Final Engagement

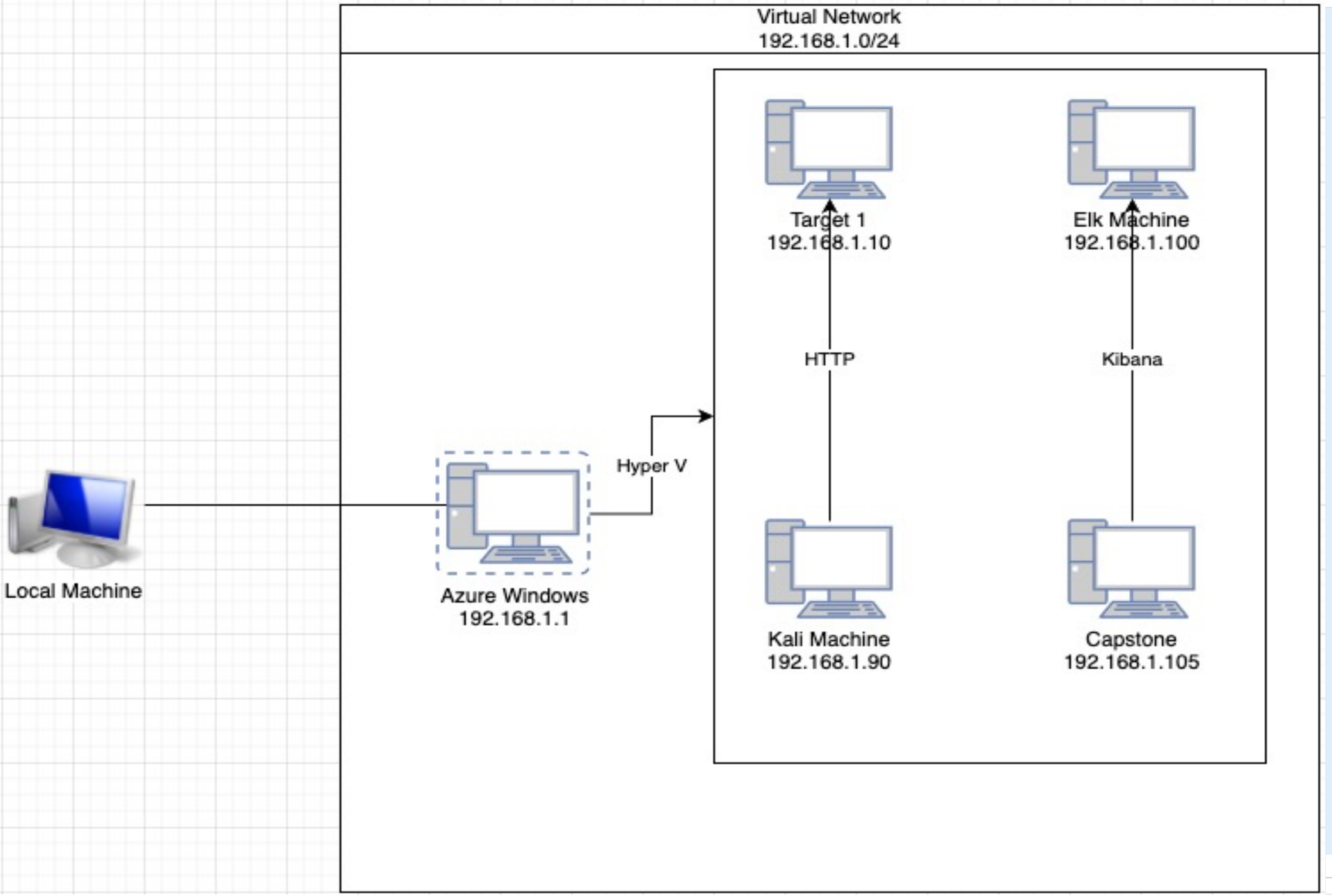
Attack, Defense & Analysis of a Vulnerable Network

Table of Contents

This document contains the following resources:

Network Topology
& Critical Vulnerabilities

Network Topology



Network
Address Range: 192.168.1.0/24
Netmask: 255.255.255.0
Gateway: 192.168.1.1

Machines
IPv4: 192.168.1.1
OS: Windows
Hostname: ML-RefV-68 4427

IPv4: 192.168.1.90
OS: Kali Linux
Hostname: Kali

IPv4: 192.168.1.110
OS: Ubuntu
Hostname: Target 1

IPv4: 192.168.105
OS: Ubuntu
Hostname: Capstone

Traffic Profile

Traffic Profile

Our analysis identified the following characteristics of the traffic on the network:

