# Final Engagement

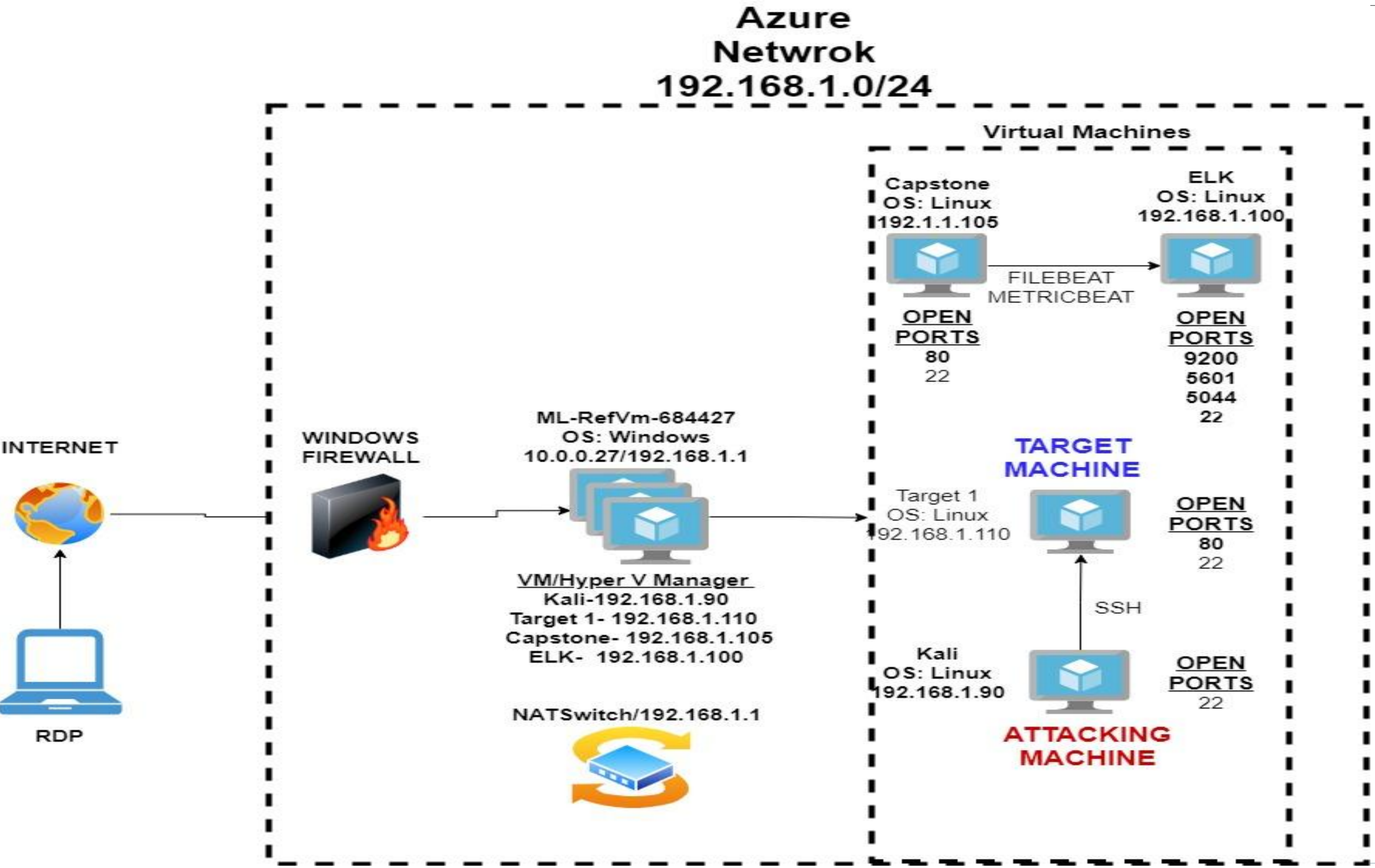
Attack, Defense & Analysis of a Vulnerable Network

# Table of Contents

- Network Topology & Critical Vulnerabilities
- Exploits Used
- Avoiding Detection
- Defensive: Critical Vulnerabilities
- Alerts Implemented
- Hardening
- Traffic Profile
- Normal/Malicious Activity

# Network Topology
# & Critical Vulnerabilities

# Network Topology



**Network**
Addr**Network**
Address Range:
192.168.1.0/24
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

# Critical Vulnerabilities: Target 1

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

| Vulnerability | Description | Impact |
|---|---|---|
| Nmap scan | Network 192.168.1.0/24 was vulnerable to nmap scan | Allowed attacker to survey the network for ip address and possible vulnerabilities such as open ports 80 and 22. |
| Wordpress User Enumeration | Enumerated the url 191.168.1.110/wordpress | Allowed attacker to gain user and password hash information from table in the wordpress site |
| Unprotected and Unsalted Hash | Weak hashes easily put in a wp_hashes.txt file and brute forced with John command. | Allowed access to Webdav server which grants access to modify web server |
| Privilege Escalation | Using Stevens credentials to log in the escalate to root. | Gave attackers root access |

# Exploits Used

# Exploitation: Nmap Scan

Summarize the following:

