GIAC CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Network Monitoring and Threat Detection In-Depth (Security 503)"
at http://www.giac.org/registration/gcia

Hunting Threats Inside Packet Captures

GIAC (GCIA) Gold Certification

Author: Muhammad Alharmeel
Advisor: Mark Stingley
Accepted: April 19, 2017

Abstract

Inspection of packet captures –PCAP- for signs of intrusions, is a typical everyday task for security analysts and an essential skill analysts should develop. Malwares have many ways to hide their activities on the system level (i.e. Rootkits), but at the end, they must leave a visible trace on the network level, regardless if it's obfuscated or encrypted. This paper guides the reader through a structured way to analyze a PCAP trace, dissect it using Bro Network Security Monitor (Bro) to facilitate active threat hunting in an efficient time to detect possible intrusions.

© 2017 The SANS Institute, Author Retains Full Rights

© 2017 The SANS Institute Author retains full rights.

Table of Contents

© 2017 The SANS Institute Author retains full rights.

1. Introduction

Attack / Defense game is well known for being asymmetric. From a prevention perspective, attackers only need a single vulnerability to penetrate the network. But fortunately, the same equation applies to detection. Once attackers are in the target environment, they have to be 100% perfect (Clark, 2016). Otherwise, analysts/threat hunters only need a single trail to unveil nefarious activities. This notion emphasizes the importance of having an efficient detection capability, regardless of the perfection of the preventive arm.

The detection arm itself can be broken down into two major parts, reactive and proactive. On the network level –the scope of this paper, one widespread reactive detection example is SNORT (SANS, n.d.), which used to be an effective approach, but it has two significant shortcomings. Firstly, SNORT depends on static signatures, which determined attackers could easily bypass. The second is that security analysts operate into a more passive mode, waiting for something malicious to happen that might –or might not- trigger an alert and only then, an investigation will kick off (Mecha, 2016). The fact that analysts only respond when they get notified hinders their detection capabilities and motivation by being positioned in the target zone psychologically and technically.

Nowadays, attacks have evolved and require more than traditional NIDS –reactive detection- to detect adversaries (Ashford, n.d.). Active detection (aka threat hunting) was introduced to fill this gap. The significant impact threat hunting has on analysts' mentality, and the way of thinking is impressive, as analysts' role is being seen as hunters who actively chase intruders as opposed to being targets. The spirit behind this change can help dramatically to unleash analysts' creativity and increase the chance to detect and stop attacks at their early stages.

APT can clearly spot the edge that threat hunting has over reactive detection. An advanced adversary will simulate attacks in a lab environment, which is identical or close to the target's environment to bypass security controls and avoid detection (i.e. SNORT rules) to the maximum possible extent, which renders reactive detection useless in such cases.

© 2017 The SANS Institute Author retains full rights.

Another example would be a system admin who goes rogue and becomes an insider, his/her suspicious activities can easily go unnoticed with reactive detection. However, with threat hunting, they should stand out clearly. These activities could vary from connecting remotely through VPN in non-usual hours, pivoting between servers in a new pattern, or transferring data from internal network to a DMZ server (i.e. Web Server) for external data exfiltration. Administrators tend to do things in the same manner unless something new was introduced to the network (i.e. new solution was deployed, or a new tool or administrative technique is being used).

Threat hunting has a higher probability of detecting such type of attacks than reactive detection because it depends heavily on spotting deviations from a predefined baseline –behavioral analysis- rather than counting on signatures. Also, adversaries cannot anticipate hunting activities because it's a random course of non-sequential actions that are not publicly documented or known to the wild.

2. Workflow

2.1. Scrub

Efficient threat hunting requires two major things; doing it in the right place and in minimal time. The former means focus on traffic patterns that have the highest probability of including attack trails.

As an example, let's consider a PCAP trace captured from DMZ network traffic, and apply the above concept. The following matrix indicates suggested scrubbing options based on traffic direction and transport protocol.

DMZ Network Traffic			
Traffic Direction	Internal to External	External to Internal	Internal & External
Transport Protocol	UDP	TCP	TCP & UDP

Although hunting activities can vary in any direction/protocol combination, as shown above, the first preference would be inspecting **TCP only** traffic **initiated from DMZ** servers for the following reasons:

© 2017 The SANS Institute Author retains full rights.

- It has the least amount of generated traffic, hence, less noise, clearer visibility, and better detection.
- TCP has a higher probability of carrying attack traffic (SANS Internet Storm Center, n.d.), considering that most traditional attack channels are TCP based (i.e. HTTP, SMB, FTP, SMTP…etc.).
- Triggered alerts have a good chance of being a serious issue that requires immediate attention. DMZ servers by nature respond (SYN/ACK) to requests initiated from outside, and should not be initiating connections (SYN) except for a few cases to grab updates.

2.2. Dissect

After applying basic scrubbing, breaking up PCAP trace can speed up the process and reduce the analysis time. An APT adversary would use legit channels to hide attack footprints, which means extra work is required to inspect those channels to distinguish between benign and malicious activities. The objective here is to divide and conquer, to break down PCAP into smaller chunks that are easier to analyze and in the same time, maintain rigorous scrutiny.

