Network Analysis Report

Overview

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.

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.

Following Wireshark Filters were Used:

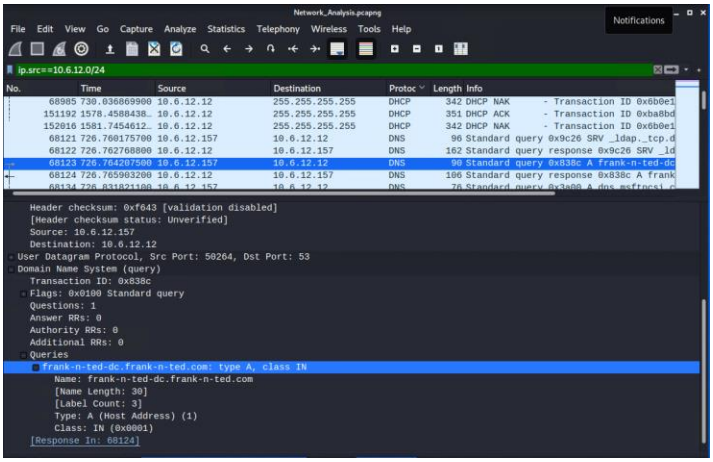
- Domain of the custom site: ip.addr == 10.6.12.0/24
- Traffic Inspection: ip.addr == 10.6.12.12
- Other Traffic Inspection: ip.addr == 10.6.12.203
- Malware Name: ip.addr == 10.6.12.203 and http.request.method == GET

Network Analysis Report

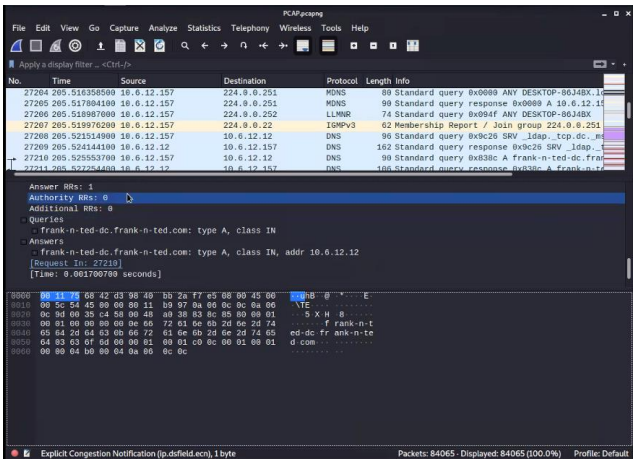
Following Wireshark filter

You must inspect your traffic capture to answer the following questions:

1. What is the domain name of the users' custom site?
    - Domain Name: Fank-nTed-DC. Farnk-n-ted.com
    - Wireshark Filter: ip.src==10.6.12.0/24



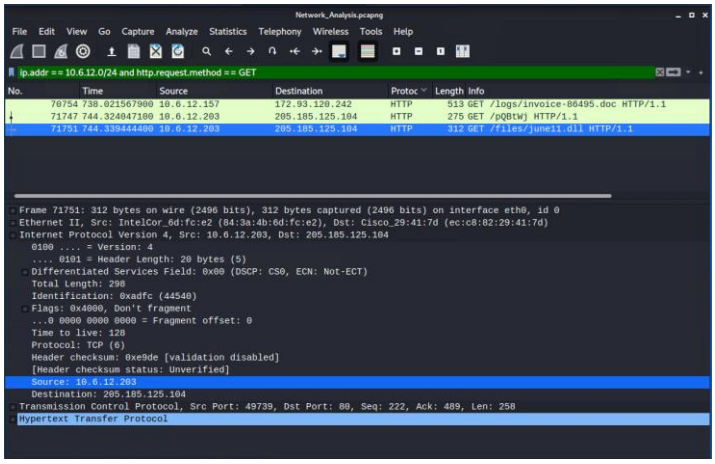
2. What is the IP address of the Domain Controller (DC) of the AD network?
    - Domain Name: 10.6.12.12 (Frank-n-Ted-DC.frank-n-ted.com)
    - Wireshark Filter: ip.src==10.6.12.0/24



