Final Engagement

Attack, Defense & Analysis of a Vulnerable Network

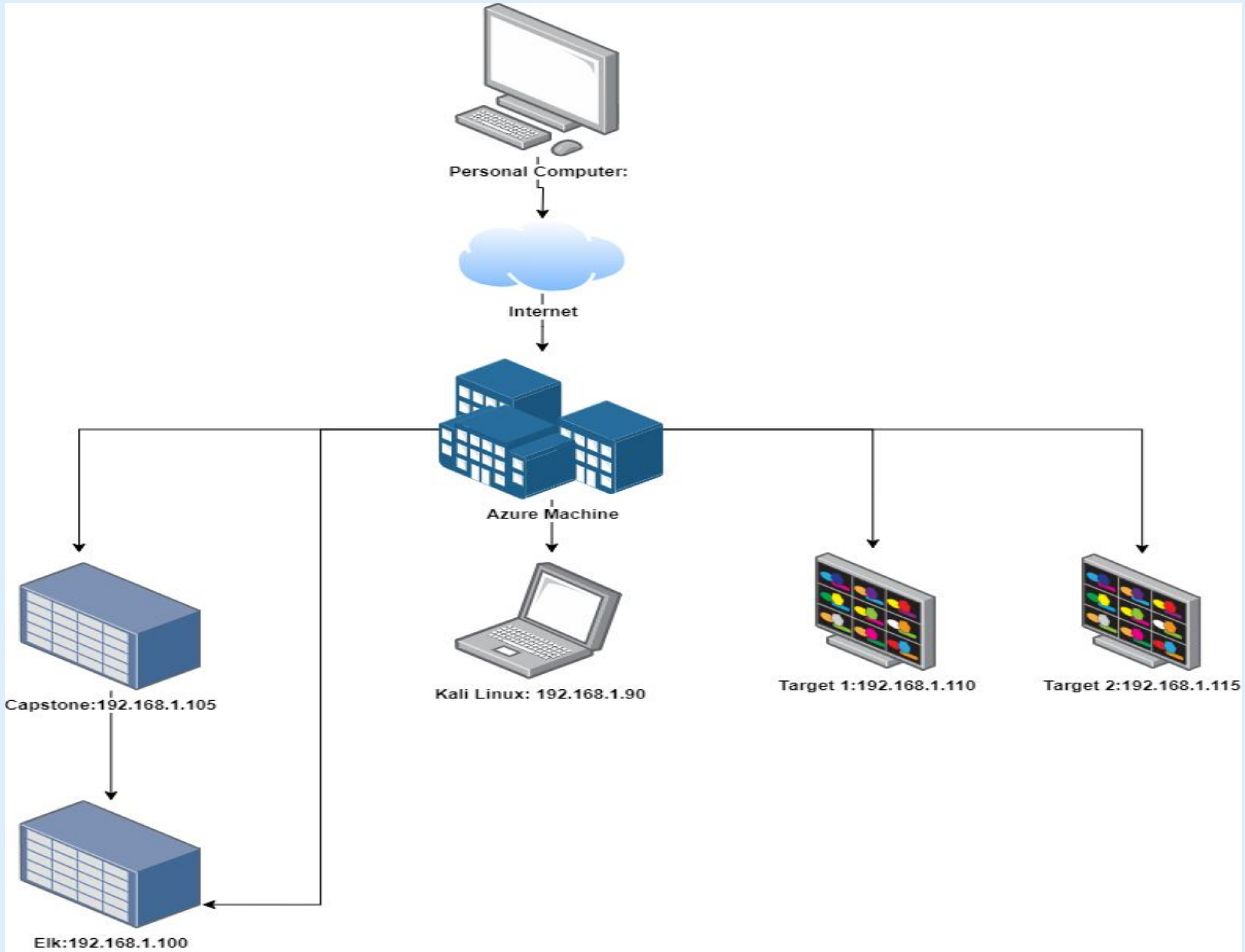
Table of Contents

This document contains the following resources:

- **Network Topology & Critical Vulnerabilities**
- **Alerts Implemented**
- **Hardening**
- **Implementing Patches**

Network Topology
& Critical Vulnerabilities

Network Topology



Network
Address
Range:192.168.0.0-192.168.255.255
Netmask: 255.255.255.0
Gateway: 192.168.1.1

Machines
IPv4:192.168.1.90
OS: Kali GNU
Hostname:Kali Linux

IPv4:192.168.1.100
OS: Linux
Hostname:ELK

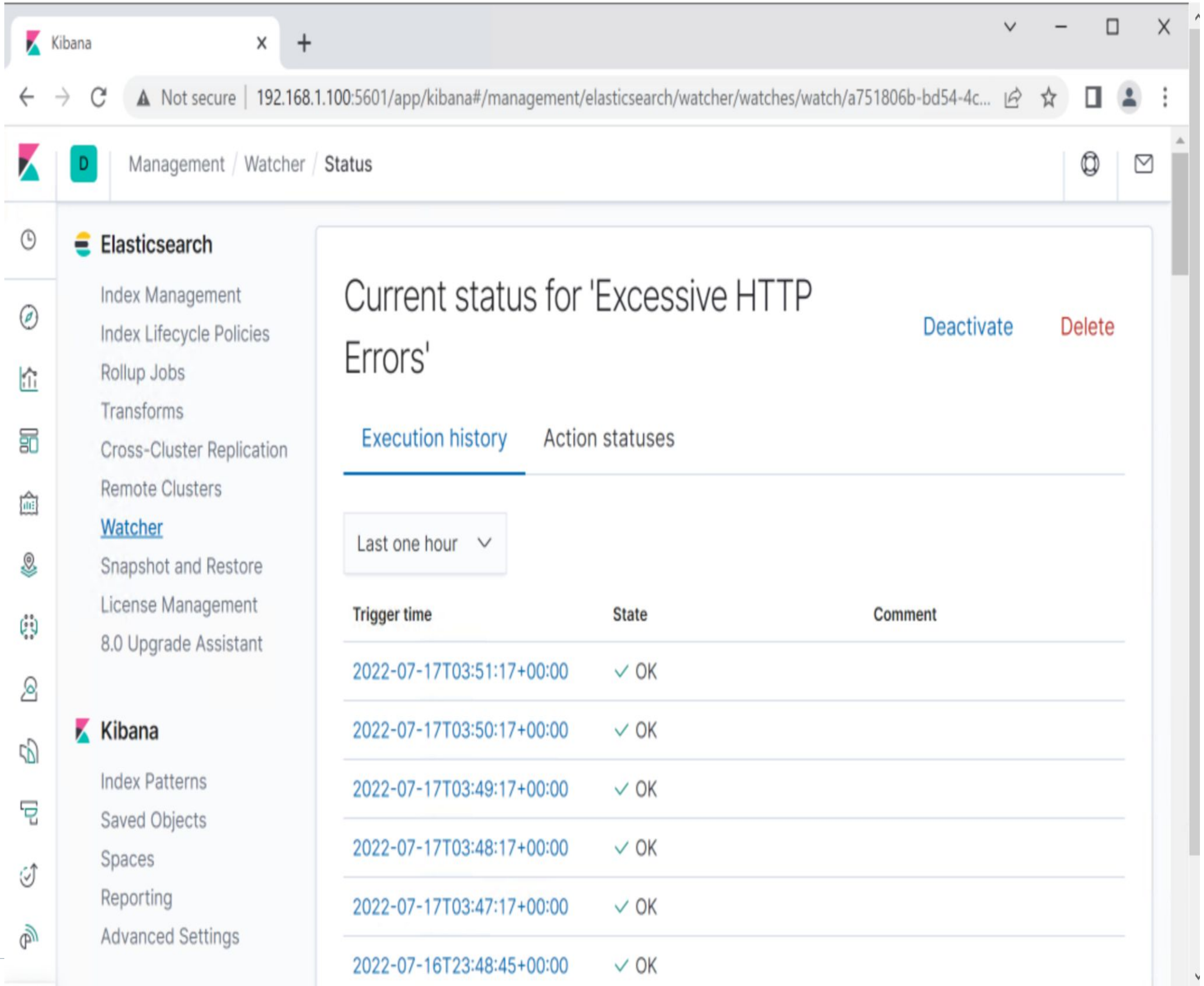
IPv4: 192.168.1.105
OS: Linux
Hostname: Capstone

IPv4:192.1.168.110
OS: Linux
Hostname: Target 1

Alerts Implemented

[Excessive HTTP Errors]

- **Metric:** WHEN count() GROUPED OVER top 5 'http.response.status_code' IS ABOVE 400 FOR THE LAST 5 minutes
- **Threshold**: ABOVE 400 FOR THE LAST 5 minutes

