Final Engagement

Attack, Defense & Analysis of a Vulnerable Network

Table of Contents: Red Team

This document contains the following resources:

01

Network Topology & Critical Vulnerabilities

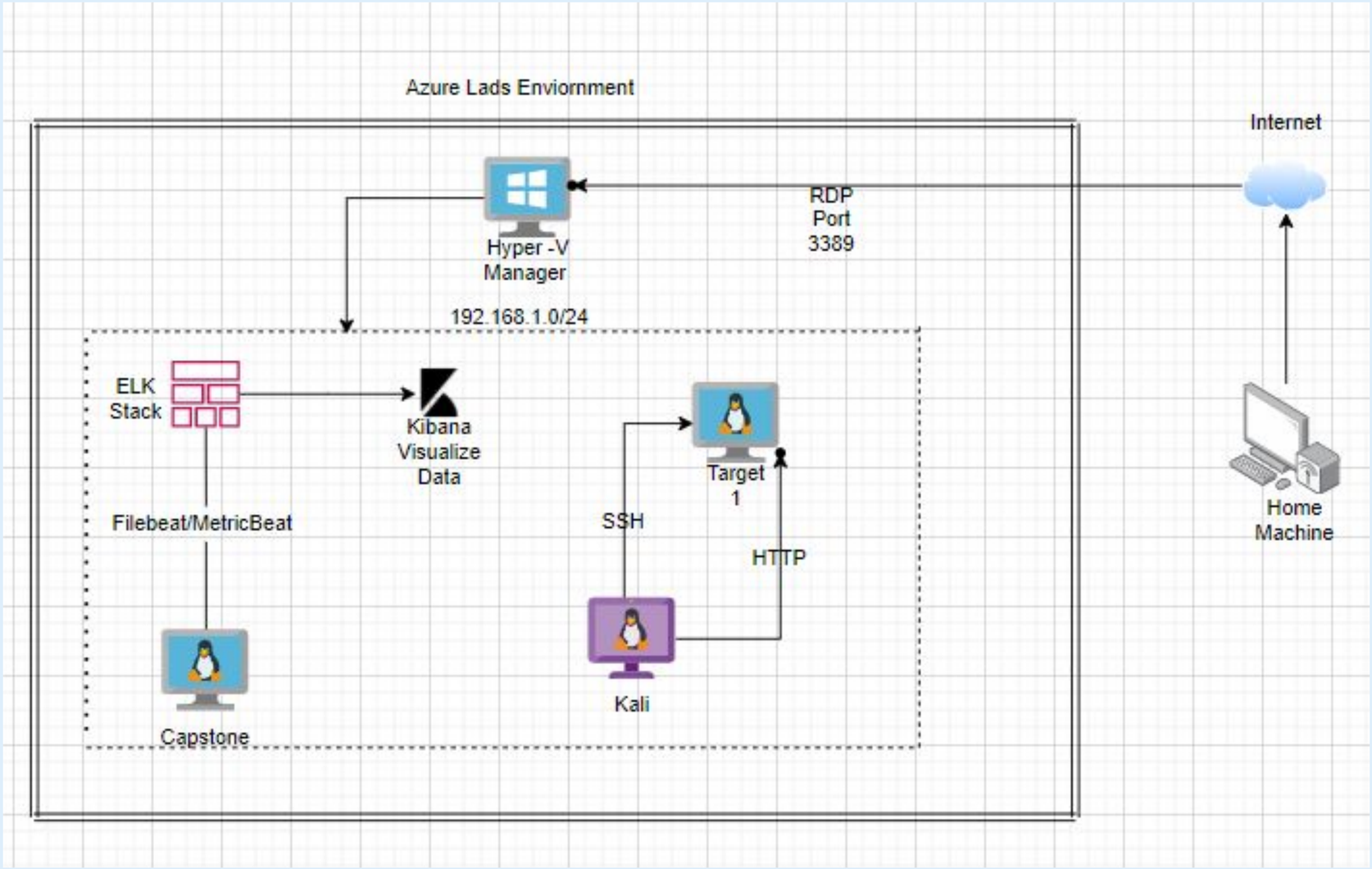
02

Exploits Used

03

Methods Used to Avoid Detection

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: Dedian kali 5.4.0
Hostname: Kali