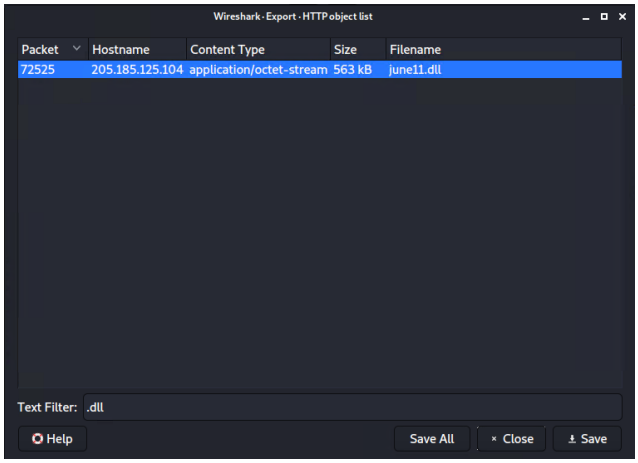
Network Analysis Report

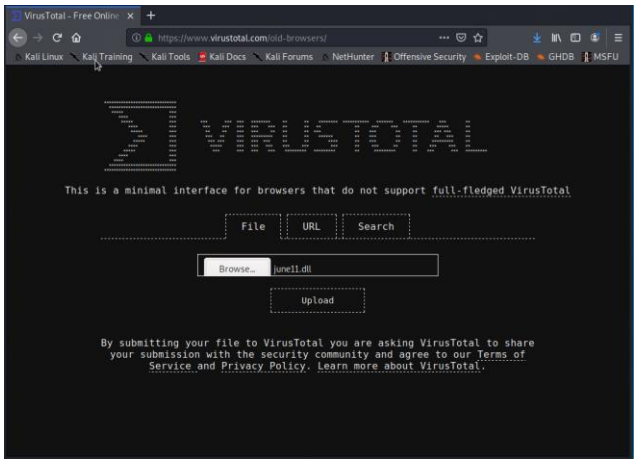
3. What is the name of the malware downloaded to the 10.6.12.203 machine? Once you have found the file, export it to your Kali machine's desktop.

- Wireshark Filter: Wireshark Filter: ip.addr == 10.6.12.0/24 and http.request.method == GET
- Malware file name: june11.dll



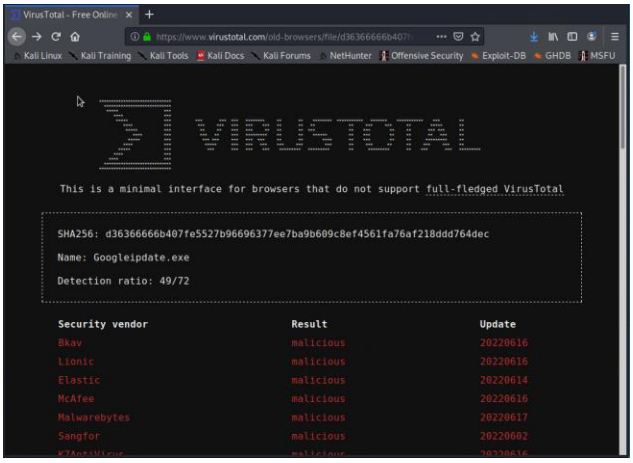
4. Upload the file to VirusTotal.com





Network Analysis Report

5. What kind of malware is this classified a
    - Malicious



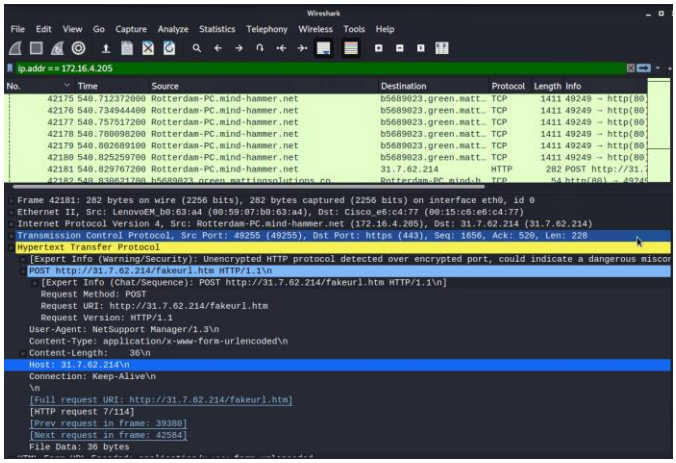
Vulnerable Windows Machines

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.