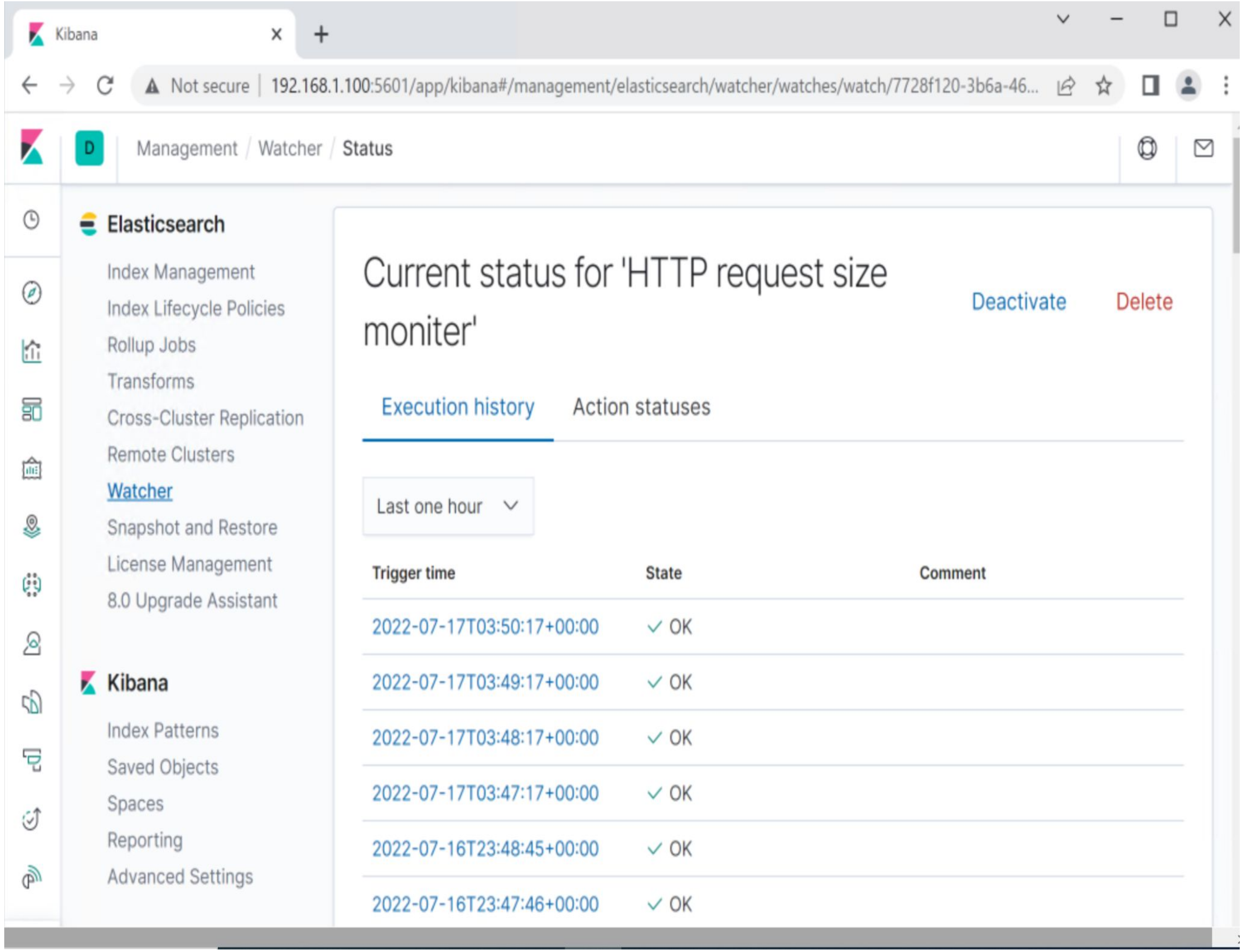


Current status for 'Excessive HTTP Errors'

Trigger time	State	Comment
2022-07-17T03:51:17+00:00	✓ OK	
2022-07-17T03:50:17+00:00	✓ OK	
2022-07-17T03:49:17+00:00	✓ OK	
2022-07-17T03:48:17+00:00	✓ OK	
2022-07-17T03:47:17+00:00	✓ OK	
2022-07-16T23:48:45+00:00	✓ OK	

[HTTP Request Size Monitor]

- **Metric**: WHEN sum() of http.request.bytes OVER all documents IS ABOVE 3500 FOR THE LAST 1 minute
- **Threshold**: ABOVE 3500 FOR THE LAST 1 minute



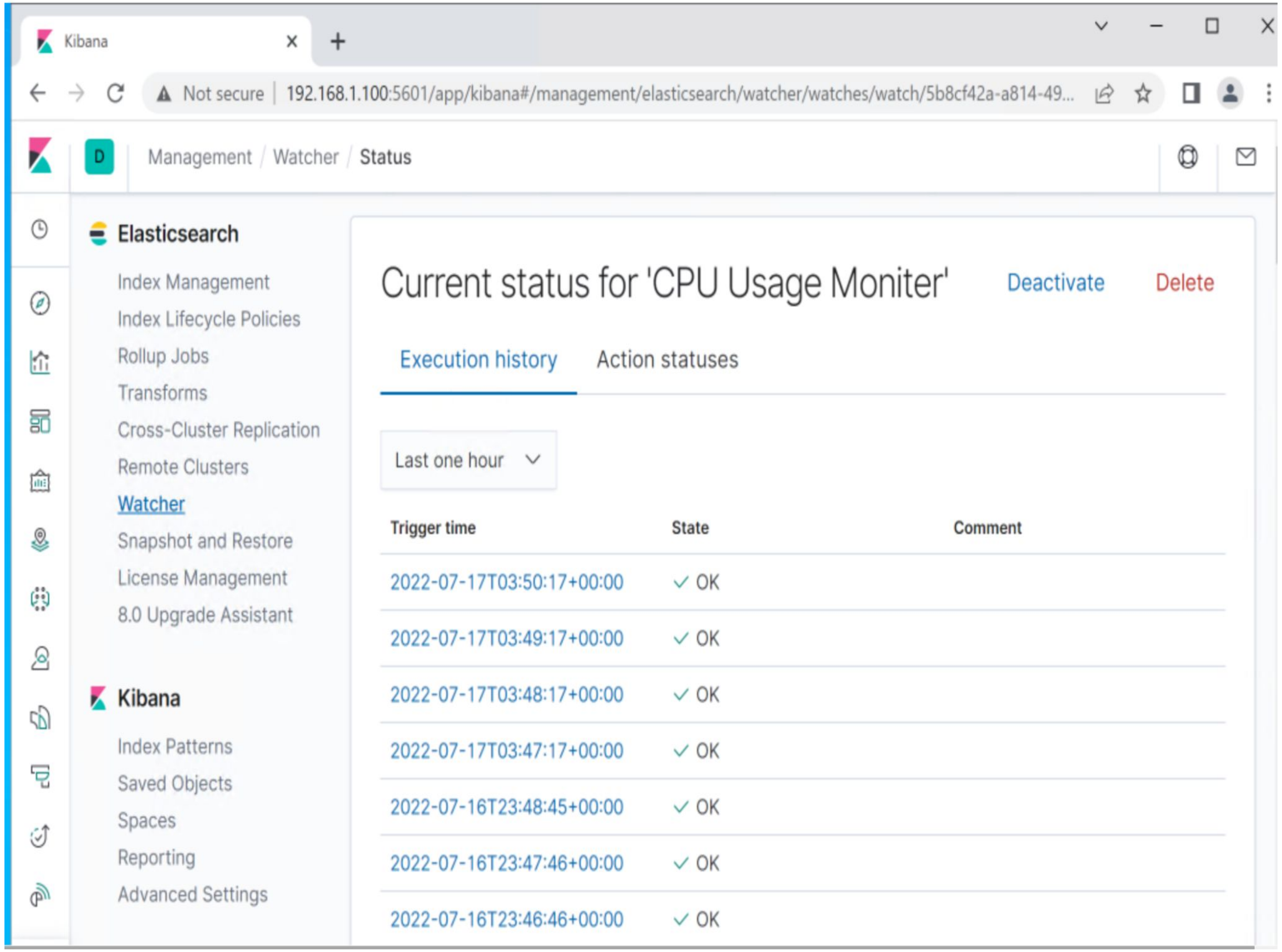
Current status for 'HTTP request size moniter'

Trigger time	State	Comment
2022-07-17T03:50:17+00:00	✓ OK	
2022-07-17T03:49:17+00:00	✓ OK	
2022-07-17T03:48:17+00:00	✓ OK	
2022-07-17T03:47:17+00:00	✓ OK	
2022-07-16T23:48:45+00:00	✓ OK	
2022-07-16T23:47:46+00:00	✓ OK	

[CPU Usage Monitor]

- **Metric:** WHEN max() OF system.process.cpu.total .pct OVER all documents IS ABOVE 0.5 FOR THE LAST 5 minutes
- **Threshold:** ABOVE 0.5 FOR THE LAST 5 minutes

.



192.168.1.100:5601/app/kibana#/management/elasticsearch/watcher/watches/watch/5b8cf42a-a814-49...