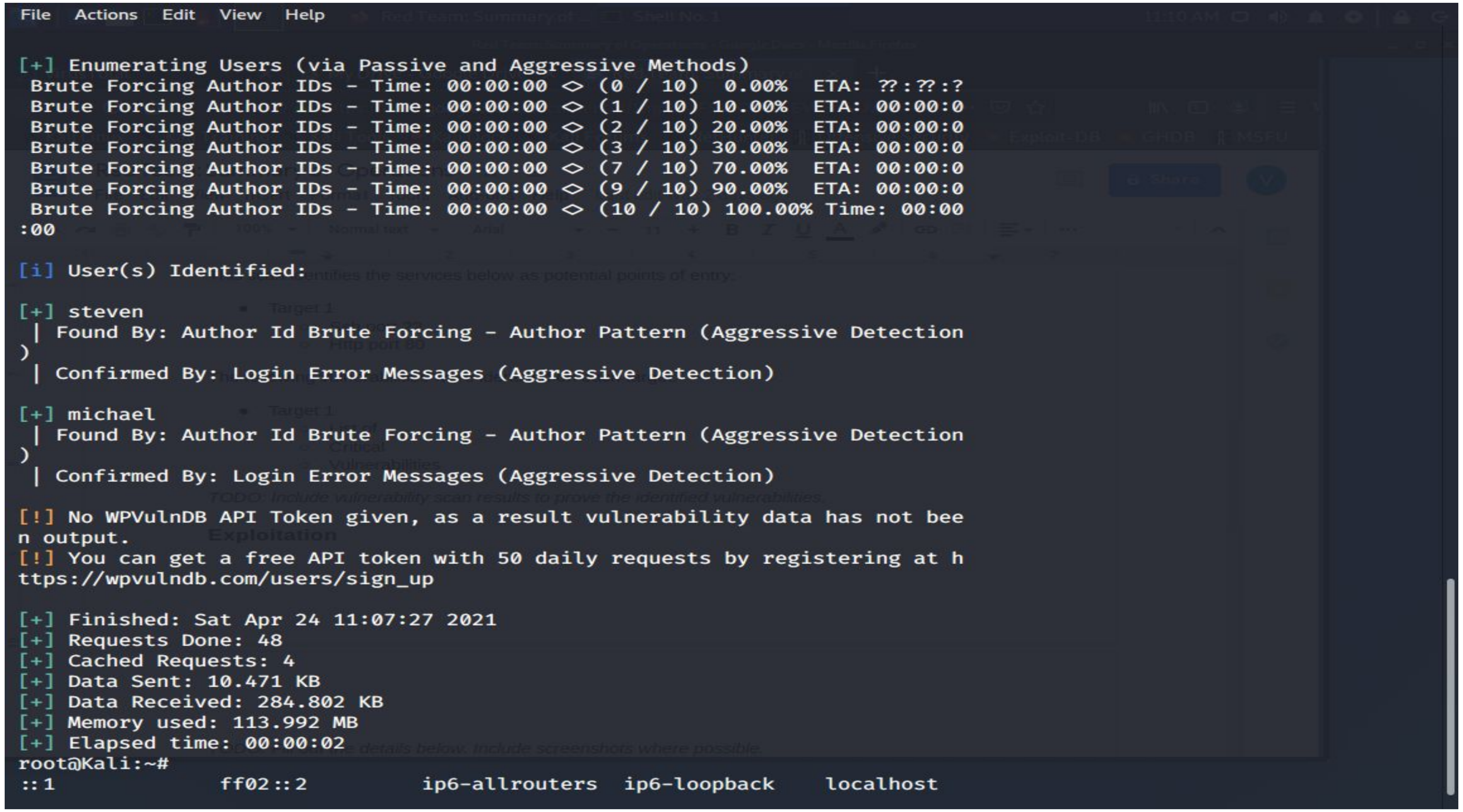
- To exploit this vulnerability we used the command : nmap -sV 192.168.1.0/24
- This exploit revealed the ip address of target one(192.168.1.110) and it’s open ports of 80 and 22

```
Nmap scan report for 192.168.1.110
Host is up (0.00093s latency).
Not shown: 995 closed ports
PORT    STATE SERVICE     VERSION
22/tcp  open  ssh         OpenSSH 6.7p1 Debian 5+deb8u4 (protocol 2.0)
80/tcp  open  http        Apache httpd 2.4.10 ((Debian))
111/tcp open  rpcbind     2-4 (RPC #100000)
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
MAC Address: 00:15:5D:00:04:10 (Microsoft)
Service Info: Host: TARGET1; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

# Exploitation: Wordpress User Enumeration

## Summarize the following:

- We exploited the vulnerability by sunnring Wpscan --url 192.168.1.110/wordpress --enumerate u
  - Allowed attacker to gain user and password hash information from table in wordpress site.

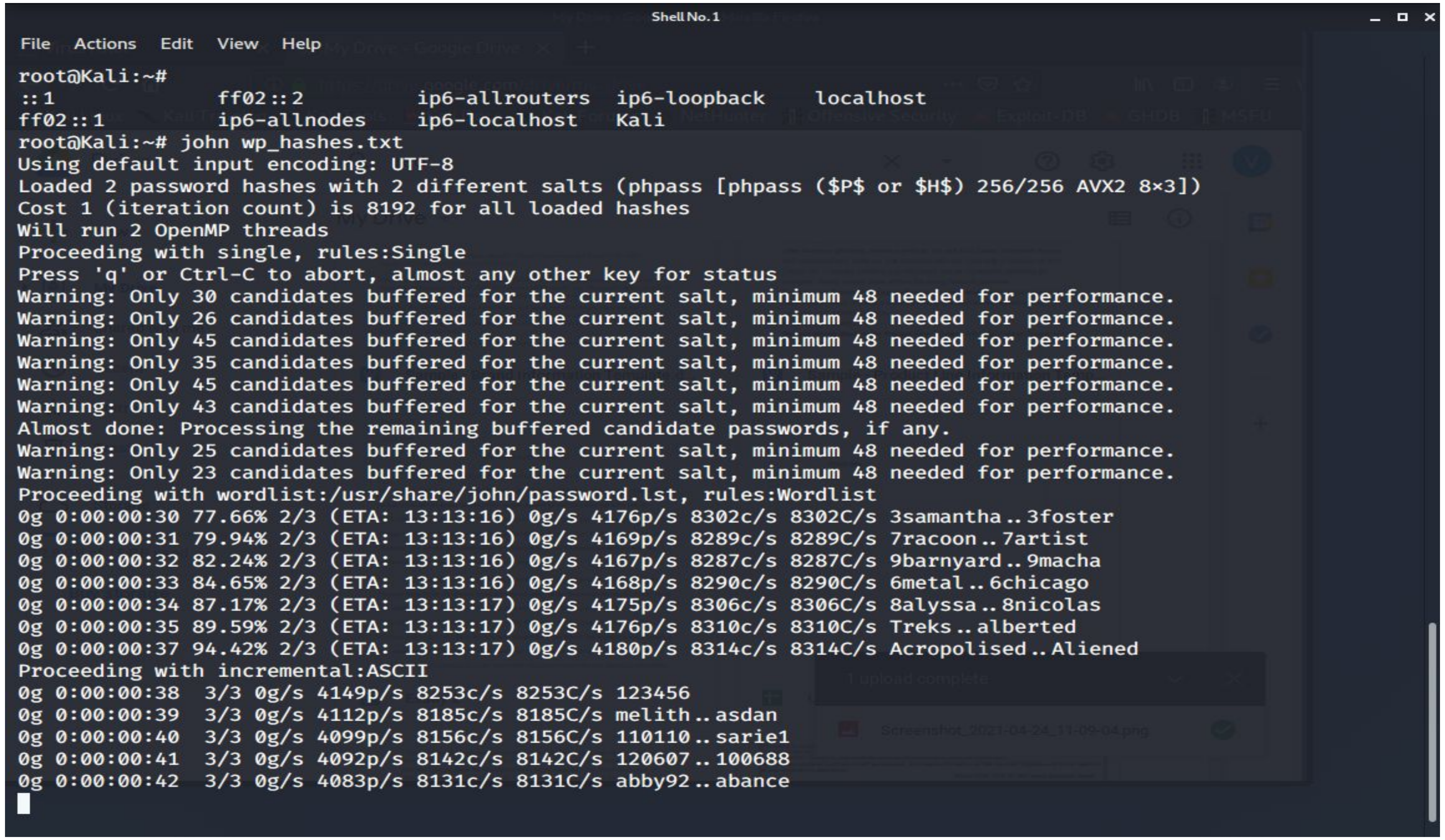


```
[+] Enumerating Users (via Passive and Aggressive Methods)
 Brute Forcing Author IDs - Time: 00:00:00 <> (0 / 10)  0.00%  ETA: ??:??:?
 Brute Forcing Author IDs - Time: 00:00:00 <> (1 / 10) 10.00%  ETA: 00:00:0
 Brute Forcing Author IDs - Time: 00:00:00 <> (2 / 10) 20.00%  ETA: 00:00:0
 Brute Forcing Author IDs - Time: 00:00:00 <> (3 / 10) 30.00%  ETA: 00:00:0
 Brute Forcing Author IDs - Time: 00:00:00 <> (7 / 10) 70.00%  ETA: 00:00:0
 Brute Forcing Author IDs - Time: 00:00:00 <> (9 / 10) 90.00%  ETA: 00:00:0
 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 bee
n output.
[!] You can get a free API token with 50 daily requests by registering at h
ttps://wpvulndb.com/users/sign_up

[+] Finished: Sat Apr 24 11:07:27 2021
[+] Requests Done: 48
[+] Cached Requests: 4
[+] Data Sent: 10.471 KB
[+] Data Received: 284.802 KB
[+] Memory used: 113.992 MB
[+] Elapsed time: 00:00:02
root@Kali:~#
::1             ff02::2          ip6-allrouters  ip6-loopback    localhost
```

# Exploitation: Weak/ Unsalted hashes

## Summarize the following:

- Through enumerating the wordpress site the users Steven and Michael along with their hashed passwords were discovered. These hashes were put into a wp_hashes.txt then cracked using the John command
- This exploit allowed the discovery of Stevens credentials. Since Steven was part of the sudoers file escalation to



