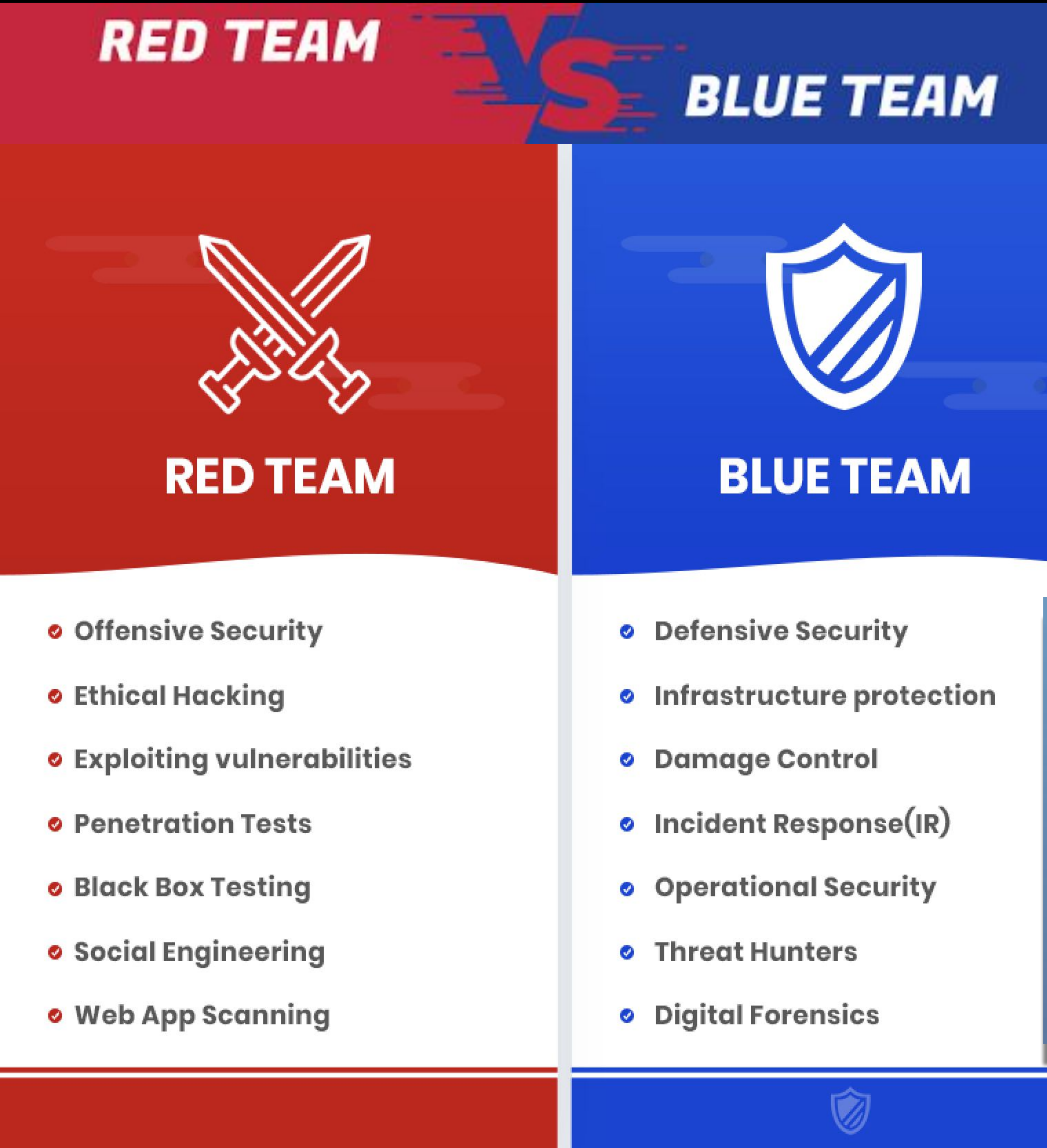
Final Engagement

Attack, Defense & Analysis of a Vulnerable Network

Table of Contents

This document contains the following resources:

- **Network Topology & Critical Vulnerabilities**
- **Traffic Profile**
- **Normal Activity**
- **Malicious Activity**



RED TEAM VS BLUE TEAM

RED TEAM

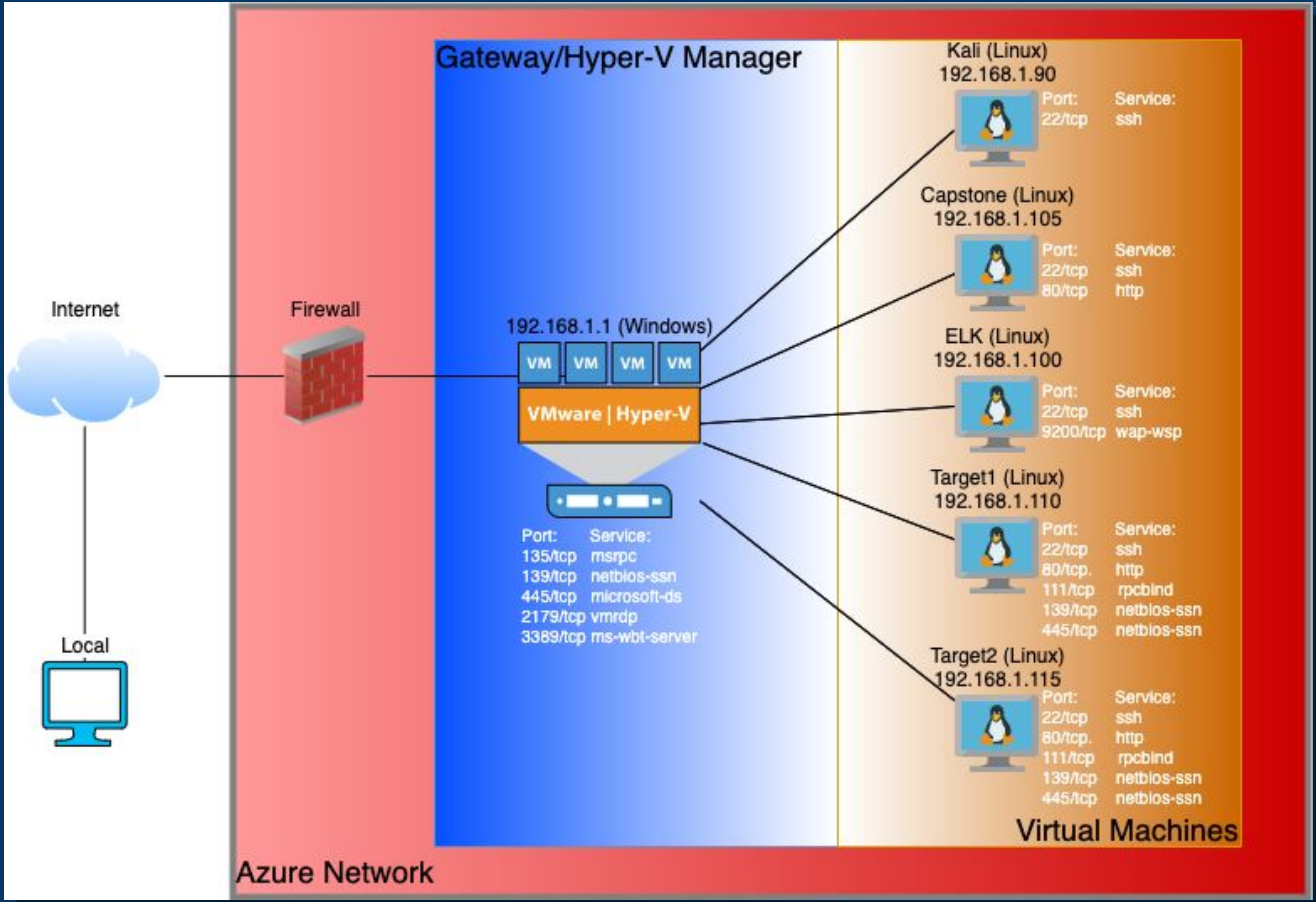
- Offensive Security
- Ethical Hacking
- Exploiting vulnerabilities
- Penetration Tests
- Black Box Testing
- Social Engineering
- Web App Scanning