Current status for 'CPU Usage Moniter'

Trigger time	State	Comment
2022-07-17T03:50:17+00:00	✓ OK	
2022-07-17T03:49:17+00:00	✓ OK	
2022-07-17T03:48:17+00:00	✓ OK	
2022-07-17T03:47:17+00:00	✓ OK	
2022-07-16T23:48:45+00:00	✓ OK	
2022-07-16T23:47:46+00:00	✓ OK	
2022-07-16T23:46:46+00:00	✓ OK	

Hardening

Hardening Against [WordPress User Enumeration] on Target 1

Explain how to patch Target 1 against Vulnerability 1. Include:

- Avoid using the username as nickname and display name which is shown publicly in WordPress.
- The best option is to choose an administrator username which consists of random characters and use a different nickname.
- WPScan scans for usernames in the URL’s so if you won’t use the username it cannot be scanned by WPScan
  - ***wp user update mary@example.tld --user_login=mary_new***

Hardening Against [CWE-521 (weak password)] on Target 1

- Using hydra, wordpress or simply guessing I could gain access to michaels account
- Limiting login attempts and requiring more complex passwords would stop many brute force attacks
- Update to a newer version of wordpress or using plugins like Password Protected
    - ***wp core update***

Hardening Against [CWE-359: Exposure of Private Personal Information to an Unauthorized Actor] on Target 1

- Hide private information with the use of salted hashes. There are generators online that can help accomplish this
- Whitelisting Michaels IP so an alert is triggered when unauthorized users attempt access.
    - firewall-cmd --permanent --add-rich-rule="rule family='ipv4' source address='192.168.1.90' reject"
    - firewall-cmd --permanent --add-source= (michael IP)
- using two factor authentication on logins could have prevented the server from being accessed in the first place.

Implementing Patches

Implementing Patches with Ansible

Playbook Overview

```
---
- name: Update WordPress Core (Major version)
  command: "{{ wpclipath }} core update"
  when: major is defined
  args:
    chdir: '{{ projects[inventory_hostname].blog_folder }}

'

-- name: Update WordPress Plugins (Major version)
  command: "{{ wpclipath }} plugin update --all"
  when: major is defined
  args:
    chdir: '{{ projects[inventory_hostname].blog_folder }}'


-
```

```
- name: Update WordPress Plugins (Minior version)
  command: "{{ wpclipath }} plugin update --all --minor"
  when: major is not defined
  args:
    chdir: '{{ projects[inventory_hostname].blog_folder }}'
```

Table of Contents

This document contains the following resources:

01 **Methods Used to Avoiding Detect**

02 **Exploits Used**

Network Topology
& Critical Vulnerabilities

Critical Vulnerabilities: Target 1

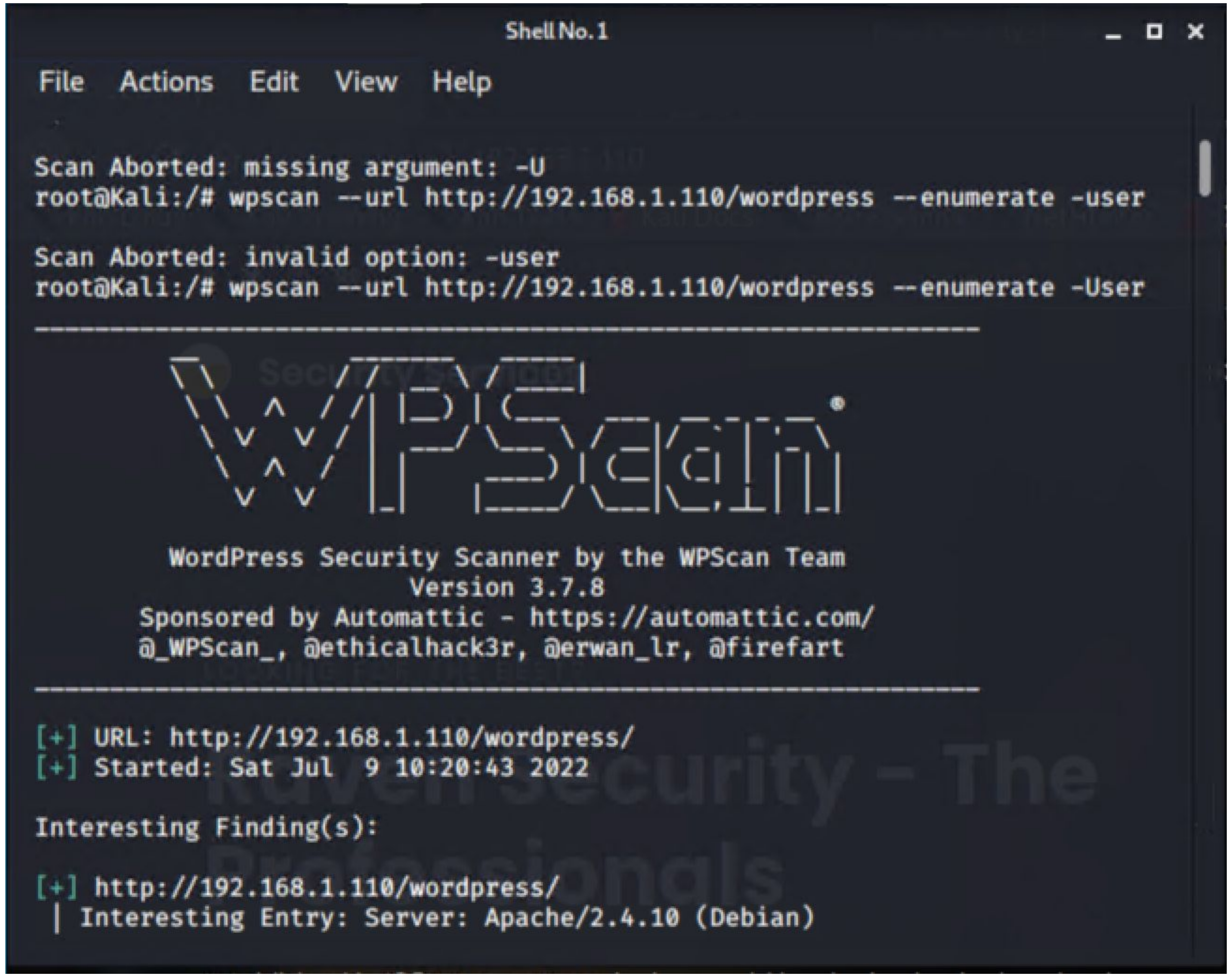
Our assessment uncovered the following critical vulnerabilities in **Target 1**.

Vulnerability	Description	Impact
WPscan	Allows me to see the wordpress users	Gave targets for eventual brute forcing
CVE-521 (weak password requirement)]	Allows me to crack michaels password	Granted access to the vulnerable system
CWE-359: Exposure of Private Personal Information to an Unauthorized Actor	Allows access to the MYSQL database	Gave information for all the wordpress databases

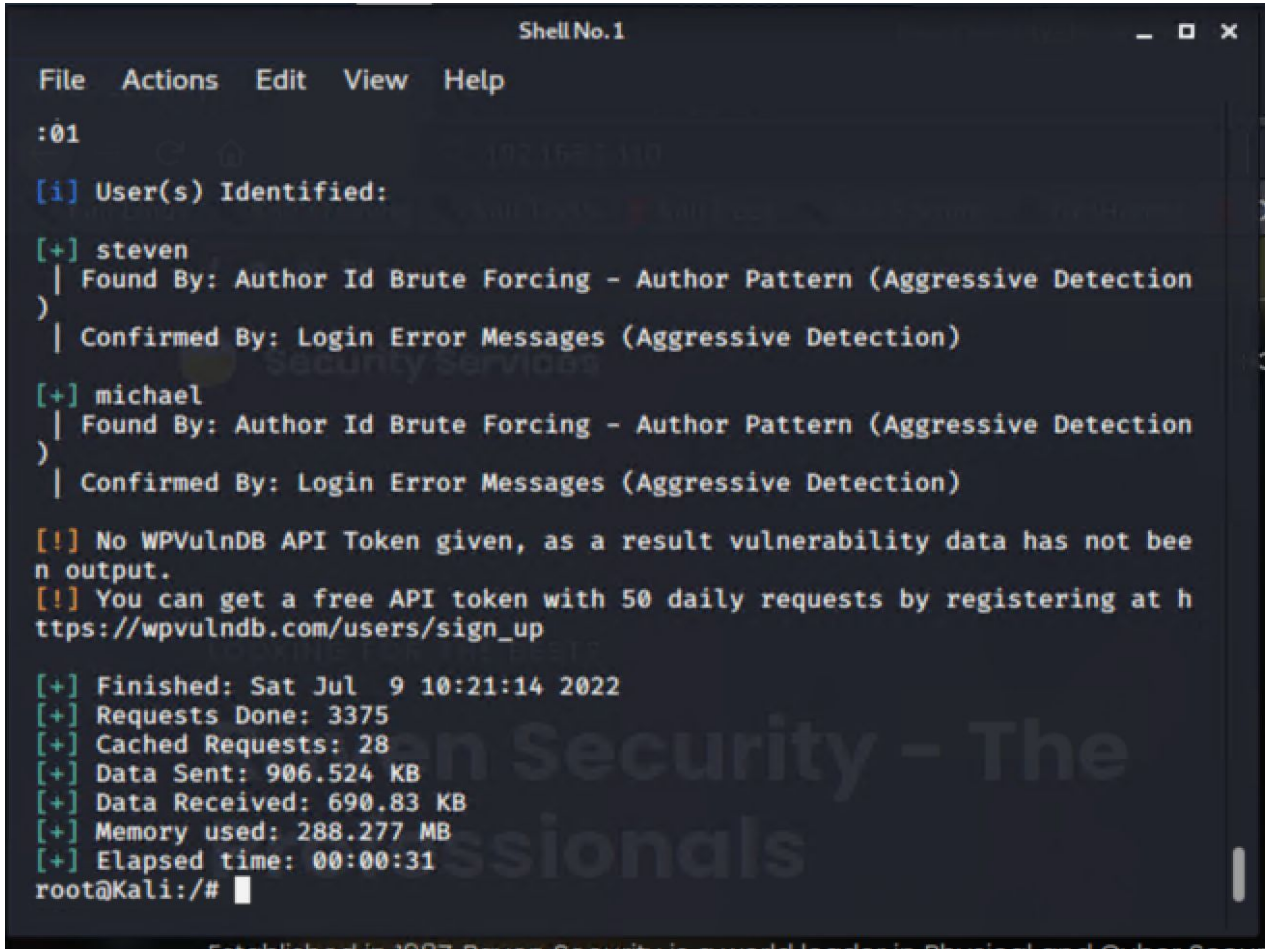
Exploits Used

Exploitation: [WPscan]

- Running a wpscan (wpscans —url 192.168.1.110 —enumerate -Users) I found users micheal and stephen).



