Final Engagement

Attack, Defense & Analysis of a Vulnerable Network

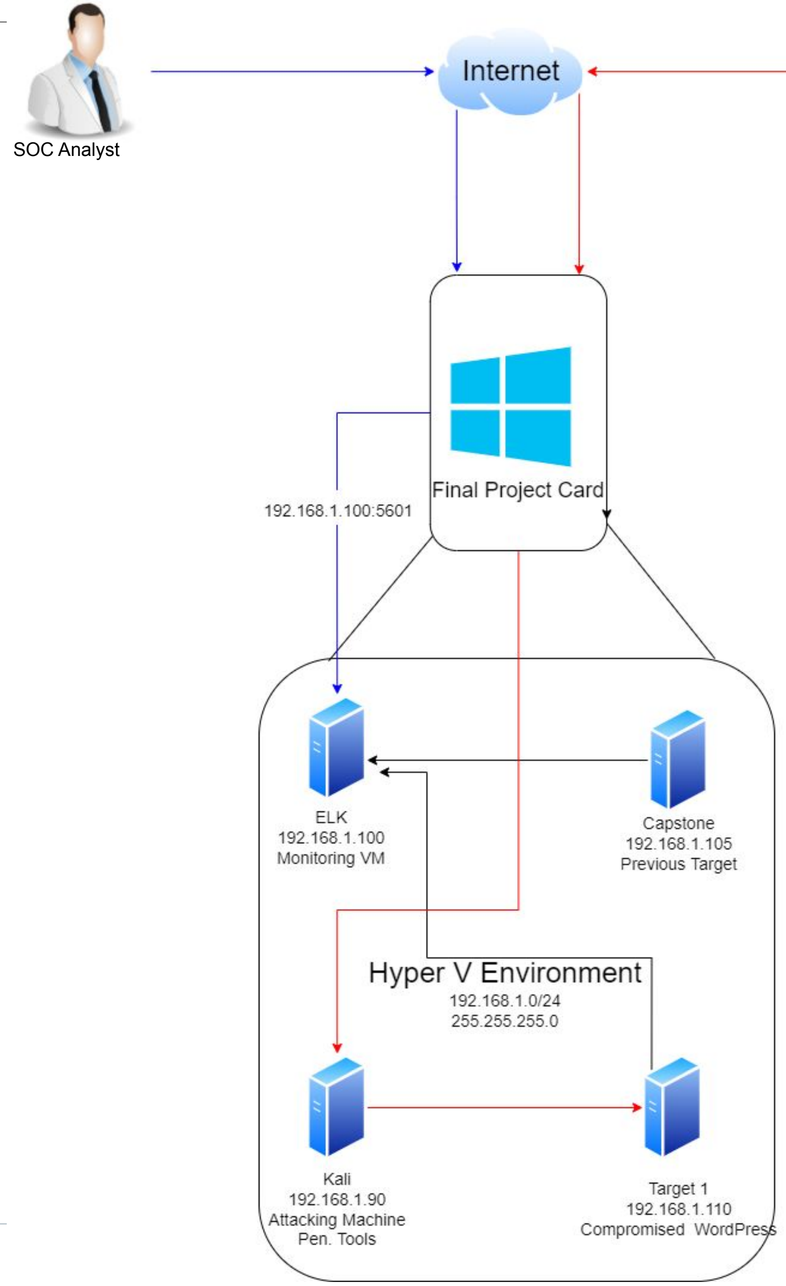
Chad Atkinson
Rick Baird
Kyle Barnes
Mike Powell
Dallin White

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
IPv4:192.168.1.100
OS:Linux
Hostname:Kibana

IPv4:192.168.1.90
OS:Linux
Hostname:Kali

IPv4:192.168.1.110
OS:Linux
Hostname:Target 1

IPv4:192.168.1.105
OS:Linux
Hostname:Capstone

Critical Vulnerabilities: Target 1

Our assessment uncovered the following critical vulnerabilities in **Target 1**.

