

UEPtSS:

*Unconstrained End-Point  
Security System*



Fatema Bannat Wala  
Security Engineer  
Technical Security Group  
University of Delaware  
[Fatema.bannatwala@gmail.com](mailto:Fatema.bannatwala@gmail.com)

# About Me

2

- A very big fan of BRO IDS
- Have been working with Bro for past two years
- Joined UD's Network and Systems Services (IT-NSS Team) in 2015
- Passionate about Cyber-Security
- Also a part-time Ph.D student

# Roadmap of today's talk

3

- What is UEPtSS?
- Motivation
- Why use Bro for UEPtSS?
- How to use Bro for UEPtSS?
- An inventory of End-Points and running software
- Usefulness of UEPtSS
- Some use-cases

# What is UEPTSS?

4

Sniff traffic



Fingerprint device



## An inventory of Unconstrained systems

client_ip	latest_time	mac	dmacs	vendor	known_services	software_type	software_info
128.4	08/20/2017 15:01:33	10:41:7f	1	Apple, Inc.		IOS-IPHONE	iPhone,10,3,Phone7,2AT&T
128	08/20/2017 14:50:17	34:17:eb	1	Dell Inc.	22,tcp,(empty)	SSH-SERVER	OpenSSH,5.3,-
128	08/20/2017 15:06:18.763725	78:2b:cb	1	Dell Inc.	22,tcp,SSH	SSH-SERVER	OpenSSH,6.6p1
128	08/20/2017 14:54:20	00:1e:68	1	QUANTA COMPUTER INC.	22,tcp,(empty)	SSH-SERVER	OpenSSH,5.9p1
128	08/20/2017 15:04:22.440988	90:b1:1c	1	Dell Inc.	22,tcp,SSH	SSH-SERVER	OpenSSH,6.6,-
128	08/20/2017 14:51:21	14:da:e9	1	ASUSTek COMPUTER INC.	22,tcp,(empty)	SSH-SERVER	OpenSSH,7.2p2
128	08/20/2017 15:02:13	4ccc:6a	1	Micro-Star INTL CO., LTD.	22,tcp,(empty)	SSH-SERVER	OpenSSH,7.2p2
128	08/20/2017 14:55:01	98:90:96	1	Dell Inc.		OS-WINDOWS	Windows,10,0,10
128	08/20/2017 14:39:30	14:fe:b5	1	Dell Inc.		OS-WINDOWS	Windows,10,0,10
128	08/20/2017 15:06:00.641491	e0:9d:31	1	Intel Corporate		OS-WINDOWS	Windows,6,1,7 or Server 2008 R2
128	08/20/2017 15:06:21.108368	ac:87:a3	1	Apple, Inc.		MACOS-MACINTOSH	Macintosh,10,10,Yosemite

# Motivation....

5

- Some organizations can't control some or all of their end user computer systems. Examples include: universities, shared startup spaces, sites offering public Internet access (e.g. restaurants), and conferences.
- If the data pertaining of end user systems is organized and cataloged as part of normal information security logging activities, an extended picture of what the end system actually is may be available to the investigator at a moment's notice.

# Solution??

6

- Two ways:
- Active Scanning: nmap, Nessus, Qualys other commercial products.
  - Pros: Accuracy, many plugins and scripts targeted towards specific software detection.
  - Cons: Have to be 'active' very frequently, commercial plugins are expensive, user intervention needed. Free versions have limited usability.
- Passive Scanning: Use existing tools, IDS/IPS systems. Ex: Bro.
  - Pros: Active all the time, no user intervention, free and open source, can be customized to detect specific s/w.
  - Cons: Not very highly accurate (depends on the traffic it sees on the n/w).

# Why Bro for UEPTSS?

- Why Not! (It's FREE, has great community support, offers different scripts)
- One of the coolest features of BRO is, it's a great sniffer and generates *[User-Friendly]* logs of what it saw on the network. Take Advantage of that!
- Works great for Unconstrained devices, as no knowledge of when and who will be connecting to the network is required

# How to use BRO for UEPTSS?

- ***Leverage the built-in scripts*** for software detection and other OS finger printing
- ***Leverage Bro's scripting FW*** to write custom scripts for detecting the interesting stuff from traffic
- ***Leverage different log files*** to dig for the client specific information: software.log, known\_services.log, sites\_open\_ports.log, TLSFingerprint.log



# Scripts to load for inventory data logging

- **windows-version-detection.bro** – built-in script
- **Mac-version-detection.bro** – custom script
- **iPhone-detection.bro** – custom script
- **tls-fingerprinting.bro** – custom script [*Courtesy: Seth Hall*]
- **host-profiling.bro** – Available with scan-NG package
- **software-browser-plugins.bro** – built-in script
- **known-services.bro** – built-in script
- **Load all the scripts that detect software in various protocols** – built-in scripts

# Gathering information for the UEPTSS

10

- ▶ **Machine type** : *Use IEEE Standards Public listing (MA-L)*
- ▶ **Operating system and version** : *Bro software.log*
- ▶ **Browsers in use**: *Bro software.log*
- ▶ **Applications and versions**: *Bro software.log*
- ▶ **Different Plugins**: *Bro software.log*
- ▶ **TLS Clients**: *custom Bro log TLSfingerprint.log*
- ▶ **Open ports (services)**: *Bro known\_services.log, site\_host\_open\_ports.log*
- ▶ **Dangerous behavior history**: *IDS/IPS (snort, Bro etc)*
- ▶ **MAC address**: *DHCP logs*

