BsidesCVG 2014

1.0

Cincinnati, OH

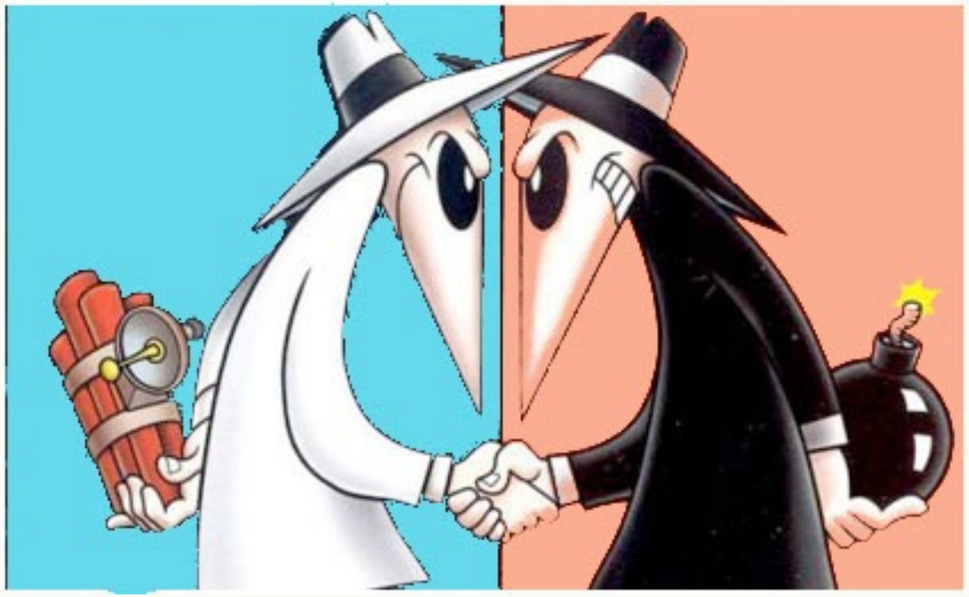
Advanced Reconnaissance Detection using Bro

Liam Randall

Critical Stack

Agenda – What you will see today

1. **Why Recon**
   Welcome
2. **Tools**
   Broverview
3. **DNS**
   Pwn all the things
4. **Demonstration**
   More Tools
5. **HTTP**
   Dirbuster, Basic Auth, Web Apps
6. **SSL**
   People do that?
7. **End**
   Questions



Defending

IDS, IPS, Routers, Policy, Procedure

Not enough content

Admins & Users Suck. Hard.

Losing.

BLUE & RED

Can not defend what you do not understand.

Good, Bad & the Ugly.

Attacking

Metasploit, Armitage,

“exciting”

Winning.

PTES Standard

Penetration Testing Execution Standard

"That means foot-printing and identifying technical systems or just identifying different routes for attack, but the way many operate, their intelligence is poor at best,"