Employing automation plays a vital role in making threat hunting an efficient, practical and doable process by reducing investigation time. To cut down on repetitive manual functions and save time during analysis a Bro script was created to automate those checks (Bro-PCAP-Dissector). The following list suggests preliminary hunts that can be performed on a PCAP trace.

© 2017 The SANS Institute Author retains full rights.

2.2.1. Connection Stats

Hunt Location:	Bytes uploaded stats
Hunt For:	Session uploaded data > 1 MB
Possible Threat:	Data exfiltration
Format:	Number of bytes (Descending), client IP, server IP, server port

```
============================================================
Bytes Uploaded > {1000000 Bytes / 1 MB}
============================================================

1510081441          192.168.4.5      -------> 207.171.185.200  : 443/tcp
1436668500          192.168.4.5      -------> 74.125.239.3     : 443/tcp
1429743201          192.168.4.5      -------> 207.171.187.117  : 443/tcp
1068033242          192.168.4.5      -------> 23.212.8.120     : 80/tcp
742832115           192.168.4.5      -------> 207.171.187.117  : 443/tcp
729590415           192.168.4.5      -------> 207.171.187.117  : 443/tcp
251404609           192.168.4.5      -------> 23.67.247.112    : 80/tcp
8393910             192.168.4.5      -------> 207.171.187.117  : 443/tcp
```

Figure 1 – Results acquired from "ISMELLPACKETS/Hidden.pcap" @ http://bit.ly/2lSdxt8.

Hunt Location:	Bytes downloaded stats
Hunt For:	Session downloaded data > 3 MB
Possible Threat:	Attacker downloading attack tools
Format:	Number of bytes (Descending), client IP, server IP, server port

```
============================================================
Bytes Downloaded > {3000000 Bytes / 3 MB}
============================================================

5366941             192.168.203.64   <-------  192.168.202.68   : 55554/tcp
5184633             192.168.204.70   <-------  192.168.202.68   : 55554/tcp
4203410             192.168.204.45   <-------  192.168.202.68   : 55554/tcp
4091323             192.168.27.100   <-------  192.168.202.110  : 4444/tcp
4086085             192.168.28.100   <-------  192.168.203.45   : 54321/tcp
3497984             192.168.27.100   <-------  192.168.203.45   : 9898/tcp
3497812             192.168.24.100   <-------  192.168.203.45   : 54322/tcp
3496305             192.168.26.100   <-------  192.168.203.45   : 54344/tcp
3476280             192.168.24.100   <-------  192.168.202.110  : 4444/tcp
```

Figure 2 – Results acquired from "National CyberWatch Mid-Atlantic Collegiate Cyber Defense Competition/maccdc2012_00001.pcap" @ http://bit.ly/2mWr0kx.

© 2017 The SANS Institute Author retains full rights.

Hunt Location:	Session duration stats
Hunt For:	Session duration > 10 minutes
Possible Threat:	Remote access
Format:	Duration in seconds (Descending), client IP, server IP, server port

```
===========================================================
Conn Duration > {600 Second / 10 Minutes}
===========================================================

1840                   192.168.202.68    <------->    192.168.28.203    : 22/tcp
1788                   192.168.202.109   <------->    192.168.22.254    : 22/tcp
1765                   192.168.204.70    <------->    192.168.202.68    : 55554/tcp
1752                   192.168.202.109   <------->    192.168.23.254    : 22/tcp
1680                   192.168.28.100    <------->    192.168.203.45    : 54321/tcp
1650                   192.168.202.109   <------->    192.168.24.254    : 22/tcp
1645                   192.168.28.100    <------->    192.168.204.45    : 1025/tcp
1632                   192.168.28.100    <------->    192.168.202.112   : 1025/tcp
1623                   192.168.202.109   <------->    192.168.25.254    : 22/tcp
1567                   192.168.202.109   <------->    192.168.27.254    : 22/tcp
1533                   192.168.202.109   <------->    192.168.28.254    : 22/tcp
1522                   192.168.24.100    <------->    192.168.202.90    : 4499/tcp
1470                   192.168.24.100    <------->    192.168.202.90    : 4499/tcp
1445                   192.168.202.109   <------->    192.168.21.254    : 22/tcp
```

Figure 3 - Results acquired from "National CyberWatch Mid-Atlantic Collegiate Cyber Defense Competition/maccdc2012_00001.pcap" @ http://bit.ly/2maxlsD.

© 2017 The SANS Institute Author retains full rights.