BLUE TEAM

- Defensive Security
- Infrastructure protection
- Damage Control
- Incident Response(IR)
- Operational Security
- Threat Hunters
- Digital Forensics

Network Topology
& Critical Vulnerabilities

Network Topology



Network
Address Range:
192.168.1.0/24
Netmask: 255.255.255.0
Gateway: 192.168.1.1

Machines
IPv4: 192.168.1.90
OS: Linux
Hostname: kali

IPv4: 192.168.1.100
OS: Linux
Hostname: ELK

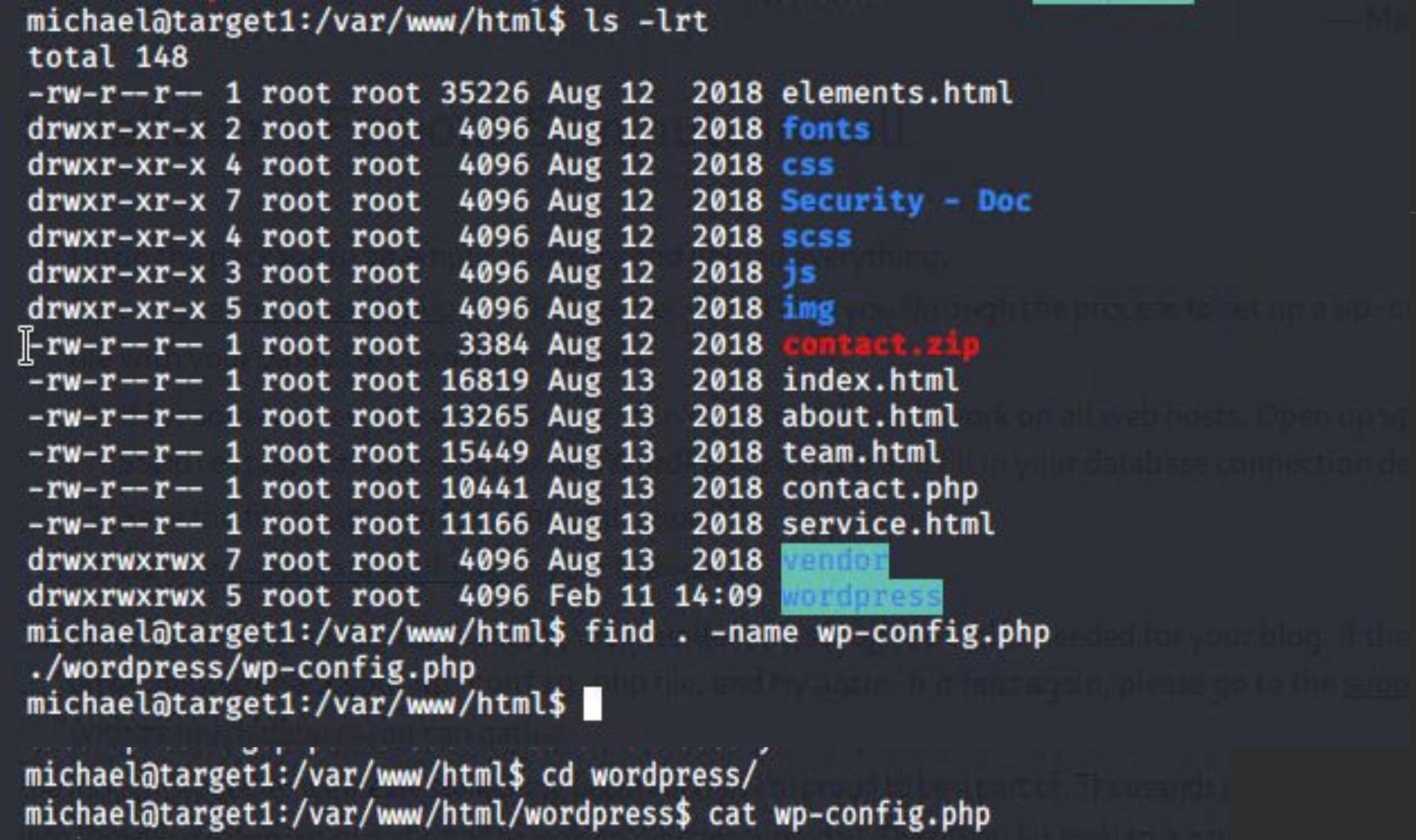
IPv4: 192.168.1.105
OS: Linux
Hostname: Capstone