```
root@Kali:~#
::1             ff02::2         ip6-allrouters  ip6-loopback    localhost
ff02::1         ip6-allnodes    ip6-localhost   Kali
root@Kali:~# john wp_hashes.txt
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (phpass [phpass ($P$ or $H$) 256/256 AVX2 8×3])
Cost 1 (iteration count) is 8192 for all loaded hashes
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 30 candidates buffered for the current salt, minimum 48 needed for performance.
Warning: Only 26 candidates buffered for the current salt, minimum 48 needed for performance.
Warning: Only 45 candidates buffered for the current salt, minimum 48 needed for performance.
Warning: Only 35 candidates buffered for the current salt, minimum 48 needed for performance.
Warning: Only 45 candidates buffered for the current salt, minimum 48 needed for performance.
Warning: Only 43 candidates buffered for the current salt, minimum 48 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Warning: Only 25 candidates buffered for the current salt, minimum 48 needed for performance.
Warning: Only 23 candidates buffered for the current salt, minimum 48 needed for performance.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
0g 0:00:00:30 77.66% 2/3 (ETA: 13:13:16) 0g/s 4176p/s 8302c/s 8302C/s 3samantha..3foster
0g 0:00:00:31 79.94% 2/3 (ETA: 13:13:16) 0g/s 4169p/s 8289c/s 8289C/s 7racoon..7artist
0g 0:00:00:32 82.24% 2/3 (ETA: 13:13:16) 0g/s 4167p/s 8287c/s 8287C/s 9barnyard..9macha
0g 0:00:00:33 84.65% 2/3 (ETA: 13:13:16) 0g/s 4168p/s 8290c/s 8290C/s 6metal..6chicago
0g 0:00:00:34 87.17% 2/3 (ETA: 13:13:17) 0g/s 4175p/s 8306c/s 8306C/s 8alyssa..8nicolas
0g 0:00:00:35 89.59% 2/3 (ETA: 13:13:17) 0g/s 4176p/s 8310c/s 8310C/s Treks..alberted
0g 0:00:00:37 94.42% 2/3 (ETA: 13:13:17) 0g/s 4180p/s 8314c/s 8314C/s Acropolised..Aliened
Proceeding with incremental:ASCII
0g 0:00:00:38  3/3 0g/s 4149p/s 8253c/s 8253C/s 123456
0g 0:00:00:39  3/3 0g/s 4112p/s 8185c/s 8185C/s melith..asdan
0g 0:00:00:40  3/3 0g/s 4099p/s 8156c/s 8156C/s 110110..sarie1
0g 0:00:00:41  3/3 0g/s 4092p/s 8142c/s 8142C/s 120607..100688
0g 0:00:00:42  3/3 0g/s 4083p/s 8131c/s 8131C/s abby92..abance
```

# Avoiding Detection

# Stealth Exploitation of Nmap Scan

**Monitoring Overview**

- **Excessive Http Request Size Monitor**
- This alert monitors the http.request.bytes
- This alert fires off when the sum of http.request.bytes reaches above 3500 bytes in the last minute.

# Stealth Exploitation of WordPress User Enumeration

**Monitoring Overview**

- Excessive Http Errors
- This alert measures http.response.status_code
- This alert fires when the number of http.response.status_code exceeds 400 in the last 5 minutes.

**Mitigating Detection**

- In order to exploit the same vulnerability we could use metasploit or gobuster. Note these will most likely trigger other alerts.

# Defensive: Critical Vulnerabilities

# Critical Vulnerabilities: Target 1

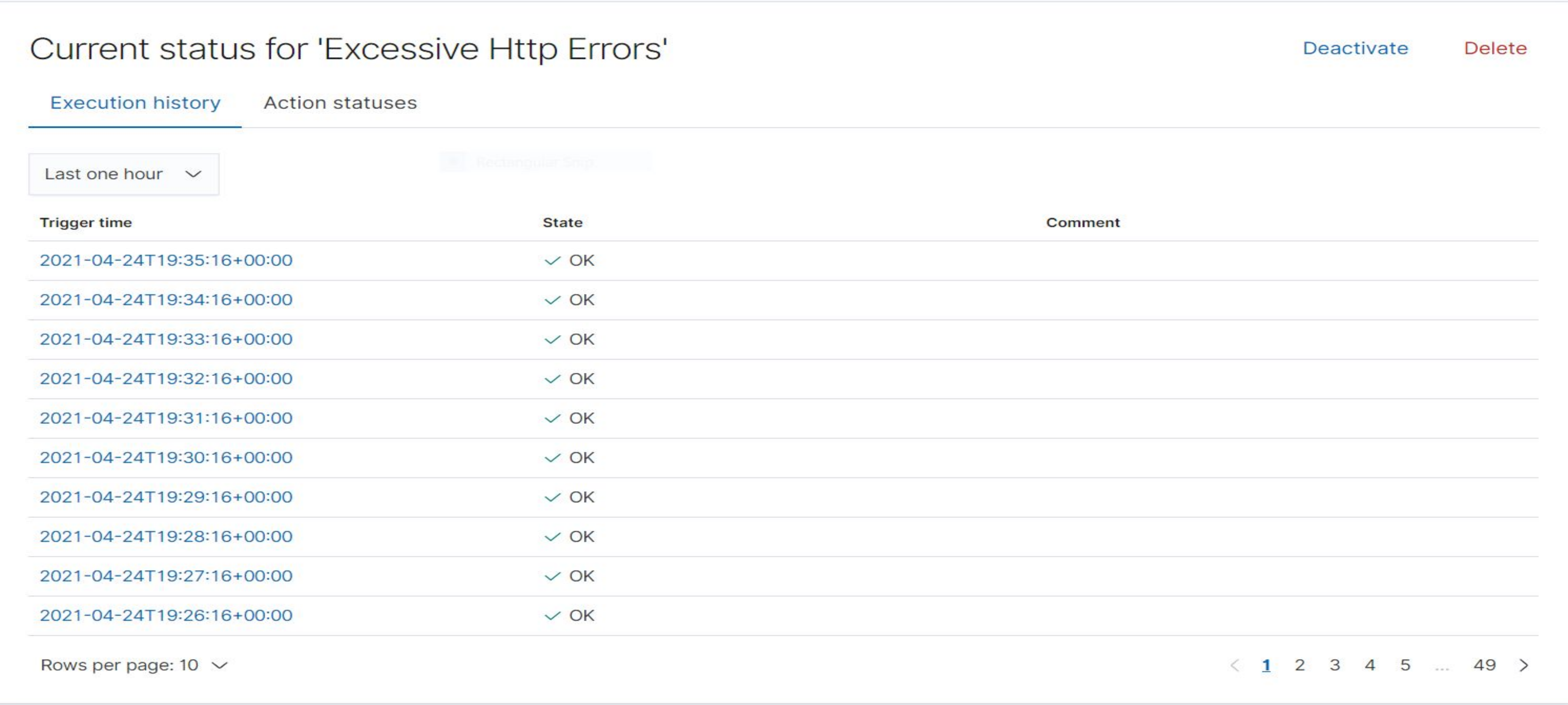
Our assessment uncovered the following critical vulnerabilities in **Target 1**.

| Vulnerability | Description | Impact |
|---|---|---|
| Nmap scan | Network 192.168.1.0/24 was vulnerable to nmap scan | Allowed attacker to survey the network for ip address and possible vulnerabilities such as open ports 80 and 22. |
| Wordpress User Enumeration | Enumerated the url 191.168.1.110/wordpress | Allowed attacker to gain user and password hash information from table in the wordpress site |
| Unprotected and Unsalted Hash | Weak hashes easily put in a wp_hashes.txt file and brute forced with John command. | Allowed access to Webdav server which grants access to modify web server |
| Privilege Escalation | Using Stevens credentials to log in the escalate to root. | Gave attackers root access |

# Alerts Implemented

# Excessive HTTP Errors

- This alert measures http.response.status_code
- This alert fires when the number of http.response.status_code exceeds 400 in the last 5 minutes.

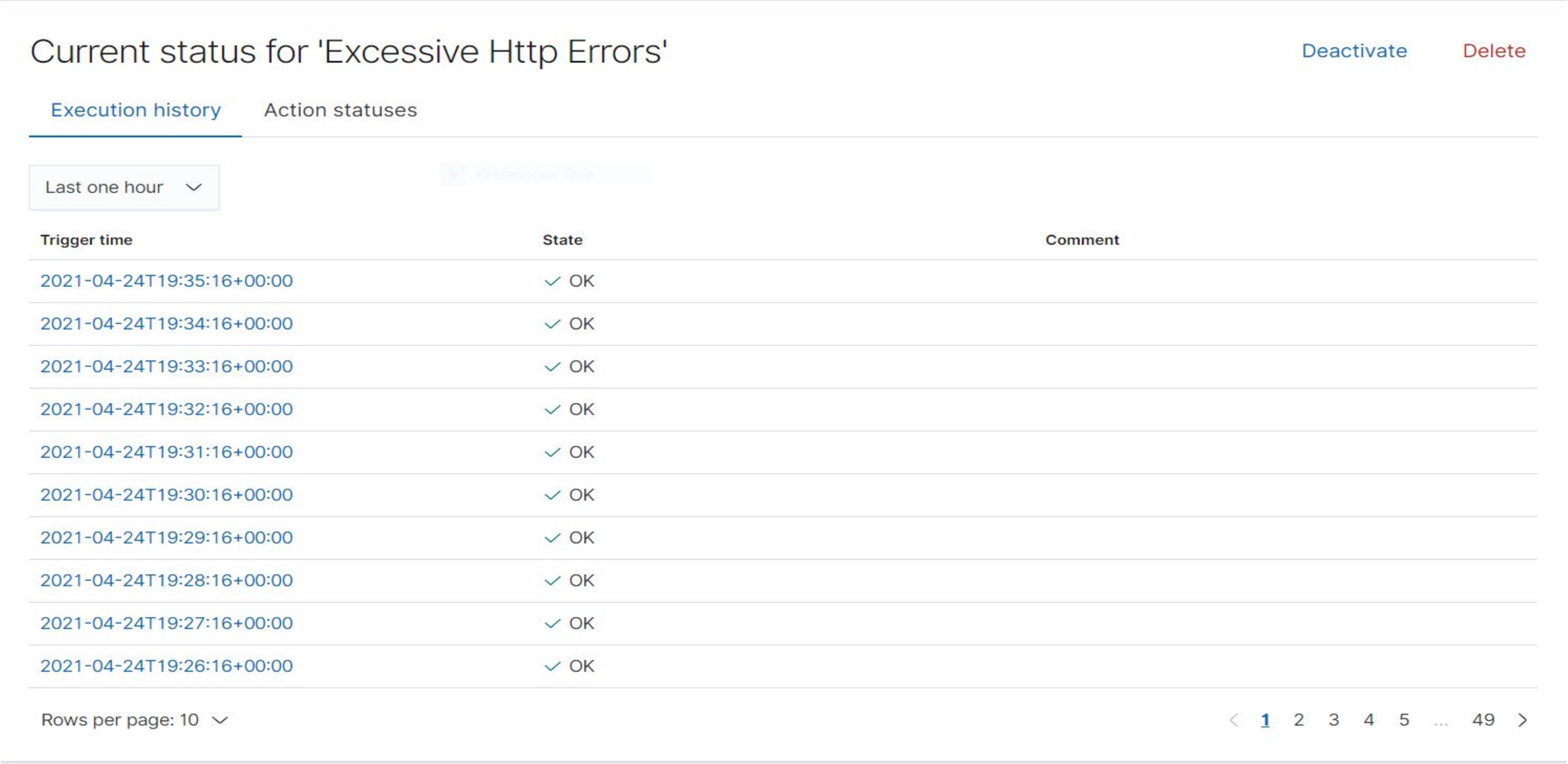


Current status for 'Excessive Http Errors'

| Trigger time | State | Comment |
|---|---|---|
| 2021-04-24T19:35:16+00:00 | ✓ OK | |
| 2021-04-24T19:34:16+00:00 | ✓ OK | |
| 2021-04-24T19:33:16+00:00 | ✓ OK | |
| 2021-04-24T19:32:16+00:00 | ✓ OK | |
| 2021-04-24T19:31:16+00:00 | ✓ OK | |
| 2021-04-24T19:30:16+00:00 | ✓ OK | |
| 2021-04-24T19:29:16+00:00 | ✓ OK | |
| 2021-04-24T19:28:16+00:00 | ✓ OK | |
| 2021-04-24T19:27:16+00:00 | ✓ OK | |
| 2021-04-24T19:26:16+00:00 | ✓ OK | |

# Excessive Http Request Size Monitor

- This alert monitors the http.request.bytes
- This alert fires off when the sum of http.request.bytes reaches above 3500 bytes in the last minute.

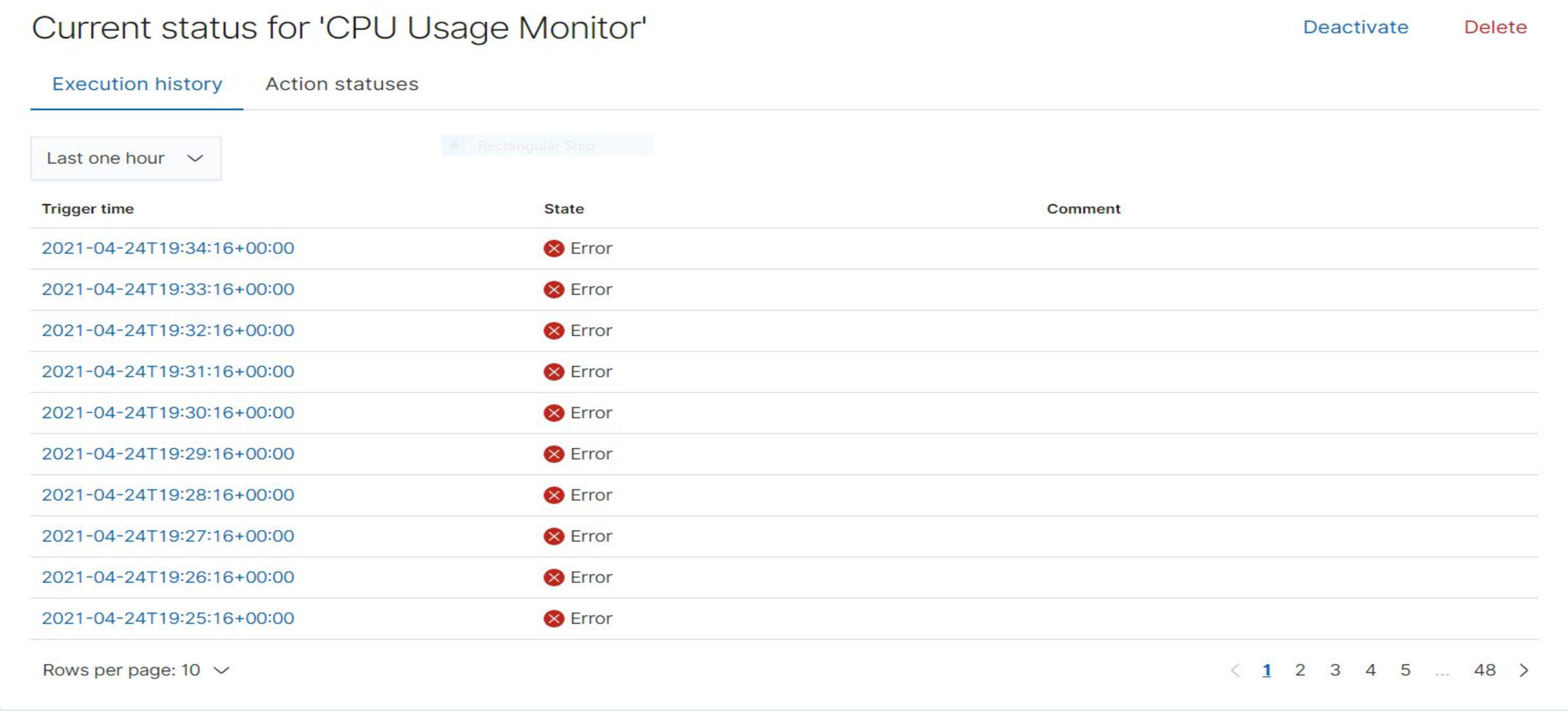


Current status for 'Excessive Http Errors'

| Trigger time | State | Comment |
|---|---|---|
| 2021-04-24T19:35:16+00:00 | ✓ OK | |
| 2021-04-24T19:34:16+00:00 | ✓ OK | |
| 2021-04-24T19:33:16+00:00 | ✓ OK | |
| 2021-04-24T19:32:16+00:00 | ✓ OK | |
| 2021-04-24T19:31:16+00:00 | ✓ OK | |
| 2021-04-24T19:30:16+00:00 | ✓ OK | |
| 2021-04-24T19:29:16+00:00 | ✓ OK | |
| 2021-04-24T19:28:16+00:00 | ✓ OK | |
| 2021-04-24T19:27:16+00:00 | ✓ OK | |
| 2021-04-24T19:26:16+00:00 | ✓ OK | |

# CPU Usage Monitor

- This alert monitors system.process.cpu.total.pkt
- This alert fires off when the max of system.process.cpu.total.pkt is above 0.5 in the last 5 minutes.



Current status for 'CPU Usage Monitor'

Last one hour

| Trigger time | State | Comment |
|---|---|---|
| 2021-04-24T19:34:16+00:00 | ⊗ Error | |
| 2021-04-24T19:33:16+00:00 | ⊗ Error | |
| 2021-04-24T19:32:16+00:00 | ⊗ Error | |
| 2021-04-24T19:31:16+00:00 | ⊗ Error | |
| 2021-04-24T19:30:16+00:00 | ⊗ Error | |
| 2021-04-24T19:29:16+00:00 | ⊗ Error | |
| 2021-04-24T19:28:16+00:00 | ⊗ Error | |
| 2021-04-24T19:27:16+00:00 | ⊗ Error | |
| 2021-04-24T19:26:16+00:00 | ⊗ Error | |
| 2021-04-24T19:25:16+00:00 | ⊗ Error | |

Rows per page: 10

# Hardening

# Hardening Against Nmap on Target 1

Explain how to patch Target 1 against Nmap Scans Include:

- To protect the network from nmap scans a “default-deny” rule on the firewall would have to be implemented. This will block all outside traffic thus inhibiting the Nmap scan. From here we can pick and choose which ports to open and from where we will accept traffic.

- sudo ufw default deny incoming
- sudo ufw default deny outgoing

# Hardening Against Wordpress Enumeration  on Target 1

## Explain how to patch Target 1 against  WordPress Enumeration:

- By adding this to the functions.php file we can set up our wordpress to check any request made to the author archive. If this request contains an integer for enumeration then the request will be blocked.

