**Network Analysis**

**Wireshark Strikes Back**

Nicole kemp

23/05/22

Instructor: Barry

Class: MONU-VIRT-CYBER-PT-11-2021-U-C

Activity File: Wireshark Strikes Back

**Table of Contents**

[**Prompt:** 3](#_Toc104236534)

[**Instructions:** 3](#_Toc104236535)

[**Time Thieves:** 4](#_Toc104236536)

[**Vulnerable Windows Machines:** 6](#_Toc104236537)

[**Illegal Downloads:** 8](#_Toc104236538)

## **Prompt:**

You are working as a Security Engineer for X-CORP, supporting the SOC infrastructure. The SOC analysts have noticed some discrepancies with alerting in the Kibana system and the manager has asked the Security Engineering team to investigate.

Yesterday, your team confirmed that newly created alerts are working. Today, you will monitor live traffic on the wire to detect any abnormalities that aren't reflected in the alerting system.

You are to report back all your findings to both the SOC manager and the Engineering Manager with appropriate analysis.

Fill out the Network Report Template as you progress through this activity.

## **Instructions:**

Connect to your Kali VM, launch Wireshark, and begin capturing on the `eth0` interface using the steps above. Let the capture run for at least fifteen minutes and then stop it. As your capture runs, read the following overview:

* The Security team requested this analysis because they have evidence that people are misusing the network. Specifically, they've received tips about
* "Time thieves" spotted watching YouTube during work hours.
* At least one Windows host infected with a virus.
* Illegal downloads.
* A number of machines from foreign subnets are sending traffic to this network. Therefore, you will see many IP ranges in your capture.
* Your task is to collect evidence confirming the Security team's intelligence.
* Be sure to use display filters. In addition, be sure to record your work by adding comments to packets as you go.
* For example, if you find a packet containing a username of interest, comment on the packet: `Illegal Downloads: Contains Windows username`.
* Record your answers in the following Google Doc. This file will be submitted as a deliverable at the end of the project. You must make a copy of this file to edit it.
* Network Analysis Report Template

## **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:

Following Wireshark Filters were Used:

* **Domain of the custom site**: ip.addr == 10.6.12.0/24
* **Traffic Inspection**: ip.addr == 10.6.12.12
* **Other Traffic Inspection**: ip.addr == 10.6.12.203
* **Malware Name:** ip.addr == 10.6.12.203 and http.request.method == GET

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

* **Domain Name:** Frank-n-Ted-DC. frank-n-ted.com
* **Dest IP:** 10.6.12.12
* **Wireshark Filter:** ip.src==10.6.12.0/24
* (**Screenshot)**: The domain name

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

* **IP Address:** 10.6.12.12 (Frank-n-Ted-DC.frank-n-ted.com)
* **Wireshark Filter**: ip.src==10.6.12.0/24
* (**Screenshot)**: The Domain Controller (DC) of the AD network)

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.

* **Malware file name:** june11.dll
* **Wireshark Filter**: ip.addr == 10.6.12.0/24 and http.request.method == GET
* (**screenshot**): Malware Downloaded to the 10.6.12.203 machine

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

Exporting file to Kali:

* Open File Tab
* Export Objects, Select HTTP
* Filter “\*.dll”
* Save june.dll
* Upload to VirusTotal.com
* (Screenshot)

1. What kind of malware is this classified as?

* The Trojan name is: Trojan.Mint.Zamg.O
* SHA256: d363666666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec
* Googleipdate.exe
* Detection ratio: 49/72
* (Screenshot)

## **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.

Following Wireshark Filters were Used:

* **Host name:** ip.addr == 172.16.4.0/24
* **IP address:** ip.src == 172.16.4.4 && kerberos.CnameString
* **Username:** ip.src == 172.16.4.205 && kerberos.CnameString
* **MAC address:** ip.addr == 172.16.4.205 && ip.addr == 185.243.115.84

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
* **Wireshark Filter:** ip.addr == 172.16.4.0/24

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

* **Username:** matthijs.devries
* **Wireshark Filter:** ip.src==172.16.4.205 && kerberos.CNameString

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

* Filter: ip.src==172.16.4.203 and kerberos.CNameString
* I found 4 IP addresses: 172.16.4.205, 185.243.115.84, 166.62.11.64 and 23.43.62.169
* Finding the IP addresses:
* Click on the Statistics Tab
* Select the Conversation
* Select the IPv4
* Sort Packets high to low
* Additional Traffic from 185.243.115.84 to infected host 172.16.4.205

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

## **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.

Following Wireshark Filters were Used:

* **MAC Address:** ip.addr == 10.0.0.201 && dhcp
* **Username**: ip.src == 10.0.0.201 && kerberos.CnameString
* **Operating System**: ip.addr == 10.0.0.201 && http.request
* **Torrent Download:** ip.addr == 10.0.0.201 && http.request.method == "GET"

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:** BLANCO-DESKTOP Windows NT 10.0
* **Wireshark Filter for MAC Address:** ip.addr == 10.0.0.201 && dhcp
* **Wireshark Filter for Username:** ip.addr == 10.0.0.201 && kerberos.CnameString
* **Wireshark Filter for OS Type and Version:** ip.addr == 10.0.0.201 && http.request

1. Which torrent file did the user download?

There were few that were downloaded, but below clip was show with the name:

* Betty\_Boop\_Rhythm\_on\_the\_Reservation.avi.torrent
* **Wireshark Filter**: ip.addr == 10.0.0.201 && http.request.method == "GET"

Finding the torrent:

* Apply the Wireshark Filter above.
* Sort the packets by the Destination files.publicdomaintorrents.com (168.215.194.14).
* Look for Download requests.
* Movie Downloaded was Betty Boop Rhythm on the Reservation.avi