# Gathering info for the UEptSS: Operating systems and version

11

```
logs [ logs]$ less current/software.log | egrep "MACOS::|OS::|iOS::" | awk -F'
\t' '{print $1, "\t", $2, "\t", $4. "\t", $10}' | more
1504803599.340398 38.  MACOS::MACINTOSH Yosemite
1504803599.696643 128 OS::WINDOWS 10
1504803599.842906 38.  MACOS::MACINTOSH Sierra
1504803600.286609 128 OS::WINDOWS 10
1504803600.280083 38.  OS::WINDOWS 10
1504803600.047552 128 MACOS::MACINTOSH EI Captain
1504803600.151087 38.  MACOS::MACINTOSH Sierra
1504803600.389451 128 OS::WINDOWS 10
1504803600.119828 128 iOS::IPHONE -
1504803600.827585 38.  MACOS::MACINTOSH Sierra
1504803600.279821 38.  MACOS::MACINTOSH Yosemite
1504803601.007100 128 iOS::IPHONE -
1504803600.860841 128 OS::WINDOWS 7 or Server 2008 R2
1504803601.038033 128 MACOS::MACINTOSH EI Captain
1504803601.501386 128 MACOS::MACINTOSH EI Captain
1504803601.377444 38.  MACOS::MACINTOSH Sierra
1504803601.360030 38.  iOS::IPHONE -
1504803601.961420 128 iOS::IPHONE iPhone9,4AT&T
1504803601.445343 38.  iOS::IPHONE -
1504803602.174284 38.  MACOS::MACINTOSH EI Captain
1504803602.164746 128 MACOS::MACINTOSH Sierra
1504803601.653305 38.  MACOS::MACINTOSH Sierra
1504803601.934646 38.  MACOS::MACINTOSH Sierra
1504803602.165810 38.  MACOS::MACINTOSH EI Captain
1504803601.854187 38.  MACOS::MACINTOSH EI Captain
1504803602.121702 38.  MACOS::MACINTOSH Sierra
1504803602.027098 38.  MACOS::MACINTOSH Sierra
1504803602.160101 128 MACOS::MACINTOSH Sierra
1504803602.623438 128 MACOS::MACINTOSH Sierra
1504803602.649276 128 MACOS::MACINTOSH EI Captain
```

# Gathering info for the UEPtSS: Browsers in use

12

```
logs
[logs]$ less current/software.log | egrep "HTTP::BROWSER" | awk -F'\t' '{print $1,"\t", $2,"\t", $4,"\t", $5,$6,$7}' | more
1504803600.782024      128      HTTP::BROWSER      cloudd 651 14
1504803601.066494      128      HTTP::BROWSER      Chrome 60 0
1504803601.396806      128      HTTP::BROWSER      MSIE 11 0
1504803601.060423      128      HTTP::BROWSER      AppleCoreMedia 1 0
1504803601.474983      128      HTTP::BROWSER      Safari 10 1
1504803601.283953      128      HTTP::BROWSER      NewsToday 1000 -
1504803600.975556      128      HTTP::BROWSER      Microsoft-CryptoAPI 10 0
1504803601.568334      128      HTTP::BROWSER      Agent 2087369893 -
1504803601.015429      128      HTTP::BROWSER      Omelette 198 -
1504803601.100742      38.      HTTP::BROWSER      Chrome 60 0
1504803601.551074      128      HTTP::BROWSER      Microsoft NCSI - -
1504803601.302071      128      HTTP::BROWSER      AppleNewsWidget 608 5
1504803601.300689      128      HTTP::BROWSER      AppleNewsWidget 608 5
1504803601.505984      128      HTTP::BROWSER      Chrome 60 0
1504803601.786981      128      HTTP::BROWSER      MSIE 8 0
1504803601.807103      128      HTTP::BROWSER      com.apple.appstored 1 0
1504803601.688483      38.      HTTP::BROWSER      Firefox 43 0
1504803602.000256      38.      HTTP::BROWSER      Safari 10 0
1504803602.016258      38.      HTTP::BROWSER      Chrome 60 0
1504803602.040124      38.      HTTP::BROWSER      Chrome 60 0
1504803602.113375      128      HTTP::BROWSER      AppNOS 2 -
1504803601.784988      38.      HTTP::BROWSER      Chrome 52 0
1504803601.906976      128      HTTP::BROWSER      NewsToday 1000 -
1504803601.994771      38.      HTTP::BROWSER      Safari 10 0
1504803601.923709      128      HTTP::BROWSER      Chrome 60 0
1504803601.836647      38.      HTTP::BROWSER      Safari 10 1
1504803601.807896      128      HTTP::BROWSER      com.apple.appstored 1 0
1504803602.031275      128      HTTP::BROWSER      trustd (unknown version) CFNetwork 811 5
1504803601.562576      38.      HTTP::BROWSER      Firefox 55 0
--More--
```

# Gathering info for the UEptSS: Applications and versions

13

```
logs
[logs]$ less current/software.log | egrep "HTTP::APPSEVER" | awk -F'\t' '{print $1,
\t", $2, " ", $3, "\t", $4, "\t", $5, $6, $7}' | more
1504804710.245566      128      80      HTTP::APPSEVER      ASP.NET - -
1504804728.687649      128      80      HTTP::APPSEVER      PHP 5 3
1504804730.652638      128      80      HTTP::APPSEVER      PHP 5 3
1504804785.110239      128      80      HTTP::APPSEVER      PHP 5 5
1504804826.774401      128      80      HTTP::APPSEVER      ASP.NET - -
1504804851.515563      128      80      HTTP::APPSEVER      ASP.NET - -
1504804863.326578      128      80      HTTP::APPSEVER      PHP 5 3
1504804911.000248      128      80      HTTP::APPSEVER      PHP 5 6
1504804918.882208      128      80      HTTP::APPSEVER      PHP 5 3
1504804939.647909      128      80      HTTP::APPSEVER      ASP.NET - -
1504804939.647909      128      80      HTTP::APPSEVER      SharePoint 14 0
1504804939.642234      128      80      HTTP::APPSEVER      ASP.NET - -
1504804939.642234      128      80      HTTP::APPSEVER      SharePoint 14 0
1504804939.649749      128      80      HTTP::APPSEVER      ASP.NET - -
1504804939.649749      128      80      HTTP::APPSEVER      SharePoint 14 0
1504804939.648653      128      80      HTTP::APPSEVER      ASP.NET - -
1504804939.648653      128      80      HTTP::APPSEVER      SharePoint 14 0
1504804939.646061      128      80      HTTP::APPSEVER      ASP.NET - -
1504804939.646061      128      80      HTTP::APPSEVER      SharePoint 14 0
1504804944.285301      128      80      HTTP::APPSEVER      PHP 7 1
1504804985.287677      128      80      HTTP::APPSEVER      PHP 7 0
1504804985.928326      128      80      HTTP::APPSEVER      PHP 7 0
1504805135.749526      128      80      HTTP::APPSEVER      PHP 5 6
1504805140.870156      38.      80      HTTP::APPSEVER      ASP.NET - -
1504805146.061972      128      80      HTTP::APPSEVER      ASP.NET - -
1504805201.409510      128      80      HTTP::APPSEVER      PHP 5 6
1504805201.730019      128      80      HTTP::APPSEVER      PHP 5 5
1504805225.476012      128      80      HTTP::APPSEVER      PHP 5 6
1504805239.808327      128      80      HTTP::APPSEVER      PHP 5 3
1504805245.854806      128      80      HTTP::APPSEVER      PHP 5 3
```