```
// block WP enum scans
// https://m0n.co/enum
if (!is_admin()) {
    // default URL format
    if (preg_match('/author=([0-9]*)/i', $_SERVER['QUERY_STRING'])) die();
    add_filter('redirect_canonical', 'shapeSpace_check_enum', 10, 2);
}
function shapeSpace_check_enum($redirect, $request) {
    // permalink URL format
    if (preg_match('/\?author=([0-9]*)(\/*)/i', $request)) die();
    else return $redirect;
}
```

- The plug-in WP Hardening by Astra Security can also be implemented. It is a tool which performs a real-time security audit of your website to find missing security best practices WordPress Version Check, Checking Outdated Plugins, Checking PHP Version, Checking File & Folder Permissions, Database Password Strength, and Checking Firewall Protection

# Hardening Against Unprotected and Unsalted Hashes on Target 1

Explain how to patch Target 1 against Unprotected and Unsalted Hashes. Include:

- To harden passwords the password requirements can be more strict such as requiring upper and lowercase numbers, numbers, characters, length, etc. Websites like https://www.symbionts.de/tools/hash/sha256-hash-salt-generator.html may also be used to generate salted passwords

# 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, TCP | Three most common protocols on the network. |
| # of Unique IP Addresses | 808 | Count of observed IP addresses. |
| Subnets | 172.16.4.0/24<br>10.6.12.0/24 | 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

- Use of websites going through the Wordpress site
- Watching youtube
- Use of APIs for basic browser interactions

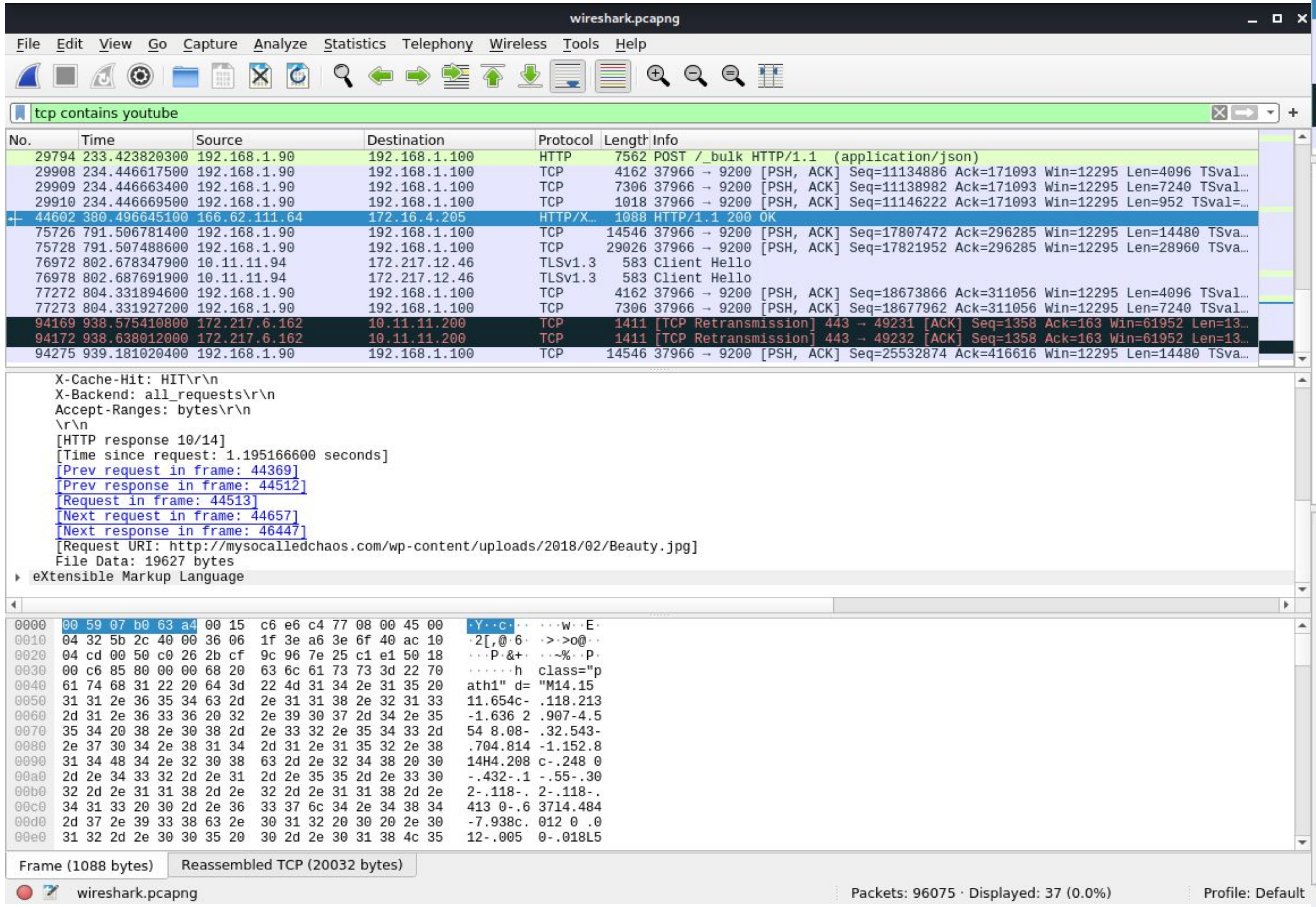
### Suspicious Activity

- files.publicdomaintorrents.com used to download “Betty_Boop_Rhythm_on_the_Reservation.avi.torrent”
- http://205.185.125.104/files/june11.dll

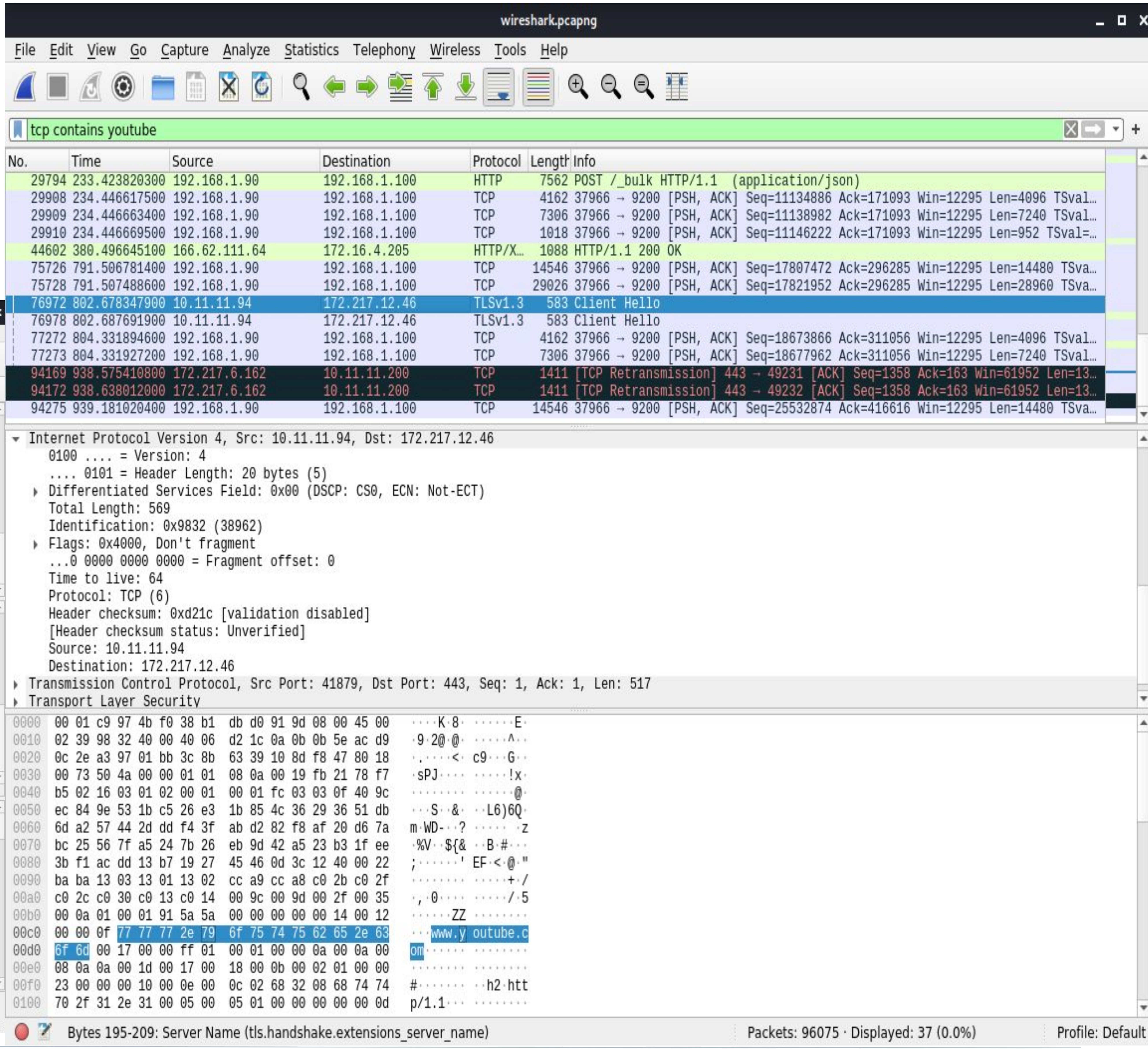
# Normal Activity

# Use of Wordpress Site

- Protocols: HTTP, TCP traffic
- The users were browsing youtube and mysocalledchaos.com


wireshark.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

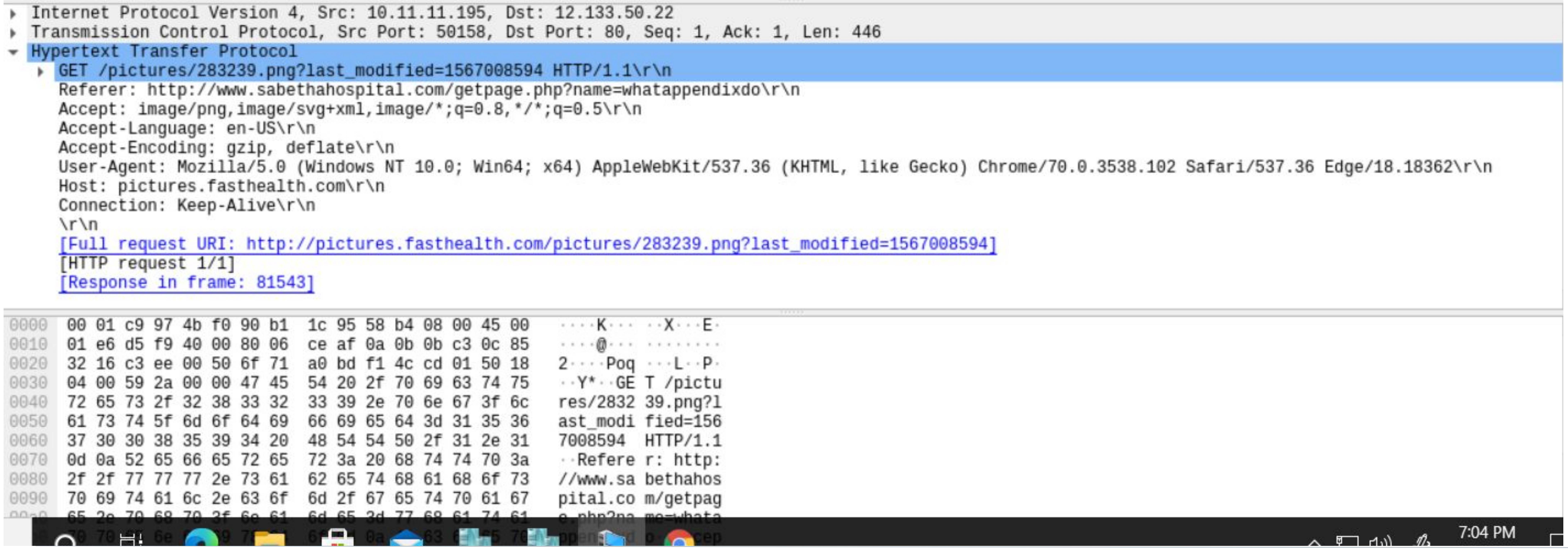
```
tcp contains youtube