March 2011

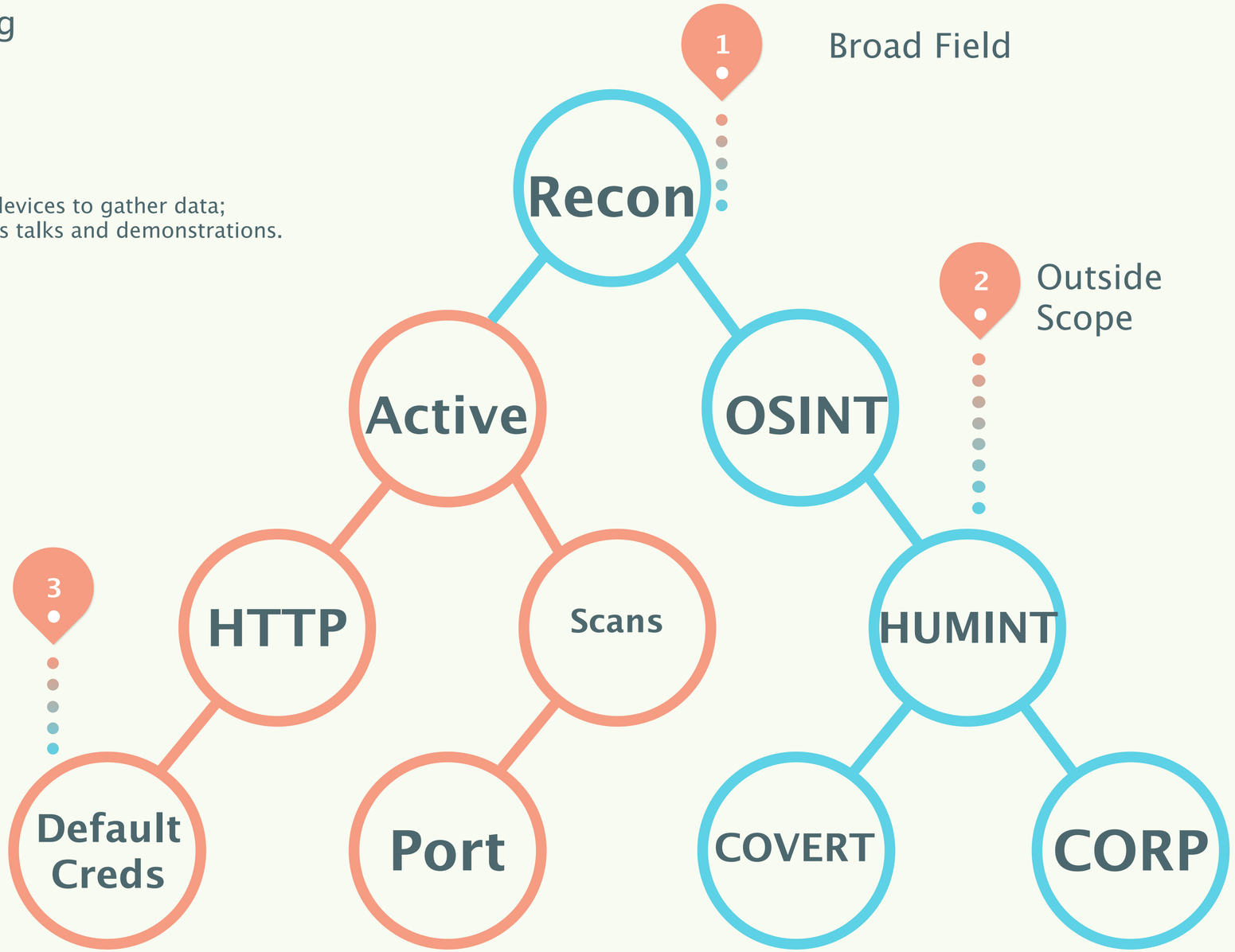
ZDNet

Chris Nickerson
on PTES Standard

PTES – Intelligence Gathering

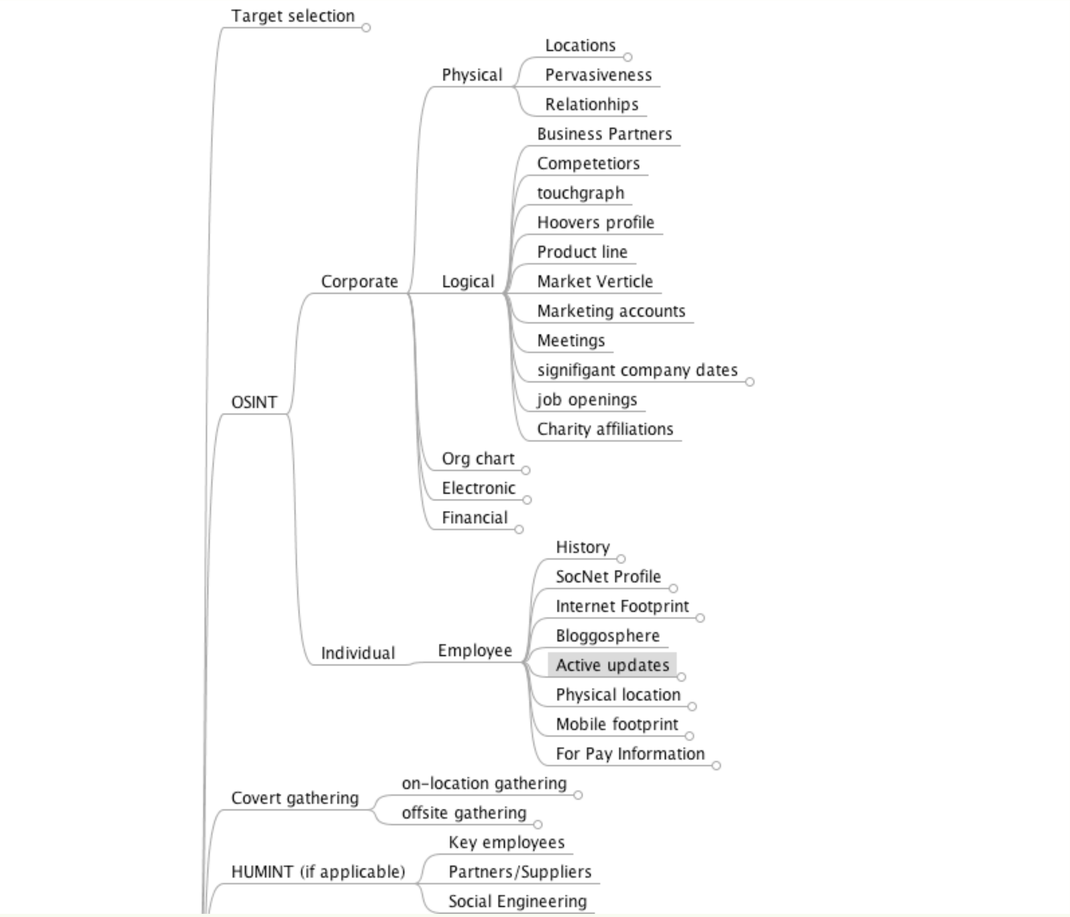
Various Approaches

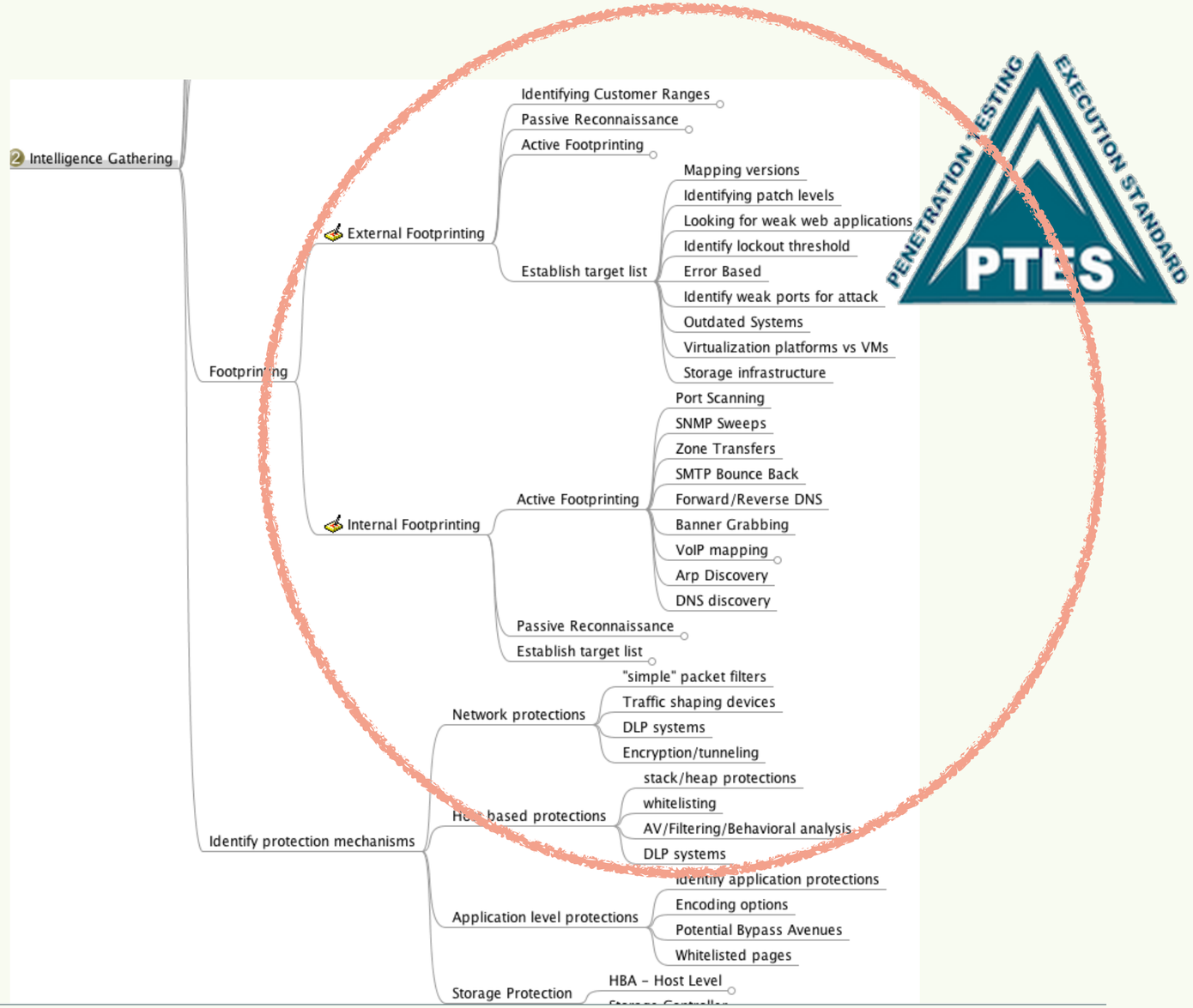
Lots of ways onto networks and devices to gather data;
many outside the scope of today's talks and demonstrations.



Focus:
Active Remote Interaction
of Attackers with our Net

Socratic Ideal– “Know Thyself”