IPv4:192.168.1.110
OS: Debian GNU/Linux 8
Hostname:Target 1

IPv4:192.168.1.105
OS:Ubuntu 18.04
Hostname: Capstone

IPv4:192.168.100
OS:Ubuntu 18.04
Hostname: ELK

Network Topology
& Critical Vulnerabilities

Critical Vulnerabilities: Target 1

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

Vulnerability	Description	Impact
Weak Passwords	Easy to manually brute foguess and SSH as Michael	Login as Michael on the Target 1 machine and find flags 1 and 2.
Unsalted SQL credentials	When looking for the MySQL credentials they were easily readable in plaintext	We were able to just login to the SQL database and find flag 3.
Unsalted hashed passwords	Able to find Steven's password with a simple john crack	Ability to use john the ripper to find Steven's password from the hashes. (pink84)
Privilege Escalation	When on Target 1we were able to use a python command to escalate to root	Once logged in as Steven we were able to escalate to root using a pseudo-terminal utility.

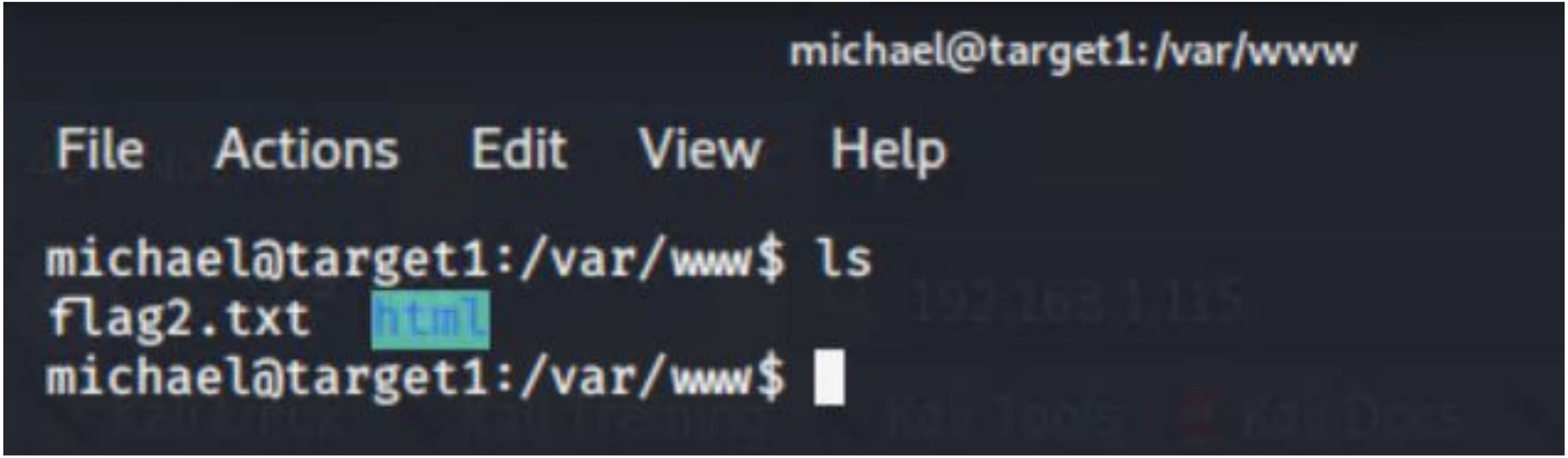
Exploits Used

Exploitation: Weak Passwords

Summarize the following:

- Using wpscan we found the usernames Michael and Steven
- We used a manual brute force to figure out Michael’s password (michael)
- It wasn’t the first password we used, but it was one of them
- This allowed us to ssh into the Target 1 machine as Michael and find flags 1 and 2


End footer Area
flag1{b9bbcb33e11b80be759c4e844862482d}


michael@target1:/var/www
File Actions Edit View Help
michael@target1:/var/www$ ls
flag2.txt html
michael@target1:/var/www$

Exploitation: Unsalted MySQL credentials

Summarize the following:

- Once logged into the target machine we found the MySQL credentials
- Navigated to the wp-config.php and found the unsalted user, password and host
- Used the credentials found in .php file to login to the MySQL database
- Looked through the tables and found flag 3.