Hunt Location:	TCP listening ports on private IPs
Hunt For:	Unauthorized service
Possible Threat:	Backdoors
Format:	Count of sessions (Ascending), TCP port, server IP, protocol

```
==========================================================
Conn Listening_TCP_Ports_on_Private_IPs
==========================================================

1             445/tcp   listening on  192.168.25.102   smb,gssapi,ntlm,dce_rpc
1             22/tcp    listening on  192.168.28.203   ssh
1             80/tcp    listening on  192.168.28.101   http
1             445/tcp   listening on  192.168.27.100   smb,ntlm,dce_rpc
1             8000/tcp  listening on  192.168.25.253   http
1             139/tcp   listening on  192.168.25.102   smb,gssapi,ntlm,dce_rpc
1             80/tcp    listening on  192.168.22.253   http
1             443/tcp   listening on  192.168.201.2    ssl
1             5432/tcp  listening on  192.168.203.45   -
1             8080/tcp  listening on  192.168.23.203   http
1             8089/tcp  listening on  192.168.22.253   ssl
1             22/tcp    listening on  192.168.21.254   ssh
1             80/tcp    listening on  192.168.21.202   http
2             80/tcp    listening on  192.168.23.101   http
2             80/tcp    listening on  192.168.25.202   http
2             55553/tcp listening on  192.168.202.68   ssl
3             22/tcp    listening on  192.168.23.101   ssh
4             445/tcp   listening on  192.168.27.100   smb,ntlm
4             80/tcp    listening on  192.168.25.102   http
5             443/tcp   listening on  192.168.25.253   ssl
5             443/tcp   listening on  192.168.22.253   ssl
7             443/tcp   listening on  192.168.22.254   ssl
13            80/tcp    listening on  192.168.202.78   http
17            443/tcp   listening on  192.168.25.254   ssl
18            22/tcp    listening on  192.168.22.253   ssh
```

Figure 4 – Results acquired from "National CyberWatch Mid-Atlantic Collegiate Cyber Defense Competition/maccdc2012_00003.pcap" @ http://bit.ly/2maxlsD.

© 2017 The SANS Institute Author retains full rights.

Hunt Location:	TCP listening ports on public IPs (Sharpe, 2015)
Hunt For:	Abnormal port / protocol combination (i.e. non-HTTP carried over port 80)
Possible Threat:	Unauthorized communication channel
Format:	Count of sessions (Ascending), TCP port, protocol

```
==========================================================
Conn Listening_TCP_Ports_on_Public_IPs
==========================================================

1             6998/tcp   -------> -
3             80/tcp     -------> http
9             443/tcp    -------> ssl
```

Figure 5 – Results acquired from "Malware Traffic Analysis/2015-06-30-traffic-analysis-exercise.pcap" @ http://bit.ly/2lSbbdH.

2.2.2. HTTP Traffic

Hunt Location:	HTTP host header
Hunt For:	Hosts not ending with .com | .net | .org & host length > 30 char
Possible Threat:	DGA, suspicious domains (i.e. http://bit.ly/2jKNAhi or HTTP traffic to an IP address instead of FQDN)
Format:	Count (Ascending), HTTP host

```
==========================================================
HTTP Odd_Hosts
==========================================================

1             magusserver.top
1             whos.amung.us
1             widgets.amung.us
1             ckea.ca
1             a.topgunn.photography
2             g00.co
2             x.ss2.us
3             mohecy.tk
4             185.82.202.170
6             ululataque-forstbea.bondcroftatvs.co.uk
7             e7qx9y.he6gnm.top
15            www.emidioleite.com.br
23            5.34.183.40
```

Figure 6 - Results acquired from "Malware Traffic Analysis/2016-05-13-traffic-analysis-exercise.pcap" @ http://bit.ly/2mvlhVA.

© 2017 The SANS Institute Author retains full rights.

Hunt Location:	HTTP referrer header
Hunt For:	Malicious referring domains
Possible Threat:	Watering hole and JS exploit kits
Format:	Count (Ascending), HTTP referrer

```
==========================================================
HTTP Referrers
==========================================================

1             ztjyuncjqvi1e.com
1             www.ecb.europa.eu
2             scoring33.com
2             leadback.advertising.com
2             www.google.com
2             folesd.tk
2             lemepackrougue.com
3             rmfytrwemvvk.com
3             fireman.carsassurance.info
3             wincepromotional.com
4             8def3da737b3b1117f05-2484ec98d956dd65605480d10636de6f.r11.cf1.rackcdn.com
4             9e886e6c4bf39d002b00-b32e53c17e846b593b21b014f11dc266.r14.cf2.rackcdn.com
6             score.feed-xml.com
8             trafficinside.me
9             fast.twc.demdex.net
10            popcash.net
16            ip.casalemedia.com
21            cmap.uac.ace.advertising.com
23            xxxsexcamera.club
29            -
63            thingstodo.viator.com
83            webmail.roadrunner.com
```

Figure 7 - Results acquired from "Malware Traffic Analysis/2016-03-30-traffic-analysis-exercise.pcap" @ http://bit.ly/2mLFlDN.

© 2017 The SANS Institute Author retains full rights.