# Gathering info for the UEptSS: Different Plugins

```
.logs
[logs]$ less current/software.log | egrep "HTTP::BROWSER_PLUGIN" | awk -F'\t' '{print $1,
\t", $2, "\t", $4, "\t", $5, $6, $7, $8, $9}' | more
1504786883.102526      128      HTTP::BROWSER_PLUGIN      AdobeAIR-Flash 22 0 0 175
1504786896.695848      128      HTTP::BROWSER_PLUGIN      ShockwaveFlash 26 0 0 151
1504786902.068335      128      HTTP::BROWSER_PLUGIN      Widevine Content Decryption Module - -
1504784154.042879      38.      HTTP::BROWSER_PLUGIN      Flash 21 0 0 213
1504786902.068335      128      HTTP::BROWSER_PLUGIN      Chrome PDF Viewer - - - -
1504784536.246883      128      HTTP::BROWSER_PLUGIN      Flash 10 0 45 2
1504788240.916485      128      HTTP::BROWSER_PLUGIN      AdobeAIR-Flash 12 0 0 38
1504788241.395144      128      HTTP::BROWSER_PLUGIN      AdobeAIR-Flash 12 0 0 38
1504786925.371715      128      HTTP::BROWSER_PLUGIN      Chrome PDF Viewer - - - -
1504786925.371715      128      HTTP::BROWSER_PLUGIN      Native Client - - - -
1504786939.263979      128      HTTP::BROWSER_PLUGIN      ShockwaveFlash 26 0 0 151
1504786940.252380      128      HTTP::BROWSER_PLUGIN      Widevine Content Decryption Module - -
- -
1504786940.252380      128      HTTP::BROWSER_PLUGIN      Chrome PDF Viewer - - - -
1504786940.252380      128      HTTP::BROWSER_PLUGIN      Native Client - - - -
1504786940.540762      128      HTTP::BROWSER_PLUGIN      ShockwaveFlash 26 0 0 151
1504786946.505579      128      HTTP::BROWSER_PLUGIN      ShockwaveFlash 26 0 0 151
1504786950.228813      128      HTTP::BROWSER_PLUGIN      Widevine Content Decryption Module - -
- -
1504786950.228813      128      HTTP::BROWSER_PLUGIN      Chrome PDF Viewer - - - -
1504786950.228813      128      HTTP::BROWSER_PLUGIN      Native Client - - - -
1504786953.808282      128      HTTP::BROWSER_PLUGIN      ShockwaveFlash 26 0 0 151
1504786957.399482      128      HTTP::BROWSER_PLUGIN      WebKit built-in PDF - - - -
1504786975.459031      128      HTTP::BROWSER_PLUGIN      WebKit built-in PDF - - - -
1504786979.478851      128      HTTP::BROWSER_PLUGIN      Widevine Content Decryption Module - -
- -
1504786979.478851      128      HTTP::BROWSER_PLUGIN      Chrome PDF Viewer - - - -
1504786979.478851      128      HTTP::BROWSER_PLUGIN      Native Client - - - -
1504787010.214084      128      HTTP::BROWSER_PLUGIN      Shockwave Flash - - - -
--More--
```

# Gathering info for the UEPTSS: Open ports (Known services)

15

```
logs [logs]$ less current/known_services.log | egrep -v "#" | more|
1504811160.392132 128 443 tcp SSL
1504811178.916706 128 80 tcp HTTP
1504811182.097852 128 80 tcp HTTP
1504811186.808373 128 16393 udp SIP
1504811199.416724 128 50247 udp DTLS
1504811222.843155 128 55141 udp DTLS
1504811258.476415 128 80 tcp HTTP
1504811273.083874 128 25 tcp SMTP
1504811343.603564 128 5060 udp SIP
1504811354.182085 128 80 tcp HTTP
1504811360.356647 128 54472 udp DTLS
1504811364.865151 128 16393 udp SIP
1504811366.567350 128 443 tcp SSL
1504811367.552843 128 80 tcp HTTP
1504811370.050212 128 16393 udp SIP
1504811387.571469 128 49902 udp DTLS
1504811391.407310 128 59428 udp DTLS
1504811395.700189 128 59550 udp DTLS
1504811396.789903 128 25 tcp SMTP
1504811397.503175 128 443 tcp SSL
1504811400.929952 128 80 tcp HTTP
1504811401.654765 128 55542 udp DTLS
1504811401.663706 128 58201 udp DTLS
1504811401.673289 128 54059 udp DTLS
1504811402.166916 128 80 tcp HTTP
1504811423.809323 128 25 tcp SMTP
1504811448.950721 128 25 tcp SMTP
1504811465.330472 128 80 tcp HTTP
1504811478.856420 128 25 tcp SMTP
1504811510.599546 128 80 tcp HTTP
1504811513.105728 128 80 tcp HTTP
```

