**Final Engagement Analysis Report**

**Attack, Defense & Analysis of Vulnerable Network**

**Team Cyber Assaulters**

Chris Duke

Chris Garcia

Donathan Williams

Heike Lohr

John Elliott

Kyle Pierce

Shea Padilla

Michael Lynn

Mozamil Ahmad

**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:

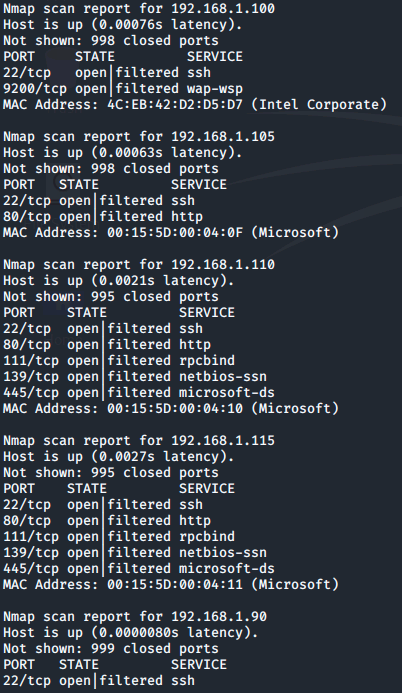
**Red Team: Summary of Operations**

**Table of Contents**

* Exposed Services
* Critical Vulnerabilities
* Exploitation

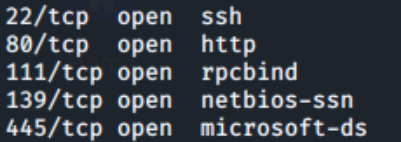
**Exposed Services**

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



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

**Target 1**



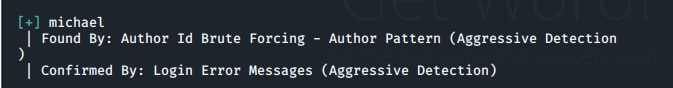
**Critical Vulnerabilities**

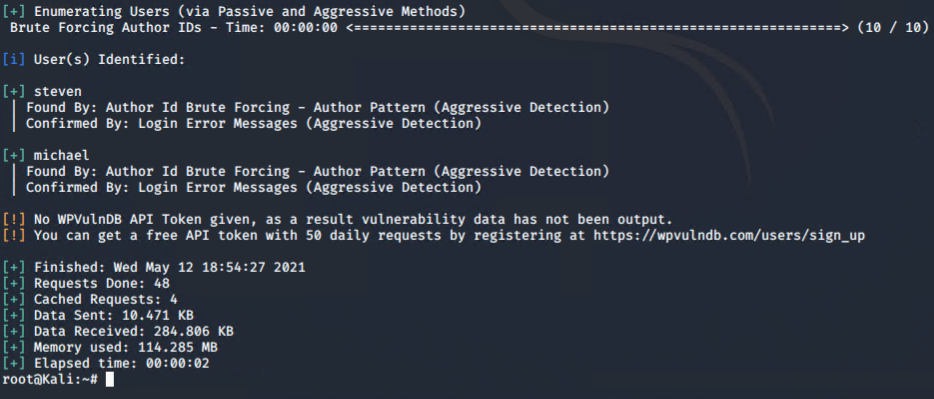
The following vulnerabilities were identified on each target:

**Target 1**

1. Port 111 rpcbind: CVE-2017-8779 DoS
2. Port 139 netbios-ssn: CVE-2018-7445 Buffer overflow, remote code execution
3. Port 139 netbios-ssn: CVE-2007-5398 Stack-based buffer overflow, arbitrary code execution

Vulnerability scan results as proof of the identified vulnerabilities:





**Target 2**

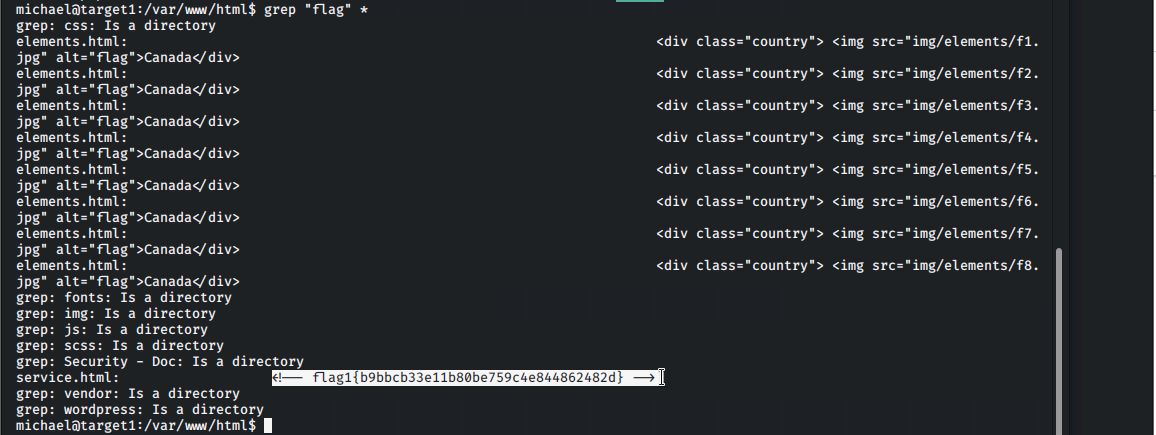
1. CVE2016-10033

**Exploitation**

The Red Team was able to penetrate both Target 1 and started Target 2 and retrieved the following confidential data:

