

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:

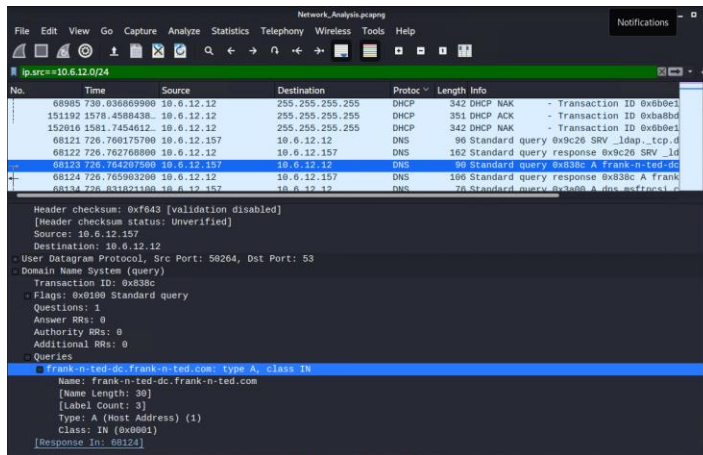
- Domain of the custom site: `ip.addr == 10.6.12.0/24`
- Traffic Inspection: `ip.addr == 10.6.12.12`
- Other Traffic Inspection: `ip.addr == 10.6.12.203`
- Malware Name: `ip.addr == 10.6.12.203 and http.request.method == GET`

Network Analysis Report

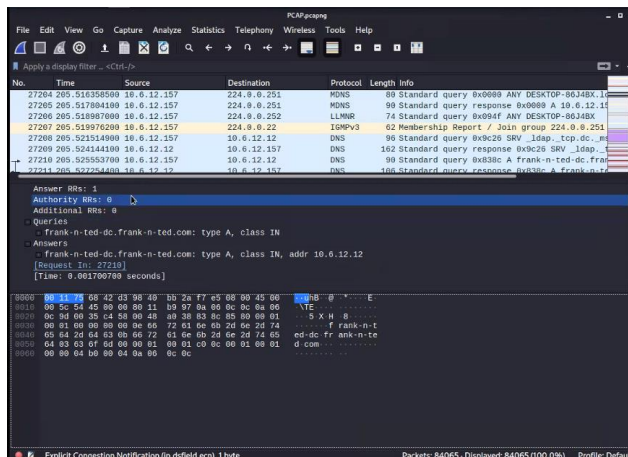
Following Wireshark filter

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

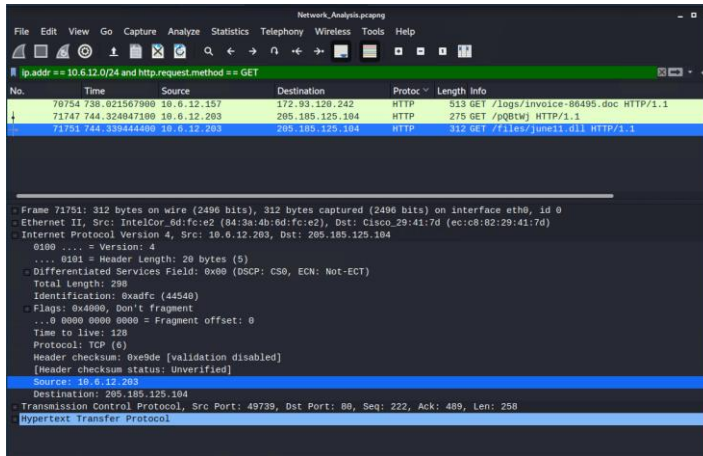


2. What is the IP address of the Domain Controller (DC) of the AD network?
 - Domain Name: 10.6.12.12 (Frank-n-Ted-DC.frank-n-ted.com)
 - Wireshark Filter: ip.src==10.6.12.0/24