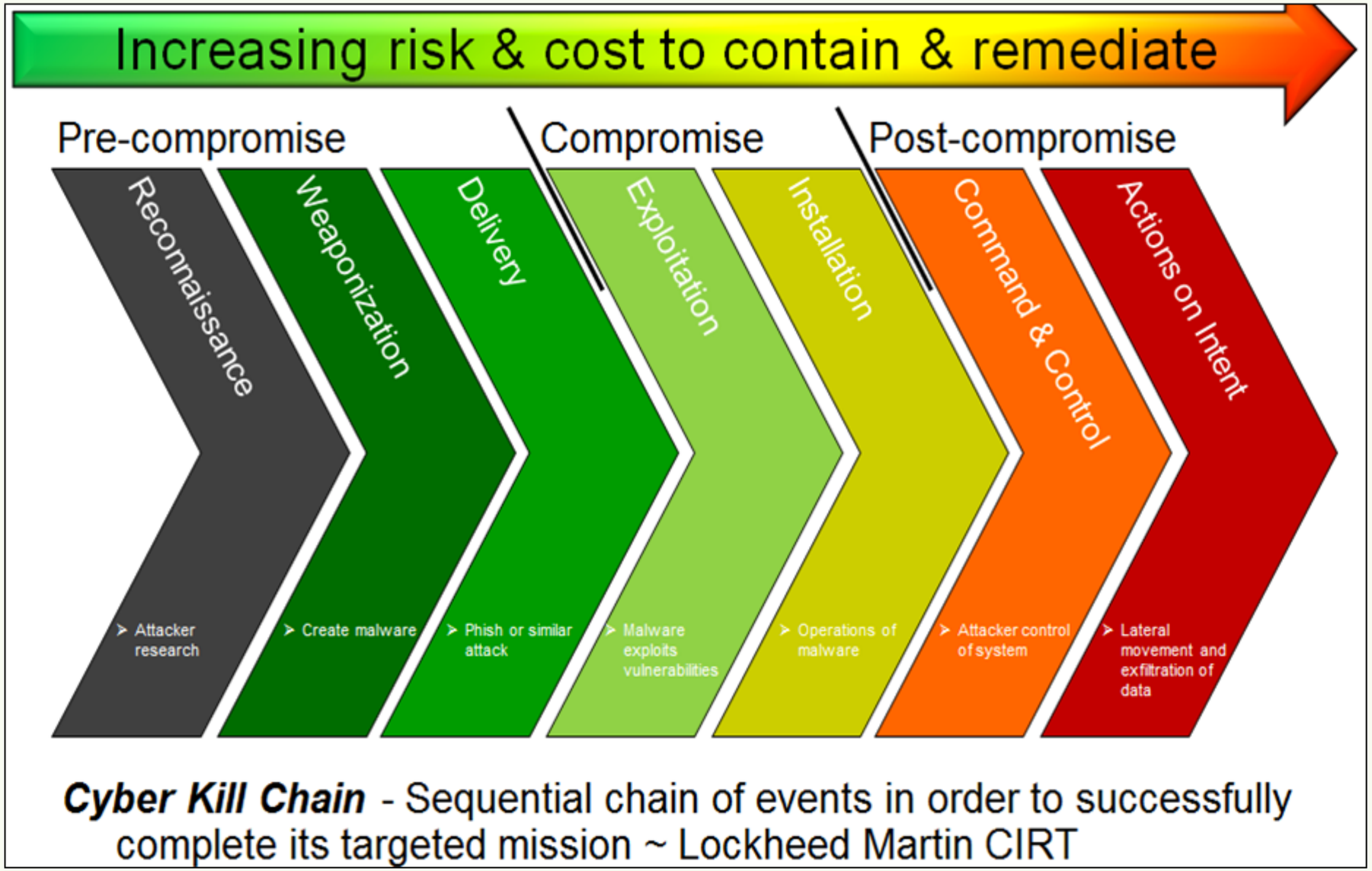




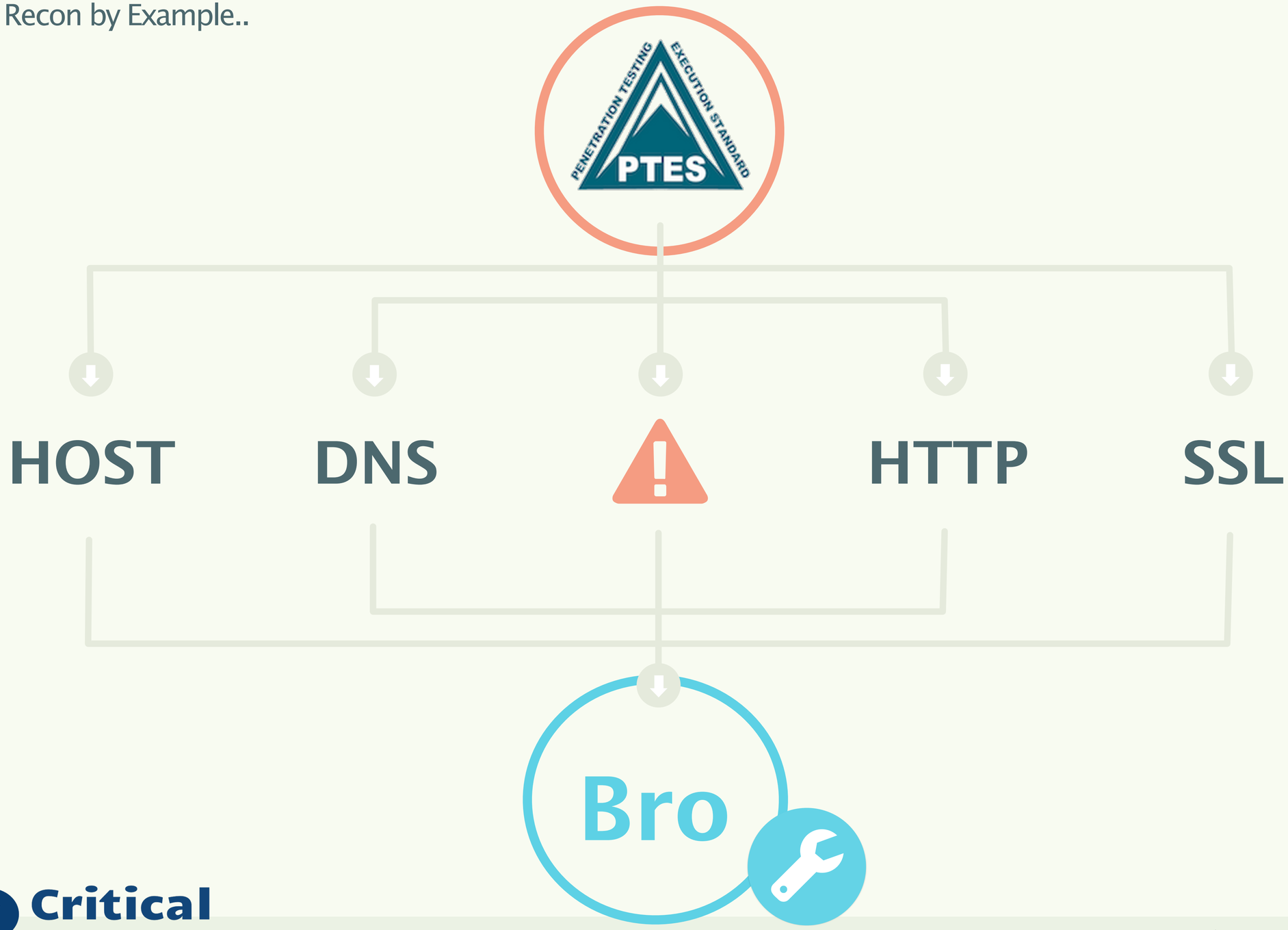
Active Part of Scanning

You can not secure what you do not understand.