Hunt Location:	HTTP user-agent header
Hunt For:	Uncommon or non-existing User-Agents
Possible Threat:	Malicious traffic
Format:	Count (Ascending), HTTP user-agent

```
==========================================================
HTTP User-Agents
==========================================================

1               Mozilla/5.00 (Nikto/2.1.5) (Evasions:None) (Test:000289)
2               Mozilla/5.00 (Nikto/2.1.5) (Evasions:None) (Test:000915)
2               Mozilla/5.00 (Nikto/2.1.5) (Evasions:None) (Test:000904)
2               login
2               Mozilla/5.00 (Nikto/2.1.5) (Evasions:None) (Test:000878)
2               Mozilla/5.00 (Nikto/2.1.5) (Evasions:None) (Test:000918)
2               Mozilla/5.00 (Nikto/2.1.5) (Evasions:None) (Test:000805)
3               Mozilla/5.00 (Nikto/2.1.5) (Evasions:None) (Test:000258)
4               Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0; Trident/4.0; SIMBAR={7DB0F6DE-8DE7-4841-9084-28FA914B0F2E}; SLCC1; .N
4               Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:11.0) Gecko/20100101 Firefox/11.0
5               Fastream NETFile Server
5               Mozilla/5.00 (Nikto/2.1.5) (Evasions:None) (Test:000408)
10              webmin
10              NESSUS::SOAP
15              Nessus SOAP v0.0.1 (Nessus.org)
16              Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/535.2 (KHTML, like Gecko) Ubuntu/11.10 Chromium/15.0.874.106 Chrome/15.0.874.106 Safari/535.2
16              Mozilla/5.0 (Windows NT 5.1; rv:11.0) Gecko/20100101 Firefox/11.0
17              Mozilla/5.0 (Windows NT 6.1; rv:7.0.1) Gecko/20100101 Firefox/7.0.1
24              Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.9.2.11) Gecko/20101013 Ubuntu/9.04 (jaunty) Firefox/3.6.11
39              Mozilla/5.0 (X11; Linux i686 on x86_64; rv:10.0.2) Gecko/20100101 Firefox/10.0.2
48              Mozilla/5.0 (X11; Linux i686; rv:10.0.2) Gecko/20100101 Firefox/10.0.2
75              Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_3) AppleWebKit/535.11 (KHTML, like Gecko) Chrome/17.0.963.79 Safari/535.11
89              Mozilla/5.0 (X11; Linux i686; rv:5.0.1) Gecko/20100101 Firefox/5.0.1
96              Nessus
199             Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:10.0.2) Gecko/20100101 Firefox/10.0.2
281             Mozilla/5.0 (Windows NT 6.1; WOW64; rv:10.0.2) Gecko/20100101 Firefox/10.0.2
405             Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
649             Mozilla/5.0 (compatible; Nmap Scripting Engine; http://nmap.org/book/nse.html)
1369            Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.0)
6342            -
8081            Mozilla/4.0 (compatible; MSIE 9.0; Windows NT 6.1)
17520           Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
481029          DirBuster-0.12 (http://www.owasp.org/index.php/Category:OWASP_DirBuster_Project)
```

Figure 8 – Results acquired from "National CyberWatch Mid-Atlantic Collegiate Cyber Defense Competition/maccdc2012_00010.pcap" @ http://bit.ly/2maxlsD.

Hunt Location:	HTTP request methods
Hunt For:	Methods other than GET/POST
Possible Threat:	Uploads (PUT method), tunneling (CONNECT method) and injection
Format:	Count (Ascending), HTTP method

```
==========================================================
HTTP Methods
==========================================================

1               SEARCH
2               PROPFIND
3               OPTIONS
3               DESCRIBE
42              PUT
76              DELETE
76              HEAD
16896           GET
42856           POST
```

Figure 9 – Results acquired from "National CyberWatch Mid-Atlantic Collegiate Cyber Defense Competition/maccdc2012_00006.pcap" @ http://bit.ly/2maxlsD.

© 2017 The SANS Institute Author retains full rights.

Hunt Location:	HTTP response status code
Hunt For:	Abnormal increase in NON 2xx/3xx codes
Possible Threat:	Directory brute-forcing (404 errors), authorization bypass (401 errors), DOS (5xx errors)
Format:	Count (Ascending), HTTP response status code

```
===========================================================
HTTP Response_Codes
===========================================================

1                502
2                417
2                206
5                301
6                501
12               411
84               503
88               303
94               405
104              403
104              302
119              304
278              400
1133             401
10705            200
401791           404
```

Figure 10 - Results acquired from "National CyberWatch Mid-Atlantic Collegiate Cyber Defense Competition/maccdc2012_00009.pcap" @ http://bit.ly/2maxlsD.

Hunt Location:	HTTP number of requests
Hunt For:	Clients sending increasing number of HTTP requests
Possible Threat:	Beacons, tunneling, and data exfiltration
Format:	Count (Ascending), client IP

```
===========================================================
HTTP Client_Requests
===========================================================

46            192.168.204.137
59            192.168.204.139
122           192.168.204.146
```

Figure 11 - Results acquired from "Malware Traffic Analysis/2014-12-15-traffic-analysis-exercise.pcap" @ http://bit.ly/2lNMcYi.

© 2017 The SANS Institute Author retains full rights.

2.2.3. DNS Traffic

Hunt Location:	DNS RCODE
Hunt For:	Abnormal increase in NX domains
Possible Threat:	Malicious traffic
Format:	Count (Ascending), client IP

```
============================================================
DNS NXDOMAIN_Queries
============================================================

1            192.168.202.76
1            192.168.202.92
1            192.168.202.85
1            192.168.202.112
1            192.168.202.102
2            192.168.203.63
2            192.168.202.115
3            192.168.204.60
4            192.168.203.61
7            192.168.202.75
9            192.168.202.83
10           192.168.202.100
12           192.168.202.108
14           192.168.202.94
17           192.168.202.77
28           192.168.202.103
141          192.168.204.70
```

Figure 12 - Results acquired from "National CyberWatch Mid-Atlantic Collegiate Cyber Defense Competition/maccdc2012_00003.pcap" @ http://bit.ly/2maxlsD.