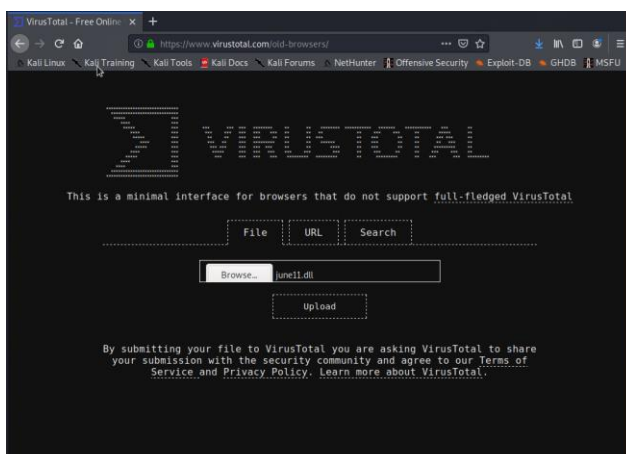
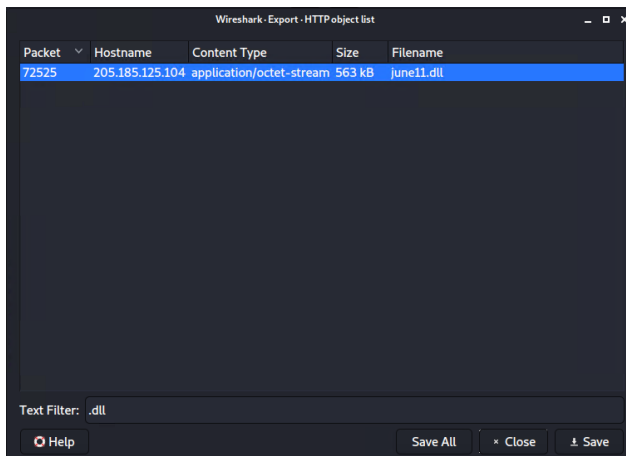


Network Analysis Report

- 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



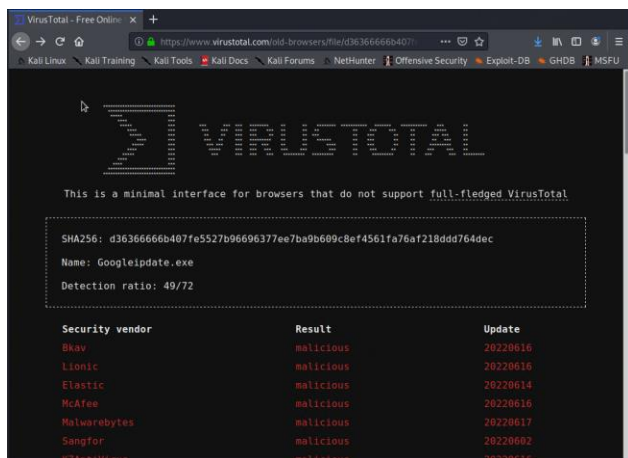
- Upload the file to [VirusTotal.com](https://www.virustotal.com)



Network Analysis Report

5. What kind of malware is this classified a

- Malicious



Vulnerable Windows Machines

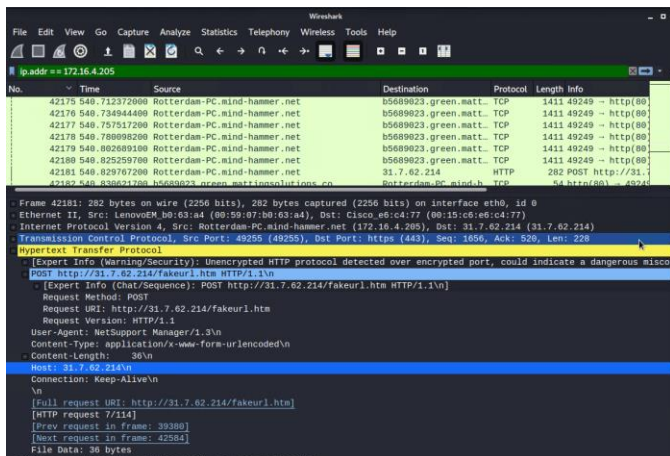
The Security team received reports of an infected Windows host on the network. They know the following:

- 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:

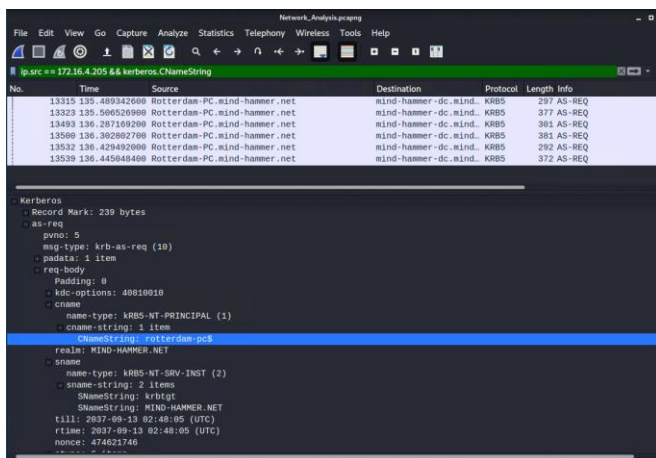
- Host name: ROTTERDAM-PC.minder-hammer.net
- IP address: 172.16.4.205
- MAC address: 00:59:07:b0:63:a4
- Wireshark Filter: ip.addr == 172.16.4.0/24