Kill Chain – Attacker Policy and Procedure

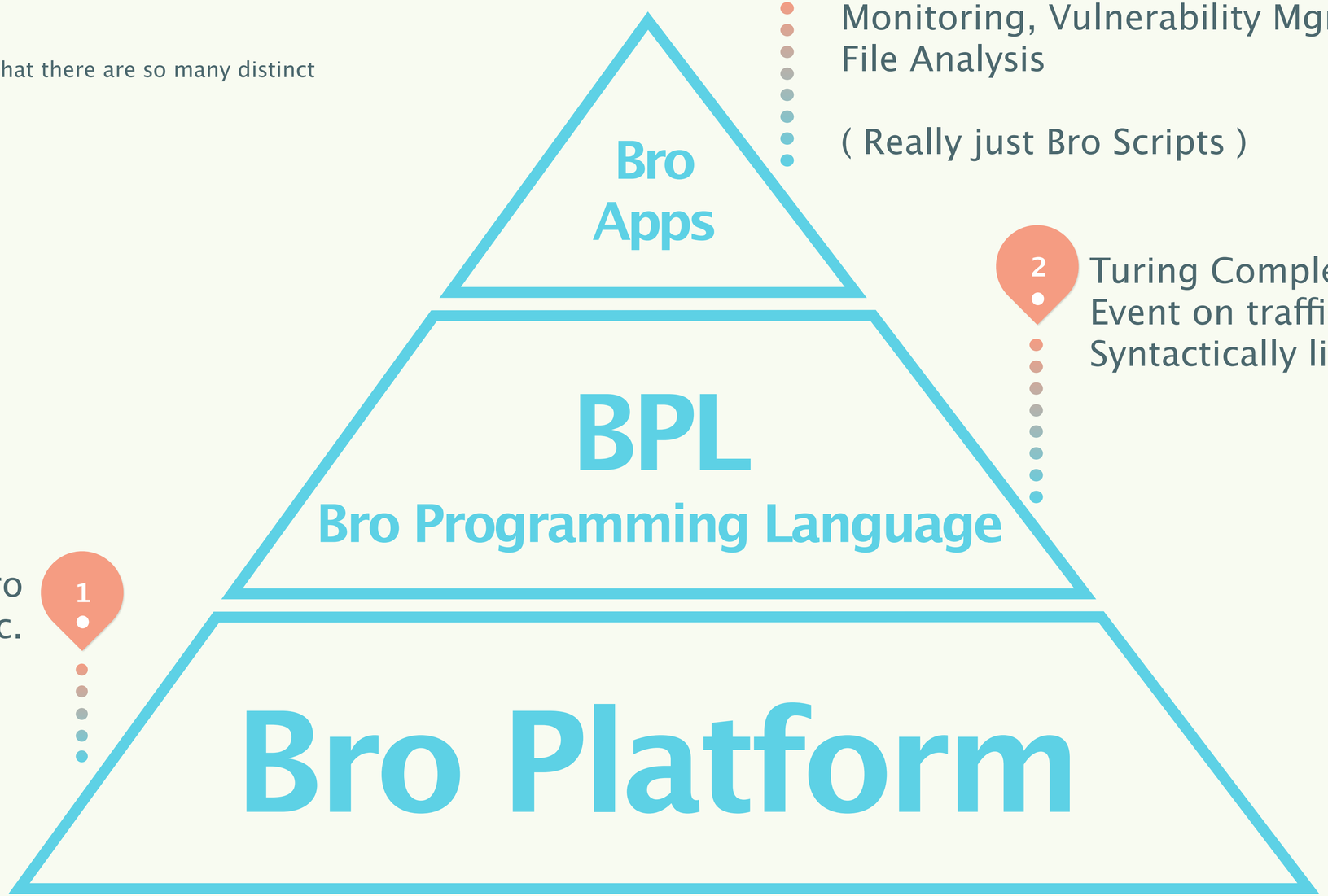


Methodology – Recon by Example..



Bro is three things ...

The hardest part about Bro is that there are so many distinct use cases for the Bro Platform



3 Bro-IDS

Monitoring, Vulnerability Mgmt, DLP, Analysis, File Analysis

(Really just Bro Scripts)

2 Turing Complete PL
Event on traffic, files, protocols
Syntactically like Python

1 Utilities to manage Bro
API, Intefaces, etc.

Bro Functions – Three things Bro does

Protocol Logs

Detailed protocol logs for each network protocol; including logs for tunnels, IPv4/6, files and more

Alerts

Bro–IDS is preconfigured with a variety of signature and anomaly notifications

Actions

Bro Programming Language is the real power; pivot to external applications, take advanced protocol based decisions & more.

Bro Functions – Three things Bro does

Protocol Logs

Detailed protocol logs for each network protocol; including logs for tunnels, IPv4/6, files and more

Alerts

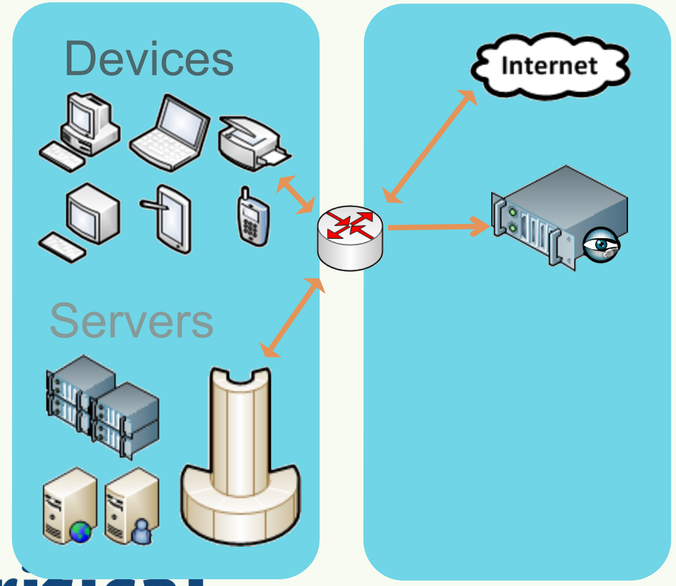
Bro–IDS is preconfigured with a variety of signature and anomaly notifications

Actions

Bro Programming Language is the real power; pivot to external applications, take advanced protocol based decisions & more.

Sensor Components

Tap:
Bro
Sensor



Bro Functions – Three things Bro does

Protocol Logs

Detailed protocol logs for each network protocol; including logs for tunnels, IPv4/6, files and more

Alerts

Bro–IDS is preconfigured with a variety of signature and anomaly notifications

Actions

Bro Programming Language is the real power; pivot to external applications, take advanced protocol based decisions & more.

Ts	uid	id.orig_h	id.orig_p	id.resp_h	id.resp_p	proto	service
Time	string	addr	port	addr	port	enum	string
1355284742	AZIHpPIejvi	192.168.4.138	68	192.168.4.1	67	udp	-
1326727285	K4xJ9AKH56g	192.168.4.148	55748	196.216.2.3	33117	tcp	ftp-data
1326727283	Jd11tlLtlE	192.168.4.148	58838	196.216.2.3	21	tcp	ftp
1326727287	bVQHYKEz2b4	192.168.4.148	54003	196.216.2.3	31093	tcp	ftp-data
1326727286	5Dki82HwJDk	192.168.4.148	58840	196.216.2.3	21	tcp	ftp
1355284761	YSJ6DDKEzGk	70.199.104.181	8391	192.168.4.20	443	tcp	ssl
1355284791	BqLVVfmVO6d	70.199.104.181	8393	192.168.4.20	443	tcp	ssl
1355284761	ya3SvH6ZxX4	70.199.104.181	8408	192.168.4.20	443	tcp	ssl
1355284812	sxrPWDvcGQ2	192.168.4.20	48433	67.228.181.219	80	tcp	http
1355284903	vlvQgRiHE54	192.168.4.20	14655	192.168.4.1	53	udp	dns
1355284792	gn5FV4jeOJ4	70.199.104.181	8387	192.168.4.20	443	tcp	ssl
1355285010	uEb3j6nYBS7	59.93.52.206	61027	192.168.4.20	25	tcp	smtp
1326962278	SE2LJ7PLwIg	189.77.105.126	3	192.168.4.20	3	icmp	-
1326962279	T6rMQFaMCie	95.165.30.73	3	192.168.4.20	3	icmp	-
1329400936	qtNmAmHhDM4	192.168.4.20	14419	65.23.158.132	6668	tcp	irc
1329400884	cOctAcZusv2	192.168.4.20	32239	89.16.176.16	6666	tcp	irc

Bro Functions – Three things Bro does

Protocol Logs

Detailed protocol logs for each network protocol; including logs for tunnels, IPv4/6, files and more

Alerts

Bro–IDS is preconfigured with a variety of signature and anomaly notifications

Actions

Bro Programming Language is the real power; pivot to external applications, take advanced protocol based decisions & more.