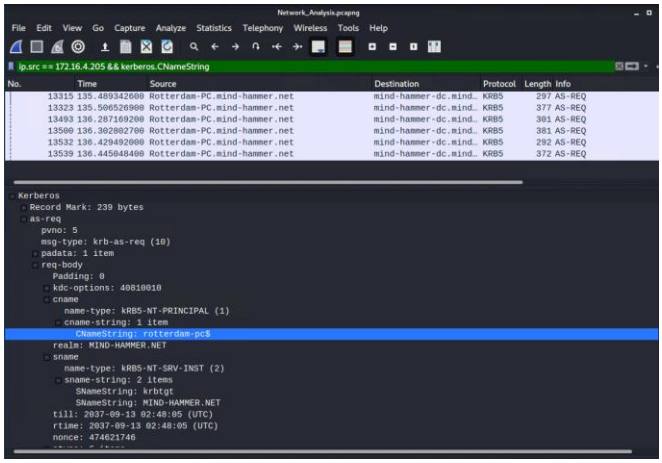
Inspect your traffic to answer the following questions:

1. Find the following information about the infected Windows machine:
    - Host name: ROTTERDAM-PC.minder-hammer.net
    - IP address: 172.16.4.205
    - MAC address: 00:59:07:b0:63:a4
    - Wireshark Filter: ip.addr == 172.16.4.0/24



Network Analysis Report

2. What is the username of the Windows user whose computer is infected?
    - Username: krbtgt
    - Wireshark Filter: ip.src==172.16.4.205 && kerberos.CNameString



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

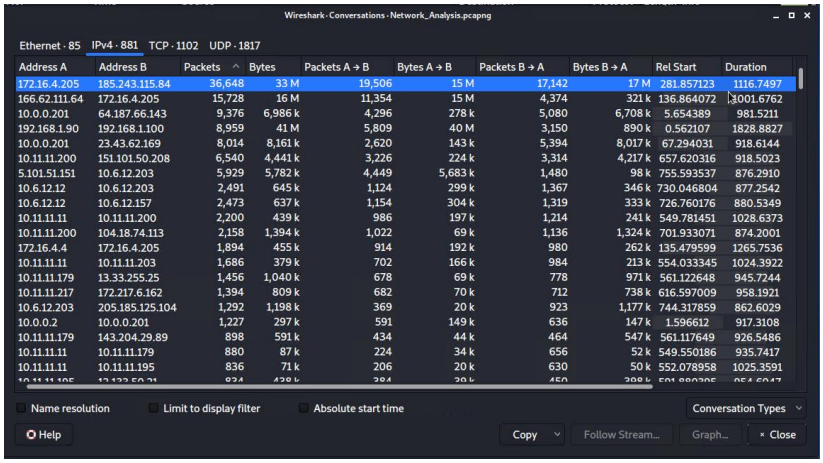
- Filter: ip.src==172.16.4.203 and kerberos.CNameString
- I found 4 IP addresses: 172.16.4.205, 185.243.115.84, 166.62.11.64 and 23.43.62.169
- Finding the IP addresses:

  Click on the Statistics Tab

  Select the Conversation

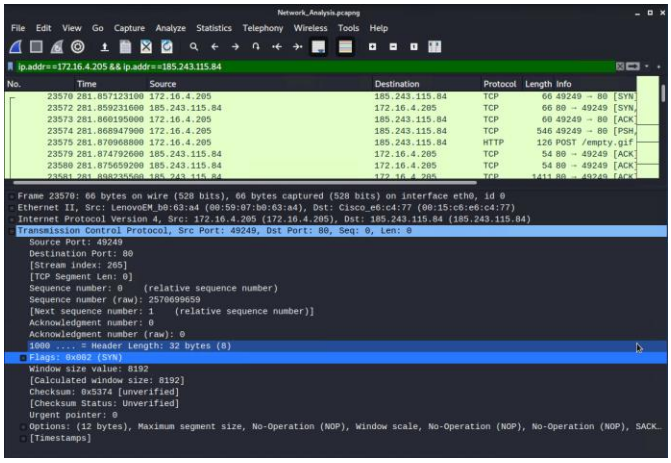
  Select the IPv4 Sort

  Packets high to low



- Additional Traffic from 185.243.115.84 to infected host 17216.4.205

Network Analysis Report



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