No.   Time          Source          Destination     Protocol Length Info
29794 233.423820300 192.168.1.90    192.168.1.100   HTTP     7562 POST /_bulk HTTP/1.1  (application/json)
29908 234.446617500 192.168.1.90    192.168.1.100   TCP      4162 37966 → 9200 [PSH, ACK] Seq=11134886 Ack=171093 Win=12295 Len=4096 TSval…
29909 234.446663400 192.168.1.90    192.168.1.100   TCP      7306 37966 → 9200 [PSH, ACK] Seq=11138982 Ack=171093 Win=12295 Len=7240 TSval…
29910 234.446669500 192.168.1.90    192.168.1.100   TCP      1018 37966 → 9200 [PSH, ACK] Seq=11146222 Ack=171093 Win=12295 Len=952 TSval=…
44602 380.496645100 166.62.111.64   172.16.4.205    HTTP/X…  1088 HTTP/1.1 200 OK
75726 791.506781400 192.168.1.90    192.168.1.100   TCP     14546 37966 → 9200 [PSH, ACK] Seq=17807472 Ack=296285 Win=12295 Len=14480 TSva…
75728 791.507488600 192.168.1.90    192.168.1.100   TCP     29026 37966 → 9200 [PSH, ACK] Seq=17821952 Ack=296285 Win=12295 Len=28960 TSva…
76972 802.678347900 10.11.11.94     172.217.12.46   TLSv1.3   583 Client Hello
76978 802.687691900 10.11.11.94     172.217.12.46   TLSv1.3   583 Client Hello
77272 804.331894600 192.168.1.90    192.168.1.100   TCP      4162 37966 → 9200 [PSH, ACK] Seq=18673866 Ack=311056 Win=12295 Len=4096 TSval…
77273 804.331927200 192.168.1.90    192.168.1.100   TCP      7306 37966 → 9200 [PSH, ACK] Seq=18677962 Ack=311056 Win=12295 Len=7240 TSval…
94169 938.575410800 172.217.6.162   10.11.11.200    TCP      1411 [TCP Retransmission] 443 → 49231 [ACK] Seq=1358 Ack=163 Win=61952 Len=13…
94172 938.638012000 172.217.6.162   10.11.11.200    TCP      1411 [TCP Retransmission] 443 → 49232 [ACK] Seq=1358 Ack=163 Win=61952 Len=13…
94275 939.181020400 192.168.1.90    192.168.1.100   TCP     14546 37966 → 9200 [PSH, ACK] Seq=25532874 Ack=416616 Win=12295 Len=14480 TSva…