# Gathering info for the UEptSS: TLS Clients

16

```
.logs
[.logs]$ less current/TLSfingerprint.log | awk -F'\t' '{print $1,"\t",$3,"\t",
$6,"\t",$8,$9}' | more
1504810808.178643      128      [REDACTED]      5222      py2app application (including box.net & go
ogle drive clients) TLSv10
1504810807.701033      128      [REDACTED]      443      AppleWebKit/600.7.12 TLSv12
1504810808.067846      128      [REDACTED]      443      Chrome 50.0.2661.102 1 TLSv12
1504810807.456551      128      [REDACTED]      443      Safari 537.78.2 TLSv12
1504810808.003970      128      [REDACTED]      443      Chrome 51.0.2704.84 5 TLSv12
1504810808.185033      128      [REDACTED]      443      AppleWebKit/600.7.12 TLSv12
1504810808.025882      128      [REDACTED]      443      Android webkit Thing TLSv12
1504810861.530974      128      [REDACTED]      443      w3m (tested: 0.5.3 OS X) TLSv12
1504810861.472116      128      [REDACTED]      443      w3m (tested: 0.5.3 OS X) TLSv12
1504810808.239639      128      [REDACTED]      443      BlueCoat Proxy TLSv12
1504810807.733206      128      [REDACTED]      443      AppleWebKit/600.7.12 or 600.1.4 TLSv12
1504810807.701031      128      [REDACTED]      443      AppleWebKit/600.7.12 TLSv12
1504810807.968403      128      [REDACTED]      443      Chrome 51.0.2704.84 5 TLSv12
1504810808.149556      128      [REDACTED]      443      AppleWebKit/600.7.12 TLSv12
1504810807.811683      128      [REDACTED]      443      Chrome 51.0.2704.84 5 TLSv12
1504810800.246142      38.      [REDACTED]      443      BlueCoat Proxy TLSv12
1504810799.850198      128      [REDACTED]      443      MS Edge TLSv12
1504810807.697424      128      [REDACTED]      443      AppleWebKit/600.7.12 TLSv12
1504810808.259722      128      [REDACTED]      443      Microsoft windows Socket (Tested: windows
10) TLSv12
1504810807.700473      128      [REDACTED]      443      AppleWebKit/600.7.12 TLSv12
1504810807.708165      128      [REDACTED]      443      Safari 537.78.2 TLSv12
1504810807.810430      128      [REDACTED]      443      Microsoft windows Socket (Tested: windows
10) TLSv12
1504810807.699767      128      [REDACTED]      443      AppleWebKit/600.7.12 TLSv12
1504810842.135542      128      [REDACTED]      443      curl 7.35.0 (tested Ubuntu 14.x openssl 1
.0.1f) TLSv12
1504810842.549057      128      [REDACTED]      443      Git-Bash (Tested v2.6.0) / curl 7.47.1 (cy
gwin) TLSv12
```



# Putting everything together

- ➔ Any log aggregation tool to glue all the info together, with IP being the primary key in each type of log file...



# UEPtSS : An inventory of *unconstrained* systems

client_ip	latest_time	mac	dmacs	vendor	known_services	software_type	software_info	TLS_client
128.4. [REDACTED]	08/20/2017 15:01:33	10:41:7f: [REDACTED]	1	Apple, Inc.		iOS::IPHONE	iPhone,10,3,iPhone7,2AT&T	
128. [REDACTED]	08/20/2017 14:50:17	34:17:eb: [REDACTED]	1	Dell Inc.	22,tcp,(empty)	SSH::SERVER	OpenSSH,5,3,-	
128. [REDACTED]	08/20/2017 15:06:18.763725	78:2b:cb: [REDACTED]	1	Dell Inc.	22,tcp,SSH	SSH::SERVER	OpenSSH,6,6,p1	AppleWebKit/535 & Ubuntu Product Search,TLSv12 OpenSSL_s_client (tested: 1.0.1f - Ubuntu 14.04TS),TLSv12
128. [REDACTED]	08/20/2017 14:54:20	00:1e:68: [REDACTED]	1	QUANTA COMPUTER INC.	22,tcp,(empty)	SSH::SERVER	OpenSSH,5,9,p1	
128. [REDACTED]	08/20/2017 15:04:22.440988	90:b1:1c: [REDACTED]	1	Dell Inc.	22,tcp,SSH	SSH::SERVER	OpenSSH,6,6,-	
128. [REDACTED]	08/20/2017 14:51:21	14:da:e9: [REDACTED]	1	ASUSTek COMPUTER INC.	22,tcp,(empty)	SSH::SERVER	OpenSSH,7,2,p2	
128. [REDACTED]	08/20/2017 15:02:13	4c:cc:6a: [REDACTED]	1	Micro-Star INTL CO., LTD.	22,tcp,(empty)	SSH::SERVER	OpenSSH,7,2,p2	
128. [REDACTED]	08/20/2017 14:55:01	98:90:96: [REDACTED]	1	Dell Inc.		OS::WINDOWS	Windows,10,0,10	
128. [REDACTED]	08/20/2017 14:39:30	14:fe:b5: [REDACTED]	1	Dell Inc.		OS::WINDOWS	Windows,10,0,10	
128. [REDACTED]	08/20/2017 15:06:00.641491	e0:9d:31: [REDACTED]	1	Intel Corporate		OS::WINDOWS	Windows,6,1,7 or Server 2008 R2	Microsoft Updater (Windows 7SP1) / TeamViewer 11.0.56083P,TLSv12 Safari 525.21 525.29 531.22.7 533.21.1 534.57.2 / Adobe Reader DC 15.x Updater,TLSv10
128. [REDACTED]	08/20/2017 15:06:21.108368	ac:87:a3: [REDACTED]	1	Apple, Inc.		MACOS::MACINTOSH	Macintosh,10,10,Yosemite	AppleWebKit/600.7.12 or 600.1.4,TLSv12 AppleWebKit/600.7.12,TLSv12
128. [REDACTED]	08/20/2017 14:16:03.244146	ac:87:a3: [REDACTED]	1	Apple, Inc.		MACOS::MACINTOSH	Macintosh,10,12,Sierra	
128. [REDACTED]	08/20/2017 15:02:41.363188	10:9a:dd: [REDACTED]	1	Apple, Inc.	22,tcp,(empty) 80,tcp,HTTP	HTTP::SERVER SSH::SERVER	Apache,2,4,Unix OpenSSH,6,9,-	Flux,TLSv12
128. [REDACTED]	08/20/2017 15:06:02.732062	70:8b:cd: [REDACTED]	1	ASUSTek COMPUTER INC.	22,tcp,(empty) 80,tcp,HTTP	HTTP::SERVER SSH::SERVER	Apache,2,4,Ubuntu OpenSSH,7,2,p2	
128. [REDACTED]	08/20/2017 14:59:34.233089	00:50:56: [REDACTED]	1	VMware, Inc.	80,tcp,(empty)	HTTP::SERVER	Microsoft-HTTPAPI,2,0,-	
128. [REDACTED]	08/20/2017 15:05:14.453996	54:9f:35: [REDACTED]	1	Dell Inc.	22,tcp,(empty) 3690,tcp,(empty) 443,tcp,SSL 80,tcp,HTTP 8080,tcp,HTTP	HTTP::SERVER	Apache,2,4,Ubuntu	wget 1.18,TLSv12
128. [REDACTED]	08/20/2017 14:43:03	00:1c:c0: [REDACTED]	1	Intel Corporate		HTTP::BROWSER_PLUGIN	ShockwaveFlash,26,0,-	