#fields ts	uid	id.orig_h	id.orig_p	id.resp_h	id.resp_p	proto	note
#types	time	string	addr	port	addr	port	enum
1359673187	TLDtWBOrstk	192.168.0.120	61537	50.76.24.57	8443	tcp	SSL::Invalid_Server_Cert
1359673187	L4bDTmPqvs2	192.168.1.8	49540	174.143.119.91	6697	tcp	SSL::Invalid_Server_Cert
1359673187	JAvYksFW1Qb	207.188.131.2	5373	160.109.68.199	8081	tcp	SSL::Invalid_Server_Cert
1359673188	-	192.168.0.57	62220	216.234.192.231 80		tcp	Rogue_Access_Point
1359673188	5OYpDdtlnfd	192.168.0.147	45009	93.174.170.9	443	tcp	SSL::Invalid_Server_Cert
1359673188	-	192.168.0.147	36511	74.125.225.194	80	tcp	Rogue_Access_Point
1359673188	-	-	-	-	-	-	Software::Vulnerable_Version
1359673188	93CIvevOuxk	192.168.0.147	51897	98.136.223.39	8996	tcp	SSL::Invalid_Server_Cert
1359673209	YpCOvC9p4Ef	208.89.42.50	48620	207.188.131.2	22	tcp	SSH::Login
1359673210	SaKFGzmdXLl	207.188.131.2	11175	23.5.112.107	443	tcp	SSL::Invalid_Server_Cert
1359673214	XLE8fYl5Tvg	207.188.131.2	11677	208.66.139.142	2145	tcp	SSL::Invalid_Server_Cert
1359673214	-	192.168.1.120	60141	74.125.225.195	80	tcp	Rogue_Access_Point
1359673218	NyPHd3qjlKe	208.89.42.50	43891	207.188.131.2	22	tcp	SSH::Login
1359673223	0skn2N4oYbj	192.168.1.116	49249	15.201.49.137	80	tcp	HTTP::MD5
1359673224	Q83ji8AFOO1	192.168.1.116	49250	15.192.45.26	80	tcp	HTTP::MD5
1359673229	WU57HOSwkEj	208.89.42.50	62165	207.188.131.2	22	tcp	SSH::Login

Bro Functions – Three things Bro does

Protocol Logs

Detailed protocol logs for each network protocol; including logs for tunnels, IPv4/6, files and more

Alerts

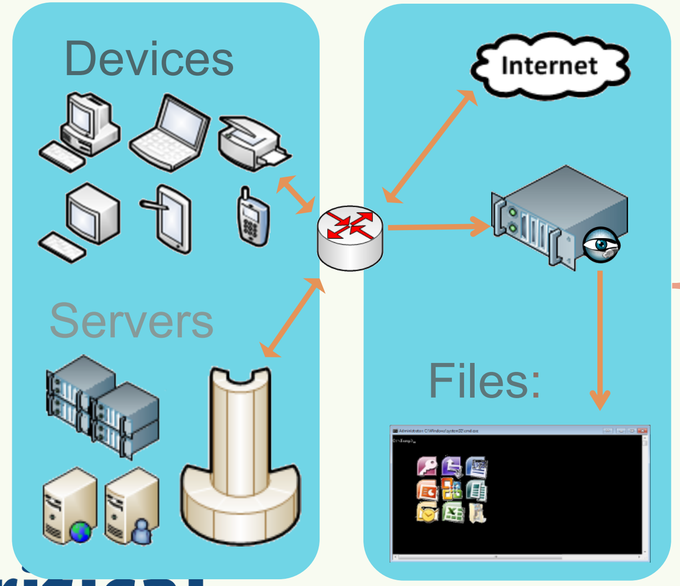
Bro–IDS is preconfigured with a variety of signature and anomaly notifications

Actions

Bro Programming Language is the real power; pivot to external applications, take advanced protocol based decisions & more.

Sensor Components

Tap: Bro Sensor



Extracted File Analysis

Signature Analysis
- Active Analysis→ Malware Hash Registry
- Intel Comparison → OSINT, FS-ISAC, DOE CIRC…

Active Analysis
- www.Malware-Tracker.com
- Static & Dynamic Analysis
- Cuckoo Box? Volatility

Long Term Analysis
- Coverage for Mobile Devices, Embedded
- Post Compromise Research
- Analysis- copy of every EXE in Company

Predicative Analysis
- AV, Malwarebytes→ Open a Ticket
- Content Analysis- Keywords,

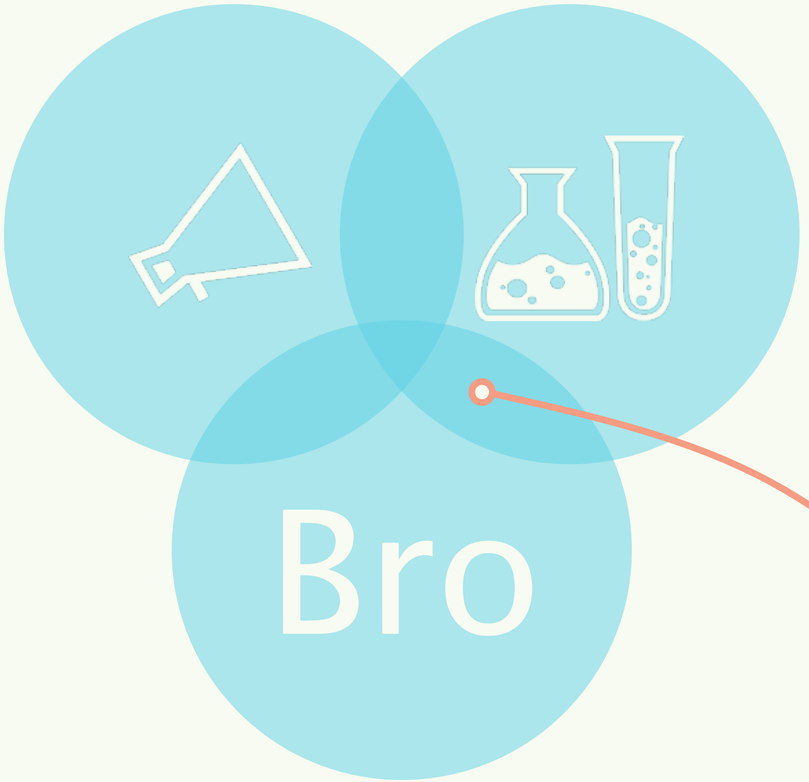
Signature Detection

atomic indicators

domains, file hashes, IPv4/6

Traditional Signatures

Algorithms



Anomaly Detection

Traffic Analysis

Flow Analysis

Protocol Analysis

+ magic

OUR FOCUS POINT

Today we concentrate on that

Classically Speaking...

In the literature you will typically find IDS's broken into two distinct categories– Signature or Anomaly based Detection.

Bro is designed to face Next Generation Challenges.