© 2017 The SANS Institute Author retains full rights.

Hunt Location:	DNS number of queries
Hunt For:	Abnormal increase in DNS queries
Possible Threat:	Beacons, tunneling, and data exfiltration
Format:	Count (Ascending), client IP

```
==========================================================
DNS Client_Queries
==========================================================

1               fe80::c62c:3ff:fe30:7333
1               fe80::3e07:54ff:fe1c:a665
1               fe80::223:dfff:fe97:4e12
1               192.168.202.65
1               192.168.204.70
1               192.168.202.115
2               192.168.202.76
3               192.168.202.83
3               192.168.202.86
3               192.168.203.64
3               192.168.202.100
3               192.168.203.45
3               192.168.202.84
4               192.168.202.79
6               192.168.202.112
6               192.168.202.116
6               192.168.202.74
6               2001:dbb:c18:204:a800:4ff:fe00:a04
6               192.168.203.62
10              fe80::a800:4ff:fe00:a04
10              fe80::ba8d:12ff:fe53:a8d8
10              fe80::f2de:f1ff:fe9b:ad6a
12              2001:dbb:c18:202:f2de:f1ff:fe9b:ad6a
12              2001:dbb:c18:202:a800:4ff:fe00:a04
13              192.168.202.103
15              fe80::c62c:3ff:fe37:efc
23              192.168.202.87
23              fe80::3e07:54ff:fe41:3ed3
51              192.168.202.110
234             192.168.202.102
```

Figure 13 - Results acquired from "National CyberWatch Mid-Atlantic Collegiate Cyber Defense Competition/maccdc2012_00000.pcap" @ http://bit.ly/2maxlsD.

© 2017 The SANS Institute Author retains full rights.

Hunt Location:	DNS query type
Hunt For:	Types other than A, AAAA, and PTR
Possible Threat:	Zone transfer (AXFR) and suspicious use of non-popular types
Format:	Count (Ascending), DNS query type

```
==========================================================
DNS Query_Types
==========================================================

8               *
10              PTR
16              A
99              AXFR
```

Figure 14 - Results acquired from "National CyberWatch Mid-Atlantic Collegiate Cyber Defense Competition/maccdc2012_00006.pcap" @ http://bit.ly/2maxlsD.

Hunt Location:	DNS query name (Bisson, 2015)
Hunt For:	Query length > 30 and Query name domain does not end with .com | .net | .org
Possible Threat:	DGA and suspicious domains
Format:	Count (Ascending), DNS query

```
==========================================================
DNS Odd_Queries
==========================================================

1               kritischerkonsum.uni-koeln.de
1               runlove.us
1               va872g.g90e1h.b8.642b63u.j985a2.v33e.37.pa269cc.e8mfzdgrf7g0.groupprograms.in
1               ip-addr.es
1               7oqnsnzwwnm6zb7y.gigapaysun.com
1               ubb67.3c147o.u806a4.w07d919.o5f.f1.b80w.r0faf9.e8mfzdgrf7g0.groupprograms.in
1               r03afd2.c3008e.xc07r.b0f.a39.h7f0fa5eu.vb8fbl.e8mfzdgrf7g0.groupprograms.in
```

Figure 15 - Results acquired from "Malware Traffic Analysis/2015-05-08-traffic-analysis-exercise.pcap" @ http://bit.ly/2lS8g4L.

© 2017 The SANS Institute Author retains full rights.

2.2.4. SMB Traffic

Hunt Location:	SMB sessions that include file transfer
Hunt For:	One to one session. (i.e. workstation to workstation)
Possible Threat:	Unauthorized session
Format:	Count (Ascending), client IP, server IP, server port

```
494          x.x.x.x    -------> x.x.x.x     :  445/tcp
532          x.x.x.x    -------> x.x.x.x     :  445/tcp
```

Figure 16.

Hunt Location:	SMB file action
Hunt For:	Abnormal increase in file read and file delete operations
Possible Threat:	Data exfiltration or disgruntled employees deleting sensitive data.
Format:	Count (Ascending), file action

```
2             SMB::FILE_WRITE
52            SMB::FILE_READ
188           SMB::FILE_CLOSE
252           SMB::FILE_OPEN
```

Figure 17.

© 2017 The SANS Institute Author retains full rights.

Hunt Location:	SMB files name
Hunt For:	Suspicious tools or files
Possible Threat:	Lateral movements
Format:	Count (Ascending), SMB file name

```
1           ui\SwDRM.dll
1           desktop.ini
1           inetpub\wwwroot\iis-85.png:Zone.Identifier
4           inetpub\history\CFGHISTORY_0000000004
4           inetpub\temp
4           inetpub\logs\LogFiles\W3SVC1
4           inetpub\history\CFGHISTORY_0000000002
4           inetpub\logs\LogFiles
4           inetpub\history
4           inetpub\custerr\en-US
4           inetpub\custerr
4           inetpub\temp\appPools
4           inetpub\history\CFGHISTORY_0000000003
4           inetpub\temp\IIS Temporary Compressed Files\DefaultAppPool
4           Thumbs.db:encryptable
4           inetpub\temp\IIS Temporary Compressed Files
4           inetpub\logs
4           temp
4           inetpub\wwwroot\Thumbs.db:encryptable
4           inetpub\history\CFGHISTORY_0000000001
4           inetpub\temp\appPools\DefaultAppPool
5           Users\desktop.ini
5           Program Files\desktop.ini
```

Figure 18.