# Usefulness: Policy enforcement1- All old OpenSSH servers

client_ip	latest_time	mac	dmacs	vendor	known_services	software_type	software_info
128. [REDACTED]	08/20/2017 15:44:24.125195	00:50:56: [REDACTED]	1	VMware, Inc.	22,tcp,(empty) 443,tcp,SSL 80,tcp,HTTP	HTTP::APPSERVER HTTP::SERVER SSH::SERVER	Apache,2,4,CentOS OpenSSH,6,6,- PHP,5,4,-
128. [REDACTED]	08/20/2017 14:33:46.886734	00:50:56: [REDACTED]	1	VMware, Inc.	22,tcp,(empty) 443,tcp,(empty) 443,tcp,SSL 80,tcp,HTTP	HTTP::APPSERVER HTTP::SERVER SMTP::MAIL_CLIENT SSH::SERVER	Apache,2,2,CentOS Drupal,-,- OpenSSH,5,3,- PHP,5,3,-
128. [REDACTED]	08/20/2017 15:52:12.183246	00:50:56: [REDACTED]	1	VMware, Inc.	22,tcp,(empty)	SSH::SERVER	FlowSsh: Bitwise SSH Server (WinSSHD),5,59,-
128. [REDACTED]	08/20/2017 15:25:17.492431	00:50:56: [REDACTED]	1	VMware, Inc.	22,tcp,(empty) 80,tcp,(empty) 80,tcp,HTTP	HTTP::APPSERVER HTTP::BROWSER HTTP::SERVER SSH::SERVER	Apache,2,4,Ubuntu Debian APT-HTTP,1,3,1.0.1ubuntu2 OpenSSH,6,6,p1 PHP,5,5,ubuntu4 Python-urllib,3,4,-
128. [REDACTED]	08/20/2017 15:46:15	00:1e:68: [REDACTED]	1	QUANTA COMPUTER INC.	22,tcp,(empty) 80,tcp,(empty) 80,tcp,HTTP 8080,tcp,(empty) 8080,tcp,HTTP	HTTP::SERVER SSH::SERVER	Apache,2,2,Ubuntu Apache-Coyote,1,1,- OpenSSH,5,9,p1
128. [REDACTED]	08/20/2017 16:03:41.976476	00:23:8b: [REDACTED]	1	QUANTA COMPUTER INC.	22,tcp,(empty)	SSH::SERVER	OpenSSH,6,6,p1
128. [REDACTED]	08/20/2017 16:08:56	00:23:8b: [REDACTED]	1	QUANTA COMPUTER INC.	22,tcp,(empty)	SSH::SERVER	OpenSSH,6,6,p1
128. [REDACTED]	08/20/2017 16:00:02.696667	c0:3f:d5: [REDACTED]	1	Elitegroup Computer Systems Co.,Ltd.	22,tcp,(empty) 22,tcp,SSH 8888,tcp,(empty) 8888,tcp,HTTP	HTTP::BROWSER HTTP::SERVER SSH::SERVER	Jetty,(9,1,v20140210 OpenSSH,5,9,p1 Python-urllib,2,7,-
128. [REDACTED]	08/20/2017 16:07:05.690758	c0:3f:d5: [REDACTED]	1	Elitegroup Computer Systems Co.,Ltd.	22,tcp,(empty) 22,tcp,SSH 88,udp,KRB 8888,tcp,(empty)	HTTP::BROWSER SSH::SERVER	OpenSSH,5,9,p1 Python-urllib,2,7,-
128. [REDACTED]	08/20/2017 15:07:23.720996	34:17:eb: [REDACTED]	1	Dell Inc.	22,tcp,(empty) 88,udp,KRB	HTTP::BROWSER SSH::SERVER	OpenSSH,5,3,- urllibgrabber,3,9,yum/3
128. [REDACTED]	08/20/2017 16:10:40.747024	78:2b:cb: [REDACTED]	1	Dell Inc.	22,tcp,(empty) 22,tcp,SSH	HTTP::BROWSER OS::WINDOWS SSH::SERVER	<unknown browser>,-,- Chrome,60,0,- Microsoft BITS,7,5,- Microsoft-CryptoAPI,6,1,- OpenSSH,6,6,p1 Windows,6,1,7 or Server 2008 R2 Windows-Update-Agent,-,-
128. [REDACTED]	08/20/2017 16:03:31.953283	a4:ba:db: [REDACTED]	1	Dell Inc.	22,tcp,(empty) 3128,tcp,(empty) 3128,tcp,HTTP 88,udp,KRB	HTTP::SERVER SSH::SERVER	OpenSSH,5,9,p1 squid,3,1,-