**Target 1**

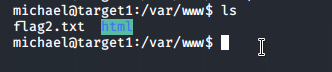
* Flag 1
  + The password which we guessed was the exploit we utilized.
  + Command utilized **grep \*flag\***





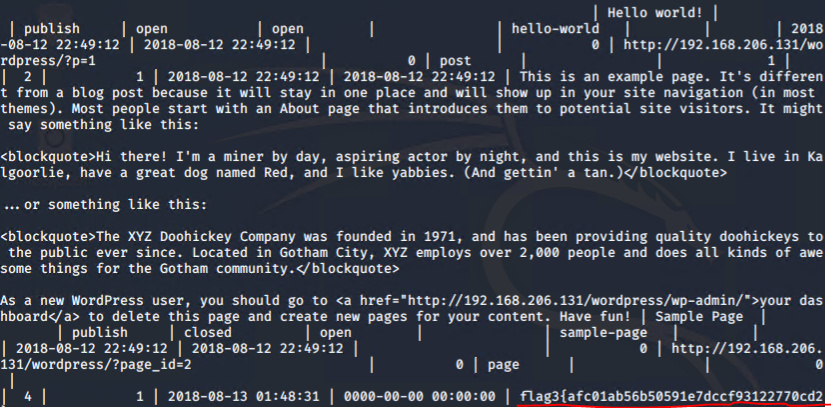
* Flag 2
  + SSH
    - No real exploit utilized just guessed the password
    - Command utilized **ssh michael@192.168.1.110**



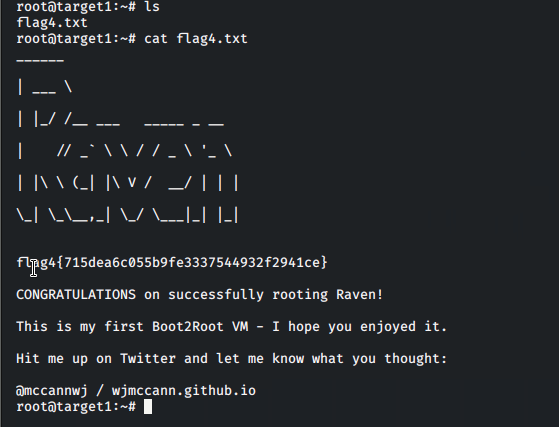




* Flag 3
  + Once access was gained to steven’s account we used mysql commands to enumerate flag 3 from the wp\_posts table within the wordpress database.
  + Command utilized **SELECT \* FROM WP\_POSTS**

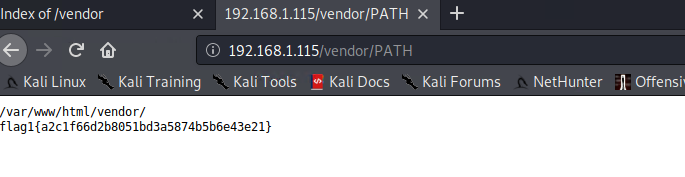


* Flag 4
  + Because steven had sudo access to the python command we were able to successfully gain a root shell using the following command;
  + Command utilized **sudo python -c 'import pty;pty.spawn(“/bin/bash")'** after using this command flag4.txt was found in the /root directory.



**Target 2**

* Flag 1
  + Exploit
  + Command utilized **/var/www/html/vendor**



* Flag 3
  + Exploit
  + Command

**Blue Team: Summary of Operations**

Table of Contents

* Network Topology
* Description of Targets
* Monitoring the Targets
* Patterns of Traffic and Behavior
* Suggestions for Going Further

**Network Topology**

The following machines were identified on the network:

**Network Topology**

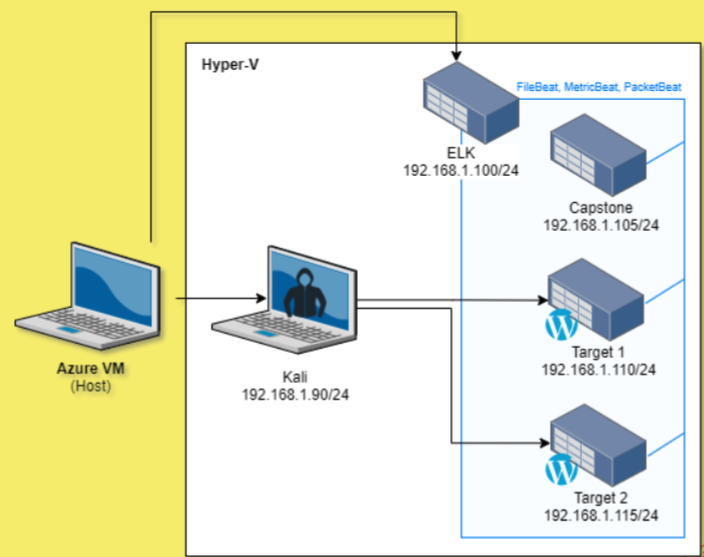
The following machines were identified on the network:

**Target 1**

* Operating System: Linux 3.2
* Purpose: Expose vulnerable Wordpress Server
* IP Address: 192.168.1.110

**Target 2**

* Operating System: Linux 3.2
* Purpose: More difficult Wordpress target
* IP Address: 192.168.1.115



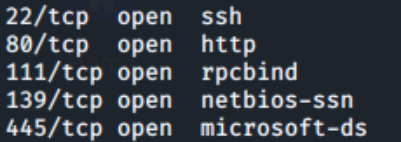
**Description of Targets**

* Two VMs on the network were vulnerable to attack: Target 1 [192.168.1.110] and Target 2 [192.168.1.115].
* Each VM functions as an Apache web server and has SSH enabled, so ports 80 and 22 are possible ports of entry for attackers.

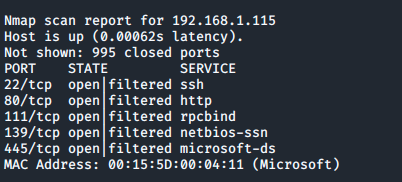
**Monitoring the Targets**

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

**Target 1**

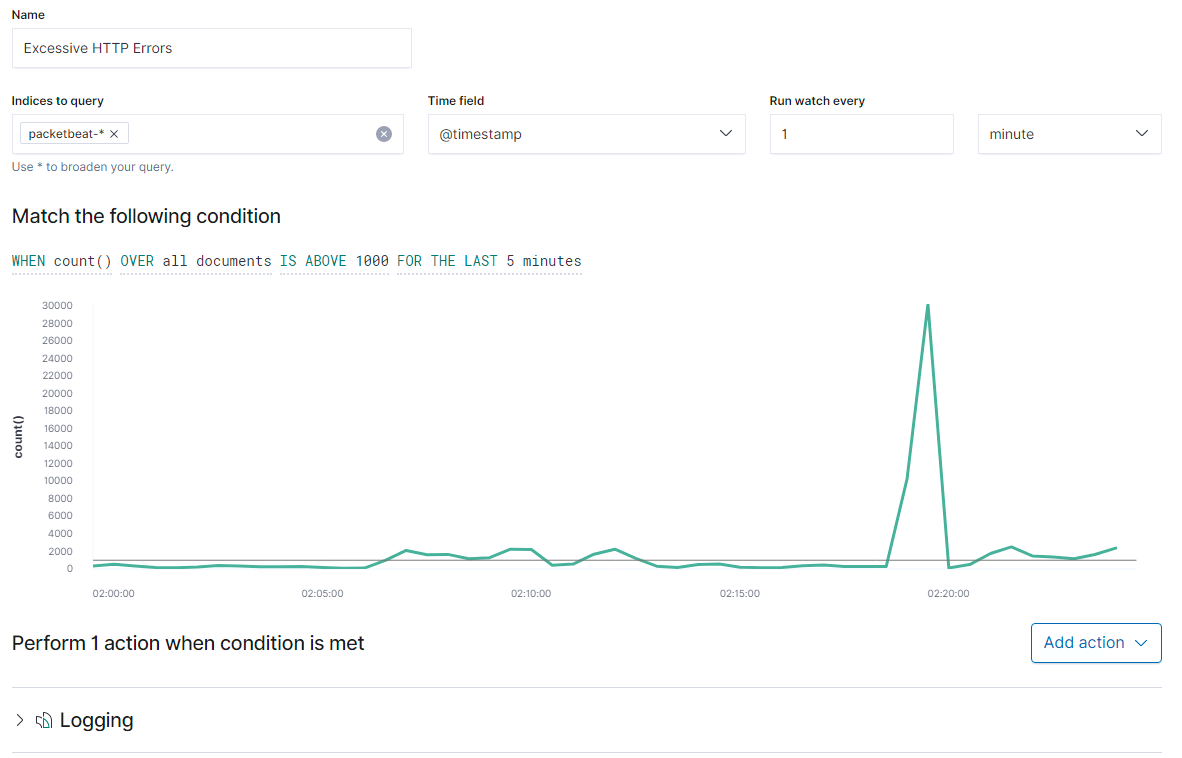


**Target 2**



**Alert 1**

**Excessive HTTP Errors**

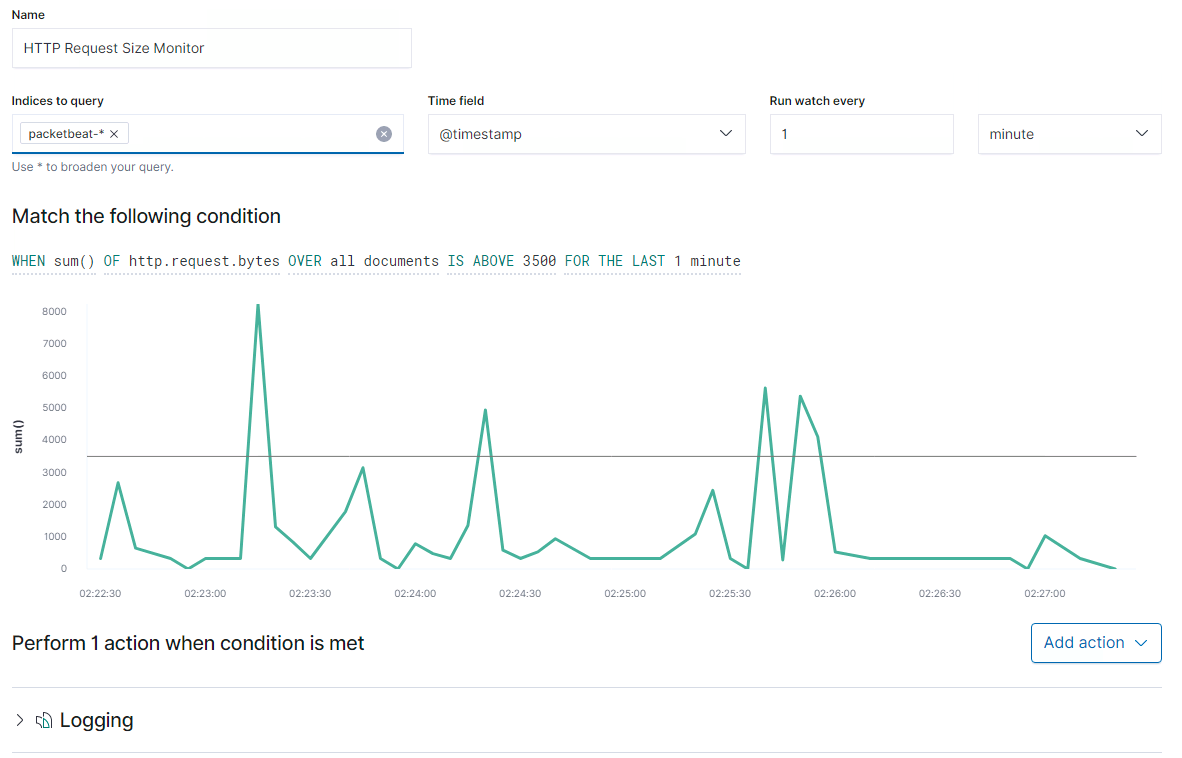


**Excessive HTTP Errors** is implemented as follows:

* Metric: count
* Threshold: 400 requests over 5 minutes
* Vulnerability Mitigated: Brute Force attack
* Reliability: Unreliable as it was not triggered during the penetration test