Hunt Location:	SMB usernames involved in file transfers
Hunt For:	High privileges and unexpected account.
Possible Threat:	Compromised accounts
Format:	Count (Ascending), domain\username

```
21        Domain        \        Username1
494       Domain        \        Username2
```

Figure 19.

© 2017 The SANS Institute Author retains full rights.

Hunt Location:	SMB hostnames involved in file transfers
Hunt For:	Sensitive servers
Possible Threat:	Compromised servers
Format:	Count (Ascending), SMB hostname

```
21          ServerABC
494         ServerXYZ
```

Figure 20.

2.2.5. SSH Traffic

Hunt Location:	SSH sessions
Hunt For:	Unexpected connections
Possible Threat:	Recon and lateral movements
Format:	Count (Ascending), client IP, server IP, server port

```
=============================================================
SSH Sessions
=============================================================

1             192.168.202.109  -------> 192.168.21.254   : 22/tcp
1             192.168.202.87   -------> 192.168.28.203   : 22/tcp
1             192.168.202.96   -------> 192.168.25.102   : 22/tcp
1             192.168.202.110  -------> 192.168.22.254   : 22/tcp
1             192.168.202.96   -------> 192.168.25.202   : 22/tcp
3             192.168.202.112  -------> 192.168.23.101   : 22/tcp
28            192.168.202.110  -------> 192.168.22.253   : 22/tcp
```

Figure 21 - Results acquired from "National CyberWatch Mid-Atlantic Collegiate Cyber Defense Competition/maccdc2012_00003.pcap" @ http://bit.ly/2maxlsD.

© 2017 The SANS Institute, Author retains Full Rights

© 2017 The SANS Institute Author retains full rights.

Hunt Location:	SSH server banners
Hunt For:	Unexpected server banners
Possible Threat:	Unauthorized SSH servers
Format:	Count (Ascending), SSH server string

```
===========================================================
SSH Server_Strings
===========================================================

2           SSH-1.99-Cisco-1.25
3           SSH-2.0-OpenSSH_5.8p1 Debian-7ubuntu1
3           SSH-2.0-OpenSSH_5.8p1 Debian-1ubuntu3
28          SSH-2.0-OpenSSH_4.5
```

Figure 22 - Results acquired from "National CyberWatch Mid-Atlantic Collegiate Cyber Defense Competition/maccdc2012_00003.pcap" @ http://bit.ly/2maxlsD.

Hunt Location:	SSH client banners
Hunt For:	Unexpected banners
Possible Threat:	Unauthorized connections
Format:	Count (Ascending), SSH client string

```
===========================================================
SSH Client_Strings
===========================================================

1
4               SSH-2.0-OpenSSH_5.2
6               SSH-1.5-NmapNSE_1.0
6               SSH-1.5-Nmap-SSH1-Hostkey
11              SSH-2.0-OpenSSH_5.3p1 Debian-3ubuntu7
12              SSH-2.0-Nmap-SSH2-Hostkey
14              SSH-2.0-OpenSSH_5.3p1 Debian-3ubuntu6
30              SSH-2.0-OpenSSH_5.0
```

Figure 23 - Results acquired from "National CyberWatch Mid-Atlantic Collegiate Cyber Defense Competition/maccdc2012_00007.pcap" @ http://bit.ly/2maxlsD.

© 2017 The SANS Institute Author retains full rights.

Hunt Location:	SSH authentication results
Hunt For:	Abnormal increase in failed authentications
Possible Threat:	Password guessing
Format:	Count (Ascending), SSH auth_success result (True/False)

```
=========================================================
SSH Auth_Success
=========================================================

17              T
73              F
```

Figure 24 - Results acquired from "National CyberWatch Mid-Atlantic Collegiate Cyber Defense Competition/maccdc2012_00008.pcap" @ http://bit.ly/2maxlsD.

2.2.6. SSL Traffic

Hunt Location:	SSL certificates' Issuers
Hunt For:	Odd Issuers
Possible Threat:	Malicious websites and encrypted C&C communication channels
Format:	Count (Ascending), SSL issuer

```
=========================================================
SSL Issuers
=========================================================

1             CN=3uat.zwdt0km.yeh.bsoj.umbg.net
1             CN=Scorebot
7             CN=192.168.22.254
18            CN=192.168.25.254
58            CN=SplunkCommonCA
1180          CN=localhost.localdomain
```

Figure 25 - Results acquired from "National CyberWatch Mid-Atlantic Collegiate Cyber Defense Competition/maccdc2012_00003.pcap" @ http://bit.ly/2maxlsD.

© 2017 The SANS Institute Author retains full rights.