    X-Cache-Hit: HIT\r\n
    X-Backend: all_requests\r\n
    Accept-Ranges: bytes\r\n
    \r\n
    [HTTP response 10/14]
    [Time since request: 1.195166600 seconds]
    [Prev request in frame: 44369]
    [Prev response in frame: 44512]
    [Request in frame: 44513]
    [Next request in frame: 44657]
    [Next response in frame: 46447]
    [Request URI: http://mysocalledchaos.com/wp-content/uploads/2018/02/Beauty.jpg]
    File Data: 19627 bytes
  eXtensible Markup Language

0000  00 59 07 b0 63 a4 00 15  c6 e6 c4 77 08 00 45 00   ·Y··c··· ···w··E·
0010  04 32 5b 2c 40 00 36 06  1f 3e a6 3e 6f 40 ac 10   ·2[,@·6· ·>·>o@··
0020  04 cd 00 50 c0 26 2b cf  9c 96 7e 25 c1 e1 50 18   ···P·&+· ··~%··P·
0030  00 c6 85 80 00 00 68 20  63 6c 61 73 73 3d 22 70   ······h  class="p
0040  61 74 68 31 22 20 64 3d  22 4d 31 34 2e 31 35 20   ath1" d= "M14.15 
0050  31 31 2e 36 35 34 63 2d  2e 31 31 38 2e 32 31 33   11.654c- .118.213
0060  2d 31 2e 36 33 36 20 32  2e 39 30 37 2d 34 2e 35   -1.636 2 .907-4.5
0070  35 34 20 38 2e 30 38 2d  2e 33 32 2e 35 34 33 2d   54 8.08- .32.543-
0080  2e 37 30 34 2e 38 31 34  2d 31 2e 31 35 32 2e 38   .704.814 -1.152.8
0090  31 34 48 34 2e 32 30 38  63 2d 2e 32 34 38 20 30   14H4.208 c-.248 0
00a0  2d 2e 34 33 32 2d 2e 31  2d 2e 35 35 2d 2e 33 30   -.432-.1 -.55-.30
00b0  32 2d 2e 31 31 38 2d 2e  32 2d 2e 31 31 38 2d 2e   2-.118-. 2-.118-.
00c0  34 31 33 20 30 2d 2e 36  33 37 6c 34 2e 34 38 34   413 0-.6 37l4.484
00d0  2d 37 2e 39 33 38 63 2e  30 31 32 20 30 20 2e 30   -7.938c. 012 0 .0
00e0  31 32 2d 2e 30 30 35 20  30 2d 2e 30 31 38 4c 35   12-.005  0-.018L5