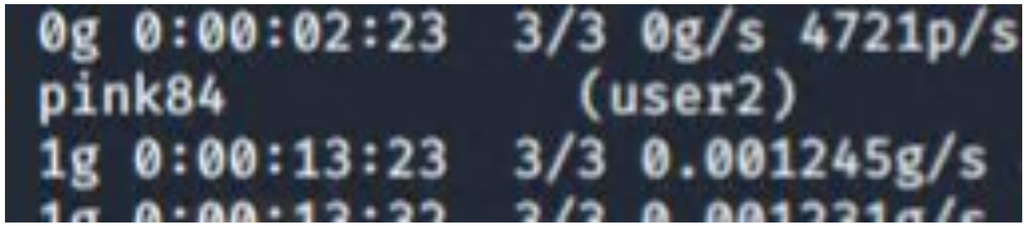
```
// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define('DB_NAME', 'wordpress');

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

```
                    | flag3       |            | draft      | open         | open       |            |            |
   |      | 2018-08-13 01:48:31 | 2018-08-13 01:48:31 |               |          0 | http://raven.local/wordpress/?p=4
                    |           0 | post     |            |           0 |
|  5 |          1 | 2018-08-12 23:31:59 | 2018-08-12 23:31:59 | flag4{715dea6c055b9fe3337544932f2941ce}




                    | flag4       |            | inherit    | closed       | closed     |            | 4-revision-v1 |
   |      | 2018-08-12 23:31:59 | 2018-08-12 23:31:59 |               |          4 | http://raven.local/wordpress/index.php/2
018/08/12/4-revision-v1/ |           0 | revision |            |           0 |
|  7 |          2 | 2018-08-13 01:48:31 | 2018-08-13 01:48:31 | flag3{afc01ab56b50591e7dccf93122770cd2}