**Alert 2**

**HTTP Request Size Monitor**

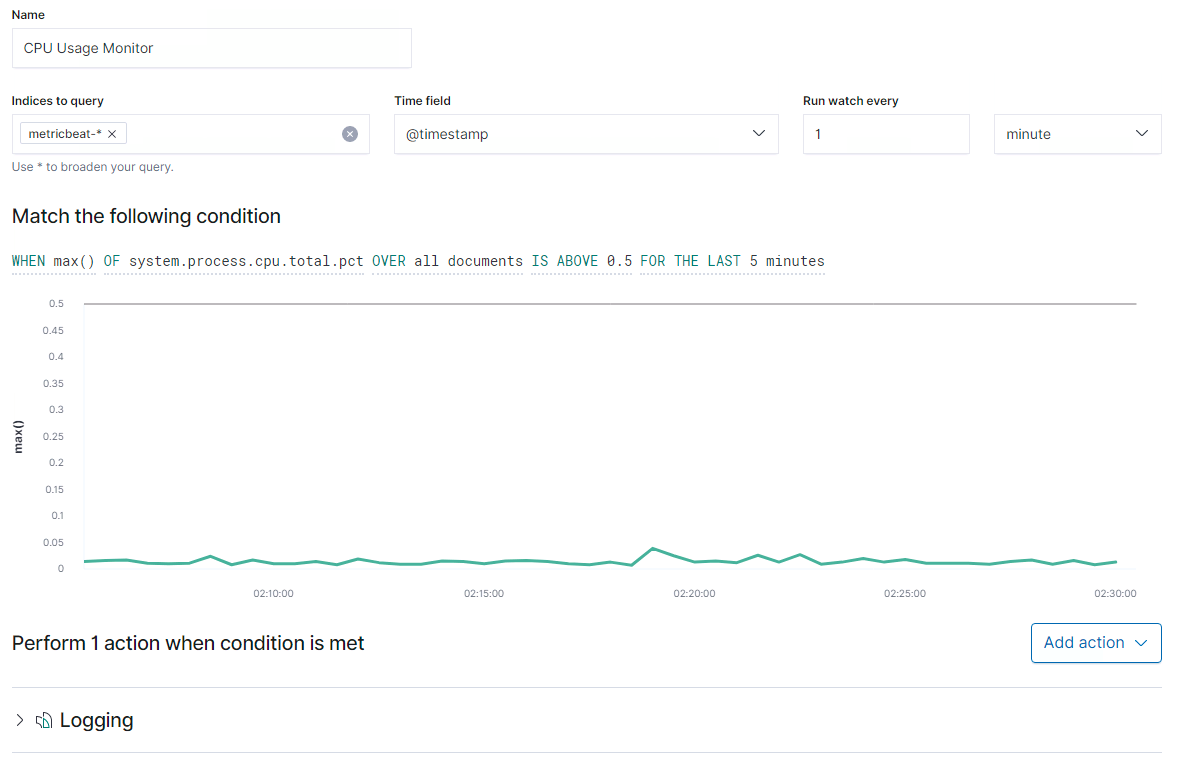
****

**HTTP Request Size Monitor** is implemented as follows:

* Metric: sum
* Threshold: 3500 or more HTTP requests in a minute
* Vulnerability Mitigated: HTTP Flood/ HTTP smuggling
* Reliability: Threshold works well; this alert does not fire off prematurely

**Alert 3**

**CPU Usage Monitor**

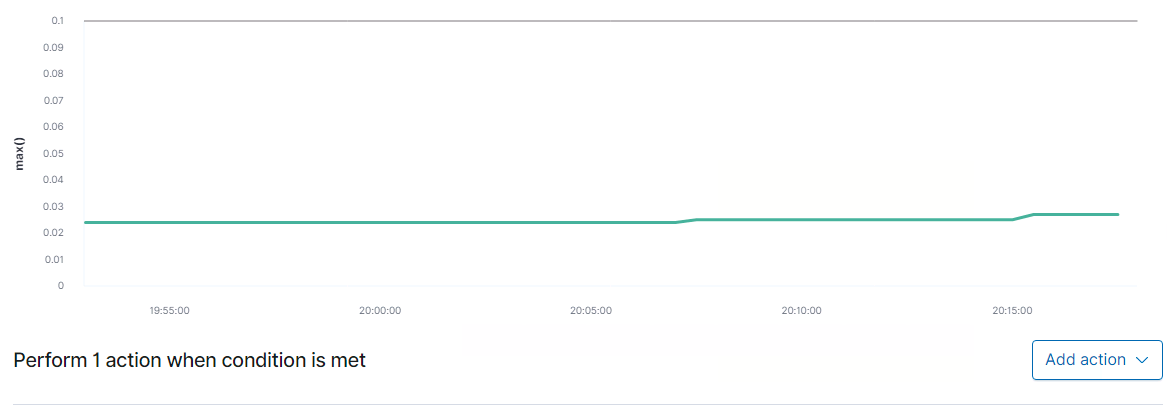
****

**CPU Usage Monitor** is implemented as follows:

* Metric: max
* Threshold: 0.5 over 5 minutes
* Vulnerability Mitigated: DDoS attack / Meltdown
* Reliability: This alert fires reliably

**Alert 4**

**Excessive RAM Usage**

****

**Excessive RAM Usage Alert** is implemented as follows:

* Metric: max
* Threshold: 0.5 over 5 minutes
* Vulnerability Mitigated: Cold boot attacks / memory dump
* Reliability: Alert monitors and triggers reliably

**Suggestions for Going Further**

The logs and alerts generated during the assessment suggest that this network is susceptible to several active threats. 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--HTTP Excessive Errors**

* Patch: Integrate an Intrusion Prevention System (IPS)
* Why It Works: To block any IP address that has more than 2500 unsuccessful requests within a 5 minute period.

**Vulnerability 2--HTTP Request Size Monitor**

* Patch: Disable reuse of back-end connections, use HTTP/2 for back-end connections, use the same web server software for front-end and back-end servers and/or utilize a WAF that has built in mitigation to detect abnormal requests.
* Why It Works: Preventing reuse of connection(s) so data can’t be transferred which forces you to utilize a new connection each time you reach the website.

Reference: <https://portswigger.net/web-security/request-smuggling>

**Vulnerability 3--CPU Usage Monitor**

* Patch: Harden systems to remove unnecessary programs and services that could be exploited.
* Why It Works: It is not draining resources as it would not allow any exploits or vulnerabilities into the system.

**Vulnerability 4--Excessive RAM Usage**

* Patch: Make sure all computers within the company network shut down completely or hibernate instead of going into sleep mode. We would need to preconfigure all networks on the host to hibernate or send a message to make sure your machine hibernates instead of going to sleep.
* Why It Works: This is not a patch but an SOP (Standard Operating Procedure) because when shut down or hibernating nothing is being stored in the RAM instead of when in sleep mode files, encryption keys, etc. can still be saved.