IPv4: 192.168.1.110
OS: Linux
Hostname: Target1

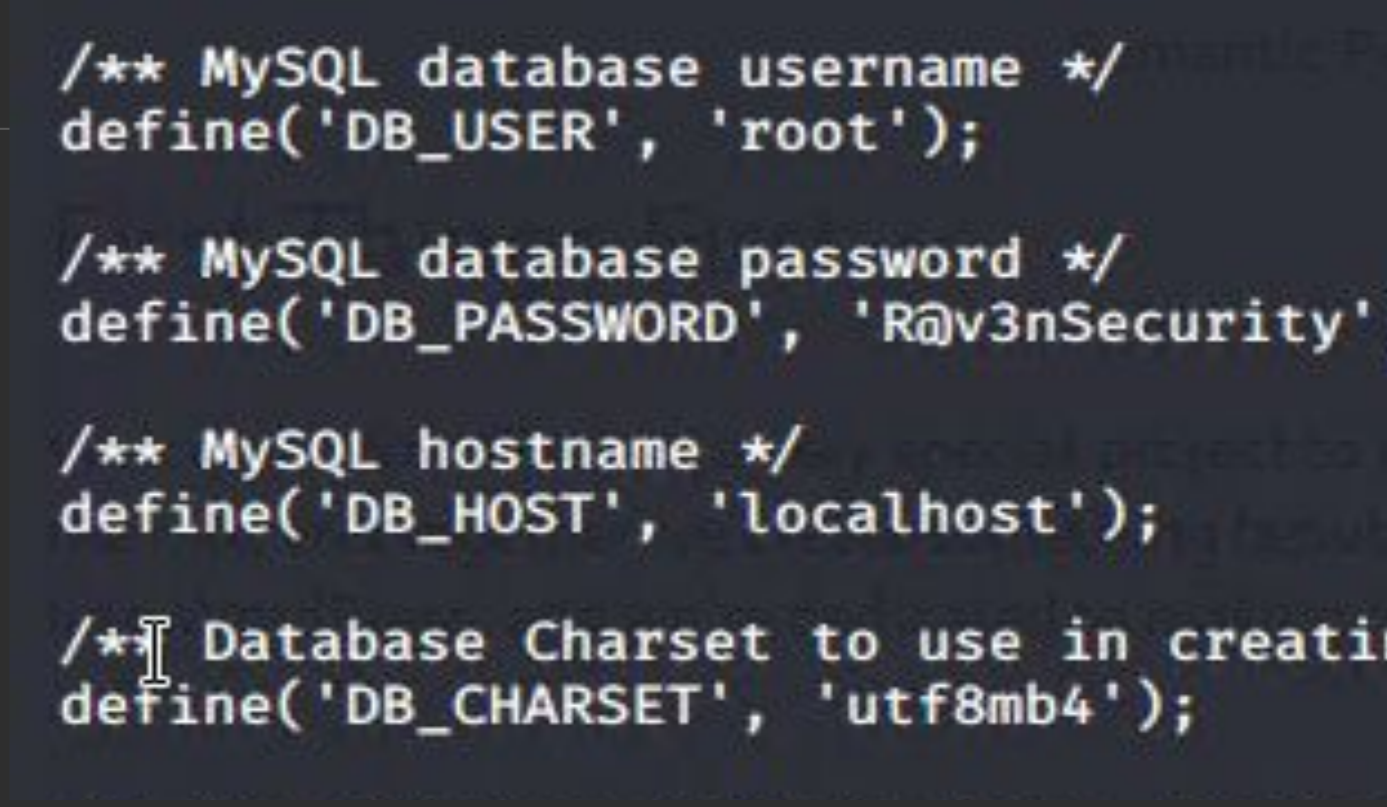
Critical Vulnerabilities: Target 1

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

Vulnerability	Description	Impact
Weak password Security	one user’s password was his name	Easy access to log on as that user
WordPress Site Enumeration	wpscan --url http://192.168.1.110/wordpress	Running this command displayed the users on this WordPress Server
Unrestricted SSH Access on Port 22	ssh michael@192.168.1.110	SSH access from any IP address with stolen Usernames and Passwords
Privilege Escalation with Python	python -c ‘import pty; pty.spawn(“/bin/bash”)’	Escalated steven’s privileges to root
Source Code Disclosure	view-source:http://192.168.1.110/service.html	Contained sensitive information and flag 1 was exfiltrated
Credentials for sql database were saved in plaintext, not hashed	backed up and publicly accessible wp-config.php files	Allowed for an attacker to obtain password credentials and gain access to exfiltrate flags 3 and 4

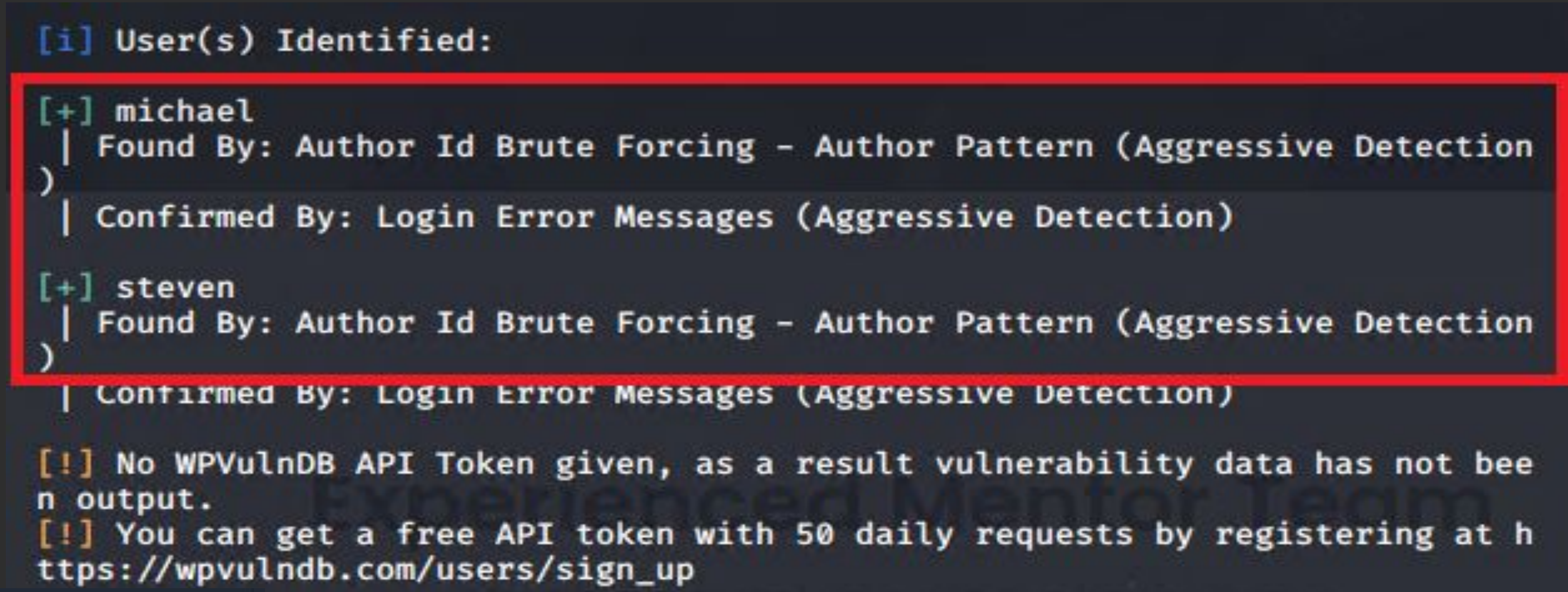


```
michael@target1:/var/www/html$ ls -lrt
total 148
-rw-r--r-- 1 root root 35226 Aug 12  2018 elements.html
drwxr-xr-x 2 root root  4096 Aug 12  2018 fonts
drwxr-xr-x 4 root root  4096 Aug 12  2018 css
drwxr-xr-x 7 root root  4096 Aug 12  2018 Security - Doc
drwxr-xr-x 4 root root  4096 Aug 12  2018 scss
drwxr-xr-x 3 root root  4096 Aug 12  2018 js
drwxr-xr-x 5 root root  4096 Aug 12  2018 img
-rw-r--r-- 1 root root  3384 Aug 12  2018 contact.zip
-rw-r--r-- 1 root root 16819 Aug 13  2018 index.html
-rw-r--r-- 1 root root 13265 Aug 13  2018 about.html
-rw-r--r-- 1 root root 15449 Aug 13  2018 team.html
-rw-r--r-- 1 root root 10441 Aug 13  2018 contact.php
-rw-r--r-- 1 root root 11166 Aug 13  2018 service.html
drwxrwxrwx 7 root root  4096 Aug 13  2018 vendor
drwxrwxrwx 5 root root  4096 Feb 11 14:09 wordpress
michael@target1:/var/www/html$ find . -name wp-config.php
./wordpress/wp-config.php
michael@target1:/var/www/html$ 

michael@target1:/var/www/html$ cd wordpress/
michael@target1:/var/www/html/wordpress$ cat wp-config.php
```



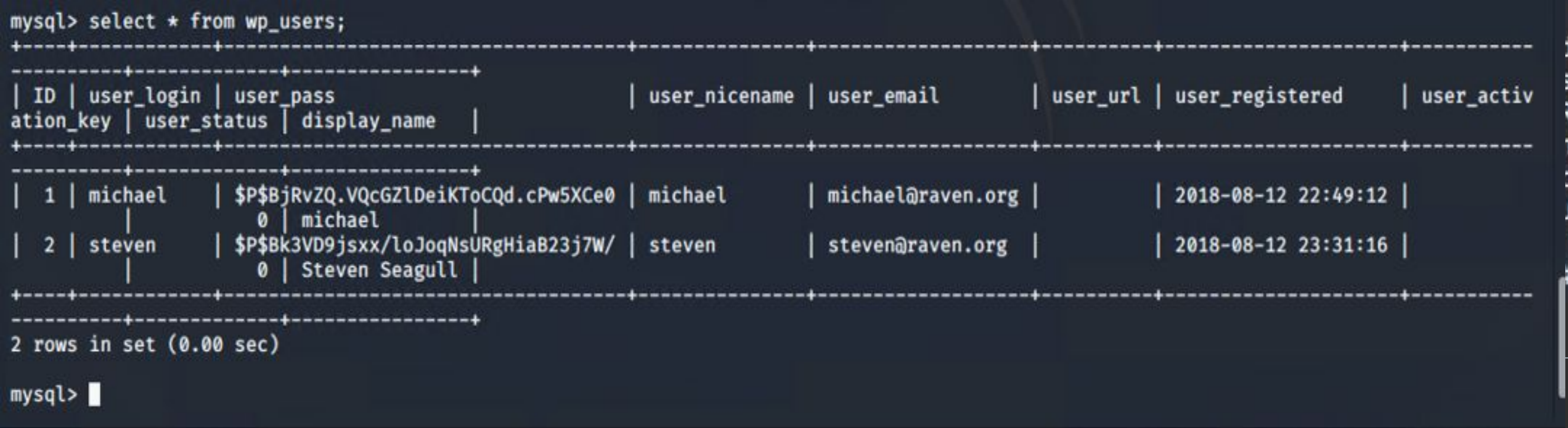
```
/** MySQL database username */
define('DB_USER', 'root');

/** 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');
```

