

# **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**

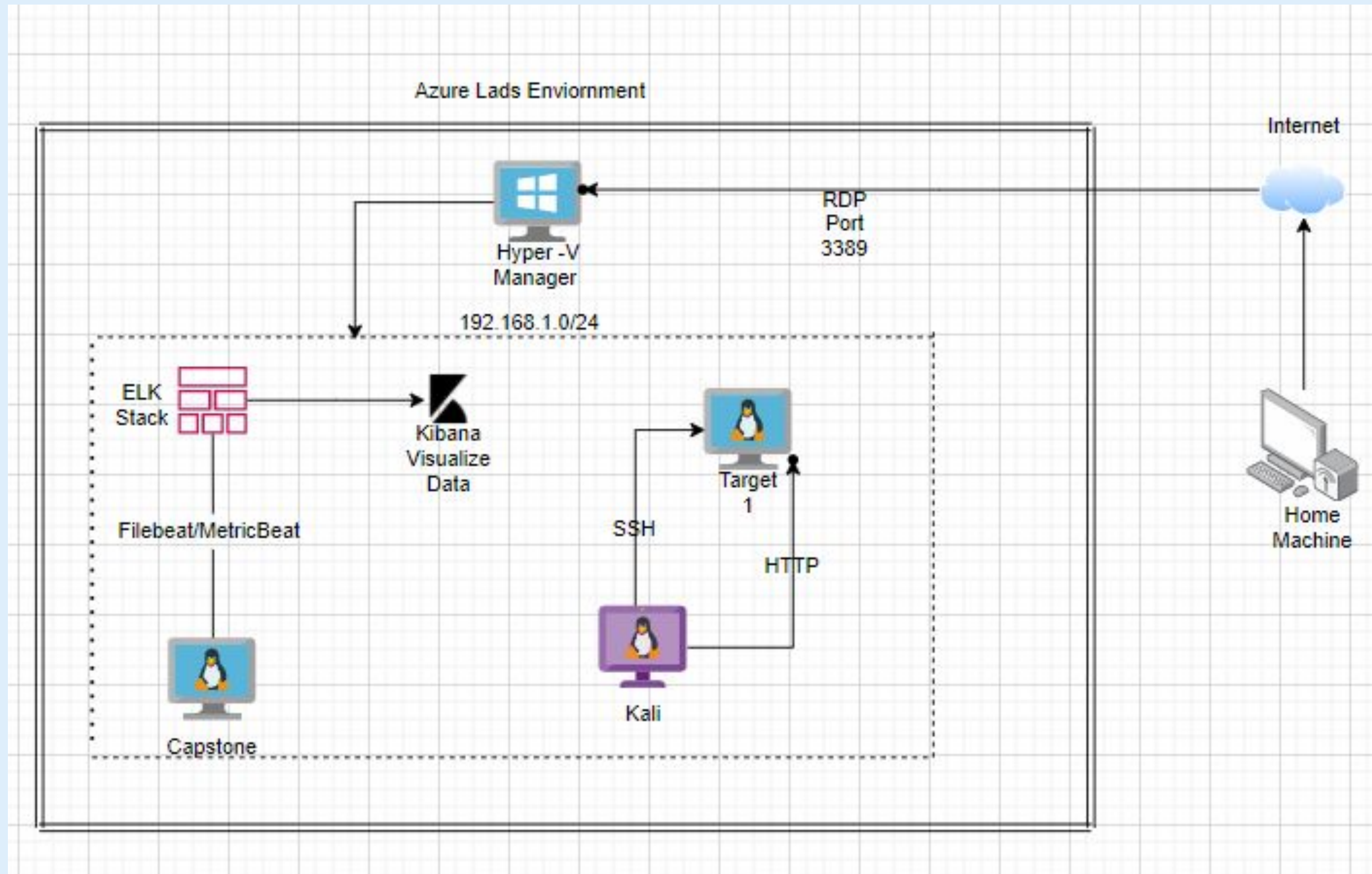
02

**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: Debian 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: 192.168.1.100  
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 1 we 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} —→  
<script src="/vendor/jquery-2.2.4.min.js"></script>
```

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', '');
```







# Exploitation: Unsalted Hashed Passwords

Summarize the following:

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

```
0g 0:00:02:23 3/3 0g/s 4721p/s
pink84 (user2)
1g 0:00:13:23 3/3 0.001245g/s
1g 0:00:13:23 3/3 0.001231g/s
```

ID	user_login	user_pass	user_nicename	user_email	user_url	user_re
gistered	user_activation_key	user_status	display_name			
1	michael	\$P\$BjRvZQ.VQcGZlDeiKToCQd.cPw5XCe0	michael	michael@raven.org		2018-08
-12 22:49:12		0	michael			
2	steven	\$P\$Bk3VD9jsxx/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:



**Network Topology & Critical Vulnerabilities**



**Traffic Profile**



**Normal Activity**



**Malicious Activity**

# 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.mattingssolutions.co downloaded empty.gif?ss&ss1img

# Normal Activity



# Standard Website Traffic

Summarize the following:

- **Protocols observed:**

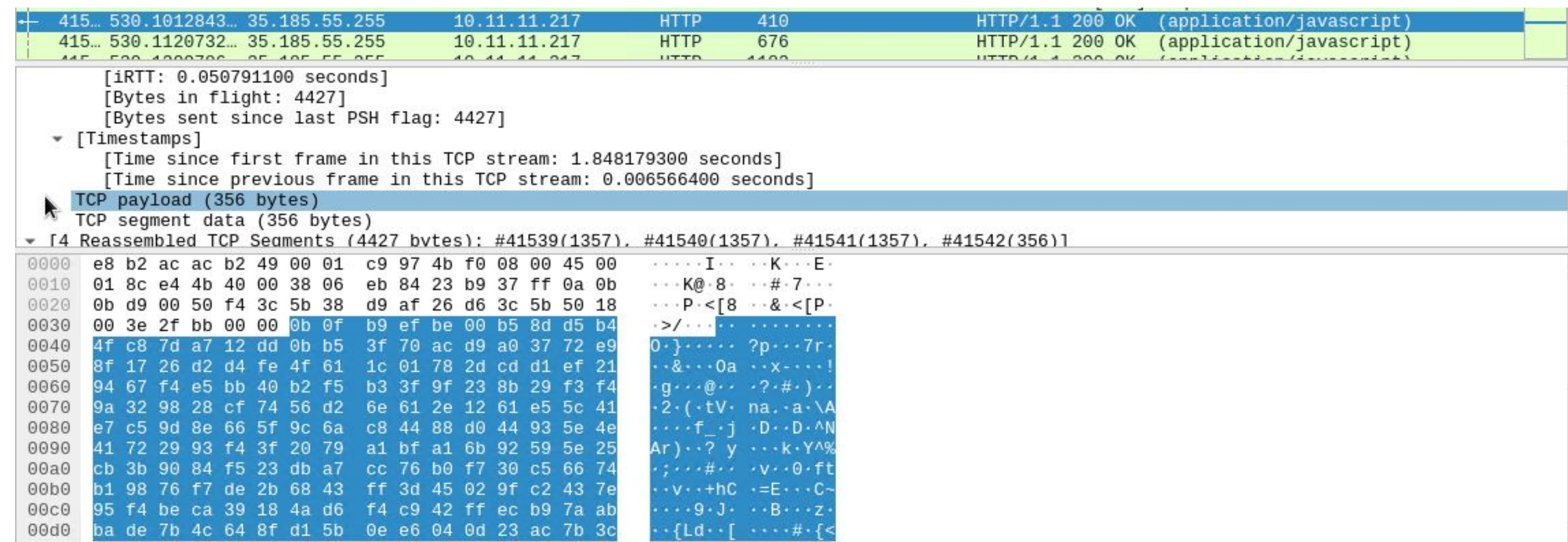
- TCP
- HTTP

- **Traffic Analyzed:**

- [www.sabethahospital.com](http://www.sabethahospital.com)
- [www.iphonhacks.com](http://www.iphonhacks.com)
- mysocalledchaos.com

- **Possibly Interesting Files:**

- jquery-migrate.min.js



415...	530.1012843...	35.185.55.255	10.11.11.217	HTTP	410	HTTP/1.1 200 OK (application/javascript)
415...	530.1120732...	35.185.55.255	10.11.11.217	HTTP	676	HTTP/1.1 200 OK (application/javascript)
415...	530.1200700...	35.185.55.255	10.11.11.217	HTTP	1400	HTTP/1.1 200 OK (application/javascript)