Hunt Location:	SSL certificates validity
Hunt For:	Self-signed and expired certs
Possible Threat:	Malicious websites and encrypted C&C communication channels
Format:	Count (Ascending), SSL cert validation result

```
===========================================================
SSL Validation_Status
===========================================================

15          ok
16          self signed certificate
```

Figure 26 - Results acquired from "Malware Traffic Analysis/2015-10-28-traffic-analysis-exercise.pcap" @ http://bit.ly/2lS8g4L.

Hunt Location:	SSL certificates server's name
Hunt For:	Odd server names
Possible Threat:	Malicious websites and encrypted C&C communication channels
Format:	Count (Ascending), TLD SSL server name

```
===========================================================
SSL Servers_Names
===========================================================

2           .live.com
4           .tor2web.org
5           .microsoft.com
```

Figure 27 - Results acquired from "Malware Traffic Analysis/2016-09-20-traffic-analysis-exercise.pcap" @ http://bit.ly/2lS8g4L.

© 2017 The SANS Institute Author retains full rights.

© 2017 The SANS Institute Author Retains Full Rights

2.2.7. RDP Traffic

Hunt Location:	RDP sessions
Hunt For:	Unexpected RDP clients/servers
Possible Threat:	Lateral movements
Format:	Count (Ascending), client IP, server IP, server port

```
2           x.x.x.x   -------> y.y.y.y    : 3389/tcp
5           x.x.x.x   -------> y.y.y.y    : 3389/tcp
15          x.x.x.x   -------> y.y.y.y    : 3389/tcp
```

Figure 28

Hunt Location:	RDP credentials
Hunt For:	Unexpected usernames
Possible Threat:	Compromised accounts
Format:	Count (Ascending), domain \ username

```
2           Domain\Username
20          Domain\Username
```

Figure 29

© 2017 The SANS Institute Author retains full rights.

2.2.8. IRC Traffic

Hunt Location:	IRC sessions
Hunt For:	IRC clients
Possible Threat:	C&C traffic and potential insider
Format:	Count (Ascending), client IP, server IP, server port

```
===========================================================
IRC session
===========================================================

7               80.117.14.44     -------> 192.168.100.28   : 7000/tcp
12              192.168.100.28   -------> 206.252.192.195  : 6667/tcp
192             192.168.100.28   -------> 206.252.192.195  : 5555/tcp
```

Figure 30 - Results acquired from "Honeynet Project/day1.pcap" @ http://bit.ly/2mdPszy.

Hunt Location:	IRC usernames
Hunt For:	Suspicious activities
Format:	Count (Ascending), IRC username

```
===========================================================
IRC username
===========================================================

9               root-poppopret
```

Figure 31 - Results acquired from "Google CTF 2016/irc.pcap" @ http://bit.ly/2lO2lgc.

© 2017 The SANS Institute Author retains full rights.

Hunt Location:	IRC nicknames
Hunt For:	Suspicious activities
Format:	Count (Ascending), IRC nickname

```
============================================================
IRC nick
============================================================

3               andrewg
3               itsl0wk3y
3               Matir
```

Figure 32 - Results acquired from "Google CTF 2016/irc.pcap" @ http://bit.ly/2lO2lgc.

2.2.9. FTP Traffic

Hunt Location:	FTP sessions
Hunt For:	Unexpected FTP clients/server
Possible Threat:	Lateral movements or data exfiltration
Format:	Count (Ascending), Client IP, Server IP, Server port

```
============================================================
FTP Sessions
============================================================

4               192.168.100.28   -------> 192.18.99.122    : 21/tcp
10              192.168.100.28   -------> 62.211.66.16     : 21/tcp
```

Figure 33 - Results acquired from "Honeynet Project/day1.pcap"
@ http://bit.ly/2mdPszy.

© 2017 The SANS Institute Author retains full rights.

Hunt Location:	FTP usernames
Hunt For:	Unexpected usernames
Possible Threat:	Compromised accounts
Format:	Count (Ascending), FTP username

```
============================================================
FTP Usernames
============================================================

4               anonymous
10              bobzz
```

Figure 34 - Results acquired from "Honeynet Project/day1.pcap" @ http://bit.ly/2mdPszy.

Hunt Location:	FTP current working directory
Hunt For:	Sensitive directories
Possible Threat:	Data exfiltration or unauthorized access
Format:	Count (Ascending), current working directory

```
============================================================
FTP Current_Working_Directories
============================================================

4               ./pub/patches
10              .
```

Figure 35 - Results acquired from "Honeynet Project/day1.pcap" @ http://bit.ly/2mdPszy.

Hunt Location:	FTP commands
Hunt For:	Abnormal increase in DELETE commands
Possible Threat:	Unauthorized Deletion
Format:	Count (Ascending), FTP command

```
============================================================
FTP Commands
============================================================

5               PORT
9               RETR
```

Figure 36 - Results acquired from "Honeynet Project/day1.pcap" @ http://bit.ly/2mdPszy.

© 2017 The SANS Institute Author retains full rights.