                    | flag3       |            | inherit    | closed       | closed     |            | 4-revision-v1 |
   |      | 2018-08-13 01:48:31 | 2018-08-13 01:48:31 |               |          4 | http://raven.local/wordpress/index.php/2
018/08/13/4-revision-v1/ |           0 | revision |            |           0 |
+----+------------+--------------------+--------------------+------------------------------------------------
----------------------------------------------------------------------------------------------------------------
----------------------------------------------------------------------------------------------------------------
----------------------------------------------------------------------------------------------------------------
----------------------------------------------------------------------------------------------------------------
----------------------------------------------------------------------------------------------------------------
----------------------------------------------------------------------------------------------------------------
------------------------+-------------+-------------+------------+--------------+------------+-------------+----
-----+-------+--------------------+--------------------+---------------------+------------+-----------------
---------------------+----------+----------+--------------+--------------+
5 rows in set (0.00 sec)
```

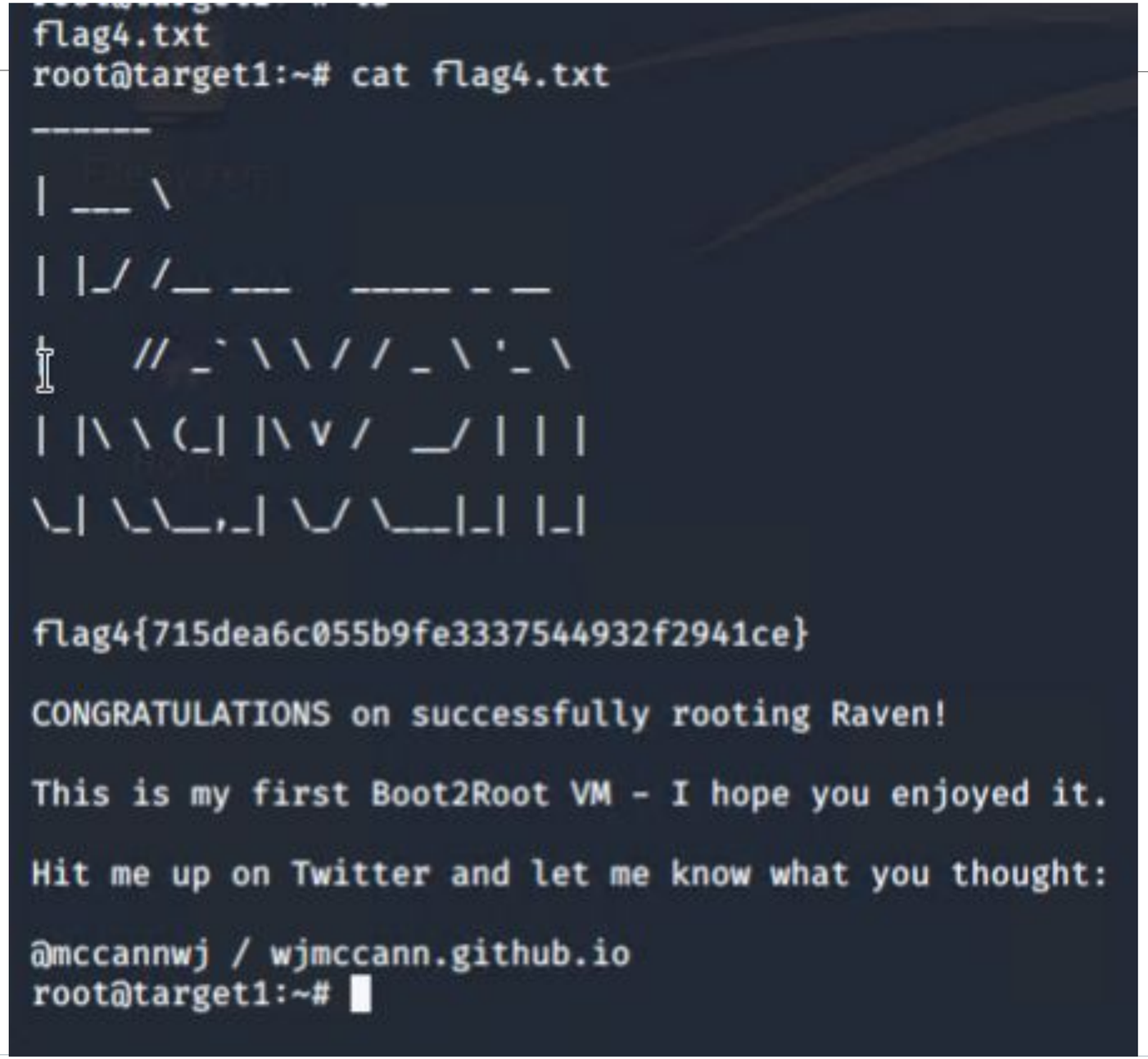
Exploitation: Unsalted Hashed Passwords

Summarize the following:

- Once logged on to the MySQL we navigated to the wp_users table and and found the unsalted hashed passwords
- Created a .txt file with the hashed passwords and used john the ripper to crack a password



ID	user_login	user_pass	user_nicename	user_email	user_url	user_registered	user_activation_key	user_status	display_name
1	michael	PBjRvZQ.VQcGZlDeiKToCQd.cPw5XCe0	michael	michael@raven.org		2018-08-12 22:49:12		0	michael
2	steven	PBk3VD9jsxx/loJoqNsURgHiaB23j7W/	steven	steven@raven.org		2018-08-12 23:31:16		0	Steven Seagull


flag4.txt
root@target1:~# cat 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@target1:~#

Avoiding Detection

Stealth Exploitation of Weak Passwords

Monitoring Overview