Frame (1088 bytes)   Reassembled TCP (20032 bytes)
wireshark.pcapng        Packets: 96075 · Displayed: 37 (0.0%)        Profile: Default
```


wireshark.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
tcp contains youtube

No.   Time          Source          Destination     Protocol Length Info
29794 233.423820300 192.168.1.90    192.168.1.100   HTTP     7562 POST /_bulk HTTP/1.1  (application/json)
29908 234.446617500 192.168.1.90    192.168.1.100   TCP      4162 37966 → 9200 [PSH, ACK] Seq=11134886 Ack=171093 Win=12295 Len=4096 TSval…
29909 234.446663400 192.168.1.90    192.168.1.100   TCP      7306 37966 → 9200 [PSH, ACK] Seq=11138982 Ack=171093 Win=12295 Len=7240 TSval…
29910 234.446669500 192.168.1.90    192.168.1.100   TCP      1018 37966 → 9200 [PSH, ACK] Seq=11146222 Ack=171093 Win=12295 Len=952 TSval=…
44602 380.496645100 166.62.111.64   172.16.4.205    HTTP/X…  1088 HTTP/1.1 200 OK
75726 791.506781400 192.168.1.90    192.168.1.100   TCP     14546 37966 → 9200 [PSH, ACK] Seq=17807472 Ack=296285 Win=12295 Len=14480 TSva…
75728 791.507488600 192.168.1.90    192.168.1.100   TCP     29026 37966 → 9200 [PSH, ACK] Seq=17821952 Ack=296285 Win=12295 Len=28960 TSva…
76972 802.678347900 10.11.11.94     172.217.12.46   TLSv1.3   583 Client Hello
76978 802.687691900 10.11.11.94     172.217.12.46   TLSv1.3   583 Client Hello
77272 804.331894600 192.168.1.90    192.168.1.100   TCP      4162 37966 → 9200 [PSH, ACK] Seq=18673866 Ack=311056 Win=12295 Len=4096 TSval…
77273 804.331927200 192.168.1.90    192.168.1.100   TCP      7306 37966 → 9200 [PSH, ACK] Seq=18677962 Ack=311056 Win=12295 Len=7240 TSval…
94169 938.575410800 172.217.6.162   10.11.11.200    TCP      1411 [TCP Retransmission] 443 → 49231 [ACK] Seq=1358 Ack=163 Win=61952 Len=13…
94172 938.638012000 172.217.6.162   10.11.11.200    TCP      1411 [TCP Retransmission] 443 → 49232 [ACK] Seq=1358 Ack=163 Win=61952 Len=13…
94275 939.181020400 192.168.1.90    192.168.1.100   TCP     14546 37966 → 9200 [PSH, ACK] Seq=25532874 Ack=416616 Win=12295 Len=14480 TSva…

▾ Internet Protocol Version 4, Src: 10.11.11.94, Dst: 172.217.12.46
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 569
    Identification: 0x9832 (38962)
  ▸ Flags: 0x4000, Don't fragment
    ...0 0000 0000 0000 = Fragment offset: 0
    Time to live: 64
    Protocol: TCP (6)
    Header checksum: 0xd21c [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.11.11.94
    Destination: 172.217.12.46
▸ Transmission Control Protocol, Src Port: 41879, Dst Port: 443, Seq: 1, Ack: 1, Len: 517
▸ Transport Layer Security

0000  00 01 c9 97 4b f0 38 b1  db d0 91 9d 08 00 45 00   ····K·8· ······E·
0010  02 39 98 32 40 00 40 06  d2 1c 0a 0b 0b 5e ac d9   ·9·2@·@· ·····^··
0020  0c 2e a3 97 01 bb 3c 8b  63 39 10 8d f8 47 80 18   ·.····<· c9···G··
0030  00 73 50 4a 00 00 01 01  08 0a 00 19 fb 21 78 f7   ·sPJ···· ·····!x·
0040  b5 02 16 03 01 02 00 01  00 01 fc 03 03 0f 40 9c   ········ ······@·
0050  ec 84 9e 53 1b c5 26 e3  1b 85 4c 36 29 36 51 db   ···S··&· ··L6)6Q·
0060  6d a2 57 44 2d dd f4 3f  ab d2 82 f8 af 20 d6 7a   m·WD-··? ····· ·z
0070  bc 25 56 7f a5 24 7b 26  eb 9d 42 a5 23 b3 1f ee   ·%V··${& ··B·#···
0080  3b f1 ac dd 13 b7 19 27  45 46 0d 3c 12 40 00 22   ;······' EF·<·@·"
0090  ba ba 13 03 13 01 13 02  cc a9 cc a8 c0 2b c0 2f   ········ ·····+·/
00a0  c0 2c c0 30 c0 13 c0 14  00 9c 00 9d 00 2f 00 35   ·,·0···· ·····/·5
00b0  00 0a 01 00 01 91 5a 5a  00 00 00 00 00 14 00 12   ······ZZ ········
00c0  00 00 0f 77 77 77 2e 79  6f 75 74 75 62 65 2e 63   ···www.y outube.c
00d0  6f 6d 00 17 00 00 ff 01  00 01 00 00 0a 00 0a 00   om······ ········
00e0  08 0a 0a 00 1d 00 17 00  18 00 0b 00 02 01 00 00   ········ ········
00f0  23 00 00 00 10 00 0e 00  0c 02 68 32 08 68 74 74   #······· ··h2·htt
0100  70 2f 31 2e 31 00 05 00  05 01 00 00 00 00 00 0d   p/1.1··· ········

Bytes 195-209: Server Name (tls.handshake.extensions_server_name)    Packets: 96075 · Displayed: 37 (0.0%)    Profile: Default
```

# Standard HTTP Traffic

- Protocols: TCP and HTTP
- Users were browsing http://www.sabethahospital.com and http://www.iphonehacks.com
- Interesting files: jquery-migrate.min.js