# **Network Analysis**

## **Time Thieves**

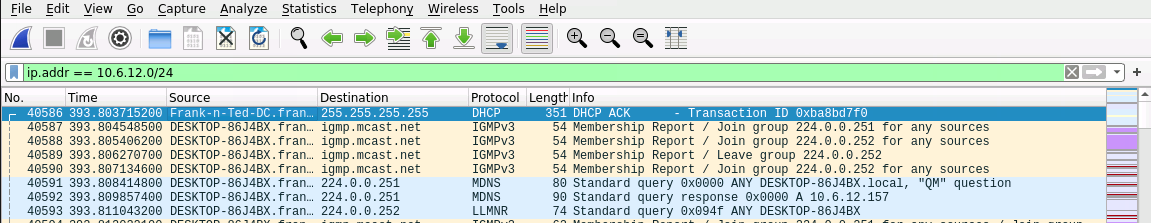
At least two users on the network have been wasting time on YouTube. Usually, IT wouldn't pay much mind to this behavior, but it seems these people have created their own web server on the corporate network. So far, Security knows the following about these time thieves:

* 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:

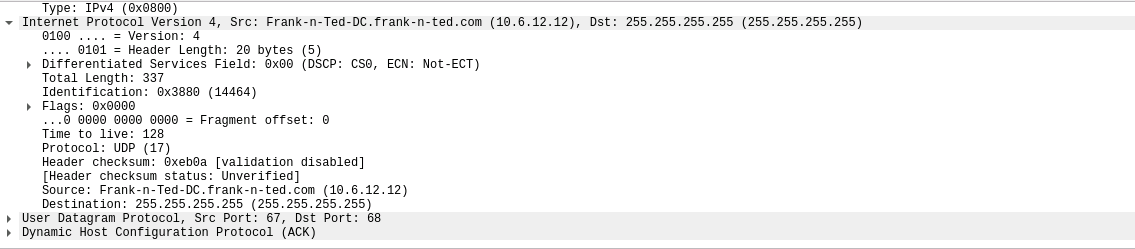
1. What is the domain name of the users' custom site?

Frank-n-Ted-DC.frank-n-ted.com



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

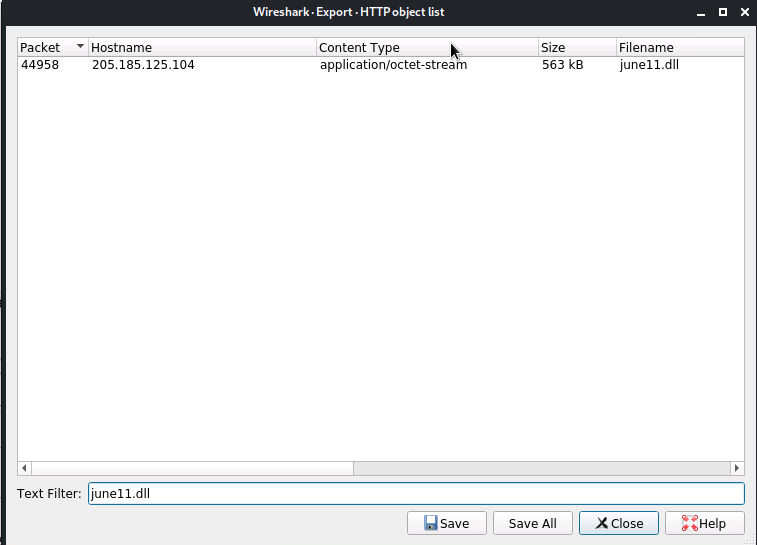
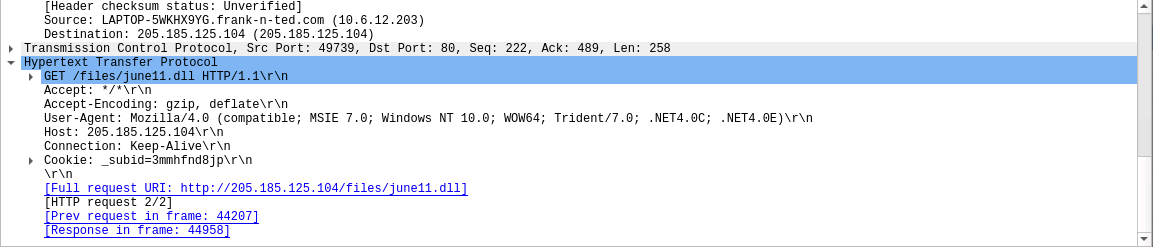
10.6.12.12



1. 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.