2.2.10. File MIME Types

Hunt Location:	Files mime types
Hunt For:	Odd types (i.e. PE files transferred over HTTP or SMB)
Possible Threat:	Malware
Format:	Count (Ascending), MIME type, communication protocol

```
============================================================
File MIME_Types
============================================================

1                application/x-shockwave-flash            -------> HTTP
2                image/x-ms-bmp                           -------> HTTP
2                application/x-dosexec                    -------> SMB
8                application/xml                          -------> HTTP
9                application/x-dosexec                    -------> HTTP
13               text/x-php                               -------> HTTP
14               image/x-icon                             -------> HTTP
70               image/gif                                -------> HTTP
95               image/png                                -------> HTTP
250              application/pkix-cert                    -------> SSL
315              text/json                                -------> HTTP
765              text/plain                               -------> FTP_DATA
1145             text/plain                               -------> HTTP
2023             text/html                                -------> HTTP
```

Figure 37 - Results acquired from "National CyberWatch Mid-Atlantic Collegiate Cyber Defense Competition/maccdc2012_00002.pcap" @ http://bit.ly/2maxlsD.

© 2017 The SANS Institute Author retains full rights.

3. Conclusion

Active threat hunting is not a new realm, although the terminology has been associated with a lot of marketing hype recently. It has been practiced and exercised by InfoSec community over the past few years (BEJTLICH, 2017) with different levels of maturity starting from basic network security monitoring along with decent intelligence, up to data visualization, heat maps, and machine learning.

Determining where to hunt and what to hunt for, impacts the quality level of the hunting trip. Often, preparing the environment for hunting requires more time and effort than doing the exercise itself. Preparation includes but not limited to, stopping unneeded services, disabling unused protocols, and doing proper network segmentation to facilitate convenient grouping. With threat hunting, there is a difference between visibility and clear visibility since it's highly sensitive to noise. The clearer the visibility, the easier the hunt would be.

Threat hunting also focuses on detection patterns that cannot be avoided or bypassed (i.e. Number of bytes uploaded will highlight data exfiltration attempts). Hence, better results could be achieved by directing hunting efforts towards legitimate channels where adversaries try to blend attack traffic with legit traffic.

Throughout the paper, we have seen how to leverage Bro to do count stacking – one of the major hunting techniques- to detect abnormalities that could be one of the footprints an advanced attack left behind on the network. The implemented checks show how network traffic metadata could be of great help for security analysts to quickly identify interesting hunt leads. Those leads have a good chance of highlighting events of interests missed by traditional signature-based/reactive detection. Although the focus of the paper was on PCAP traces, there are endless ways to apply the same concept to other parts of the network and possibilities are limited by analysts' creativity.

© 2017 The SANS Institute Author retains full rights.

References

Clark, J. (2016, July 27). *Introduction to Threat Hunting*, [Video file]. Retrieved from https://www.youtube.com/watch?v=4odBNTRdskE

SANS - Information Security Resources. (n.d.). Retrieved from https://www.sans.org/security-resources/idfaq/what-is-intrusion-detection/1/1

Mecha, B. (2016, October 13). How threat hunting is different from an intrusion detection system. Retrieved from https://www.cybereason.com/how-threat-hunting-is-different-from-an-intrusion-detection-system/

Ashford, W. (n.d.). Hunters: a rare but essential breed of enterprise cyber defenders. Retrieved from http://www.computerweekly.com/feature/Hunters-a-rare-but-essential-breed-of-enterprise-cyber-defenders

TCP/UDP Port Activity - SANS Internet Storm Center. (n.d.). Retrieved from https://isc.sans.edu/port.html

Sharpe, D. (2015, September 28). *Intrusion Hunting for the Masses a Practical Guide David Sharpe* [Video file]. Retrieved from https://www.youtube.com/watch?v=MUUseTJp3jM

Valenzuela, I. (2014, March 11). Open Security Research: Identifying Malware Traffic with Bro and the Collective Intelligence Framework (CIF). Retrieved from http://blog.opensecurityresearch.com/2014/03/identifying-malware-traffic-with-bro.html

Threat Hunting Project (An informational repo about hunting for adversaries in your IT environment.) Retrieved February 13, 2017, from https://github.com/ThreatHuntingProject/ThreatHunting

© 2017 The SANS Institute Author retains full rights.

Bisson, D. (2015, September 13). *Most Suspicious TLDs Revealed by Blue Coat Systems*. Retrieved from https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/most-suspicious-tlds-revealed-by-blue-coat-systems/

Bro-PCAP-Dissector (Bro script to dissect PCAP files in a way that facilitates active threat hunting by employing stack counting techniques.) Retrieved March 13, 2017, from https://github.com/0xhandler/Bro-PCAP-Dissector/.

BEJTLICH, R. (2017, March 14). Tao Security: The Origin of Threat Hunting. Retrieved from https://taosecurity.blogspot.qa/2017/03/the-origin-of-threat-hunting.html

Valenzuela, I. (2014, March 11). Open Security Research: Identifying Malware Traffic with Bro and the Collective Intelligence Framework (CIF). Retrieved from http://blog.opensecurityresearch.com/2014/03/identifying-malware-traffic-with-bro.html

Threat Hunting Project (An informational repo about hunting for adversaries in your IT environment.) Retrieved February 13, 2017, from https://github.com/ThreatHuntingProject/ThreatHunting

© 2017 The SANS Institute, Author Retains Full Rights

© 2017 The SANS Institute

Author retains full rights.