SQL Credentials saved in Plaintext format



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

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

[+] steven
 | 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 bee
n output.
[!] You can get a free API token with 50 daily requests by registering at h
ttps://wpvulndb.com/users/sign_up

d: Wed Feb 10 19:12:53 2021
s Done: 27
Requests: 25
nt: 6.177 KB
ceived: 171.226 KB
used: 111.789 MB
 time: 00:00:03
# 
```

SQL Credentials then used to access SQL database table containing Password hashes



```
mysql> select * from wp_users;
+----+------------+------------------------------------+---------------+-------------------+----------+---------------------+----------
-----------+-------------+-----------------+
| ID | user_login | user_pass                          | user_nicename | user_email        | user_url | user_registered     | user_activ
ation_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 |
+----+------------+------------------------------------+---------------+-------------------+----------+---------------------+----------
-----------+-------------+-----------------+
2 rows in set (0.00 sec)

mysql> 
```

WordPress Site Enumeration showing usernames

Traffic Profile

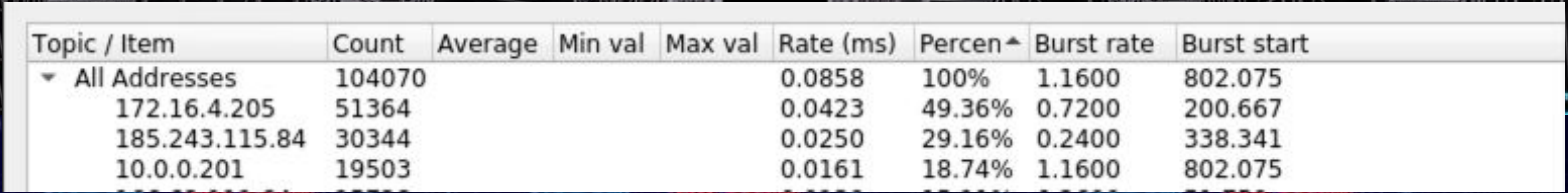
Traffic Profile

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

Feature	Value	Description
Top Talkers (IP Addresses)	172.16.2.205 - 49.36% 185.243.115.84 - 29.16% 10.0.0.201 - 18.74%	Machines that sent the most traffic.
Most Common Protocols	TCP - 88.5% UDP - 11.2% ARP - 0.2%	Three most common protocols on the network.
# of Unique IP Addresses	IPv4 - 808 IPv6 - 2	Count of observed IP addresses.
Subnets	10.0.0.0/24 10.6.12.0/24 192.168.1.0/24	Observed subnet ranges.
# of Malware Species	1 (one): june11.dll	Number of malware binaries identified in traffic.

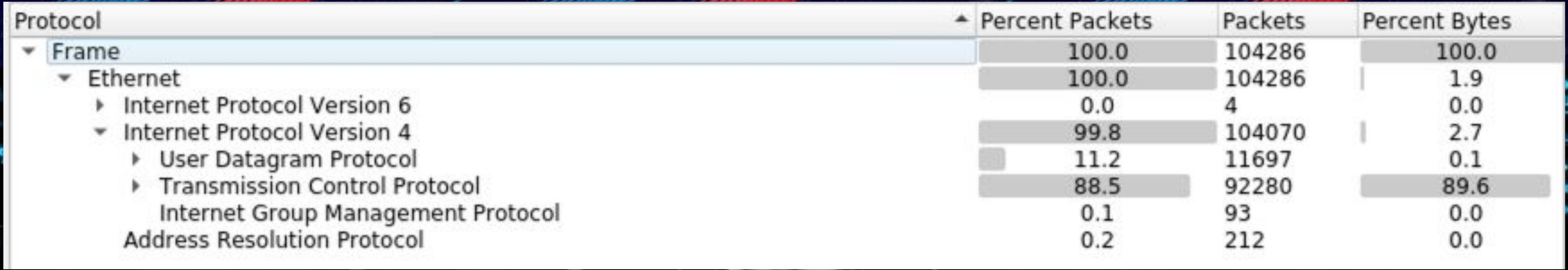
Traffic Profile

Top Talkers



Topic / Item	Count	Average	Min val	Max val	Rate (ms)	Percen	Burst rate	Burst start
All Addresses	104070				0.0858	100%	1.1600	802.075
172.16.4.205	51364				0.0423	49.36%	0.7200	200.667
185.243.115.84	30344				0.0250	29.16%	0.2400	338.341
10.0.0.201	19503				0.0161	18.74%	1.1600	802.075

Most Common Protocols



Protocol	Percent Packets	Packets	Percent Bytes
Frame	100.0	104286	100.0
Ethernet	100.0	104286	1.9
Internet Protocol Version 6	0.0	4	0.0
Internet Protocol Version 4	99.8	104070	2.7
User Datagram Protocol	11.2	11697	0.1
Transmission Control Protocol	88.5	92280	89.6
Internet Group Management Protocol	0.1	93	0.0
Address Resolution Protocol	0.2	212	0.0

Behavioral Analysis

Purpose of Traffic on the Network

Users were observed engaging in the following kinds of activity.

“Normal” Activity

- Watching YouTube Videos
- Searching .gif’s
- Researching how to flatten warped vinyl records
-

Suspicious Activity

- malware download
- illegal video download

Normal Activity

Internet Browsing - 1

- Observed traffic stream for standard query, GET requests and TCP retransmissions.
- The packet captures were for DNS, HTTP and TCP protocols
- Browsing the blog on the website - http://mysocalledchaos.com/
- Some of the files which got captured as part of the traffic stream - icons and images used in the blogsite, javascript files to enable cookies (cookie-enabler.min.js), count comments (comment_count.js)

No.	Time	Source	Destination	Protocol	Length	Info
12814	194.106890000	172.16.4.205	166.62.111.64	HTTP	522	GET /wp-content/uploads/2018/02/cropped-MSCCIcon-192x192.png HTTP/1.1
12825	194.257406900	172.16.4.205	93.95.100.178	HTTP	419	GET /docs/article.php?y=241&c=123080&m=8491edf39d1a8b498bbca9cd1bd6bbaa&st=1 HTTP/1.1
12844	194.551727700	172.16.4.205	166.62.111.64	HTTP	618	GET /?ginger_action=log&time=1563562388&url=http://mysocalledchaos.com/&status=Y HTTP/1.1
82407	902.840186600	172.16.4.205	172.16.4.4	DNS	79	Standard query 0x8c6e A mysocalledchaos.com
82412	902.850027500	172.16.4.4	172.16.4.205	DNS	95	Standard query response 0x8c6e A mysocalledchaos.com A 166.62.111.64
82413	902.851291400	172.16.4.205	172.16.4.4	DNS	79	Standard query 0xaf26 A mysocalledchaos.com
82414	902.852811100	172.16.4.4	172.16.4.205	DNS	95	Standard query response 0xaf26 A mysocalledchaos.com A 166.62.111.64
82431	902.886745600	172.16.4.205	166.62.111.64	TCP	390	[TCP Retransmission] 49190 → 80 [PSH, ACK] Seq=1 Ack=1 Win=66304 Len=336
82553	903.526105600	172.16.4.205	166.62.111.64	TCP	446	[TCP Retransmission] 49198 → 80 [PSH, ACK] Seq=1 Ack=1 Win=66304 Len=392
82554	903.532705300	172.16.4.205	166.62.111.64	TCP	412	[TCP Retransmission] 49200 → 80 [PSH, ACK] Seq=1 Ack=1 Win=66304 Len=358
82566	903.550644500	172.16.4.205	166.62.111.64	TCP	411	[TCP Retransmission] 49199 → 80 [PSH, ACK] Seq=1 Ack=1 Win=66304 Len=357

Internet Browsing - 2

- Observed traffic stream for standard query, GET requests and TCP retransmissions.
- The packet captures were for DNS, HTTP and TCP protocols
- Browsing the blog on the website - https://www.iphonehacks.com/ - contains various articles on iphone hacks and jailbreak tool for IOS
- Some of the files which got captured as part of the traffic stream - icons and images used in the website

No.	Time	Source	Destination	Protocol	Length	Info
40995	525.167914000	10.11.11.11	205.251.192.97	DNS	106	Standard query 0xe485 A iphonehacks.wpengine.netdna-cdn.com OPT
40996	525.173419200	205.251.192.…	10.11.11.11	DNS	344	Standard query response 0xe485 A iphonehacks.wpengine.netdna-cdn.com A 94.31.29.96 NS dns1.p04.ns…
40997	525.175663500	10.11.11.11	10.11.11.217	DNS	141	Standard query response 0x7d70 A cdn.iphonehacks.com CNAME iphonehacks.wpengine.netdna-cdn.com A …
41317	527.867962800	10.11.11.217	35.185.55.255	HTTP	476	GET /jailbreak-ios-13 HTTP/1.1
41320	527.892825800	35.185.55.255	10.11.11.217	TCP	1411	80 → 62521 [ACK] Seq=1 Ack=423 Win=29696 Len=1357 [TCP segment of a reassembled PDU]
41340	528.125375800	10.11.11.217	35.185.55.255	HTTP	459	GET /wp-content/themes/iphonehacks/css/font-awesome.min.css HTTP/1.1
41360	528.268688300	10.11.11.217	35.185.55.255	HTTP	446	GET /wp-content/themes/iphonehacks/css/app.css HTTP/1.1
41372	528.290126200	10.11.11.217	172.217.12.42	HTTP	423	GET /ajax/libs/jquery/1.12.4/jquery.min.js HTTP/1.1
41373	528.297856300	10.11.11.217	172.217.6.170	HTTP	483	GET /css?family=Open+Sans%3A300%2C400%2C600%2C700%7CLora%3A400%2C700%7CDroid+Sans+Mono HTTP/1.1

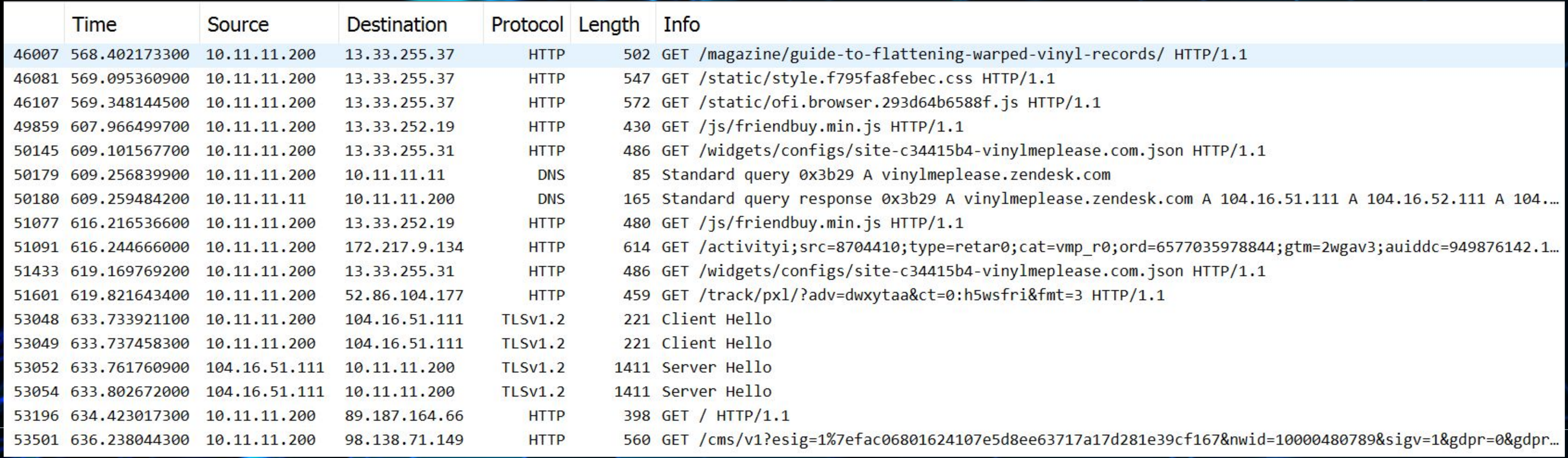
Internet Browsing - 3

- Observed traffic stream for standard query, GET requests
- The packet captures were for DNS and HTTP protocols
- Browsing the blog on the website - https://www.sabethahospitals.com
- Some of the files which got captured as part of the traffic stream - icons, clickable buttons and images used in the website, javascript files for embedded functions