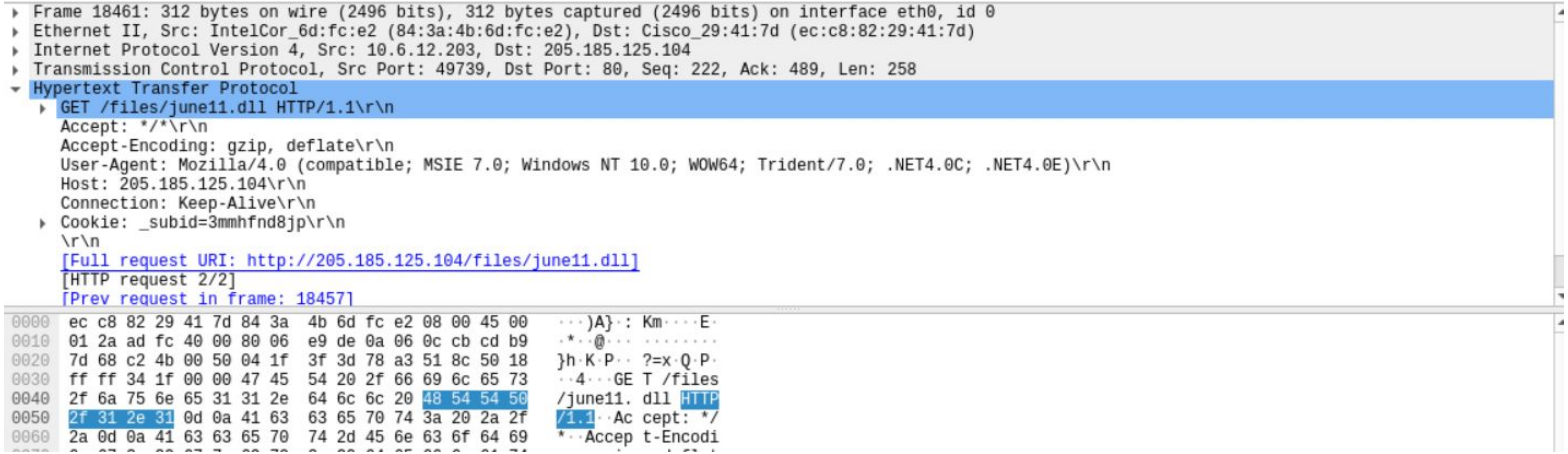
```
▸ Internet Protocol Version 4, Src: 10.11.11.195, Dst: 12.133.50.22
▸ Transmission Control Protocol, Src Port: 50158, Dst Port: 80, Seq: 1, Ack: 1, Len: 446
▾ Hypertext Transfer Protocol
  ▸ GET /pictures/283239.png?last_modified=1567008594 HTTP/1.1\r\n
    Referer: http://www.sabethahospital.com/getpage.php?name=whatappendixdo\r\n
    Accept: image/png,image/svg+xml,image/*;q=0.8,*/*;q=0.5\r\n
    Accept-Language: en-US\r\n
    Accept-Encoding: gzip, deflate\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.102 Safari/537.36 Edge/18.18362\r\n
    Host: pictures.fasthealth.com\r\n
    Connection: Keep-Alive\r\n
    \r\n
    [Full request URI: http://pictures.fasthealth.com/pictures/283239.png?last_modified=1567008594]
    [HTTP request 1/1]
    [Response in frame: 81543]
```

```
0000  00 01 c9 97 4b f0 90 b1  1c 95 58 b4 08 00 45 00   ····K··· ··X···E·
0010  01 e6 d5 f9 40 00 80 06  ce af 0a 0b 0b c3 0c 85   ····@··· ········
0020  32 16 c3 ee 00 50 6f 71  a0 bd f1 4c cd 01 50 18   2····Poq ···L··P·
0030  04 00 59 2a 00 00 47 45  54 20 2f 70 69 63 74 75   ··Y*··GE T /pictu
0040  72 65 73 2f 32 38 33 32  33 39 2e 70 6e 67 3f 6c   res/2832 39.png?l
0050  61 73 74 5f 6d 6f 64 69  66 69 65 64 3d 31 35 36   ast_modi fied=156
0060  37 30 30 38 35 39 34 20  48 54 54 50 2f 31 2e 31   7008594  HTTP/1.1
0070  0d 0a 52 65 66 65 72 65  72 3a 20 68 74 74 70 3a   ··Refere r: http:
0080  2f 2f 77 77 77 2e 73 61  62 65 74 68 61 68 6f 73   //www.sa bethahos
0090  70 69 74 61 6c 2e 63 6f  6d 2f 67 65 74 70 61 67   pital.co m/getpag
00a0  65 2e 70 68 70 3f 6e 61  6d 65 3d 77 68 61 74 61   e.php?na me=whata
```

# Malicious Activity

# Illegal Download

- Protocol: HTTP, TCP
- User downloaded a Trojan from [http://205.185.125.104/files/june11.dll](http://205.185.125.104/files/june11.dll) to machine 10.6.12.203
- Interesting File: Trojan junn11.dll

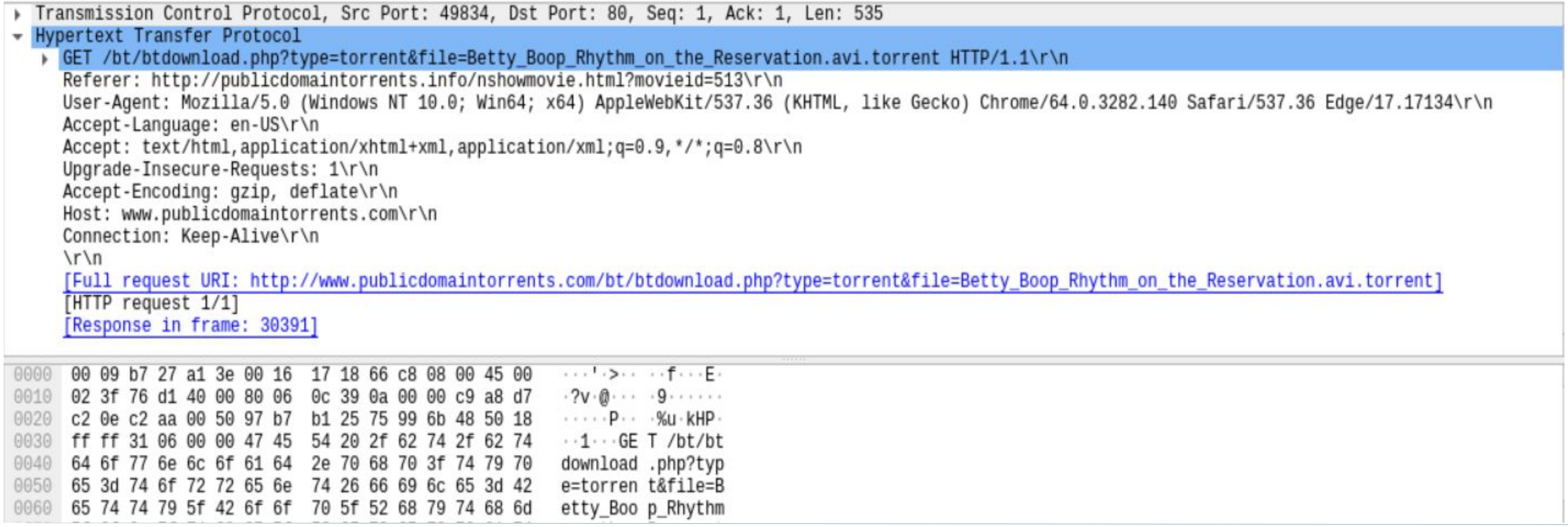


```
▸ Frame 18461: 312 bytes on wire (2496 bits), 312 bytes captured (2496 bits) on interface eth0, id 0
▸ Ethernet II, Src: IntelCor_6d:fc:e2 (84:3a:4b:6d:fc:e2), Dst: Cisco_29:41:7d (ec:c8:82:29:41:7d)
▸ Internet Protocol Version 4, Src: 10.6.12.203, Dst: 205.185.125.104
▸ Transmission Control Protocol, Src Port: 49739, Dst Port: 80, Seq: 222, Ack: 489, Len: 258
▾ Hypertext Transfer Protocol
  ▸ GET /files/june11.dll HTTP/1.1\r\n
    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: 18457]
```

```
0000  ec c8 82 29 41 7d 84 3a  4b 6d fc e2 08 00 45 00   ···)A}·: Km····E·
0010  01 2a ad fc 40 00 80 06  e9 de 0a 06 0c cb cd b9   ·*··@··· ········
0020  7d 68 c2 4b 00 50 04 1f  3f 3d 78 a3 51 8c 50 18   }h·K·P·· ?=x·Q·P·
0030  ff ff 34 1f 00 00 47 45  54 20 2f 66 69 6c 65 73   ··4···GE T /files
0040  2f 6a 75 6e 65 31 31 2e  64 6c 6c 20 48 54 54 50   /june11. dll HTTP
0050  2f 31 2e 31 0d 0a 41 63  63 65 70 74 3a 20 2a 2f   /1.1··Ac cept: */
0060  2a 0d 0a 41 63 63 65 70  74 2d 45 6e 63 6f 64 69   *··Accep t-Encodi
```

# Illegal Download

- Protocol: HTTP, TCP
- User was browsing publicdomaintorrents.com and downloaded torrent Betty_Boop_Rhythm_on_the_Reservation.avi.torrent.
- Interesting File: Torrent Betty_Boop_Rhythm_on_the_Reservation.avi.torrent



```
▸ 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/nshowmovie.html?movieid=513\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: 30391]

0000  00 09 b7 27 a1 3e 00 16  17 18 66 c8 08 00 45 00   ···'·>·· ··f···E·
0010  02 3f 76 d1 40 00 80 06  0c 39 0a 00 00 c9 a8 d7   ·?v·@··· ·9······
0020  c2 0e c2 aa 00 50 97 b7  b1 25 75 99 6b 48 50 18   ·····P·· ·%u·kHP·
0030  ff ff 31 06 00 00 47 45  54 20 2f 62 74 2f 62 74   ··1···GE T /bt/bt
0040  64 6f 77 6e 6c 6f 61 64  2e 70 68 70 3f 74 79 70   download .php?typ
0050  65 3d 74 6f 72 72 65 6e  74 26 66 69 6c 65 3d 42   e=torren t&file=B
0060  65 74 74 79 5f 42 6f 6f  70 5f 52 68 79 74 68 6d   etty_Boo p_Rhythm
```

# The End