# 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 question

s:

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

FRANK N TED

Used “ip.addr == 10.6.12.0/24 and dns” to find the custom site.

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

10.6.12.12

I used “ip.addr == 10.6.12.0/24 and dhcp” in order to find the Address of the Domain Controller.

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.

The malware that was downloaded was june11.dll. The Trojan downloaded is referred to as Trojan.GenericKD. I found this by applying the filter “ip.addr == 10.6.12.0/24 and http.request.method” then looking at a GET method with a file. Used file > export Objects > http > search “june11” to download the file.

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

This malware is classified as a Trojan because it contains a payload.

#### 

#### 

## 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: mind-hammer-dc.mind-hammer.net
   * IP address: 172.16.4.205
   * MAC address: (a4:ba:db:19:49:50)

Used “ip.addr == 172.16.4.0/24 and dns” and saw this was the machine sending alot of information off.

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

mathijs.devries

Used “Ip.addr == 172.16.4.0/24 and kerberos.CNameString”. I looked for an AS-Rep as that's where it would give me back a name. I looked through kerberos > as-rep > cname > cname-string then got the name from there.

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

172.16.4.205

166.62.111.64

185.243.115.84

Went to statistics > conversations. Then I sorted by bytes in order to see where the traffic was coming from.

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

empty.gif

Went to file > export object >https. Then I searched for the host b56 and looked for the trojan gif named empty.gif.

## 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 64 bit (hypertext Transfer Protocol > Get > user agent)
2. Which torrent file did the user download?

Betty Boop Rhythm on the Reservation

Went to file > export object >https. Then searched for torrent and found the one that was downloaded.