```
      Time           Source          Destination     Protocol  Length  Info
37290 494.442524000  10.11.11.195    10.11.11.11          DNS      83  Standard query 0xfd32 A www.sabethahospital.com
37291 494.444106700  10.11.11.11     10.11.11.195         DNS      99  Standard query response 0xfd32 A www.sabethahospital.com A 12.133.50.21
38737 506.191258700  10.11.11.195    12.133.50.21        HTTP     460  GET /getpage.php?name=whatappendixdo HTTP/1.1
38756 506.370957000  10.11.11.195    12.133.50.21        HTTP     436  GET /style.php HTTP/1.1
38774 506.395569300  10.11.11.195    12.133.50.21        HTTP     471  GET /splash/logo.png HTTP/1.1
38775 506.403172500  10.11.11.195    12.133.50.21        HTTP     475  GET /splash/button-2.jpg HTTP/1.1
38776 506.410725400  10.11.11.195    12.133.50.21        HTTP     472  GET /common_js/common_css.php?c=3281&mt=1573231401 HTTP/1.1
38777 506.417949700  10.11.11.195    12.133.50.21        HTTP     439  GET /common_js/start_facebook.js HTTP/1.1
38778 506.424691800  10.11.11.195    12.133.50.21        HTTP     434  GET /common_js/polyfills.js HTTP/1.1
```

Internet Browsing - 4

- Observed traffic stream for standard query, GET requests, client-server handshake
- The packet captures were for DNS, HTTP, TLS1.2 protocols
- Browsing the blog on the website - https://www.vinlymeplease.com
- Some of the files which got captured as part of the traffic stream - html file “guide-to-flatenning-warped-vinyl-records”, javascript file to enable browser access



	Time	Source	Destination	Protocol	Length	Info
46007	568.402173300	10.11.11.200	13.33.255.37	HTTP	502	GET /magazine/guide-to-flattening-warped-vinyl-records/ HTTP/1.1
46081	569.095360900	10.11.11.200	13.33.255.37	HTTP	547	GET /static/style.f795fa8febec.css HTTP/1.1
46107	569.348144500	10.11.11.200	13.33.255.37	HTTP	572	GET /static/ofi.browser.293d64b6588f.js HTTP/1.1
49859	607.966499700	10.11.11.200	13.33.252.19	HTTP	430	GET /js/friendbuy.min.js HTTP/1.1
50145	609.101567700	10.11.11.200	13.33.255.31	HTTP	486	GET /widgets/configs/site-c34415b4-vinylmeplease.com.json HTTP/1.1
50179	609.256839900	10.11.11.200	10.11.11.11	DNS	85	Standard query 0x3b29 A vinylmeplease.zendesk.com
50180	609.259484200	10.11.11.11	10.11.11.200	DNS	165	Standard query response 0x3b29 A vinylmeplease.zendesk.com A 104.16.51.111 A 104.16.52.111 A 104.…
51077	616.216536600	10.11.11.200	13.33.252.19	HTTP	480	GET /js/friendbuy.min.js HTTP/1.1
51091	616.244666000	10.11.11.200	172.217.9.134	HTTP	614	GET /activityi;src=8704410;type=retar0;cat=vmp_r0;ord=6577035978844;gtm=2wgav3;auiddc=949876142.1…
51433	619.169769200	10.11.11.200	13.33.255.31	HTTP	486	GET /widgets/configs/site-c34415b4-vinylmeplease.com.json HTTP/1.1