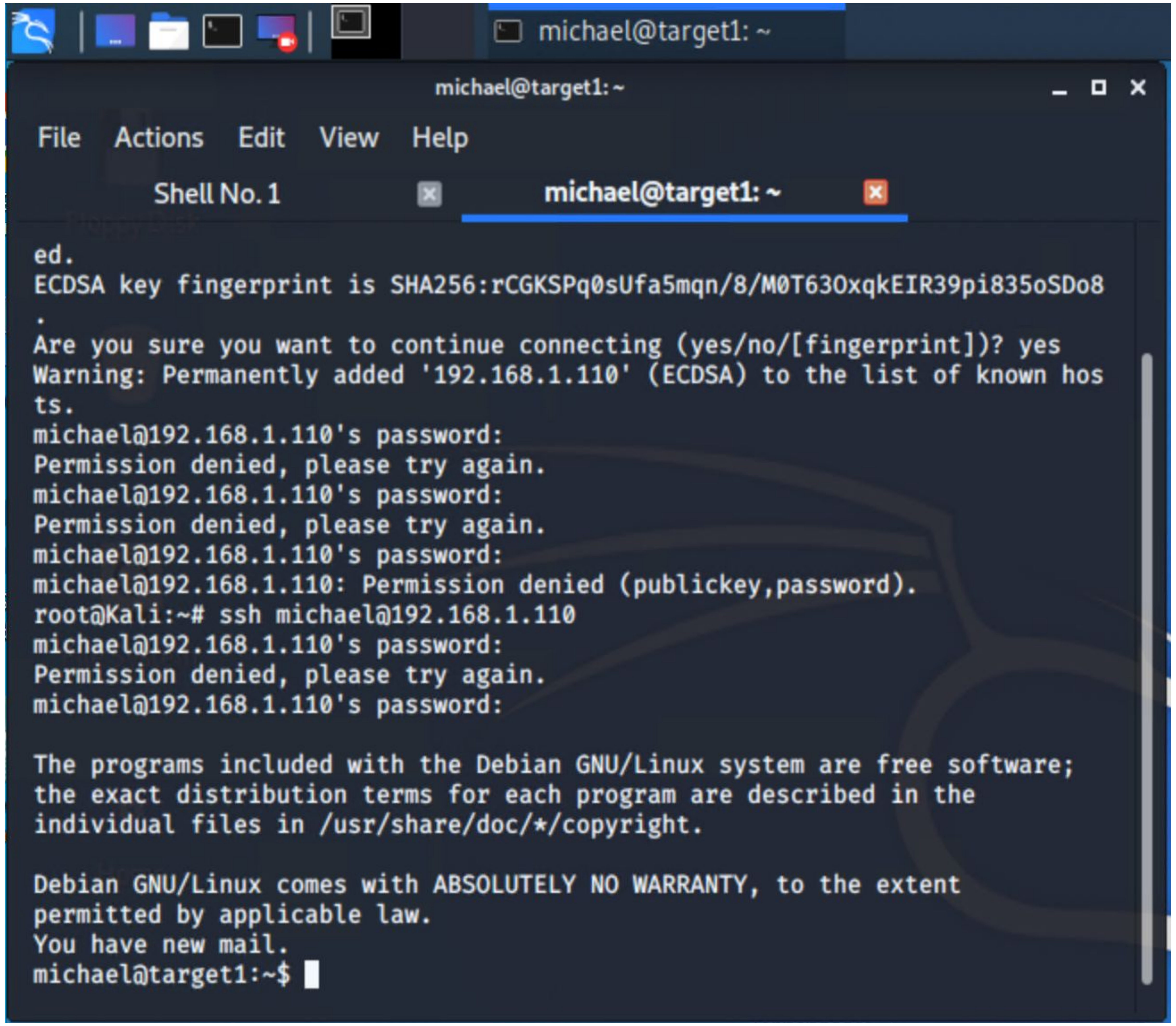
```
Scan Aborted: missing argument: -U
root@Kali:/# wpscan --url http://192.168.1.110/wordpress --enumerate -user

Scan Aborted: invalid option: -user
root@Kali:/# wpscan --url http://192.168.1.110/wordpress --enumerate -User
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.7.8
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: http://192.168.1.110/wordpress/
[+] Started: Sat Jul  9 10:20:43 2022

Interesting Finding(s):

[+] http://192.168.1.110/wordpress/
 | Interesting Entry: Server: Apache/2.4.10 (Debian)
```



```
:01

[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 Jul  9 10:21:14 2022
[+] Requests Done: 3375
[+] Cached Requests: 28
[+] Data Sent: 906.524 KB
[+] Data Received: 690.83 KB
[+] Memory used: 288.277 MB
[+] Elapsed time: 00:00:31
root@Kali:/# █
```

Exploitation: [CVE-521 (weak password requirement)]

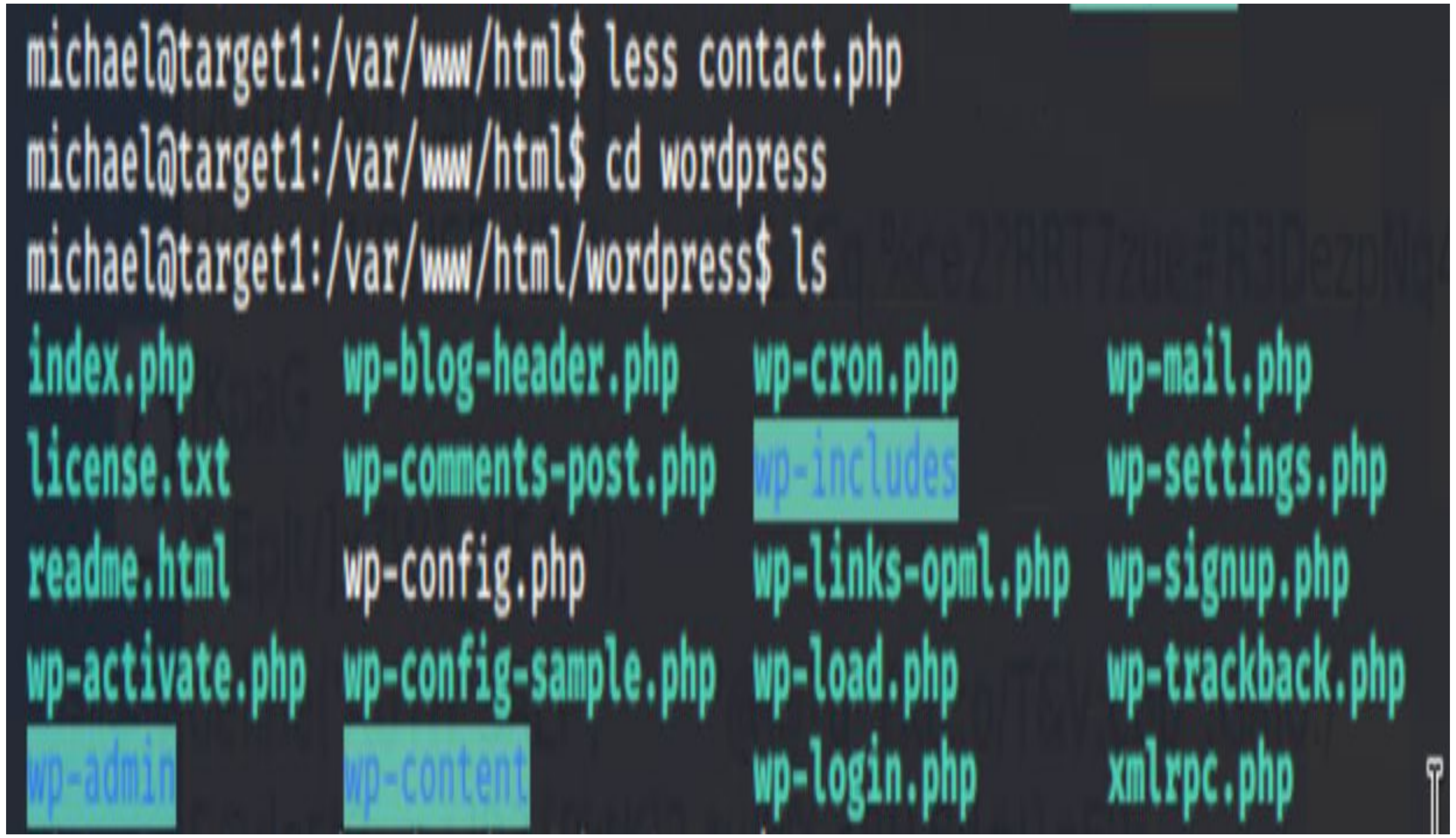
- After finding the Users I guessed michaels password to ssh into his account (ssh michael@192.168.1.110, password: michael).
- His password also could have been brute forced using hydra or wordpress