- Logging in with external IP addresses, or logging of failed login attempts leading up to proper login
- Time, IP address, attempts
- When HTTP response codes of 400 are recorded more than 5 times in a 5 minute span

Mitigating Detection

- Use internal IPs (i.e. SSH into an already exploited machine) and space out login attempts
- Phishing techniques to gain more direct access would be more efficient and effective

Stealth Exploitation of Unsalted SQL credentials

Monitoring Overview

- External IP addresses and user alerts
- Time, IP addresses, usernames, databases accessed
- Thresholds could be as low as 1 depending on rules set up for database protection

Mitigating Detection

- The best way to mitigate detection would also be with internal IP addresses and/or the use of proper administrative account
- Potentially scripting events to gain the administrative access up front might hide tracks easier

Stealth Exploitation of Privilege Escalation

Monitoring Overview

- Alert escalation would notify when the escalation to root occurs.
- The alert is triggered any time user escalates privileges to root,
- They fire each time root user is accesses

Mitigating Detection

- You cannot use this exploit undetected because of all of the alerts going off
- An alternative exploit would be to find the root password a different way.

Network Topology
& Critical Vulnerabilities

Table of Contents : Network Analysis

This document contains the following resources:

Critical Vulnerabilities: Target 1

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

Vulnerability	Description	Impact
Weak Passwords	Was able to find passwords using dictionary brute force against web form	Allowed attacker to gain access to protected web directories
Wordpress User Enumeration	Utilized enum4linux to gather user information for the web server	Allows attacker to gather usernames to gain access to the web server
Unprotected and Unsalted Hash	Used Rainbow table to compare an unprotected hash to a corresponding password	Allowed attacker to gain access to WebDav to alter contents of web server
Privilege Escalation	Used Stevens sudo Python access to escalate from ‘Steven to root’	Allowed privilege escalation to root

Traffic Profile

Traffic Profile

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

Feature	Value	Description