51601	619.821643400	10.11.11.200	52.86.104.177	HTTP	459	GET /track/pxl/?adv=dwxytaa&ct=0:h5wsfri&fmt=3 HTTP/1.1
53048	633.733921100	10.11.11.200	104.16.51.111	TLSv1.2	221	Client Hello
53049	633.737458300	10.11.11.200	104.16.51.111	TLSv1.2	221	Client Hello
53052	633.761760900	104.16.51.111	10.11.11.200	TLSv1.2	1411	Server Hello
53054	633.802672000	104.16.51.111	10.11.11.200	TLSv1.2	1411	Server Hello
53196	634.423017300	10.11.11.200	89.187.164.66	HTTP	398	GET / HTTP/1.1
53501	636.238044300	10.11.11.200	98.138.71.149	HTTP	560	GET /cms/v1?esig=1%7efac06801624107e5d8ee63717a17d281e39cf167&nwid=10000480789&sigv=1&gdpr=0&gdpr…

Internet Browsing - 5

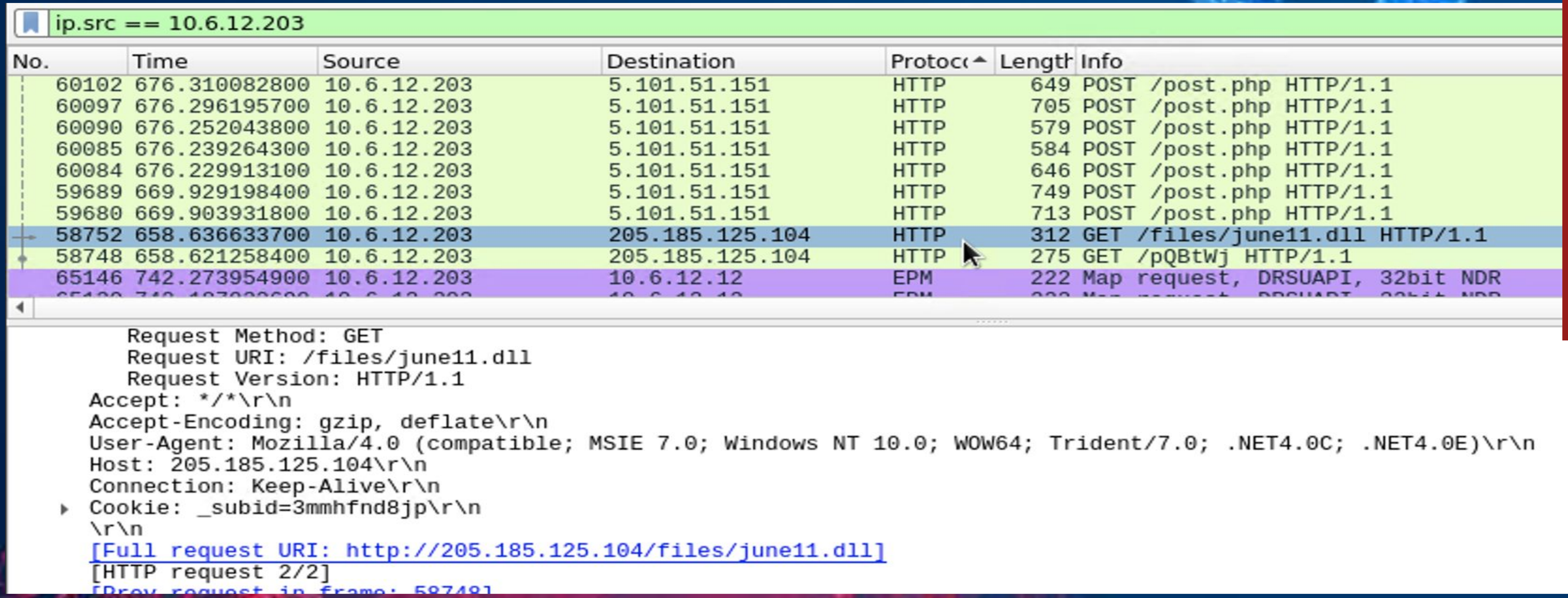
- Observed traffic stream for standard query, client-server handshake, TCP segments
- The packet captures were for DNS, TLSv1.3, TCP protocols
- Browsing the blog on the website - https://www.youtube.com

	Time	Source	Destination	Protocol	Length	Info
34388	470.584027200	10.11.11.94	10.11.11.11	DNS	75	Standard query 0x72cb A www.youtube.com
34389	470.589641000	10.11.11.11	10.11.11.94	DNS	349	Standard query response 0x72cb A www.youtube.com CNAME youtube-ui.l.google.com A 172.217.12.46 A …
35675	482.819410100	10.11.11.94	172.217.12.46	TLSv1.3	583	Client Hello
35676	482.828738500	10.11.11.94	172.217.12.46	TLSv1.3	583	Client Hello
51355	618.716454900	172.217.6.162	10.11.11.200	TCP	1411	443 → 49231 [ACK] Seq=1358 Ack=163 Win=61952 Len=1357 [TCP segment of a reassembled PDU]
51358	618.779055400	172.217.6.162	10.11.11.200	TCP	1411	443 → 49232 [ACK] Seq=1358 Ack=163 Win=61952 Len=1357 [TCP segment of a reassembled PDU]
67546	754.683640000	172.217.9.2	10.0.0.201	TLSv1.2	1484	Server Hello
67548	754.708253700	172.217.9.2	10.0.0.201	TCP	1484	443 → 49771 [PSH, ACK] Seq=1431 Ack=210 Win=64240 Len=1430 [TCP segment of a reassembled PDU]
67550	754.733324000	172.217.9.2	10.0.0.201	TLSv1.2	1514	Server Hello
68298	761.180894200	172.217.9.163	10.0.0.201	TLSv1.2	1484	Server Hello
68299	761.204646700	172.217.9.163	10.0.0.201	TCP	1484	443 → 49785 [PSH, ACK] Seq=1431 Ack=207 Win=64240 Len=1430 [TCP segment of a reassembled PDU]
68306	761.242300100	172.217.9.163	10.0.0.201	TLSv1.2	1514	Server Hello
68891	764.431557400	216.58.218.2…	10.0.0.201	TLSv1.2	1514	Server Hello
68894	764.479909800	216.58.218.2…	10.0.0.201	TLSv1.2	1514	Server Hello
68958	764.668552700	10.0.0.201	10.0.0.2	DNS	79	Standard query 0x33a7 A fcmatch.youtube.com
68959	764.670074100	10.0.0.2	10.0.0.201	DNS	95	Standard query response 0x33a7 A fcmatch.youtube.com A 216.58.218.206

Malware
DDoS ATTACKS
Spyware
Spam Email
Virus
malicious activity
Keylogger
TECHMUSA
TECHNOLOGY TO THE POINT

Malware (trojan): june11.dll

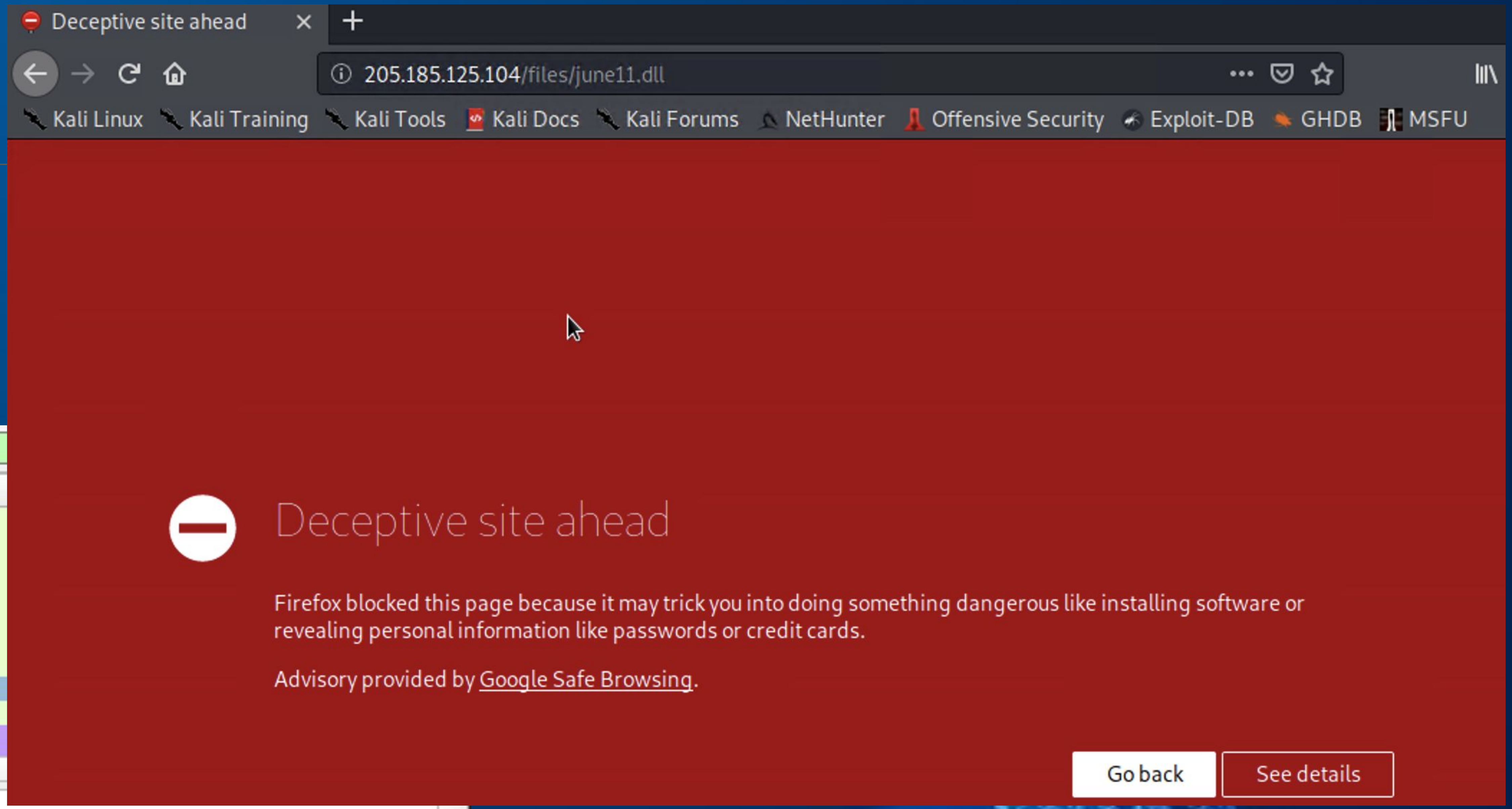
- This traffic was over HTTP
- The user was viewing 205.185.125.104/files/june11.dll