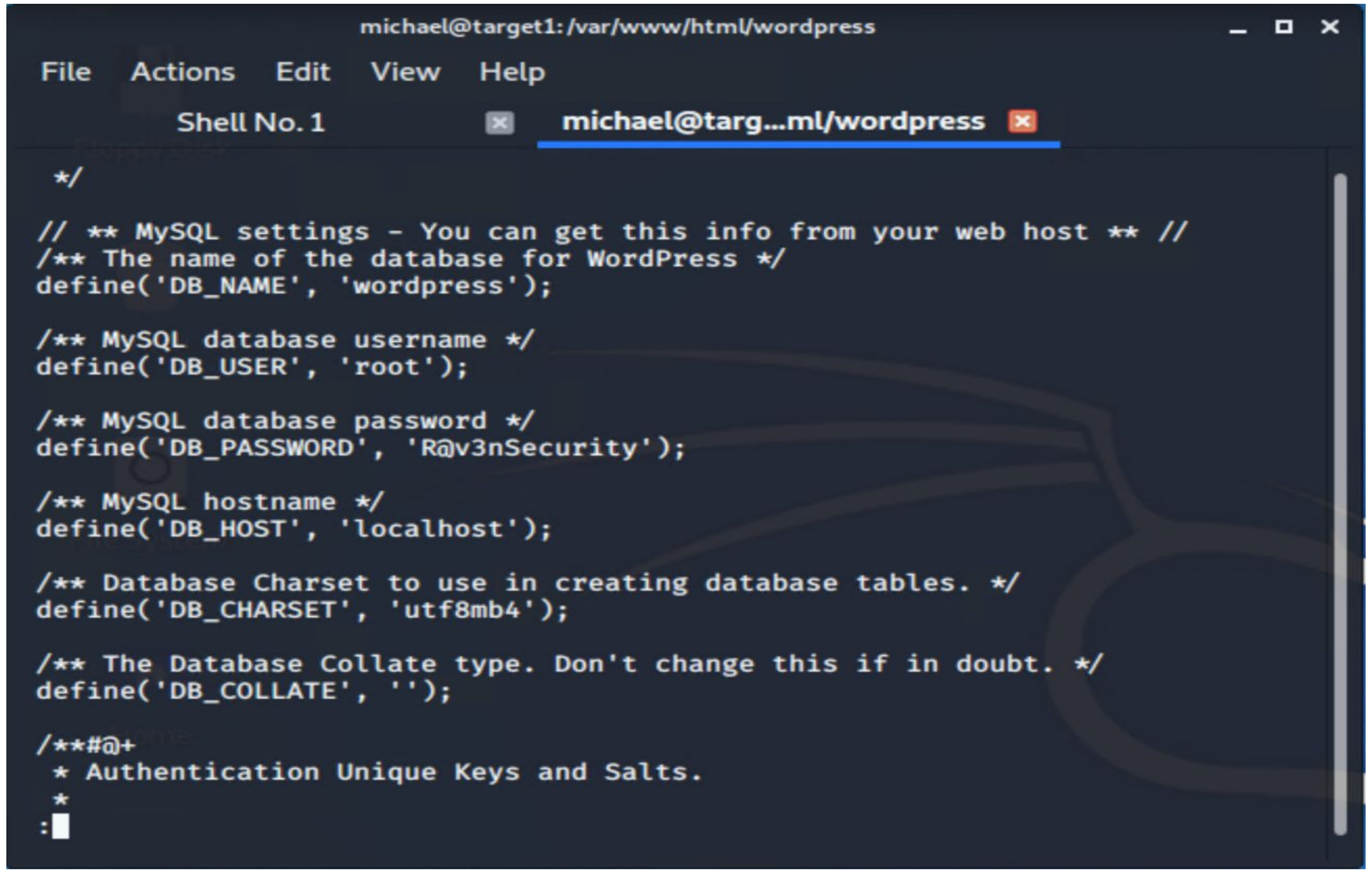
```
ed.
ECDSA key fingerprint is SHA256:rCGKSPq0sUfa5mqn/8/M0T63OxqkEIR39pi835oSDo8
.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.110' (ECDSA) to the list of known hos
ts.
michael@192.168.1.110's password:
Permission denied, please try again.
michael@192.168.1.110's password:
Permission denied, please try again.
michael@192.168.1.110's password:
michael@192.168.1.110: Permission denied (publickey,password).
root@Kali:~# ssh michael@192.168.1.110
michael@192.168.1.110's password:
Permission denied, please try again.
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.
michael@target1:~$ 
```

Exploitation: [CWE-359: Exposure of Private Personal Information to an Unauthorized Actor]

- From inside var/www/html I ran the command grep -ir wp-config.php letting me know it was in the wordpress directory
- After finding the file i found the mysql username:root and password: R@v3nSecurity



```
michael@target1:/var/www/html$ less contact.php
michael@target1:/var/www/html$ cd wordpress
michael@target1:/var/www/html/wordpress$ ls
index.php      wp-blog-header.php    wp-cron.php        wp-mail.php
license.txt    wp-comments-post.php  wp-includes        wp-settings.php
readme.html    wp-config.php         wp-links-opml.php  wp-signup.php
wp-activate.php wp-config-sample.php wp-load.php        wp-trackback.php
wp-admin       wp-content            wp-login.php       xmlrpc.php
```



michael@target1: /var/www/html/wordpress
File
Actions
Edit
View
Help
Shell No. 1
michael@targ...ml/wordpress

```
 */

// ** 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', '');

/**#@+
 * Authentication Unique Keys and Salts.
 *
:
```

Avoiding Detection

Stealth Exploitation of [WPscan]

Monitoring Overview

- **Excessive HTTP Errors**
- **Metric**: WHEN count() GROUPED OVER top 5 'http.response.status_code' IS ABOVE 400 FOR THE LAST 5 minutes
- **Threshold:** ABOVE 400 FOR THE LAST 5 minutes

Mitigating Detection

- Make the scan harder to detect by changing the variables
- wpscan —url 192.168.1.110 —enumerate -Users --random-user-agent --detection-mode passive --plugins-version-detection passive (--stealthy)

Stealth Exploitation of [CWE-521 (weak password)]

Monitoring Overview

- **Excessive HTTP Errors**
- **Metric:** WHEN count() GROUPED OVER top 5 'http.response.status_code' IS ABOVE 400 FOR THE LAST 5 minutes
- **Threshold**: ABOVE 400 FOR THE LAST 5 minutes

Mitigating Detection

- Running a slower brute force can keep you under the number of requests needed to trigger an alert
- Using hydra: hydra -l michael -P /usr/opt/wordlists.txt -s 80 -w 32

Stealth Exploitation of [CWE-359: Exposure of Private Personal Information to an Unauthorized Actor]

Monitoring Overview

- No current configured alerts would have been triggered by someone already in the system, but the alert would cover an alert being sent when an IP from an unauthorized region tries to access the server.

Mitigating Detection

- This can be overcome by spoofing ones IP to an authorized region
- If possible it can also be avoided by gaining physical access to an authorized IP (e.x- a laptop)

Table of Contents

This document contains the following resources:

Traffic Profile

Traffic Profile

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

Feature	Value	Description
Top Talkers (IP Addresses)	172.16.4.20 & 185.243.115.84	Machines that sent the most traffic.
Most Common Protocols	UDP, TCP, HTTP	Three most common protocols on the network.
# of Unique IP Addresses	881	Count of observed IP addresses.
Subnets	10.6.12.0/24 & 172.16.4.0/24.	Observed subnet ranges.
# of Malware Species	1	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