Feature	Value	Description
Top Talkers (IP Addresses)	*172.16.4.205*	*Machines that sent the most traffic.*
Most Common Protocols	*HTTP, TCP, UDP*	*Three most common protocols on the network.*
# of Unique IP Addresses	*122,537*	*Count of observed IP addresses.*
Subnets	*172.16.4.0/24*	*Observed subnet ranges.*
# of Malware Species	*Trojan (june11.dll)*	*Number of malware binaries identified in traffic.*

Behavioral Analysis

Purpose of Traffic on the Network

Users were observed engaging in the following kinds of activity.

“Normal” Activity

- *Watching Youtube*
- *Downloading torrents for legit reasons such as operating systems*

Suspicious Activity

- *Created own web server (frank - n ted.com)*
- *Downloading malware (june11.dll)*
- *Downloading torrents*

Normal Activity

[Name of Normal Behavior 1]

Summarize the following:

- *What kind of traffic did you observe? HTTP Traffic*
- *What, specifically, was the user doing? Watching YouTube*

Downloading Torrents for Legitimate Purposes

Summarize the following:

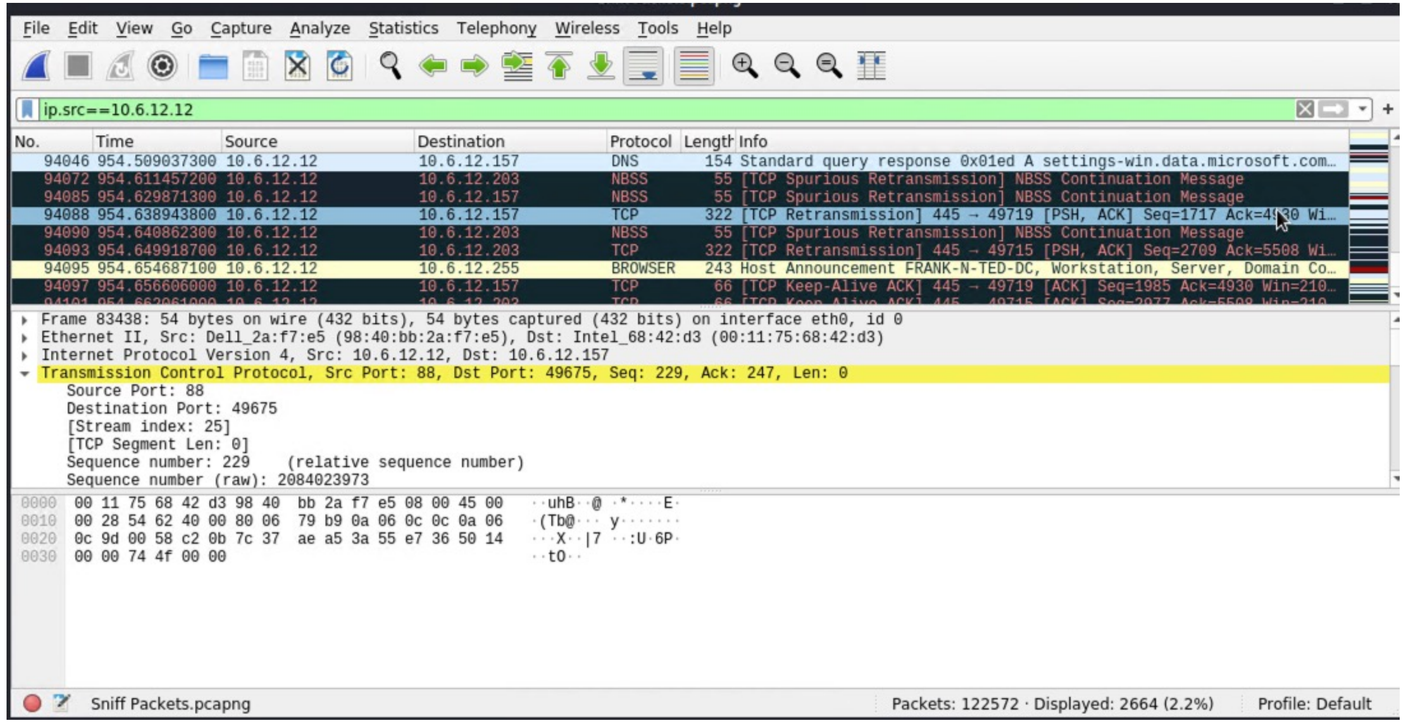
- *What kind of traffic did you observe? HTTP Traffic*
- *What, specifically, was the user doing? Downloading torrents for legit purposes*