```
ip.src == 10.6.12.203
```

```
No.     Time            Source          Destination       Protocol  Length Info
  60102 676.310082800 10.6.12.203     5.101.51.151      HTTP       649 POST /post.php HTTP/1.1
  60097 676.296195700 10.6.12.203     5.101.51.151      HTTP       705 POST /post.php HTTP/1.1
  60090 676.252043800 10.6.12.203     5.101.51.151      HTTP       579 POST /post.php HTTP/1.1
  60085 676.239264300 10.6.12.203     5.101.51.151      HTTP       584 POST /post.php HTTP/1.1
  60084 676.229913100 10.6.12.203     5.101.51.151      HTTP       646 POST /post.php HTTP/1.1
  59689 669.929198400 10.6.12.203     5.101.51.151      HTTP       749 POST /post.php HTTP/1.1
  59680 669.903931800 10.6.12.203     5.101.51.151      HTTP       713 POST /post.php HTTP/1.1
  58752 658.636633700 10.6.12.203     205.185.125.104   HTTP       312 GET /files/june11.dll HTTP/1.1
  58748 658.621258400 10.6.12.203     205.185.125.104   HTTP       275 GET /pQBtWj HTTP/1.1
  65146 742.273954900 10.6.12.203     10.6.12.12        EPM        222 Map request, DRSUAPI, 32bit NDR
```

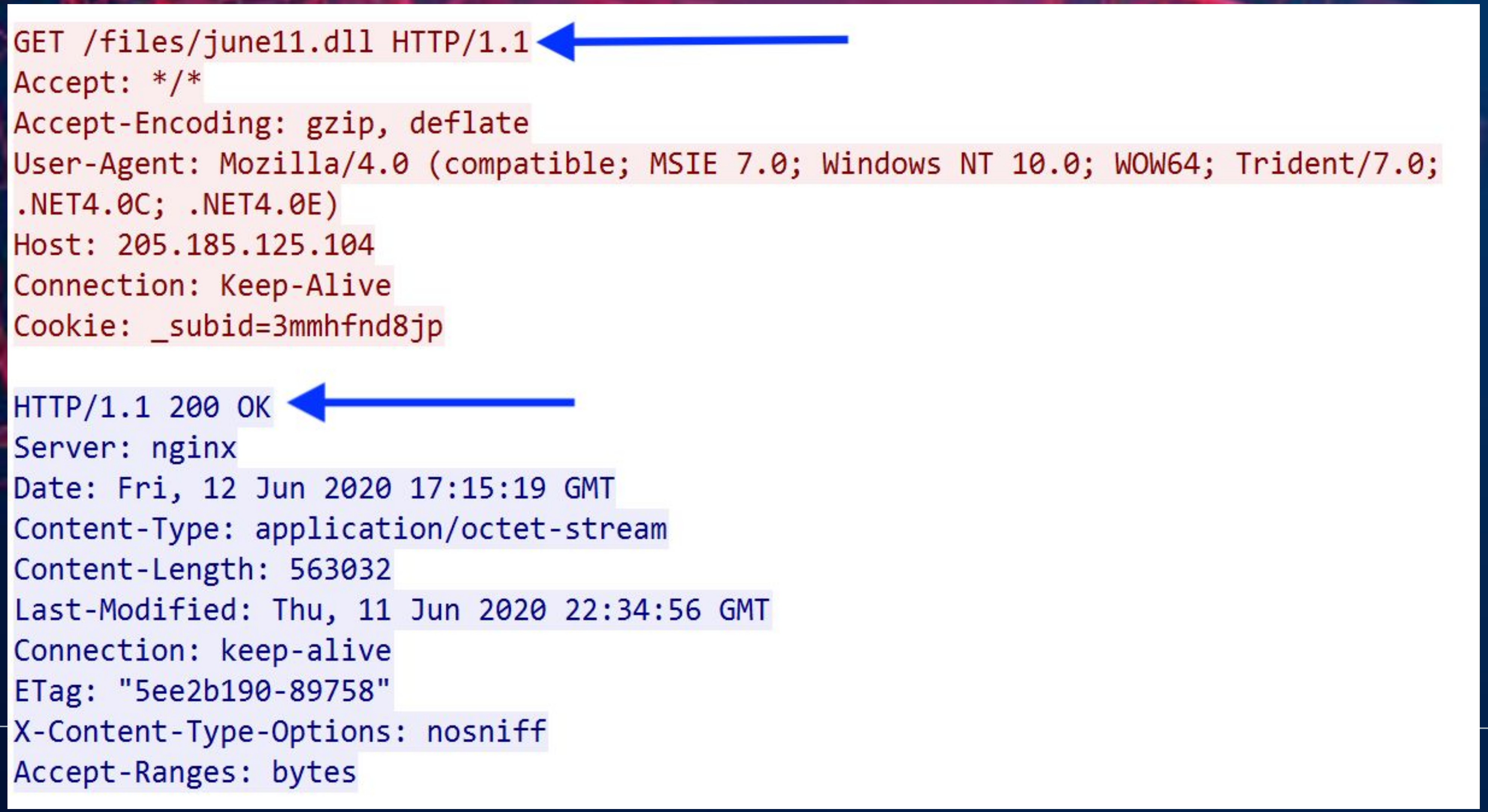
```
        Request Method: GET
        Request URI: /files/june11.dll
        Request Version: HTTP/1.1
    Accept: */*\r\n
    Accept-Encoding: gzip, deflate\r\n
    User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E)\r\n
    Host: 205.185.125.104\r\n
    Connection: Keep-Alive\r\n
  ▸ Cookie: _subid=3mmhfnd8jp\r\n
    \r\n
    [Full request URI: http://205.185.125.104/files/june11.dll]
    [HTTP request 2/2]
    [Prev request in frame: 58748]
```



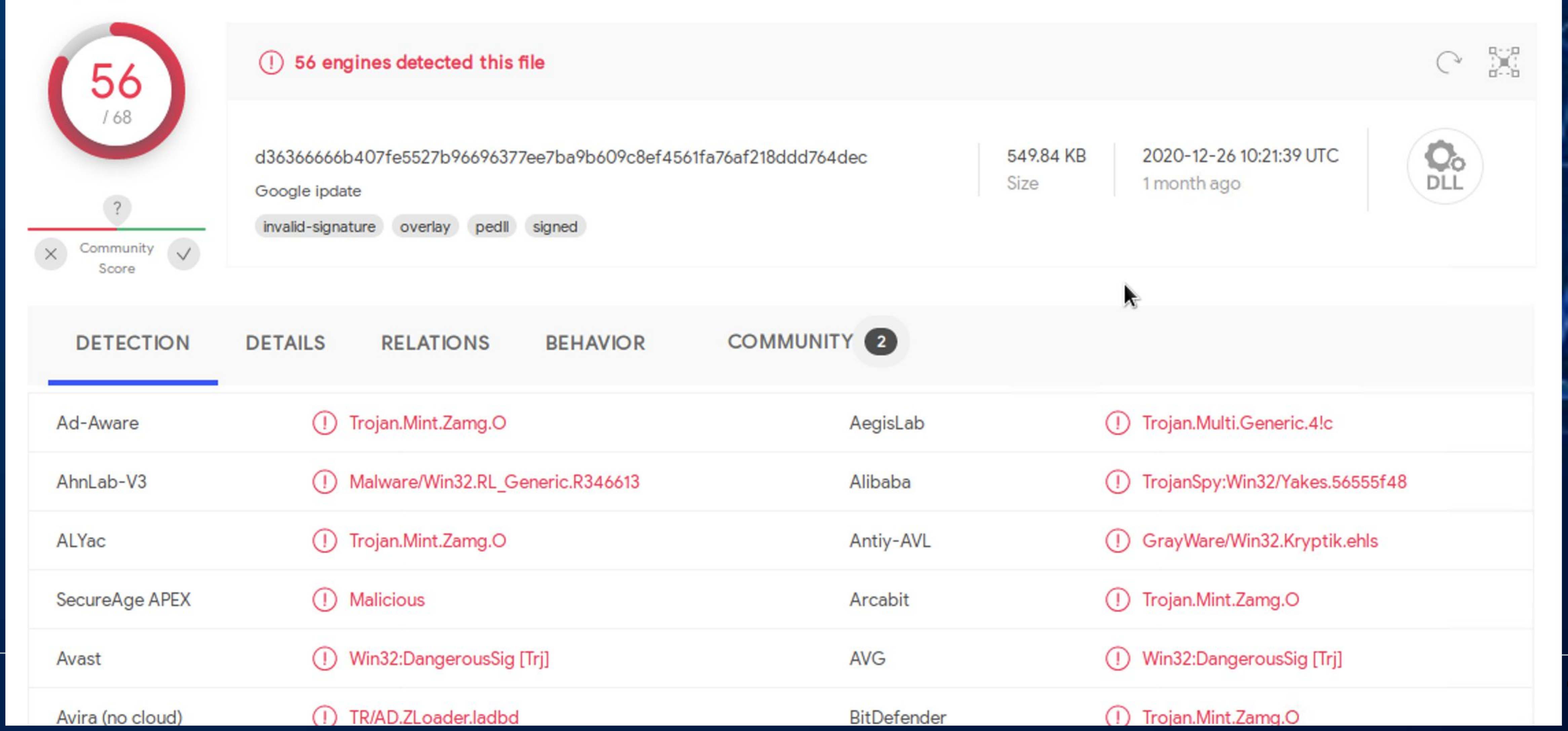
Deceptive site ahead

Firefox blocked this page because it may trick you into doing something dangerous like installing software or revealing personal information like passwords or credit cards.

Advisory provided by Google Safe Browsing.