# Taking a look at software.log: All Old OpenSSL versions

_time	client_ip	software_name	unparsed_version	software_type	version_major	version_minor
8/20/17 4:25:25.775 PM	128. [REDACTED]	Apache	Apache/2.4.25 (Fedora) OpenSSL/1.0.2k-fips PHP/7.0.20 mod_perl/2.0.10 Perl/v5.24.1	HTTP::SERVER	2	4
8/20/17 4:25:23.206 PM	128. [REDACTED]	Apache	Apache/2.4.25 (Fedora) OpenSSL/1.0.2k-fips PHP/7.0.20 mod_perl/2.0.10 Perl/v5.24.1	HTTP::SERVER	2	4
8/20/17 4:20:41.372 PM	128. [REDACTED]	Apache	Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips mod_auth_gssapi/1.4.0 mod_auth_kerb/5.4 mod_fcgid/2.3.9 SVN/1.7.14 mod_wsgi/3.4 Python/2.7.5	HTTP::SERVER	2	4
8/20/17 4:16:30.994 PM	128. [REDACTED]	Apache	Apache/2.4.9 (Unix) OpenSSL/1.0.1e-fips PHP/5.4.27	HTTP::SERVER	2	4
8/20/17 4:08:10.901 PM	128. [REDACTED]	Apache	Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips mod_fcgid/2.3.9 PHP/5.4.16	HTTP::SERVER	2	4
8/20/17 3:41:02.251 PM	128. [REDACTED]	Apache	Apache/2.2.22 (Unix) mod_ssl/2.2.22 OpenSSL/1.0.1e-fips	HTTP::SERVER	2	2
8/20/17 3:34:42.261 PM	128. [REDACTED]	Apache	Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips mod_fcgid/2.3.9 PHP/5.4.16	HTTP::SERVER	2	4
8/20/17 3:33:44.377 PM	128. [REDACTED]	Apache	Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips mod_fcgid/2.3.9 PHP/5.4.16	HTTP::SERVER	2	4
8/20/17 3:32:53.064 PM	128. [REDACTED]	Apache	Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips	HTTP::SERVER	2	4
8/20/17 3:29:46.740 PM	128. [REDACTED]	Apache	Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips	HTTP::SERVER	2	4
8/20/17 3:25:31.876 PM	128. [REDACTED]	Apache	Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips mod_fcgid/2.3.9 PHP/5.4.16	HTTP::SERVER	2	4
8/20/17 3:22:47.964 PM	128. [REDACTED]	Apache	Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips mod_fcgid/2.3.9 PHP/5.4.16	HTTP::SERVER	2	4

# Continued, OpenSSL (getting a list of systems)....

21

ip	mac	Operating System	unparsed_version
128. [REDACTED]	0c:c4:7a:[REDACTED]	CentOS	Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips
128. [REDACTED]	00:e0:81:[REDACTED]	Unix	Apache/2.4.9 (Unix) OpenSSL/1.0.1e-fips
128. [REDACTED]	00:19:e3:[REDACTED]	Unix	Apache/2.2.26 (Unix) OpenSSL/0.9.8za
128. [REDACTED]	00:14:4f:[REDACTED]	CentOS	Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips
128. [REDACTED]	00:14:4f:[REDACTED]	Fedora	Apache/2.4.23 (Fedora) OpenSSL/1.0.2j-fips
128. [REDACTED]	b8:27:eb:[REDACTED]	CentOS	Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips
128. [REDACTED]	60:eb:69:[REDACTED]	Fedora	Apache/2.4.18 (Fedora) OpenSSL/1.0.2j-fips
128. [REDACTED]	0c:c4:7a:[REDACTED]	CentOS	Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips
128. [REDACTED]	00:16:cb:[REDACTED]	Unix	Apache/2.2.17 (Unix) OpenSSL/0.9.7l DAV/2
128. [REDACTED]	c0:8c:60:[REDACTED]	Unix	Apache/2.2.17 (Unix) OpenSSL/0.9.7l DAV/2
128. [REDACTED]	0c:c4:7a:[REDACTED]	CentOS	Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips
128. [REDACTED]	0c:c4:7a:[REDACTED]	Unix	Apache/2.4.11 (Unix) OpenSSL/1.0.1e-fips
128. [REDACTED]	00:50:56:[REDACTED]	Unix	Apache/2.2.29 (Unix) OpenSSL/1.0.1e-fips
128. [REDACTED]	40:6c:8f:[REDACTED]	Unix	Apache/2.2.31 (Unix) OpenSSL/1.0.2d DAV/2
128. [REDACTED]	ac:cc:8e:[REDACTED]	Unix	Apache/2.4.16 (Unix) OpenSSL/1.0.2d
128. [REDACTED]	ac:cc:8e:[REDACTED]	Unix	Apache/2.4.16 (Unix) OpenSSL/1.0.2d
128. [REDACTED]	44:a8:42:[REDACTED]	Red Hat Enterprise Linux	Apache/2.4.6 (Red Hat Enterprise Linux) OpenSSL/1.0.1e-fips
128. [REDACTED]	00:22:19:[REDACTED]	CentOS	Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips
128. [REDACTED]	00:22:19:[REDACTED]	CentOS	Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips
128. [REDACTED]	00:56:cd:[REDACTED]	Unix	Apache/2.2.29 (Unix) OpenSSL/0.9.8zg
128. [REDACTED]	a0:39:f7:[REDACTED]	Unix	Apache/2.2.29 (Unix) OpenSSL/0.9.8zg
128. [REDACTED]	60:e3:ac:[REDACTED]	Unix	Apache/2.2.29 (Unix) OpenSSL/0.9.8zg
128. [REDACTED]	00:56:cd:[REDACTED]	Unix	Apache/2.2.17 (Unix) OpenSSL/0.9.7l
128. [REDACTED]	48:d7:05:[REDACTED]	Unix	Apache/2.2.17 (Unix) OpenSSL/0.9.7l
128. [REDACTED]	00:50:56:[REDACTED]	CentOS	Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips
128. [REDACTED]	00:50:56:[REDACTED]	CentOS	Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips
128. [REDACTED]	00:50:56:[REDACTED]	CentOS	Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips
128. [REDACTED]	00:50:56:[REDACTED]	CentOS	Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips
128. [REDACTED]	00:50:56:[REDACTED]	CentOS	Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips
128. [REDACTED]	00:50:56:[REDACTED]	CentOS	Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips
128. [REDACTED]	34:e6:d7:[REDACTED]	Win32	Apache/2.4.17 (Win32) OpenSSL/1.0.2d
128. [REDACTED]	90:e2:ba:[REDACTED]	CentOS	Apache/2.2.15 (CentOS) OpenSSL/1.0.1e-fips
128. [REDACTED]	64:00:6a:[REDACTED]	Fedora	Apache/2.4.25 (Fedora) OpenSSL/1.0.2k-fips
128. [REDACTED]	00:50:56:[REDACTED]	Ubuntu	Apache/2.4.7 (Ubuntu) OpenSSL/1.0.1f