Malicious Activity

Watching YouTube on their Own Webserver

Summarize the following:

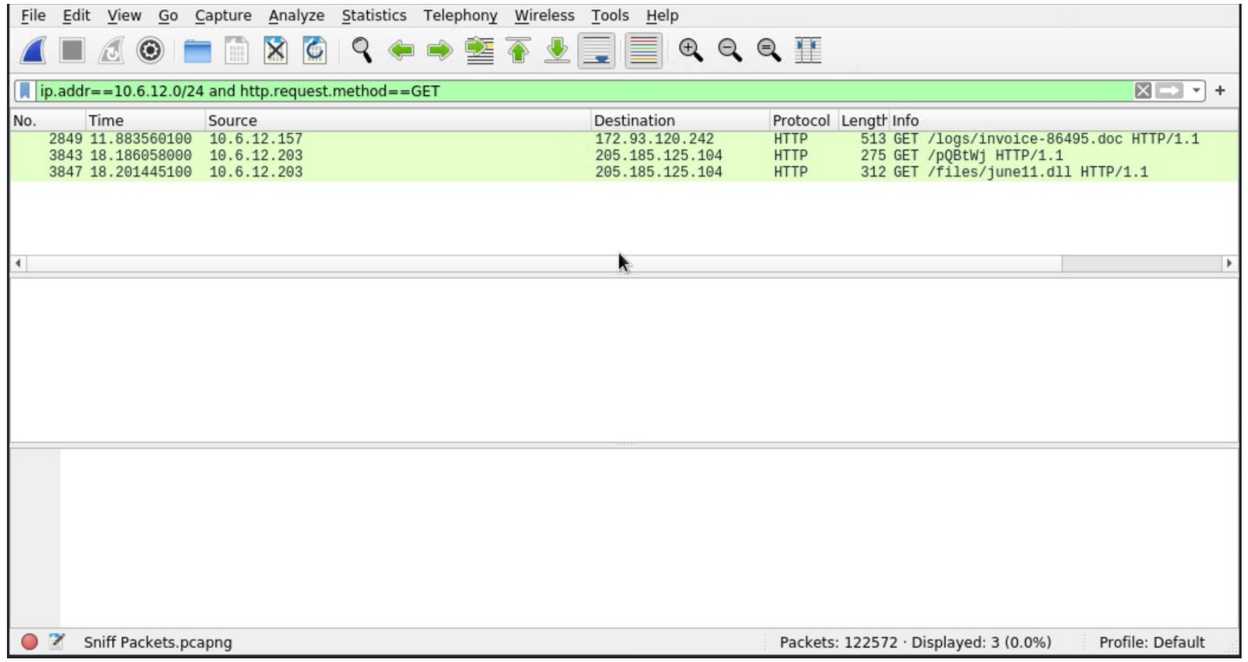
- What kind of traffic did you observe? Which protocol(s)?HTTP
- What, specifically, was the user doing? Created their own webserver on the corporate network