Top Talkers (IP Addresses)	172.16.4.205, 185.243.115.84, 166.62.111.64	Machines that sent the most traffic.
Most Common Protocols	VSS Monitoring Ethernet trailer, HTTP, (TLS)	Three most common protocols on the network.
# of Unique IP Addresses	808	Count of observed IP addresses.
Subnets	24-bit block	Observed subnet ranges.
# of Malware Species	Trojan (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.
- Normal use of the website via wordpress traffic
- Standard files transferred (Favicons, standard scripts, supporting images)
- Application Programming Interfaces (APIs) necessary to support the browser-site interaction

Suspicious Activity

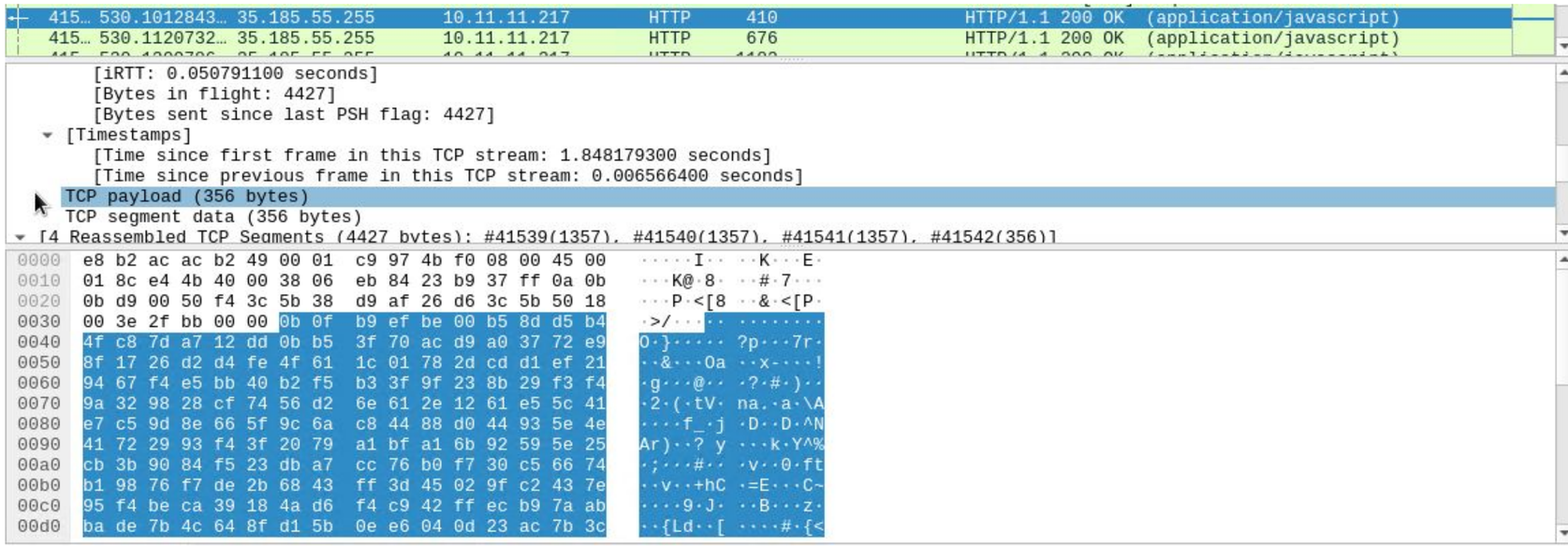
- For example: Sending malware, phishing.
- files.publicdomaintorrents.com used to download “Betty_Boop_Rhythm_on_the_Reservation.avi.torrent”
- http://205.185.125.104/files/june11.dll
- b5689023.green.mattingsolutions.co downloaded empty.gif?ss&ss1img

Normal Activity

Standard Website Traffic

Summarize the following:

- **Protocols observed:**
  - TCP
  - HTTP
- **Traffic Analyzed:**
  - www.sabethahospital.com
  - www.iphonehacks.com
  - mysocalledchaos.com
- **Possibly Interesting Files:**
  - jquery-migrate.min.js

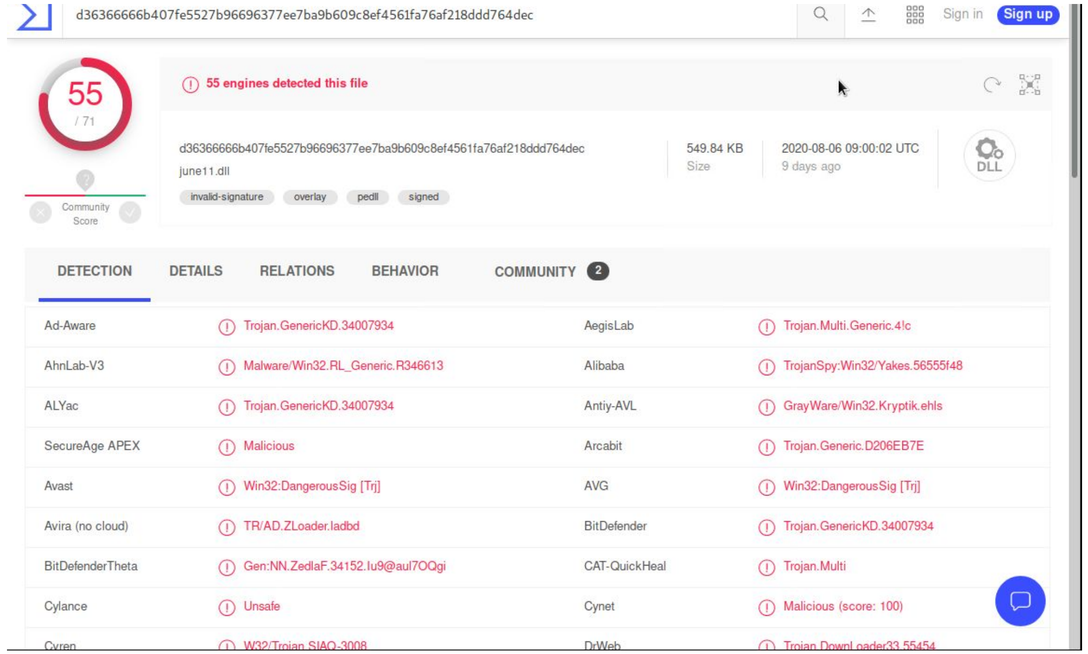


Malicious Activity

Illegal Downloads

Summarize the following:

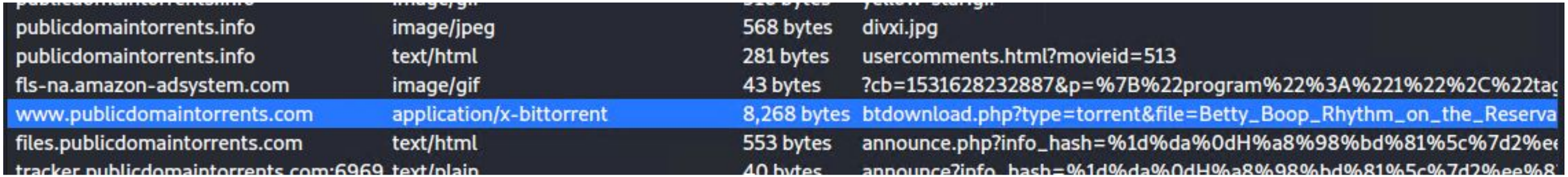
- **Protocol Observed:**
  - HTTP
- **Traffic Analyzed:**
  - User downloaded a Trojan from http://205.185.125.104/files/june11.dll
- **Possibly Interesting Files:**
  - june11.dll



Illegal Downloads

Summarize the following:

- **Protocol Observed:**
  - HTTP
- **Traffic Analyzed:**
  - User was browsing publicdomaintorrents.com and downloaded a torrent.
- **Possibly Interesting Files:**
  - Betty_Boop_Rhythm_on_the_Reservation.avi.torrent



publicdomaintorrents.info	image/jpeg	568 bytes	divxi.jpg
publicdomaintorrents.info	text/html	281 bytes	usercomments.html?movieid=513
fls-na.amazon-adsystem.com	image/gif	43 bytes	?cb=1531628232887&p=%7B%22program%22%3A%221%22%2C%22tag
www.publicdomaintorrents.com	application/x-bittorrent	8,268 bytes	btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reserva
files.publicdomaintorrents.com	text/html	553 bytes	announce.php?info_hash=%1d%da%0dH%a8%98%bd%81%5c%7d2%ee

Fin