- Searching blogs
- opening pictures
- general personal queries

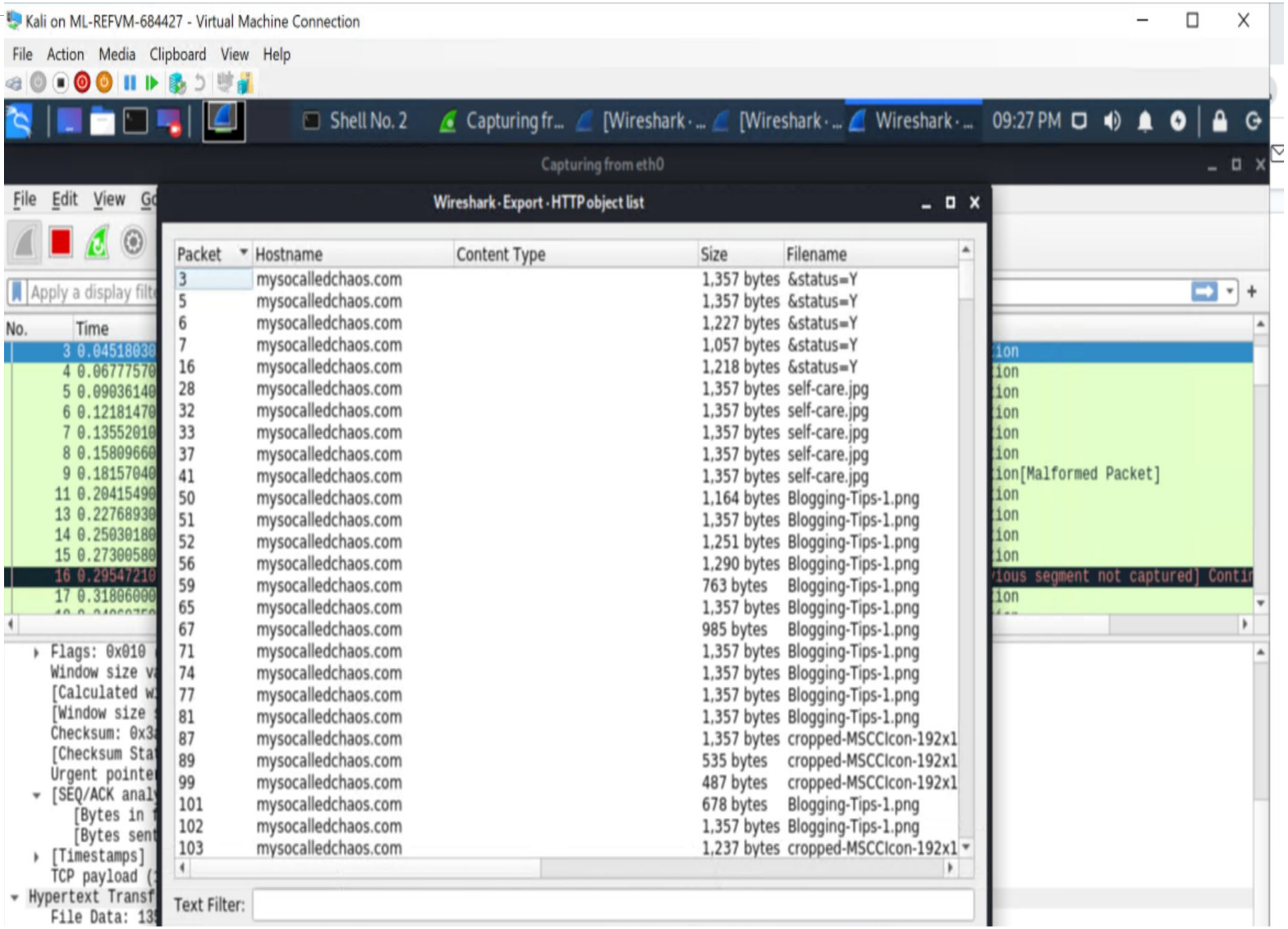
Suspicious Activity

- Trying to access suspicious files on the network
- Higher than usual amounts of packet traffic

Normal Activity

[Reading blogs]

- When I export HTTP traffic I can see the URL and what was accessed
- Normal behavior looks like someone accessing a website for tips on blogging and self care
- ***mysocalledchaos.com*** seems like it would be something looked up for personal gratification.

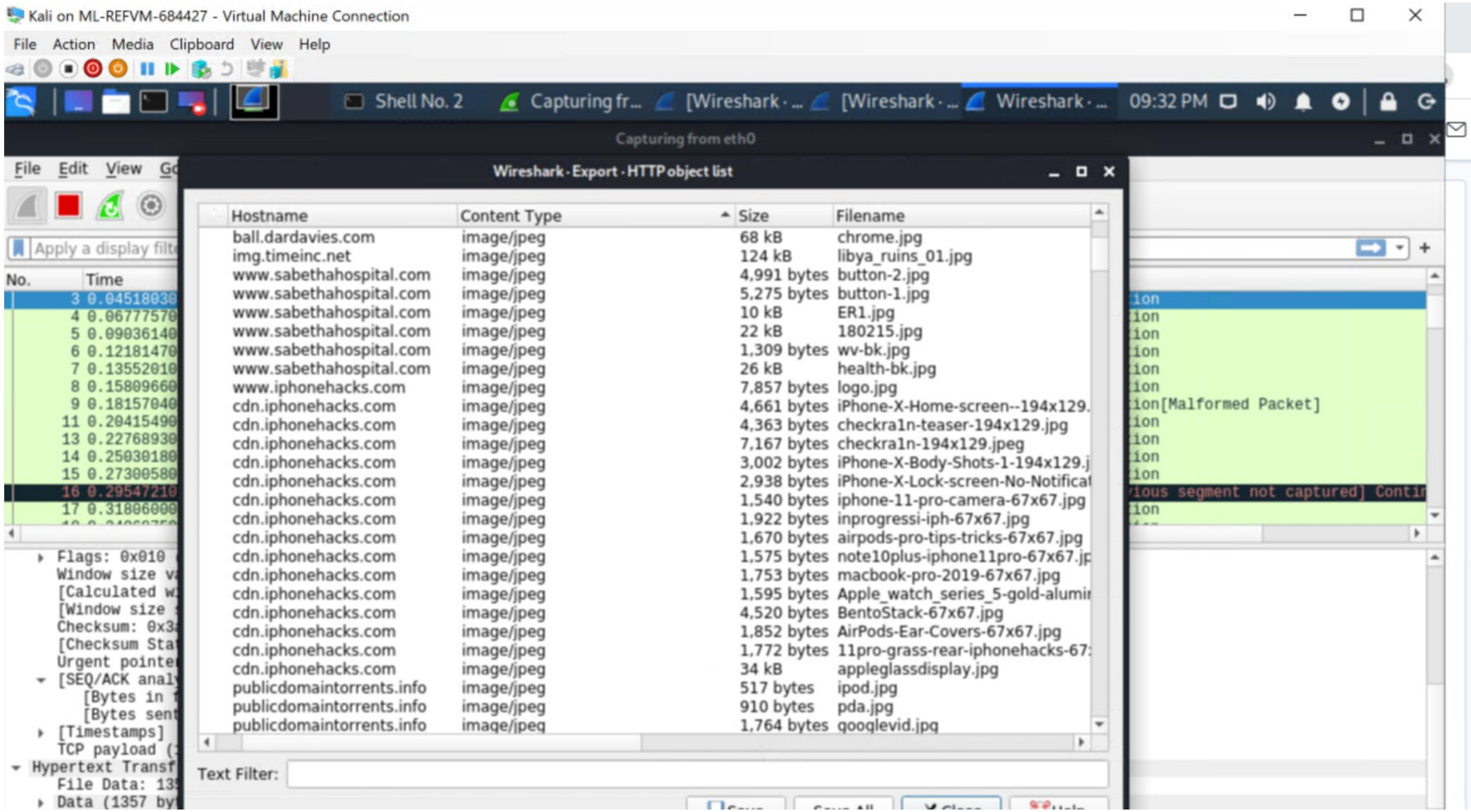


Packet	Hostname	Content Type	Size	Filename
3	mysocalledchaos.com		1,357 bytes	&status=Y
5	mysocalledchaos.com		1,357 bytes	&status=Y
6	mysocalledchaos.com		1,227 bytes	&status=Y
7	mysocalledchaos.com		1,057 bytes	&status=Y
16	mysocalledchaos.com		1,218 bytes	&status=Y
28	mysocalledchaos.com		1,357 bytes	self-care.jpg
32	mysocalledchaos.com		1,357 bytes	self-care.jpg
33	mysocalledchaos.com		1,357 bytes	self-care.jpg
37	mysocalledchaos.com		1,357 bytes	self-care.jpg
41	mysocalledchaos.com		1,357 bytes	self-care.jpg
50	mysocalledchaos.com		1,164 bytes	Blogging-Tips-1.png
51	mysocalledchaos.com		1,357 bytes	Blogging-Tips-1.png
52	mysocalledchaos.com		1,251 bytes	Blogging-Tips-1.png
56	mysocalledchaos.com		1,290 bytes	Blogging-Tips-1.png
59	mysocalledchaos.com		763 bytes	Blogging-Tips-1.png
65	mysocalledchaos.com		1,357 bytes	Blogging-Tips-1.png
67	mysocalledchaos.com		985 bytes	Blogging-Tips-1.png
71	mysocalledchaos.com		1,357 bytes	Blogging-Tips-1.png
74	mysocalledchaos.com		1,357 bytes	Blogging-Tips-1.png
77	mysocalledchaos.com		1,357 bytes	Blogging-Tips-1.png
81	mysocalledchaos.com		1,357 bytes	Blogging-Tips-1.png
87	mysocalledchaos.com		1,357 bytes	cropped-MSCCIcon-192x1
89	mysocalledchaos.com		535 bytes	cropped-MSCCIcon-192x1
99	mysocalledchaos.com		487 bytes	cropped-MSCCIcon-192x1
101	mysocalledchaos.com		678 bytes	Blogging-Tips-1.png
102	mysocalledchaos.com		1,357 bytes	Blogging-Tips-1.png
103	mysocalledchaos.com		1,237 bytes	cropped-MSCCIcon-192x1

[General Queries]

Summarize the following:

- Normal users were also found looking at normal websites that would help them with day to day tasks/issues
- ***cdn.iphonehacks.com*** is a place where one can learn tips for improving Iphone usage and understanding



