (source.ip:"10.0.0.0/8" OR
source.ip:"172.16.0.0/12" OR source.ip:"192.168.0.0/16")
AND (destination.ip:"10.0.0.0/8" OR
destination.ip:"172.16.0.0/12" OR
destination.ip:"192.168.0.0/16" )
```

Internal to external traffic

GO LOOKING FOR IT

```
event.dataset:"zeek.conn" AND (source.ip:"10.0.0.0/8" OR
source.ip:"172.16.0.0/12" OR source.ip:"192.168.0.0/16")
AND (destination.ip:"10.0.0.0/8" OR
destination.ip:"172.16.0.0/12" OR
destination.ip:"192.168.0.0/16" ) | groupby observer.name
```

Stack on sensors

GO LOOKING FOR IT

```
event.dataset:"zeek.conn" AND (source.ip:"10.0.0.0/8" OR
source.ip:"172.16.0.0/12" OR source.ip:"192.168.0.0/16")
AND (destination.ip:"10.0.0.0/8" OR
destination.ip:"172.16.0.0/12" OR
destination.ip:"192.168.0.0/16" ) | groupby observer.name
| groupby network.transport, connection.state_description
```

Stack on transport and state

GO LOOKING FOR IT

```
event.dataset:"zeek.conn" AND (source.ip:"10.0.0.0/8" OR
source.ip:"172.16.0.0/12" OR source.ip:"192.168.0.0/16")
AND (destination.ip:"10.0.0.0/8" OR
destination.ip:"172.16.0.0/12" OR
destination.ip:"192.168.0.0/16" ) | groupby observer.name
| groupby network.transport, connection.state_description
| groupby -pie connection.state, connection.history
```

Stack on state and history

WHAT DO WE DO ABOUT IT?

FIX IT!

- Sometimes easier said than done
  - How are your people skills?
  - Change seasons
- Fix your configuration
- Get a TAP
- Move your capture point

LIVE WITH IT!

- Sometimes, no choice
- Identify weak segments
- Defense in depth
- Understand what data you can use

THANK YOU!

https://linktr.ee/scott.hall

- Packet captures and slides
- https://github.com/foodiddy/theyre-digging-in-the-wrong-place
- Fatema Bannat Wala – Is Weird Still Weird?
- https://www.youtube.com/watch?v=s4V5YwfHP0s
- Connection interpreter script reference
- https://docs.zeek.org/en/master/scripts/base/protocols/conn/main.zeek.html