# Usefulness: Policy enforcement2- All Windows systems on the N/W

client_ip	latest_time	mac	dmacs	vendor	known_services	software_type	software_info	dhcp_comment	TLS_client
128. [REDACTED]	08/20/2017 15:00:38	a4:1f:72: [REDACTED]	1	Dell Inc.		OS::WINDOWS	Windows,6,1,7 or Server 2008 R2		Safari 525.21 525.29 531.22.7 533.21.1 534.57.2
128. [REDACTED]	08/20/2017 15:00:34	a4:1f:72: [REDACTED]	1	Dell Inc.		OS::WINDOWS	Windows,6,1,7 or Server 2008 R2		Safari 525.21 525.29 531.22.7 533.21.1 534.57.2
128. [REDACTED]	08/20/2017 16:12:39	90:b1:1c: [REDACTED]	1	Dell Inc.		OS::WINDOWS	Windows,10,0,10	PROV-SSA-09	
128. [REDACTED]	08/20/2017 11:30:25	6c:0b:84: [REDACTED]	1	Universal Global Scientific Industrial Co., Ltd.	88,udp,KRB	HTTP::BROWSER OS::WINDOWS	Microsoft-CryptoAPI,6,3,- Windows,6,3,8.1 or Server 2012 R2 client connection,,-,-		
128. [REDACTED]	08/20/2017 15:41:50	00:50:56: [REDACTED]	1	VMware, Inc.		HTTP::BROWSER OS::WINDOWS	Microsoft-CryptoAPI,6,3,- Windows,6,3,8.1 or Server 2012 R2 client connection,,-,-		
128. [REDACTED]	08/20/2017 12:48:21	00:50:56: [REDACTED]	1	VMware, Inc.		HTTP::BROWSER OS::WINDOWS	Microsoft-CryptoAPI,6,3,- Windows,6,3,8.1 or Server 2012 R2 client connection,,-,-		
128. [REDACTED]	08/20/2017 07:43:33	00:50:56: [REDACTED]	1	VMware, Inc.		HTTP::BROWSER OS::WINDOWS	Microsoft-CryptoAPI,6,3,- Windows,6,3,8.1 or Server 2012 R2 client connection,,-,-		
128. [REDACTED]	08/20/2017 15:17:22	00:50:56: [REDACTED]	1	VMware, Inc.		HTTP::BROWSER OS::WINDOWS	Microsoft-CryptoAPI,6,3,- Windows,6,3,8.1 or Server 2012 R2		
128. [REDACTED]	08/20/2017 16:15:18	20:1a:06: [REDACTED]	1	COMPAL INFORMATION (KUNSHAN) CO., LTD.		HTTP::BROWSER OS::WINDOWS	Microsoft-CryptoAPI,6,3,- Windows Store,1,0,- Windows,6,3,8.1 or Server 2012 R2 Windows-Update-Agent,7,9,Client	Jiao-VersaStat	
128. [REDACTED]	08/20/2017 16:16:52	74:86:7a: [REDACTED]	1	Dell Inc.		HTTP::BROWSER OS::WINDOWS	Microsoft-CryptoAPI,6,3,- Windows Store,1,0,- Windows,6,3,8.1 or Server 2012 R2	ADSA	
128. [REDACTED]	08/20/2017 16:30:57	74:e2:8c: [REDACTED]	1	Microsoft Corporation		HTTP::BROWSER OS::WINDOWS	Microsoft-CryptoAPI,6,3,- Windows Phone Search (Windows Phone OS,8,10,NOKIA Windows,6,3,8.1 or Server 2012 R2	Windows-Phone	Trident/7.0,TLSv12
128. [REDACTED]	08/20/2017 16:13:38.630316	00:50:56: [REDACTED]	1	VMware, Inc.	20000,udp,DNP3_UDP 80,tcp,(empty) 80,tcp,HTTP 8000,tcp,HTTP 88,udp,KRB	HTTP::BROWSER HTTP::SERVER OS::WINDOWS	Microsoft-CryptoAPI,6,3,- Microsoft-HTTPAPI,2,0,- Microsoft-IIS,8,5,- Windows,6,3,8.1 or Server 2012 R2 client connection,,-,-		
128. [REDACTED]	08/20/2017 16:27:52	98:90:96: [REDACTED]	1	Dell Inc.		HTTP::BROWSER OS::WINDOWS	Microsoft-CryptoAPI,6,2,- Windows,6,2,8 or Server 2012 Windows-Update-Agent,,-,- client connection,,-,-	WINDOWS-RRASK6T	FireFox 49 (dev edition),TLSv12 Tracking something (noted with Dropbox Installer)