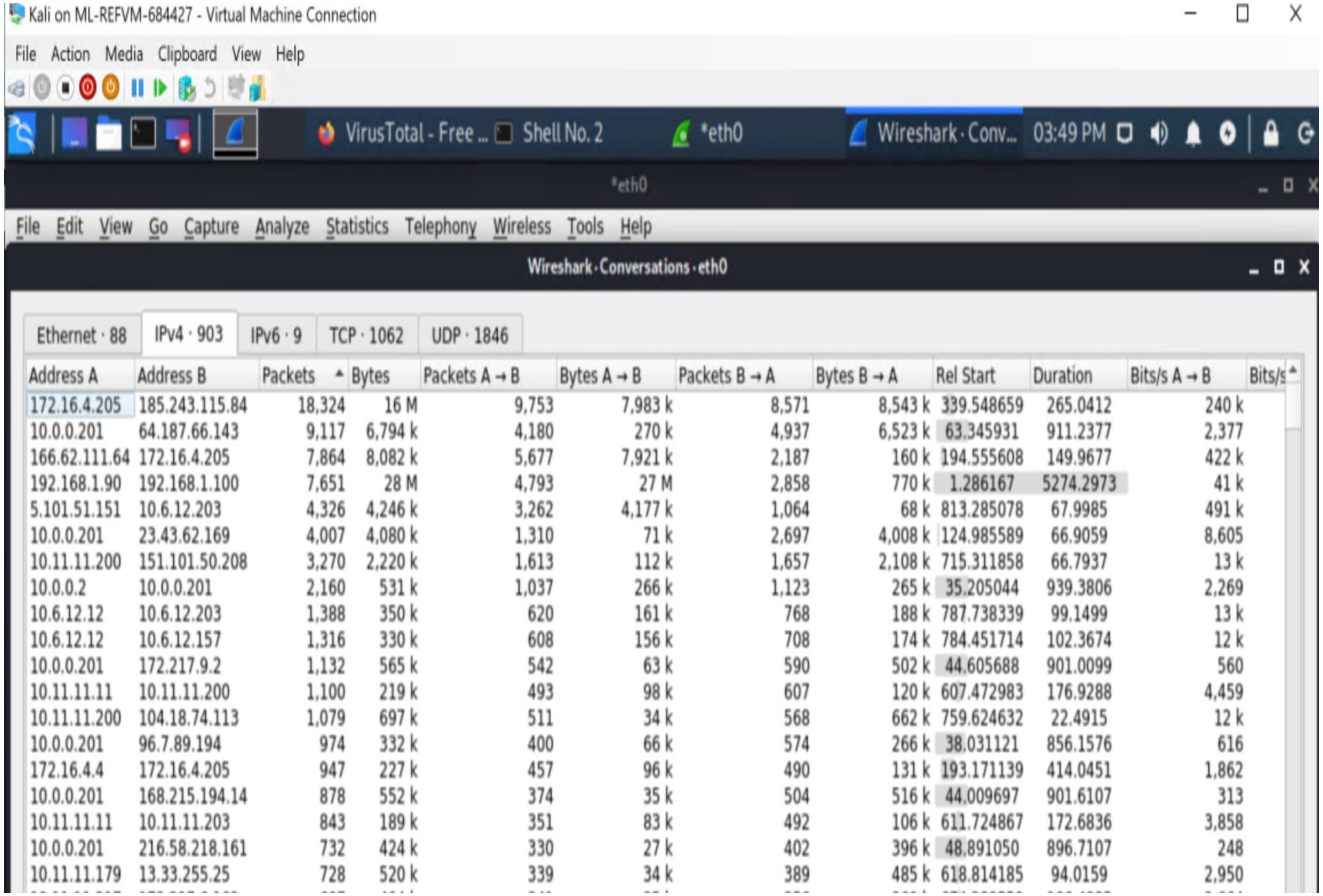
Hostname	Content Type	Size	Filename
ball.dardavies.com	image/jpeg	68 kB	chrome.jpg
img.timeinc.net	image/jpeg	124 kB	libya_ruins_01.jpg
www.sabethahospital.com	image/jpeg	4,991 bytes	button-2.jpg
www.sabethahospital.com	image/jpeg	5,275 bytes	button-1.jpg
www.sabethahospital.com	image/jpeg	10 kB	ER1.jpg
www.sabethahospital.com	image/jpeg	22 kB	180215.jpg
www.sabethahospital.com	image/jpeg	1,309 bytes	wv-bk.jpg
www.sabethahospital.com	image/jpeg	26 kB	health-bk.jpg
www.iphonehacks.com	image/jpeg	7,857 bytes	logo.jpg
cdn.iphonehacks.com	image/jpeg	4,661 bytes	iPhone-X-Home-screen--194x129.
cdn.iphonehacks.com	image/jpeg	4,363 bytes	checkra1n-teaser-194x129.jpg
cdn.iphonehacks.com	image/jpeg	7,167 bytes	checkra1n-194x129.jpeg
cdn.iphonehacks.com	image/jpeg	3,002 bytes	iPhone-X-Body-Shots-1-194x129.j
cdn.iphonehacks.com	image/jpeg	2,938 bytes	iPhone-X-Lock-screen-No-Notificat
cdn.iphonehacks.com	image/jpeg	1,540 bytes	iphone-11-pro-camera-67x67.jpg
cdn.iphonehacks.com	image/jpeg	1,922 bytes	inprogressi-iph-67x67.jpg
cdn.iphonehacks.com	image/jpeg	1,670 bytes	airpods-pro-tips-tricks-67x67.jpg
cdn.iphonehacks.com	image/jpeg	1,575 bytes	note10plus-iphone11pro-67x67.jp
cdn.iphonehacks.com	image/jpeg	1,753 bytes	macbook-pro-2019-67x67.jpg
cdn.iphonehacks.com	image/jpeg	1,595 bytes	Apple_watch_series_5-gold-alumin
cdn.iphonehacks.com	image/jpeg	4,520 bytes	BentoStack-67x67.jpg
cdn.iphonehacks.com	image/jpeg	1,852 bytes	AirPods-Ear-Covers-67x67.jpg
cdn.iphonehacks.com	image/jpeg	1,772 bytes	11pro-grass-rear-iphonehacks-67:
cdn.iphonehacks.com	image/jpeg	34 kB	appleglassdisplay.jpg
publicdomaintorrents.info	image/jpeg	517 bytes	ipod.jpg
publicdomaintorrents.info	image/jpeg	910 bytes	pda.jpg
publicdomaintorrents.info	image/jpeg	1,764 bytes	googlevid.jpg

Text Filter:

Malicious Activity

[Higher than usual packets]

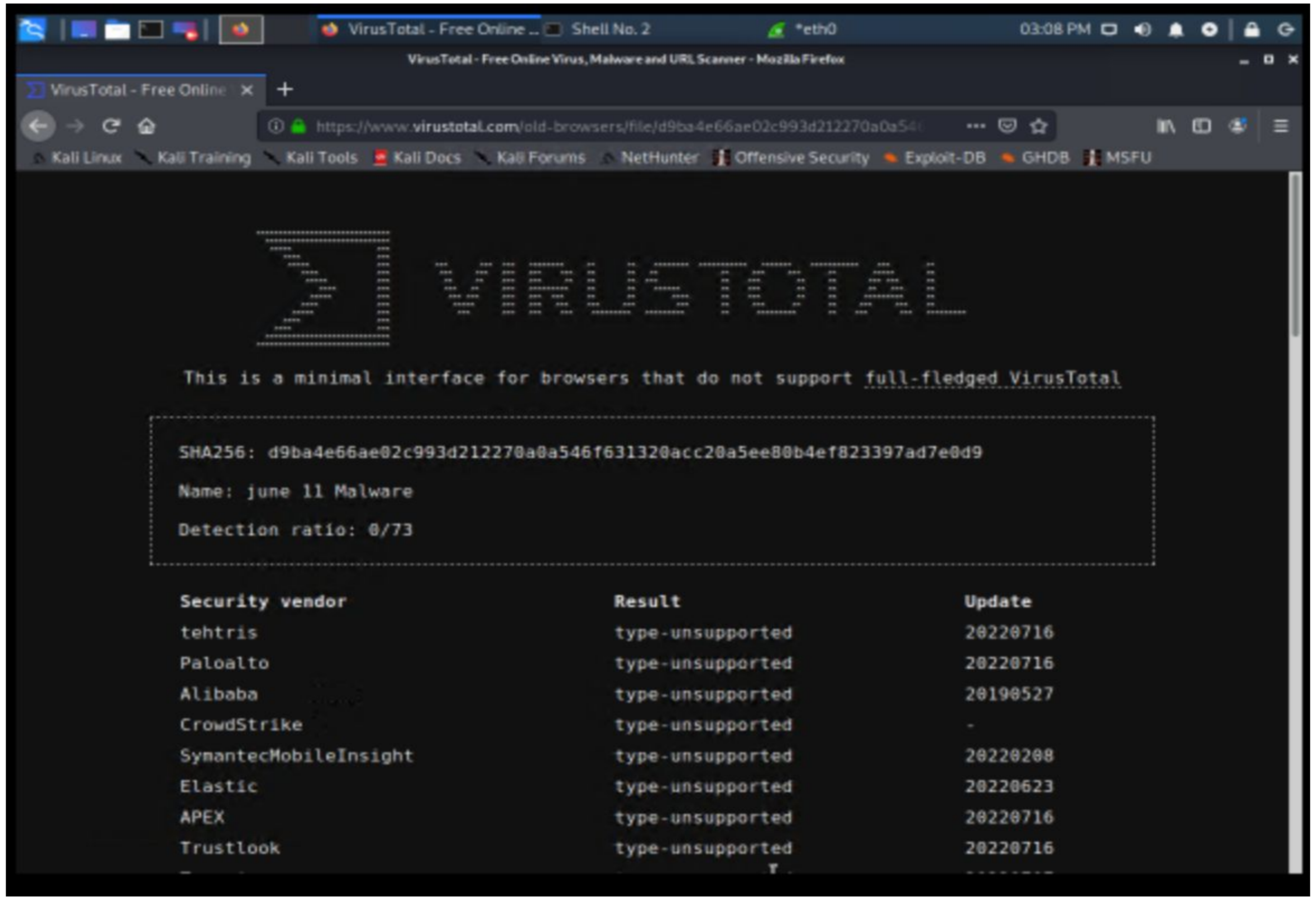
- *172.16.4.205 and 185.243.115.84 have an abnormal amount of packets and bytes compared to the rest of the IPs. WIth that high amount of TCP traffic*