Bro Platform

Hybrid System

Best of Both Worlds

+ a programming language

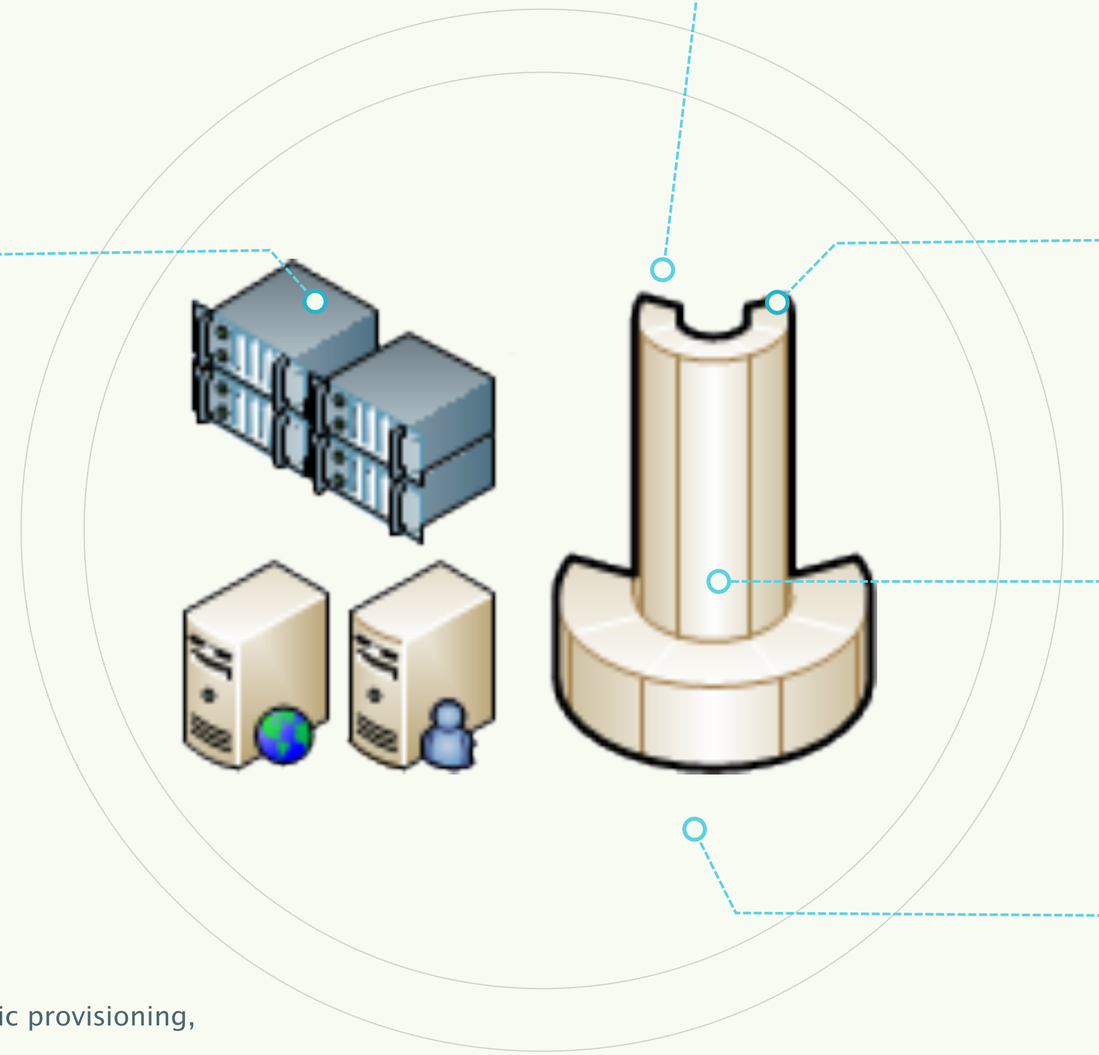
General Scan– Host Based, Port Based, ICMP Probing

Host Based

Laterally from host to host
Typically for a type of service
“Worm”

Concepts

General Case is Host / Port
Map the network
Forward / Reverse DNS
Lots of Record Types



Abuse Tools

Dnmap, zenmap, scapy, nc, etc.

Protocol Tools

sipvicious, sslscan,

Tracerouting

Map depth and routes of the network

TCP, UDP, ICMP Probing

Key internet protocol frequently used for dynamic provisioning, service location; only some details documented

Traditional Scanning

Many people only think of traditional recon

Host Scan

Recon multiple ports for services, typically common, looking for banners.

Tag out specific services.

Tracerouting

Probe infrastructure; relationships, depth.

Learn about network complexity.

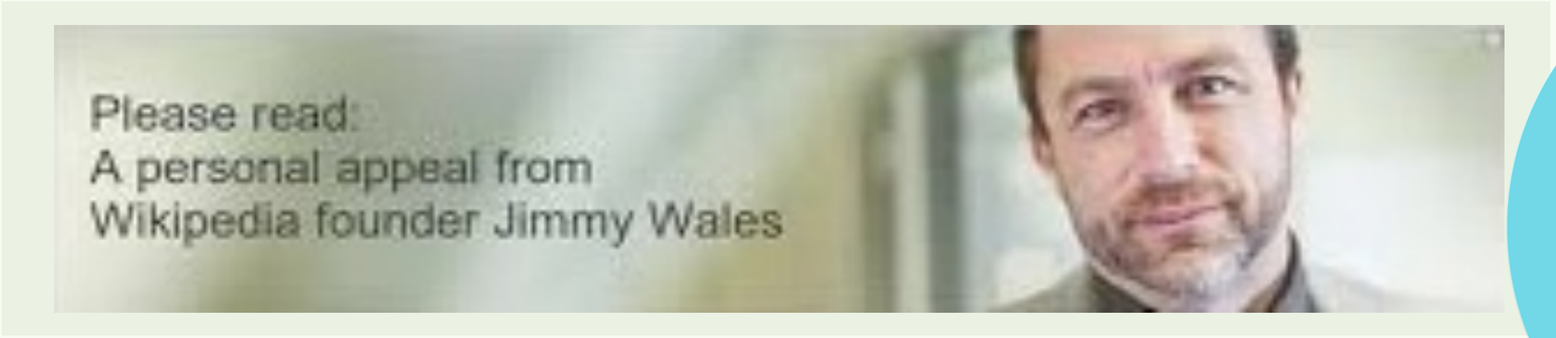
Port Scan

Taking the general many DNS Attacks are noisy and fail.

Let's watch for some extreme failures.

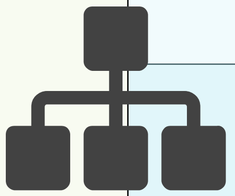
"Summary statistics are used to summarize a set of observations, in order to communicate the largest amount as simply as possible."

General Purpose Measurement



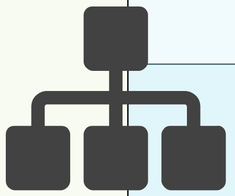
Cluster Safe!

Traffic Mapping – Map amount of traffic to CPU load



CPU	CPU	CPU	CPU
CPU	CPU	CPU	CPU
CPU	CPU	CPU	CPU
CPU	CPU	CPU	CPU
CPU	CPU	CPU	CPU

Big Idea – Map reduce on data in Motion



bro	bro	bro	bro
bro	bro	bro	bro
bro	bro	bro	bro
bro	bro	bro	bro
bro	bro	bro	bro

Measurement

Sumstats is our cluster safe library for measuring "stuff"