[iRTT: 0.050791100 seconds]  
[Bytes in flight: 4427]  
[Bytes sent since last PSH flag: 4427]  
[Timestamps]  
[Time since first frame in this TCP stream: 1.848179300 seconds]  
[Time since previous frame in this TCP stream: 0.006566400 seconds]  
TCP payload (356 bytes)  
TCP segment data (356 bytes)  
[4 Reassembled TCP Segments (4427 bytes): #41539(1357), #41540(1357), #41541(1357), #41542(356)]

0000	e8 b2 ac ac b2 49 00 01	c9 97 4b f0 08 00 45 00	.....I...K...E.
0010	01 8c e4 4b 40 00 38 06	eb 84 23 b9 37 ff 0a 0b	...K@.8...#7...
0020	0b d9 00 50 f4 3c 5b 38	d9 af 26 d6 3c 5b 50 18	...P.<[8...&<[P.
0030	00 3e 2f bb 00 00 0b 0f	b9 ef be 00 b5 8d d5 b4	...>/.....
0040	4f c8 7d a7 12 dd 0b b5	3f 70 ac d9 a0 37 72 e9	0.}.....?p...7r.
0050	8f 17 26 d2 d4 fe 4f 61	1c 01 78 2d cd d1 ef 21	..&...0a...x...!
0060	94 67 f4 e5 bb 40 b2 f5	b3 3f 9f 23 8b 29 f3 f4	.g...@...?·#·)·.
0070	9a 32 98 28 cf 74 56 d2	6e 61 2e 12 61 e5 5c 41	.2·(·tV·na·a·\A
0080	e7 c5 9d 8e 66 5f 9c 6a	c8 44 88 d0 44 93 5e 4e	...f_·j·D·D·^N
0090	41 72 29 93 f4 3f 20 79	a1 bf a1 6b 92 59 5e 25	Ar)··? y ...k·Y^%
00a0	cb 3b 90 84 f5 23 db a7	cc 76 b0 f7 30 c5 66 74	·;...#...v·0·ft
00b0	b1 98 76 f7 de 2b 68 43	ff 3d 45 02 9f c2 43 7e	..v...+hC ·=E...C~
00c0	95 f4 be ca 39 18 4a d6	f4 c9 42 ff ec b9 7a ab	...·9·J·...B...z·
00d0	ba de 7b 4c 64 8f d1 5b	0e e6 04 0d 23 ac 7b 3c	..{Ld...[ ...·#·{<

# 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`

55

/ 71

Community Score

55 engines detected this file

d36366666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec

june11.dll

549.84 KB

Size

2020-08-06 09:00:02 UTC

9 days ago

DLL

invalid-signature

overlay

peidl

signed

DETECTION

DETAILS

RELATIONS

BEHAVIOR

COMMUNITY 2

Ad-Aware	Trojan.GenericKD.34007934	AegisLab	Trojan.Multi.Generic.41c
AhnLab-V3	Malware/Win32.RL_Generic.R346613	Alibaba	TrojanSpy:Win32/Yakes.56555f48
ALYac	Trojan.GenericKD.34007934	Antiy-AVL	GrayWare/Win32.Kryptik.ehls
SecureAge APEX	Malicious	Arcabit	Trojan.Generic.D206EB7E
Avast	Win32:DangerousSig [Trj]	AVG	Win32:DangerousSig [Trj]
Avira (no cloud)	TR/AD.ZLoader.ladbd	BitDefender	Trojan.GenericKD.34007934
BitDefenderTheta	Gen:NN.ZedlaF.34152.lu9@aul70Qgi	CAT-QuickHeal	Trojan.Multi
Cylance	Unsafe	Cynet	Malicious (score: 100)
Cyren	W32/Trojan.SIAQ-3008	DrWeb	Trojan.Downloader33.55454



# 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
tracker.publicdomaintorrents.com:6969	text/plain	40 bytes	announce?info_hash=%1d%da%0dH%a8%98%bd%81%5c%7d2%ee%8

Fin