Kali on ML-REFVM-684427 - Virtual Machine Connection
File Action Media Clipboard View Help
VirusTotal - Free ...
Shell No. 2
*eth0
Wireshark · Conv...
03:49 PM
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Wireshark · Conversations · eth0
Ethernet · 88
IPv4 · 903
IPv6 · 9
TCP · 1062
UDP · 1846

Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s
172.16.4.205	185.243.115.84	18,324	16 M	9,753	7,983 k	8,571	8,543 k	339.548659	265.0412	240 k	
10.0.0.201	64.187.66.143	9,117	6,794 k	4,180	270 k	4,937	6,523 k	63.345931	911.2377	2,377	
166.62.111.64	172.16.4.205	7,864	8,082 k	5,677	7,921 k	2,187	160 k	194.555608	149.9677	422 k	
192.168.1.90	192.168.1.100	7,651	28 M	4,793	27 M	2,858	770 k	1.286167	5274.2973	41 k	
5.101.51.151	10.6.12.203	4,326	4,246 k	3,262	4,177 k	1,064	68 k	813.285078	67.9985	491 k	
10.0.0.201	23.43.62.169	4,007	4,080 k	1,310	71 k	2,697	4,008 k	124.985589	66.9059	8,605	
10.11.11.200	151.101.50.208	3,270	2,220 k	1,613	112 k	1,657	2,108 k	715.311858	66.7937	13 k	
10.0.0.2	10.0.0.201	2,160	531 k	1,037	266 k	1,123	265 k	35.205044	939.3806	2,269	
10.6.12.12	10.6.12.203	1,388	350 k	620	161 k	768	188 k	787.738339	99.1499	13 k	
10.6.12.12	10.6.12.157	1,316	330 k	608	156 k	708	174 k	784.451714	102.3674	12 k	
10.0.0.201	172.217.9.2	1,132	565 k	542	63 k	590	502 k	44.605688	901.0099	560	
10.11.11.11	10.11.11.200	1,100	219 k	493	98 k	607	120 k	607.472983	176.9288	4,459	
10.11.11.200	104.18.74.113	1,079	697 k	511	34 k	568	662 k	759.624632	22.4915	12 k	
10.0.0.201	96.7.89.194	974	332 k	400	66 k	574	266 k	38.031121	856.1576	616	
172.16.4.4	172.16.4.205	947	227 k	457	96 k	490	131 k	193.171139	414.0451	1,862	
10.0.0.201	168.215.194.14	878	552 k	374	35 k	504	516 k	44.009697	901.6107	313	
10.11.11.11	10.11.11.203	843	189 k	351	83 k	492	106 k	611.724867	172.6836	3,858	
10.0.0.201	216.58.218.161	732	424 k	330	27 k	402	396 k	48.891050	896.7107	248	
10.11.11.179	13.33.255.25	728	520 k	339	34 k	389	485 k	618.814185	94.0159	2,950	

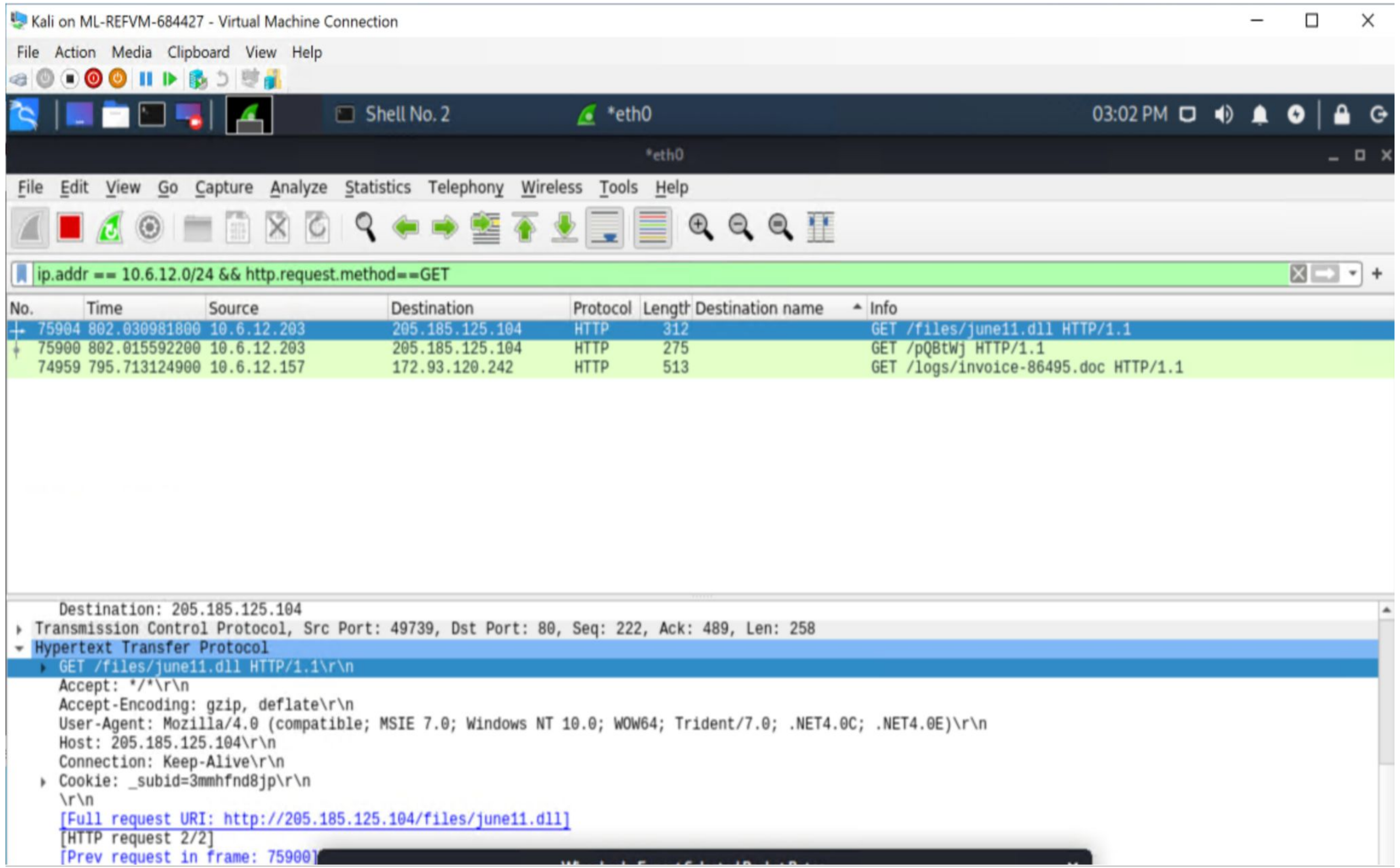
[June11.dll]

- *WIthin users frank and teds IP address is malware called /files/june11.dll*
- *HTTP protocol request protocol*
- *When uploaded virustotal.com designates it as malicious software*



VirusTotal - Free Online ...
Shell No. 2
*eth0
03:08 PM
VirusTotal - Free Online Virus, Malware and URL Scanner - Mozilla Firefox
VirusTotal - Free Online
https://www.virustotal.com/old-browsers/file/d9ba4e66ae02c993d212270a0a54
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU
VIRUSTOTAL

```
This is a minimal interface for browsers that do not support full-fledged VirusTotal

SHA256: d9ba4e66ae02c993d212270a0a546f631320acc20a5ee80b4ef823397ad7e0d9

Name: june 11 Malware

Detection ratio: 0/73

Security vendor              Result              Update
tehtris                      type-unsupported    20220716
Paloalto                     type-unsupported    20220716
Alibaba                      type-unsupported    20190527
CrowdStrike                  type-unsupported    -
SymantecMobileInsight        type-unsupported    20220208
Elastic                      type-unsupported    20220623
APEX                         type-unsupported    20220716
Trustlook                    type-unsupported    20220716
```



```
ip.addr == 10.6.12.0/24 && http.request.method==GET

No.   Time           Source        Destination      Protocol Length Destination name  Info
75904 802.030981800  10.6.12.203   205.185.125.104  HTTP     312                      GET /files/june11.dll HTTP/1.1
75900 802.015592200  10.6.12.203   205.185.125.104  HTTP     275                      GET /pQBtWj HTTP/1.1
74959 795.713124900  10.6.12.157   172.93.120.242   HTTP     513                      GET /logs/invoice-86495.doc HTTP/1.1

    Destination: 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: 75900]
```

The End