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

Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel. Start	Duration
172.16.4.205	185.243.115.84	36,648	33 M	19,506	15 M	17,142	17 M	281.857123	1116.7497
166.62.111.64	172.16.4.205	15,728	16 M	11,354	15 M	4,374	321 k	136.864072	3001.6762
10.0.0.201	64.187.66.143	9,376	6,986 k	4,296	278 k	5,080	6,708 k	5.654389	981.5211
192.168.1.90	192.168.1.100	8,959	41 M	5,809	40 M	3,150	890 k	0.852107	1838.8827
10.0.0.201	23.43.62.169	8,014	8,161 k	2,620	143 k	5,394	8,017 k	67.294031	918.6144
10.11.11.200	151.101.50.208	6,540	4,441 k	3,226	224 k	3,314	4,217 k	657.620316	918.5023
5.101.51.151	10.6.12.203	5,929	5,782 k	4,449	5,683 k	1,480	98 k	755.593537	876.2910
10.6.12.12	10.6.12.203	2,491	645 k	1,124	299 k	1,367	346 k	730.046804	877.2542
10.6.12.12	10.6.12.157	2,473	637 k	1,154	304 k	1,319	333 k	726.760176	880.5349
10.11.11.11	10.11.11.200	2,200	439 k	986	197 k	1,214	241 k	549.781451	1028.6373
10.11.11.200	104.18.74.113	2,158	1,394 k	1,022	69 k	1,136	1,324 k	701.933071	874.2001
172.16.4.4	172.16.4.205	1,894	455 k	914	192 k	980	262 k	135.479599	1265.7536
10.11.11.11	10.11.11.203	1,686	379 k	702	166 k	984	213 k	554.033345	1024.3922
10.11.11.179	13.33.255.25	1,456	1,040 k	678	69 k	778	971 k	561.122648	945.7244
10.11.11.217	172.217.6.162	1,394	809 k	682	70 k	712	738 k	616.597009	958.1921
10.6.12.203	205.185.125.104	1,292	1,198 k	369	20 k	923	1,177 k	744.317859	862.6029
10.0.0.2	10.0.0.201	1,227	297 k	591	149 k	636	147 k	1.596612	917.3108
10.11.11.179	143.204.29.89	898	591 k	434	44 k	464	547 k	561.117649	926.5486
10.11.11.11	10.11.11.179	880	87 k	224	34 k	656	52 k	549.550186	935.7417
10.11.11.11	10.11.11.195	836	71 k	206	20 k	630	50 k	552.078958	1025.3591
10.11.11.11	10.11.11.195	824	420 k	204	20 k	620	300 k	552.078958	1025.3591

- Additional Traffic from 185.243.115.84 to infected host 172.16.4.205

Network Analysis Report

The image shows the Wireshark network analysis tool interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The main display area is divided into three panes. The top pane shows a list of captured packets with columns for No., Time, Source, Destination, Protocol, Length, and Info. The middle pane shows the details of the selected packet (No. 23579), including Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol (TCP). The bottom pane shows the raw packet data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
23579	281.657123100	172.16.4.205	185.243.115.84	TCP	60	49249 → 80 [SYN]
23572	281.859231600	185.243.115.84	172.16.4.205	TCP	60	80 → 49249 [SYN]
23573	281.860195000	172.16.4.205	185.243.115.84	TCP	60	49249 → 80 [ACK]
23574	281.860947000	172.16.4.205	185.243.115.84	TCP	546	49249 → 80 [PSH]
23575	281.870968000	172.16.4.205	185.243.115.84	HTTP	126	POST /empty.gif
23579	281.874792600	185.243.115.84	172.16.4.205	TCP	54	80 → 49249 [ACK]
23580	281.875659200	185.243.115.84	172.16.4.205	TCP	54	80 → 49249 [ACK]
23581	281.880235000	185.243.115.84	172.16.4.205	TCP	54	80 → 49249 [ACK]

Frame 23579: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface eth0, id 0
Ethernet II, Src: lenovoM-b0:63:a4 (08:59:87:b0:63:a4), Dst: Cisco-e6:c4:77 (08:15:c5:e6:c4:77)
Internet Protocol Version 4, Src: 172.16.4.205 (172.16.4.205), Dst: 185.243.115.84 (185.243.115.84)
Transmission Control Protocol, Src Port: 49249, Dst Port: 80, Seq: 0, Len: 0
Source Port: 49249
Destination Port: 80
[Stream index: 265]
[TCP Segment Len: 0]
Sequence number: 0 (relative sequence number)
Sequence number (raw): 2570699659
Next sequence number: 1 (relative sequence number)
Acknowledgment number: 0
Acknowledgment number (raw): 0
1000 = Header length: 32 bytes (8)
Flags: 0x002 [SYN]
Window size value: 8192
[Calculated window size: 8192]
Checksum: 0x5374 [unverified]
[Checksum status: Unverified]
Urgent pointer: 0
Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP), No-Operation (NOP), SACK, Timestamps

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