```
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
```



56 / 68

56 engines detected this file

d36366666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec

Google ipdate

invalid-signature overlay pedll signed

549.84 KB Size

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

Ad-Aware	Trojan.Mint.Zamg.O	AegisLab	Trojan.Multi.Generic.4!c
AhnLab-V3	Malware/Win32.RL_Generic.R346613	Alibaba	TrojanSpy:Win32/Yakes.56555f48
ALYac	Trojan.Mint.Zamg.O	Antiy-AVL	GrayWare/Win32.Kryptik.ehls
SecureAge APEX	Malicious	Arcabit	Trojan.Mint.Zamg.O
Avast	Win32:DangerousSig [Trj]	AVG	Win32:DangerousSig [Trj]
Avira (no cloud)	TR/AD.ZLoader.ladbd	BitDefender	Trojan.Mint.Zamg.O

Illegal Download - Betty Boop Rhythm on the Reservation

- MAC address Destination: Msi_18:66:c8 (00:16:17:18:66:c8)
- Windows username **elmer.blanco**
- OS version Windows NT 10.0
- User downloaded the file Betty_Boop_Rhythm_on_the_Reservation.avi.torrent

```
      Time          Source          Destination     Protocol  Length  Info
69167 765.416418700 10.0.0.201      168.215.194.14      HTTP     500  GET /grabs/bettybooprythmonthereservationgrab.jpg HTTP/1.1
69213 765.837950500 10.0.0.201      168.215.194.14      HTTP     465  GET /divxi.jpg HTTP/1.1
69298 766.857868300 10.0.0.201      52.94.240.125       HTTP     415  GET /s/ads.js HTTP/1.1
69347 767.585292600 10.0.0.201      168.215.194.14      HTTP     531  GET /usercomments.html?movieid=513 HTTP/1.1
69434 768.625230500 10.0.0.201      52.94.240.125       HTTP     427  GET /s/ads-common.js HTTP/1.1
69470 768.919511100 10.0.0.201      72.21.202.62        HTTP     885  GET /e/cm?t=publicdomai0f-20&o=1&p=48&l=op1&pvid=40C236A13FDD0B68&ref-url=http%3A//publicdomainto…
69542 769.560506300 10.0.0.201      52.94.233.131       HTTP    1067  GET /1/associates-ads/1/OP/?cb=1531628232887&p=%7B%22program%22%3A%221%22%2C%22tag%22%3A%22public…
69700 770.351745800 10.0.0.201      10.0.0.2             DNS      88  Standard query 0xdee1 A www.publicdomaintorrents.com
69701 770.353627000 10.0.0.2        10.0.0.201           DNS     118  Standard query response 0xdee1 A www.publicdomaintorrents.com CNAME publicdomaintorrents.com A 16…
69706 770.366956400 10.0.0.201      168.215.194.14      HTTP     589  GET /bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent HTTP/1.…
69710 770.393856600 168.215.194.…   10.0.0.201           TCP    1514  80 → 49834 [PSH, ACK] Seq=1 Ack=536 Win=64240 Len=1460 [TCP segment of a reassembled PDU]
69729 770.525334900 10.0.0.201      10.0.0.2             DNS      81  Standard query 0xe7bb A router.bittorrent.com
```

The End

The End.

The Endkddkjskfjsjdfjsdjflks