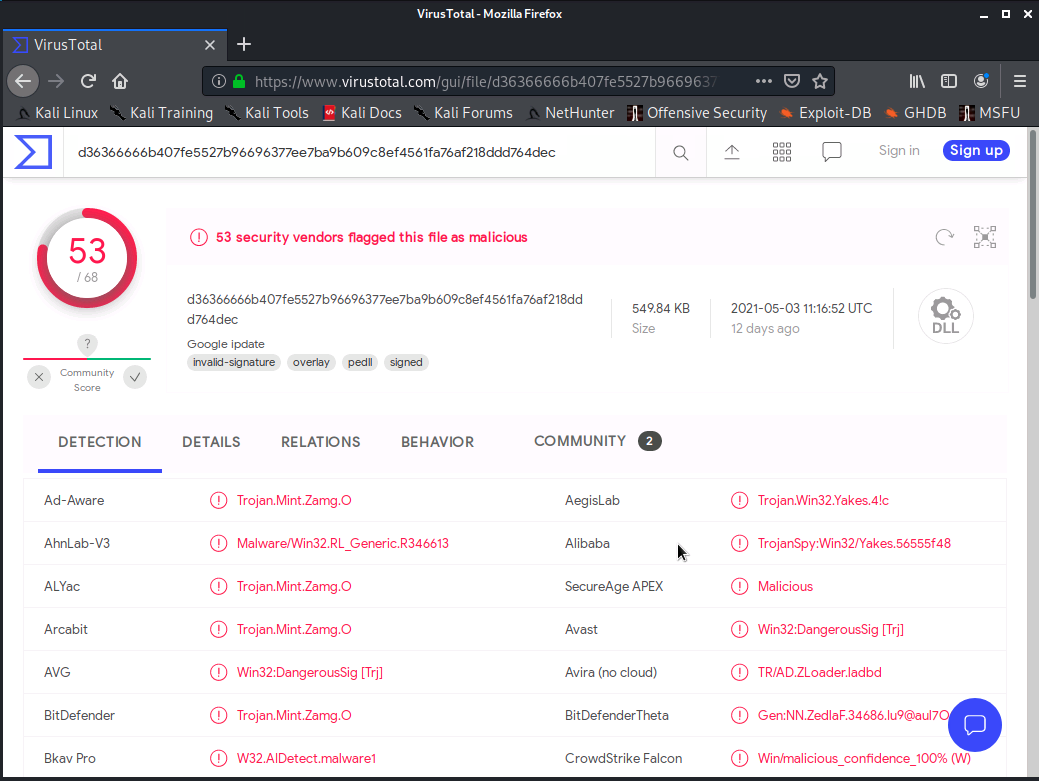
ip.addr==10.16.12.203 and http.request.method==GET

June11.dll is the malware file



1. Upload the file to [VirusTotal.com](https://www.virustotal.com/gui/). What kind of malware is this classified as?

June11.dll is classified as a Trojan



## **Vulnerable Windows Machines**

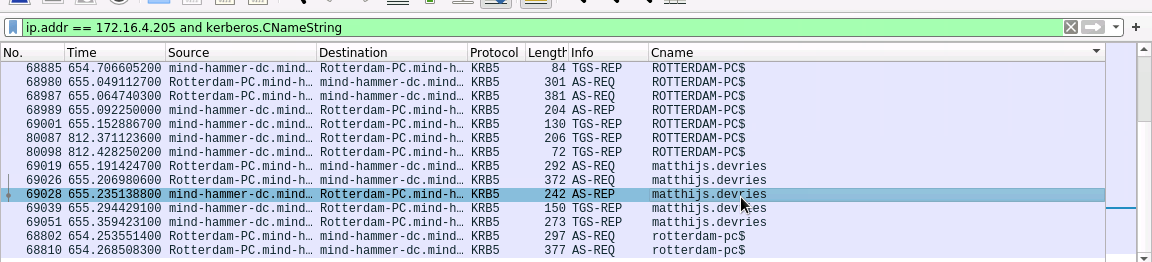
The Security team received reports of an infected Windows host on the network. They know the following:

* 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:00:15:c6:e6:c4:77
2. What is the username of the Windows user whose computer is infected?