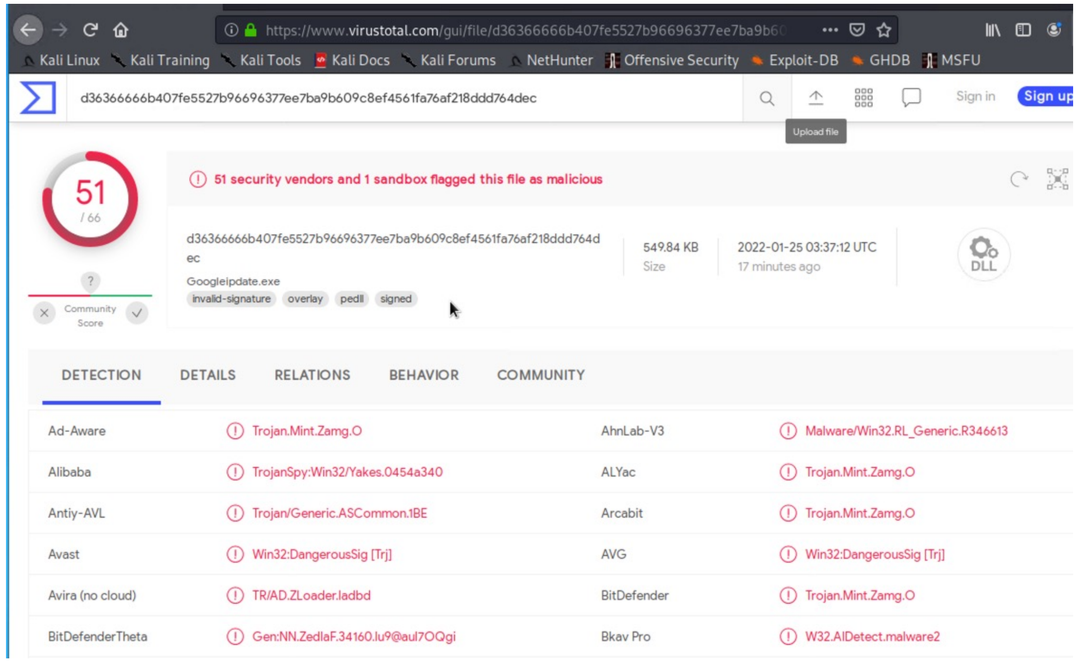


Downloading Malware

Summarize the following:

- *What kind of traffic did you observe? Which protocol(s)? HTTP Traffic*
- *What, specifically, was the user doing? Which site were they browsing? They were downloading malware specifically a trojan june11.dll. Seems like they were just browsing the internet*
- *Include a description of any interesting files. See june11.dll*





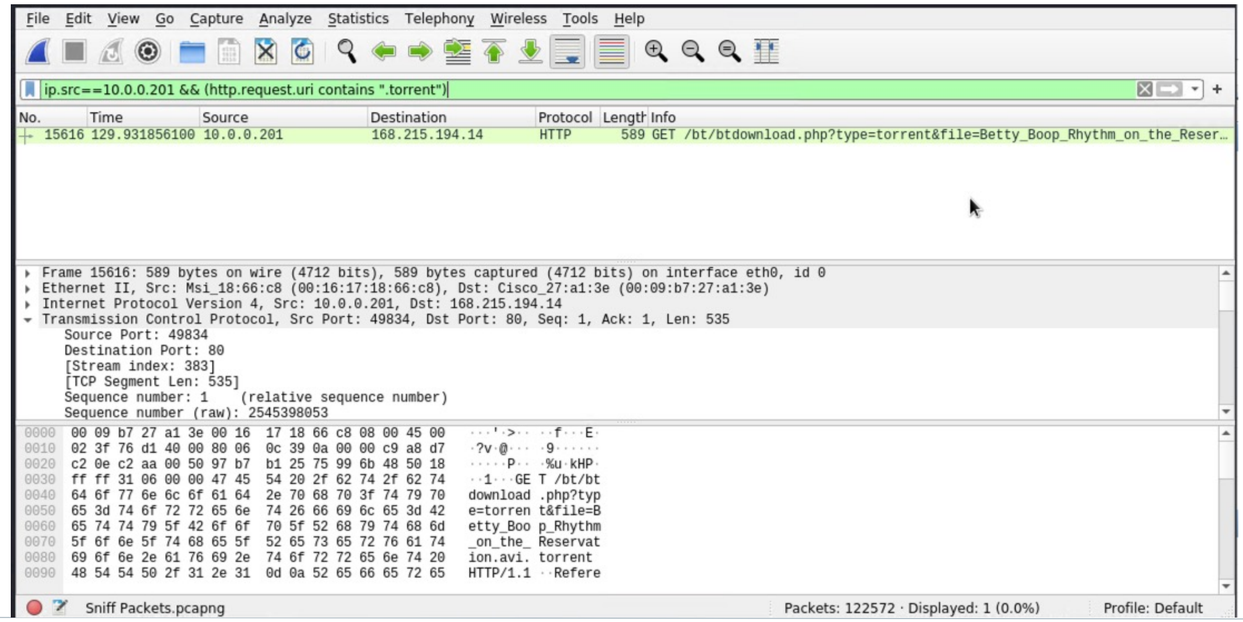
Illegal Downloads on Windows Machine

Summarize the following:

- What kind of traffic did you observe? Which protocol(s)?HTTP

  What, specifically, was the user doing?

  - Created their own AD domain that is named DogOfTheYear-DC
  - Were downloading torrents for copyright infringement.
  - Downloaded torrent file Betty_Boop_Rhythm_on_the_Reservation.avi.torrent



The End