Epoch

Discrete Time Slices

Streaming

Realtime Data Handling

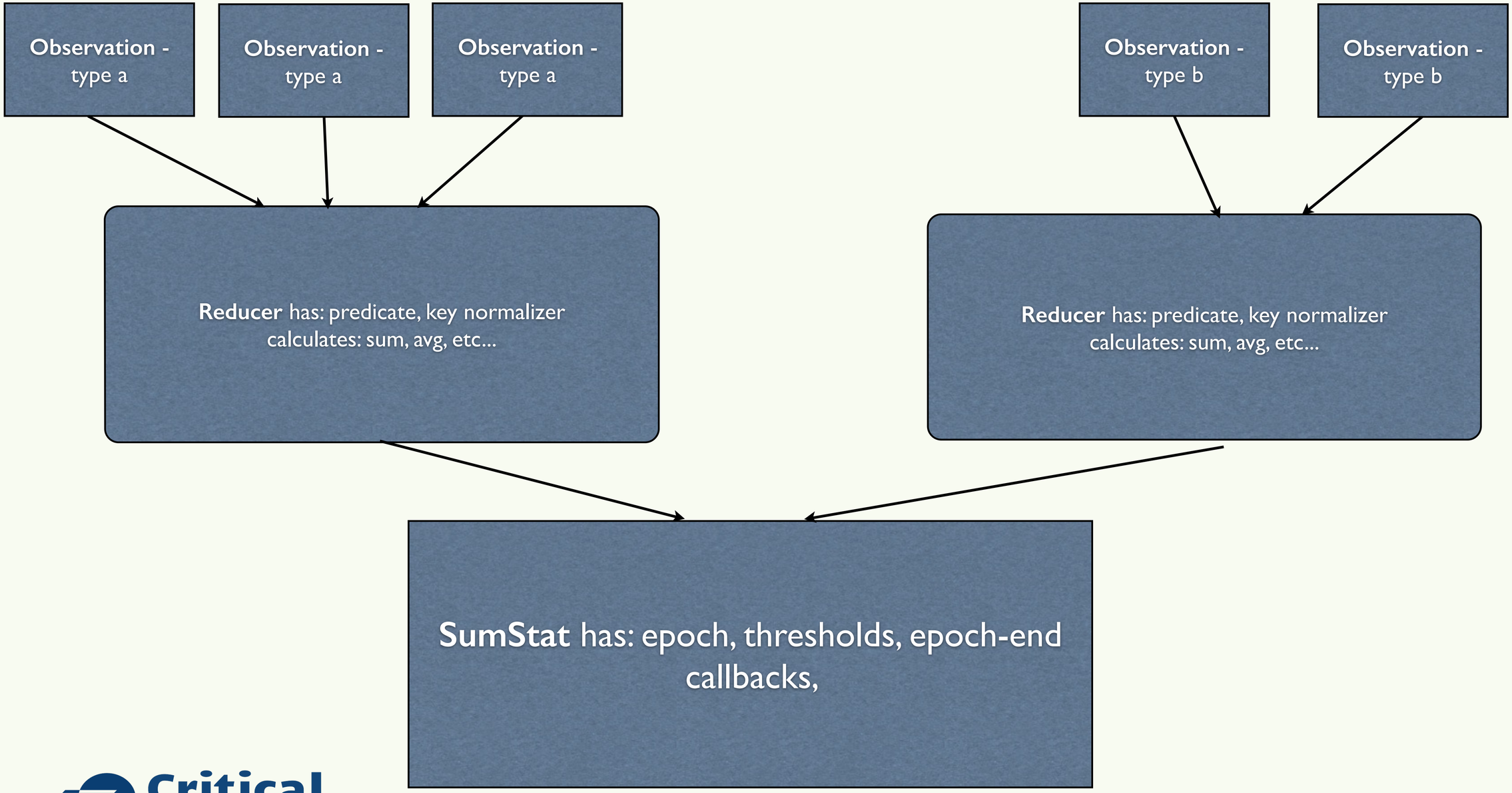
Composable

Measurements MUST be **merge-able** for Cluster Support

Probabilistic

HyperLogLog
Top-K

Model – She may not look like much, but she's got it where it counts..



Traditional Scanning

Many people only think of traditional recon

Host Scan

Recon multiple ports for services, typically common, looking for banners.

Tag out specific services.

Tracerouting

Probe infrastructure; relationships, depth.

Learn about network complexity.

Port Scan

Taking the general many DNS Attacks are noisy and fail.

Let's watch for some extreme failures.

Protocol Details

RFC 1035
Stateless
UDP or TCP

Concepts

Authoritative Server (Recursive)
Key / Value Store
Forward / Reverse DNS
Lots of Record Types

Abuse Tools

DNS Recon, DNS Map,
DNS Enum, DNS Tracer,
DNS Walk

Record Types

A, CNAME, SRV, AAAA, MX
DNAME, SOA

Security Problems

Information Disclosure, DNS
Amplification, Spoofing, MitM

Domain Name System

Key internet protocol frequently used for dynamic provisioning, service location; only some details documented

AXFR / IXFR

Attacker asks DNS Server for a copy of the DNS Zone.

Frequently fails, try it anyway.

PTR Abuse

Attacker mines DNS infrastructure for host details PTR Records.

Typically see reverse of entire subnet.

NXDomain

Taking the general many DNS Attacks are noisy and fail.

Let's watch for some extreme failures.

Protocol Details

RFC 2616
Stateless
TCP

Concepts

Common Exploit Vector
High Profile Attacks
Frequent Target

Abuse Tools

DirBuster
Burp
sqlmap

Exploitability

Abused frequently on both client side and server side assaults

Security Problems

sql injection, information disclosure, default apps

Hypertext Transfer Protocol

Key internet protocol frequently used for dynamic provisioning, service location; only some details documented

HTTP Bruteforce

Attacker queries server for common URIs.

May be used to look for default apps, CMSs, common names, etc.

HTTP Basic Auth

Attacker attempts brute force of protected web resources.

Hacking like it's 1996.

HTTP SQL Injection

Attacker abuses web resources to extract information from back end DB.

Common exploit vector.

TLS/SSL– Target 4, commonly used to transport...

Protocol Details

RFC 5246 + others
Stateful
TCP based

Concepts

Used to conceal traffic
Attacks Surface?
Little publicly known

Abuse Tools

sslscan
sslcaudit
tor, ssltrip

Exploitability

Typically used as a transport
Are you monitoring Gear?

Security Problems

Running in / through your network

Transport Layer Security/ Secure Socket Layer

Key internet protocol frequently used for dynamic provisioning, service location; only some details documented

TOR

Transport.

May be malicious.

Lucky 13

Latest in a series of high profile SSL/TLS Attacks.

This space is not nearly as safe as people assume.

SSL Attacks – Lucky 13 Attack

NEEDLE IN A HAYSTACK?

1

client_hello_count:	11
server_hello_count:	11
extension_count:	142
ssl_established_count:	11
ssl_alert_count:	0
ssl_ticket_handshake_count:	7
x509_certificate_count:	14
x509_extension_count:	0
x509_error_count:	0

2

l_client_hello_count:	12
l_server_hello_count:	12
l_extension_count:	128
ssl_established_count:	12
ssl_alert_count:	0
ssl_ticket_handshake_count:	6
x509_certificate_count:	21
x509_extension_count:	0
x509_error_count:	0

3

_client_hello_count:	2
ssl_server_hello_count:	2
ssl_extension_count:	0
ssl_established_count:	2
ssl_alert_count:	0
ssl_ticket_handshake_count:	0
x509_certificate_count:	1
x509_extension_count:	0
x509_error_count:	0

4

l_client_hello_count:	4096
ssl_server_hello_count:	0
ssl_extension_count:	12288
ssl_established_count:	0
ssl_alert_count:	4
ssl_ticket_handshake_count:	0
x509_certificate_count:	0
x509_extension_count:	0
x509_error_count:	0

Carna Botnet

aka “Alien Worm”

aka Internet Census 2012

Image 1 – Aashish Sharma

Aashish Sharma

Lawrence Berkeley National Lab

Works with an incredible team of IR.

Incredible speaker.

Bro Power User

Catch and Release with Bro

System acts as an Internet Telescope

Sample of Anomalies

June 2011– Morto Worm
June 2012– “Alien Worm”
June 2012– CVE-2012-2122-mysql-authentication-bypass

Link

http://ee.lbl.gov
http://www.lbl.gov

Carna Botnet – "Port scanning /0 using insecure embedded devices"

"..we discovered an amazing number of open embedded devices on the Internet.

