# **Network Analysis**

## Time Thieves

**(USED PCAP FILE FROM** [**http://tinyurl.com/yaajh8o8**](http://tinyurl.com/yaajh8o8)**)**

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?

Filter: ip.addr==10.6.12.0/24

FRANK-N-TED.COM

Graphical user interface, table

Description automatically generated with medium confidence

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

Filter: ip.addr==10.6.12.0/24

10.6.12.12 ……………Frank-n-Ted.com

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.

Filter : ip.addr==10.6.12.203 and http.request.method==GET

Export File > Export Object >HTTP

A screenshot of a computer

Description automatically generated

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

The malware is classified as TROJAN

#### A screenshot of a computer Description automatically generated

#### 

#### 

## 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

A screenshot of a computer

Description automatically generated

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



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

166.62.111.64

185.243.115.84

172.16.4.205

Graphical user interface, application, table, Excel

Description automatically generated

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

On the packet I followed the steps FILE -> EXPORT OBJECTS -> HTTP -> SEARCH FOR IMG (IMAGE FILES

Found the image below with recycle icon on desktop and the taskbar with date and time

A screenshot of a computer

Description automatically generated with medium confidence

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: 00:16:17:66:c8
   * Windows username: elmer.blanco
   * OS version: windows 10 64bit

Graphical user interface

Description automatically generated with medium confidence

Used filter: http.request and !(ssdp)

A screenshot of a computer

Description automatically generated with medium confidence

1. Which torrent file did the user download?

[Full request URI: http://www.publicdomaintorrents.com/bt/btdownload.php?type=torrent&file=Betty\_Boop\_Rhythm\_on\_the\_Reservation.avi.torrent]

Filter: ip.addr==10.0.0.201 and (http.request.full\_uri contains ".torrent")

Text

Description automatically generated