Vulnerability	Description	Impact
Open Access to ports	port 22 and port 80 both open and easy to access	Vulnerable to Brute force attacks
Enumerating usernames in Wordpress	Easy to find usernames to use to exploit	Able to find usernames makes easy access for attackers
Simple Passwords	Passwords are not following good password qualities	Easiest way to get in by brute forcing or being guessed
Root vulnerability with Python	Vulnerable to a local user attack using a Python script	Can gain full administrative access

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 (51364 packets) 185.243.115.84 (30344 packets) 10.0.0.201 (19503 packets)	Machines that sent the most traffic.
Most Common Protocols	Transmission Control Protocol (TCP) (92280 packets) User Datagram Protocol (UDP) (11697 packets) HTTP (2848 Packets)	Most common protocols on the network.
# of Unique IP Addresses	808 unique addresses	Count of observed IP addresses.
Subnets	10.11.11.0/24, 10.6.12.0/24, 172.217.9.0/24, 172.217.12.0/24, 204.3.251.0/24, 205.251.12.0/24	Observed subnet ranges.
# of Malware Species	2 (spyware, command and control)	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

- Normal activity included activities like shopping, reading news articles and light browsing on instagram

Suspicious Activity

- We found a number of suspicious activities on the Network, Signs of malware and malicious downloads causing the network to become vulnerable. Also it was found that a youtube channel was being hosted on the network

Normal Activity

Normal Behavior - Wireshark

- What kind of traffic did you observe? Which protocol(s)?
  - **TLSv1.2-3** (Transport Layer Security)

    Which is the newest SSL protocol that implements the SHA-256 hash to better protect the integrity of the data.
  - **DNS** (Domain Name System)
  - **LDAP** (Lightweight Directory Access Protocol)

- What, specifically, was the user doing? Which site were they browsing? Etc.

  The LDAP traffic shows persons in the network moving about throughout the file system and other resources. We can see some websites accessed like bing.com and skype with DNS. The TLS just shows encrypted data being moved between different parts of the network. Here are some snippets of the packets themselves.

```
57631 2020-06-30 10:04:31.596263800 10.6.12.203      10.6.12.12      DNS       81 Standard query 0x7d86 A config.edge.skype.com
57458 2020-06-30 10:04:30.819530200 10.6.12.203      10.6.12.12      DNS       72 Standard query 0xf54e A www.bing.com
58550 2020-06-30 10:04:38.670118300 10.6.12.157      10.6.12.12      LDAP      404 searchRequest(1) "<ROOT>" baseObject
65261 2020-06-30 10:06:03.955991000 52.114.74.45     10.6.12.203     TLSv1.2   411 Application Data
```

Normal Behavior Continued…

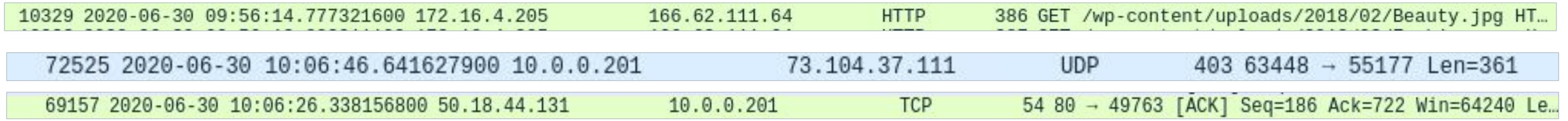
Summarize the following:

- What kind of traffic did you observe? Which protocol(s)?
  - **HTTP** (Hypertext Transfer Protocol)
  - **UDP** (User Datagram Protocol)

    Connectionless, meaning it will send the information even if the whole thing isn't being received.
  - **TCP** (Transmission Control Protocol)

    Uses the 3 Way Handshake to establish connections beforehand.
- What, specifically, was the user doing? Which site were they browsing? Etc.

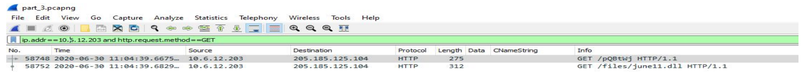
  Looking at HTTP we found some users downloading simple files and photos like the Beauty.jpg. We see talk with UDP moving between ports 63448 to 55177. As well as a good amount of TCP communication with the 3 way handshake from port 80 (as seen below).



Malicious Activity

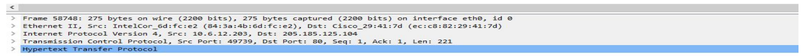
Trojan Horse (Zloader)

Summarize the following: Frank-n-ted.com(10.6.12.20) file was downloaded that was malicious