ip.addr==172.16.4.205 and kerberos.CnameString

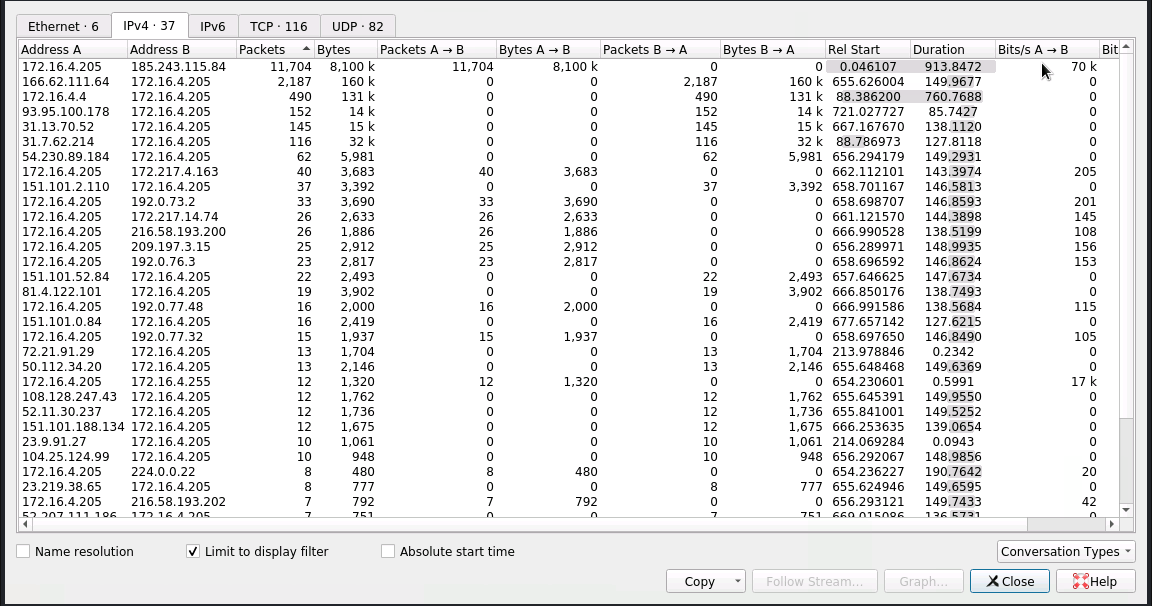
Username: matthijs.devries 

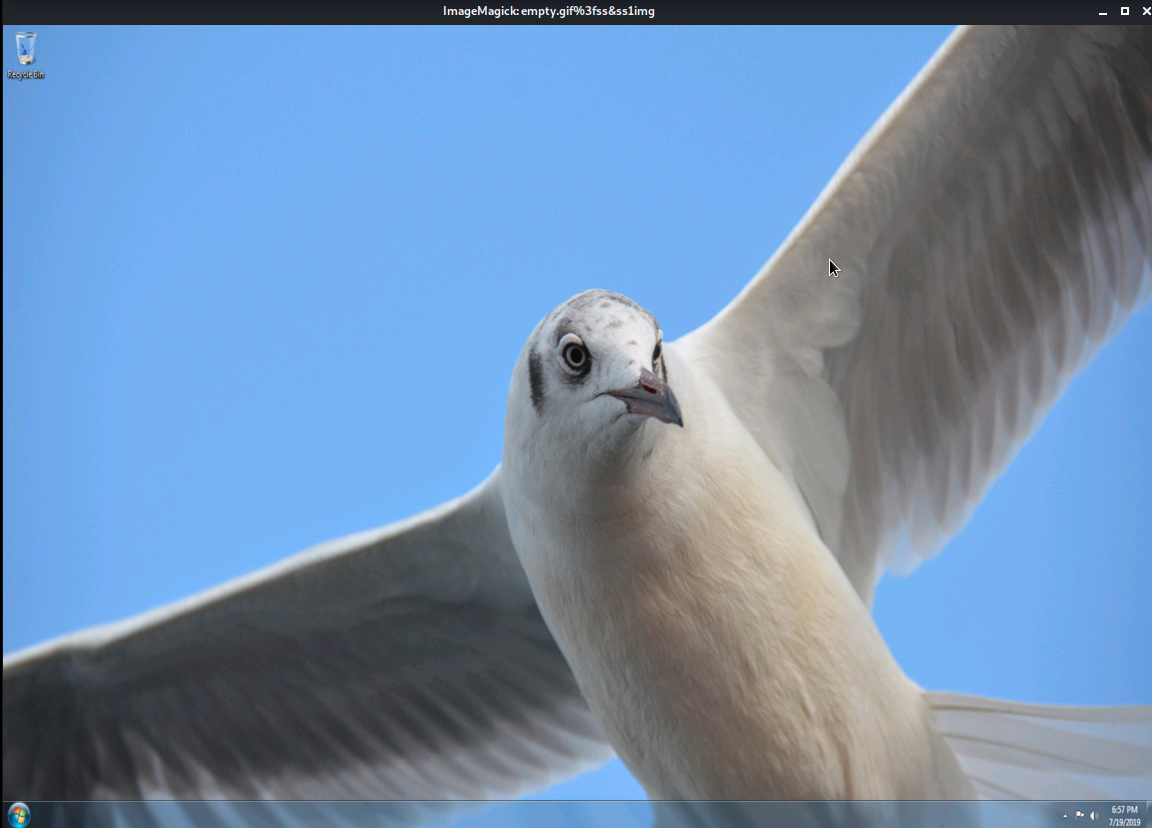
https://unit42.paloaltonetworks.com/using-wireshark-identifying-hosts-and-users/

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

172.16.4.205, 185.243.115.84, 166.62.111.64

Based off of conversation traffic (Statistics > Conversations)



1. Desktop background of the Windows host: 

## **Illegal Downloads**

IT was informed that some users were 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.

We isolated the torrent traffic to one machine here is what we concluded: a

IP address 10.0.0.201 was the perpetrator:

* + MAC address: 00:16:17:18:66:c8
  + Windows username: elmer.blanco
  + OS version: Windows 10

1. The torrent file downloaded by the user was:

The movie Betty Boop Rhythm on the Reservation

**Who did what for the Final Project (Slides and Report)**

We pretty much did everything as a team, I will say that everyone shared their expertise when needed and provided assistance and guidance to those who were struggling and had questions.

* Chris G focused on the Network Topology along with providing assistance and input on Offensive Operations including Target 2 and backoors.
* Chris D focused on Network Analysis including traffic profiles.
* Donathan focused on Network Analysis including normal behaviors.
* Heike focused on Defensive Operations including Hardening and Implementing the patches.
* Kyle focused on Offensive Operations including exploits used
* and stealth exploitation.
* John focused on Offensive Operations including Target 2.
* Michael focused on the Network Analysis & Critical Vulnerabilities.
* Mozamil focused on Defensive Operations including Hardening and Implementing the patches.
* Shea focused on developing the slides, report, keeping everyone on track, providing input for research of topics, Defensive Operations including alerts and providing a different perspective to the Network Topology.