# Summary: Ask UEptSS anything you want

23

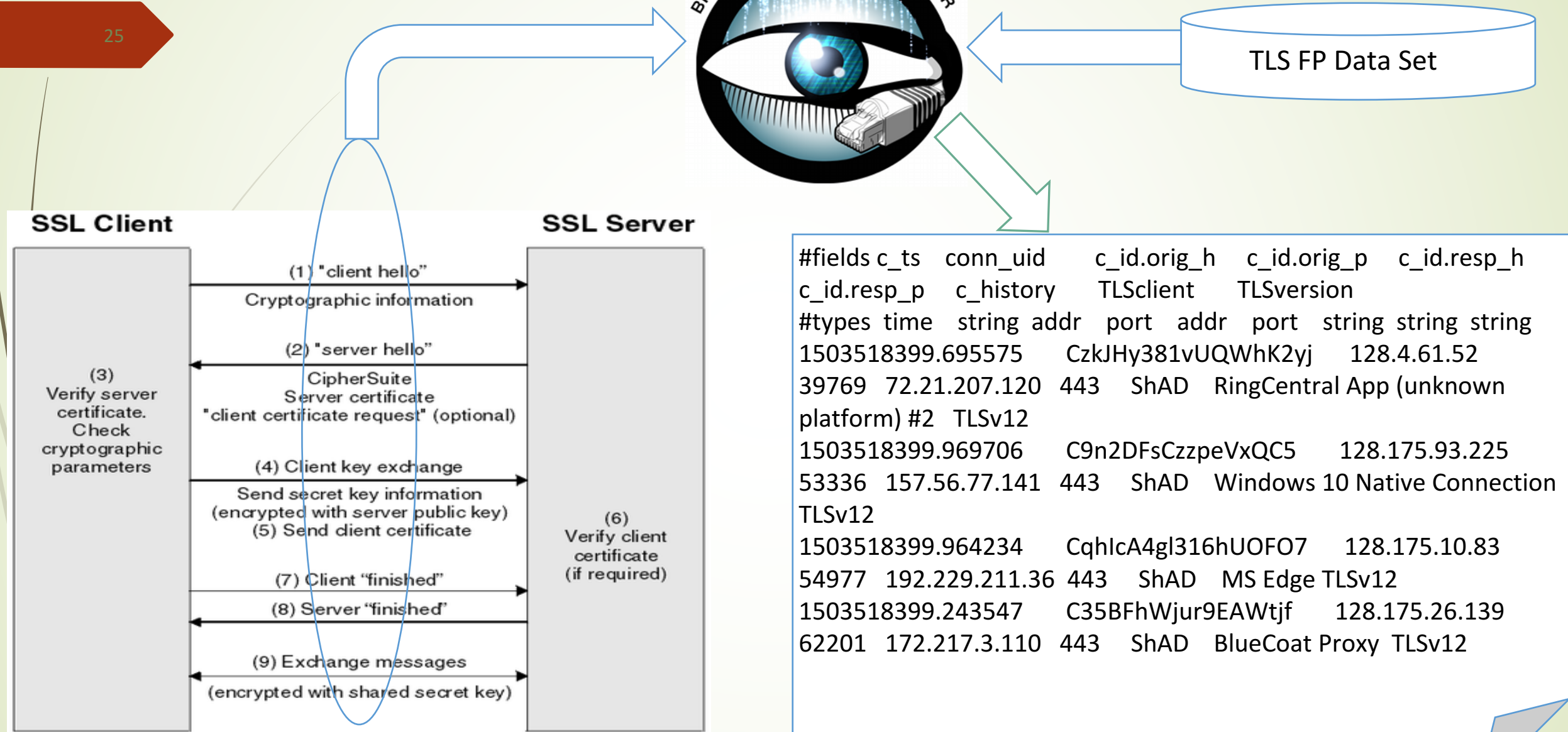
- ▶ Enumerating various services/servers: Which services & How many servers:
  - ▶ What all servers providing DNS service on the network?
  - ▶ What all servers providing Web service on the Network?
  - ▶ What all systems have xyz service running or xx port open?
- ▶ Malware IR: Get all possible information of an infected system
  - ▶ Hmm, one of the IDSs has detected Petya downloaded on a box.
  - ▶ Is the system actually vulnerable To Petya?
  - ▶ A new vulnerability just got released that exploits a particular software/version. What all systems on my Network are running that piece of software.

# TLS Fingerprinting

*[Special Thanks to Seth]*

- Detecting the TLS Client in use by fingerprinting TLS traffic.
- Use a table of data set to compare the sniffed TLS traffic to fingerprint the known TLS client.
- Bro has all the events to capture all the information transpired in TLS handshake.
- How it works? Explained in next Slide.





```
#fields c_ts conn_uid c_id.orig_h c_id.orig_p c_id.resp_h
c_id.resp_p c_history TLSclient TLSversion
#types time string addr port addr port string string string
1503518399.695575 CzkJHy381vUQWhK2yj 128.4.61.52
39769 72.21.207.120 443 ShAD RingCentral App (unknown
platform) #2 TLSv12
1503518399.969706 C9n2DFsCzzpeVxQC5 128.175.93.225
53336 157.56.77.141 443 ShAD Windows 10 Native Connection
TLSv12
1503518399.964234 CqhlcA4gl316hUOFO7 128.175.10.83
54977 192.229.211.36 443 ShAD MS Edge TLSv12
1503518399.243547 C35BFhWjur9EAWtjf 128.175.26.139
62201 172.217.3.110 443 ShAD BlueCoat Proxy TLSv12
```

# TLS Fingerprinting- Block the Offensive clients

26

- Look for 'Metasploit' OR 'BurpSuite' OR 'SkipFish' OR 'w3af' OR 'mitmproxy' in the log file.

_time	src_ip	src_port	dest_ip	dest_port	TLSCClient	TLSVersion	Country	Region
2017-08-15 21:44:05.118	23.1	56692	128	443	Metasploit SSL Scanner	TLSv10	United States	Arizona
2017-08-15 15:15:47.134	23.1	57973	128	443	Metasploit SSL Scanner	TLSv10	United States	Arizona
2017-08-15 14:40:01.856	149	60940	128	443	BurpSuite Free (1.6.01)	TLSv10	France	
2017-08-15 22:38:46.128	128	14765	128	443	w3af (tested: v1.6.54 Kali 2)	TLSv12	Canada	Ontario
2017-08-15 22:07:06.339	131	58158	128	443	w3af (tested: v1.6.54 Kali 2)	TLSv12	United States	Washington
2017-08-15 07:08:24.083	23.1	41349	128	443	Metasploit SSL Scanner	TLSv10	United States	Arizona
2017-08-15 02:02:28.008	149	46979	128	443	BurpSuite Free (1.6.01)	TLSv10	France	
2017-08-15 16:02:46.018	54.2	60912	128	4450	BurpSuite Free (1.6.01)	TLSv10	United States	Oregon
2017-08-15 16:02:45.696	54.2	60867	128	4450	BurpSuite Free (1.6.01)	TLSv10	United States	Oregon
2017-08-15 08:53:32.030	54.2	39672	128	4450	BurpSuite Free (1.6.01)	TLSv10	United States	Oregon
2017-08-15 08:53:31.708	54.2	39591	128	4450	BurpSuite Free (1.6.01)	TLSv10	United States	Oregon
2017-08-15 05:04:34.312	23.1	51485	128	443	Metasploit SSL Scanner	TLSv10	United States	Arizona
2017-08-15 05:04:19.293	23.1	58384	128	443	Metasploit SSL Scanner	TLSv10	United States	Arizona

# Where to find scripts?

27

- Custom scripts used in this presentation can be found at :

<https://github.com/fatemabw/bro-scripts>

- The TLS Fingerprint Dataset can be found at:

<https://github.com/LeeBrotherston/tls-fingerprinting/blob/master/fingerprints/fingerprints.js>  
on

# Acknowledgements 😊

- *Thanks to the Awesome Bro Team for the support, and providing answers/solutions to all the Bro related questions. [@bro.org mail list]*
- *Thanks for the opportunity to be a presenter at BROCON17 !!*



Questions???