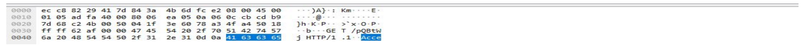


User was trying to download a file when file was downloaded

it was malware and corrupted users machine

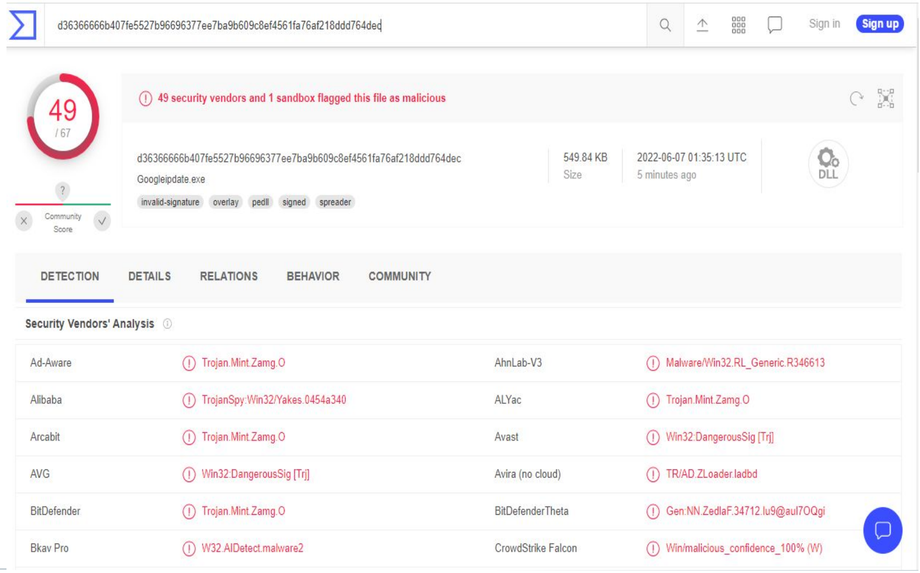


frank-n-ted.com (10.6.12.203) downloaded a file malicious file from 205.185.125.104



Saw that malicious file June11.dll was downloaded to

Machine 10.6.12.203



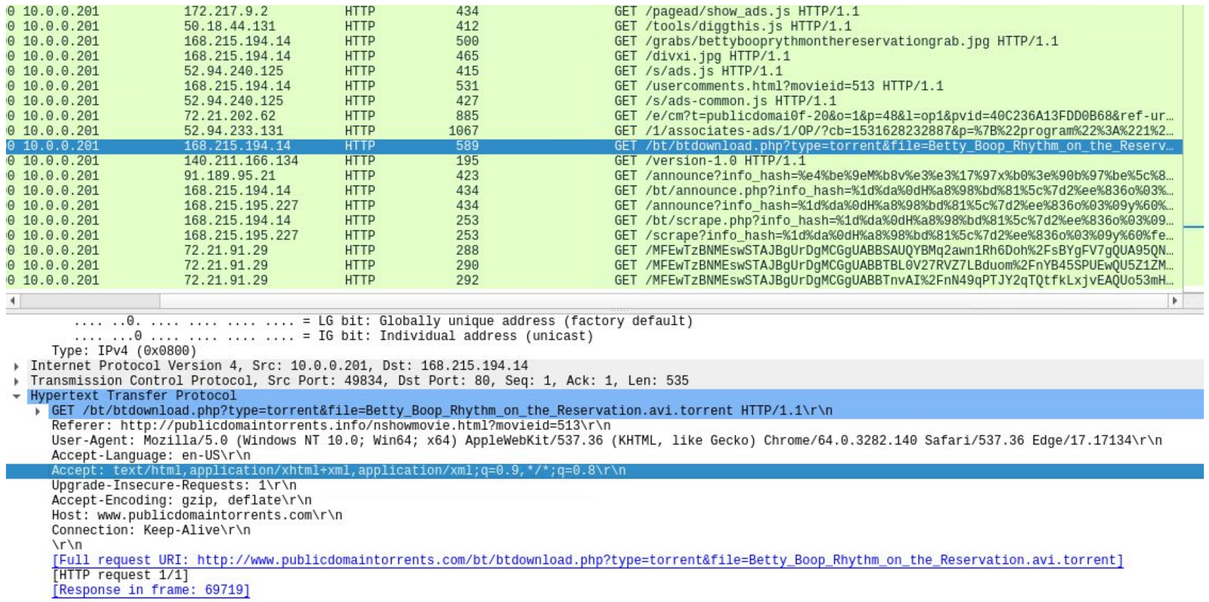
When we export the file with wireshark and

Identify it we see it is classified as a trojan

Illegal Torrent Download

Summarize the following:

- We noticed a user visiting many suspicious websites and downloading .jpg and .gif files
- The user visited a site http://public domianstorrents.info/grabs/bettybooprythmonthereservationgrab.jpg to download a photo, this ended up being a torrent file



(Look of Disapproval)

The End