Many of them are based on Linux and allow login to standard BusyBox with empty or default credentials."

?

Default Credentials

ACCESS

"..insecure devices are located basically everywhere on the Internet. They are not specific to one ISP or country.

So the problem of default or empty passwords is an Internet and industry wide phenomenon."

25%

420,000 Devices

SCOPE

"The binary on the router was written in plain C. It was compiled for 9 different architectures using the **OpenWRT Buildroot**.

In its latest and largest version this binary was between 46 and 60 kb in size depending on the target architecture."

/0

Scan Stuff

PAYLOAD

http://internetcensus2012.bitbucket.org/paper.html

Default Password

root / <blank>

root / 123456

"Hilinux" Busybox

```
Linux (none) 2.6.24-rt1-hi3520v100
#2010033002 Wed Mar 31 13:05:50 EST
2010 armv6l unknown
```

Custom Payload

4 ARM Binaries

Revision Jun 28, 2012

Activity Back to May 30, 2012

```
-rwxr-xr-x  0 root   root     8610 Jun 28 19:19 t2.arm_v6k
-rwxr-xr-x  0 root   root    13492 Jun 28 04:44 sp.arm_v6k
drwxr-xr-x  0 root   root        0 Jul 23  2007 run/
-rw-r--r--  0 root   root       33 Jun 28 04:02 response
-rw-r--r--  0 root   root      371 Jun 28 04:02 readme
-rw-r--r--  0 root   root    49152 Jul  5 09:19 pz
-rw-r--r--  0 root   root        0 Jul  3 13:01 j
-rw-r--r--  0 root   root       33 Jun 28 04:02 idhash
-rwxr-xr-x  0 root   root     5013 Jun 28 19:19 ht.arm_v6k
-rw-r--r--  0 root   root       33 Jun 28 04:02 challenge
-rwxr-xr-x  0 root   root    10938 Jun 28 04:05 b.arm_v6k
-rw-r--r--  0 root   root       10 Jul  3 13:21 1.run
-rw-r--r--  0 root   root       10 Jul  3 13:21 0.run
```

4K Payload

Scanning files

Logs

Daemon tcp/210

https://isc.sans.edu/port.html?port=210

Directory Listing Compromised Device

This is from one sample device– there would be minor differences between the 9 different architectures.

"Hello,

Your router had a very simple or no telnet password at all. We temporary use it for a non-profit research project to map the internet, all research results will be made public. We have no intent to damage your device or harm your privacy in any way."

May 2012

readme- Carna Botnet Author

Listed an email to contact "them."

Device – What do the devices look like?

Image 1 – Vulnerable Wansview PTZ Camera

Image 2 – Vulnerable Q-See DVR

Image 3 – Vulnerable Smarteye PTZ Camera

Dozens of Vulnerable Models

Consider where in your network these resources would be deployed.
- Sensitive area's
- Behind your firewall

One "Chinese" OEM

Production traced by to single OEM
Initially very concerning

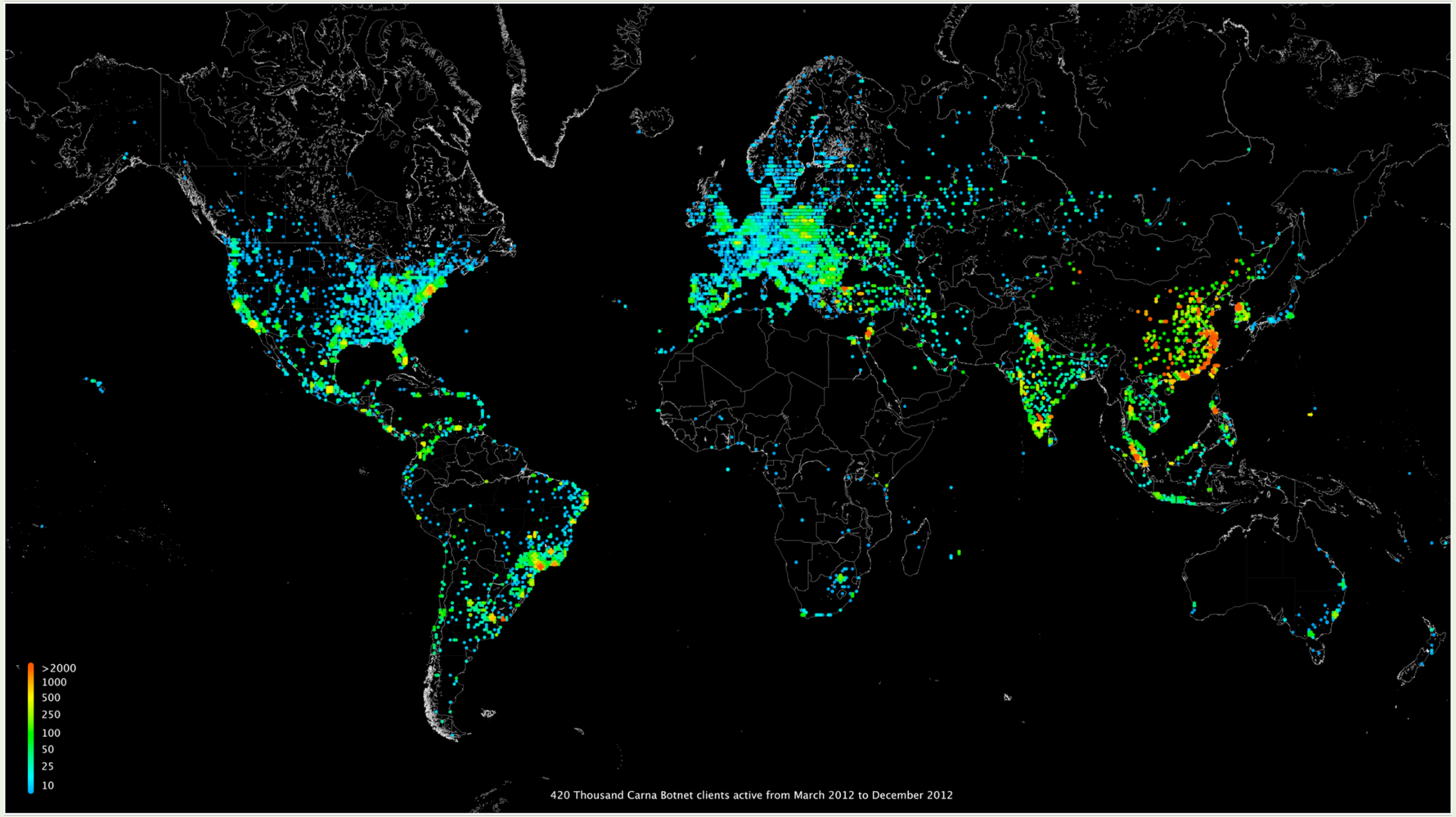
Retailed By

Meier Grocery Store
Sams Club
Amazon.com
Costco
100's of Retailers online

Link

https://www.q-see.com/
http://wansview.net/

A Picture – is worth 420,000 devices....



Carna Botnet Details

Most camera's on Asian based networks.
Scattered activity, single origin.
SYN Packets Only

Top ASN (4134) = 25% of Infections
ASN 4134 (CN)– China Telcom

Top 5 ASN– 50% of Infections
–ASN 3462 (TW)– Data Communications Business Group
–ASN 4837 (CN)– China Unicom
–ASN 9121 (TUR)– Turk Telcom
–ASN 4788 (MY)– TM Net

Top 16 = 60% of Infections
Long Tail of Infections
Global in Scope

http://internetcensus2012.bitbucket.org/paper.html

?

Questions?

Thank you!

BYE!