

Final Engagement

Attack, Defense & Analysis of a Vulnerable Network

Table of Contents

This document contains the following resources:



Network Topology & Critical Vulnerabilities



Traffic Profile



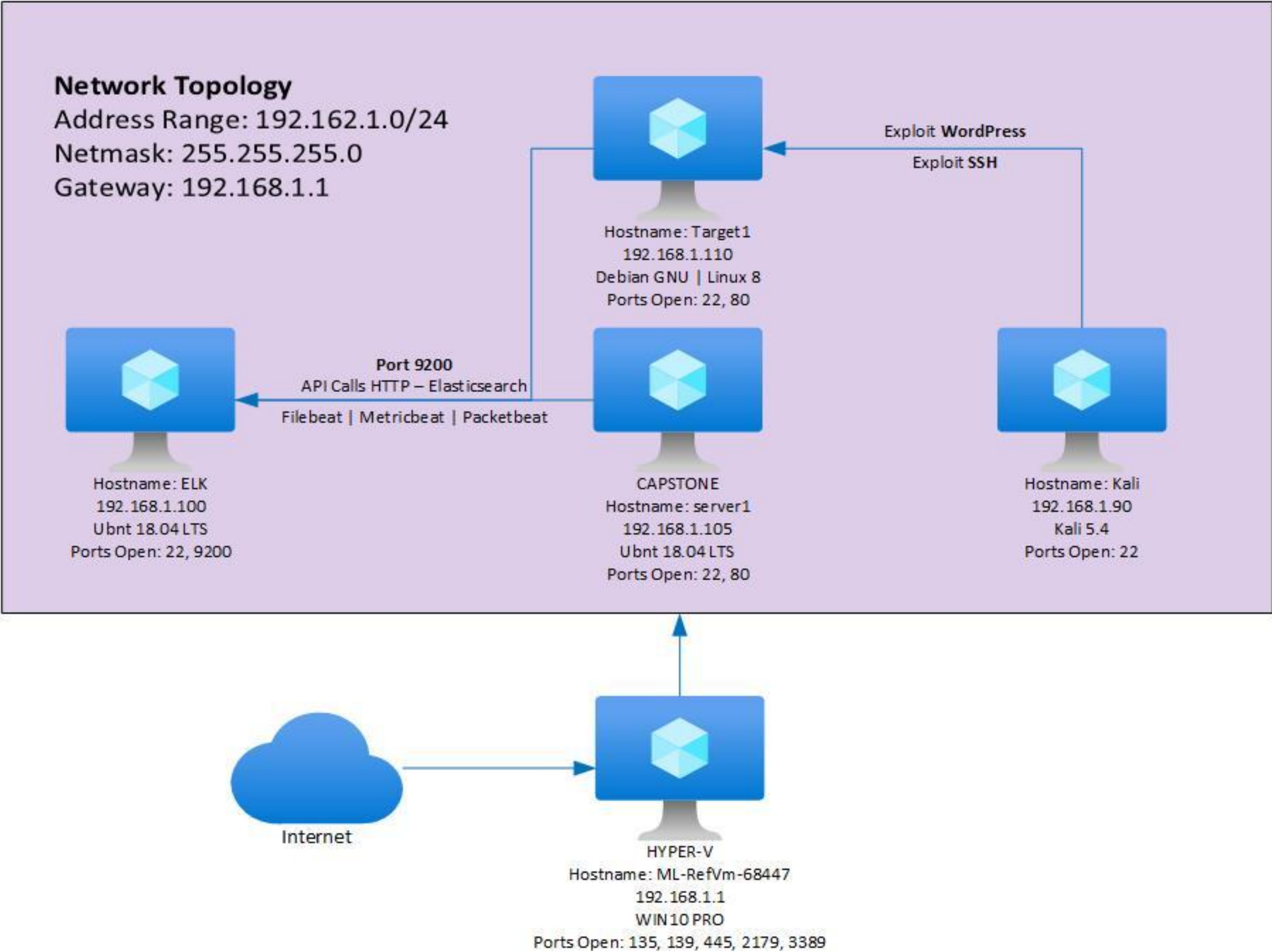
Normal Activity



Malicious Activity

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: Ubuntu 18.04 LTS
Hostname: ELK

IPv4: 192.168.1.105
OS: Ubuntu 18.04 LTS
Hostname: Capstone

IPv4: 192.168.1.110
OS: Debian GNU | Linux 8
Hostname: Target1

IPv4: 192.168.1.90
OS: Kali 5.4
Hostname: Kali

Critical Vulnerabilities: Target 1

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

Vulnerability	Description	Impact
Weak Password	Passwords were simple to break as they were short in length and did not require special characters.	Brute force attack on passwords were made simple by using John to crack passwords.
User Enumeration	Enumeration was gathered to expose account usernames and unprotected files and directories.	Allowed us to gain to access to usernames which could then be used in the brute force attack.
Privilege Escalation	File permissions and exposed files allowed access to sensitive files.	Allowed access to wp_config.php which had the database password in plain text, which allowed further escalation.

Traffic Profile

Traffic Profile

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

Feature	Value	Description
Top Talkers (IP Addresses)	185.243.115.84; 166.62.111.64; 172.16.4.205	Machines that sent the most traffic.
Most Common Protocols	HTTP; Netbios (SMB); DNS	Three most common protocols on the network.
# of Unique IP Addresses	808	Count of observed IP addresses.
Subnets	*/24	Observed subnet ranges.
# of Malware Species	june11.dll - Trojan Reference: https://www.virustotal.com/gui/file/d36366666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec	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

- Regular website browsing in WP content
- We can also see different types of media such as images
- Normal CSS content loading
- API calls related to website content

Suspicious Activity

- <http://205.185.125.104/files/june11.dll> - **Trojan** activity
- www.publicdomaintorrents.com torrent download for **betty_boop_rhythm_on_the_reservation.avi.torrent**



Normal Activity

Normal Web Traffic

Summarize the following:

- Which protocol(s)?
 - HTTP
 - TCP
- Which site were they browsing?
 - time.com
 - vinylmeplease.com
 - sabethahospital.com

41002	525.198950000	DESKTOP-B49J3FD.loc...	www.sabethahospital.com	TCP	60	50180	→	80
41003	525.199909700	DESKTOP-B49J3FD.loc...	www.sabethahospital.com	TCP	60	50186	→	80
50125	609.070703600	DESKTOP-B49J3FD.loc...	www.sabethahospital.com	TCP	60	50185	→	80
50128	609.073741300	DESKTOP-B49J3FD.loc...	www.sabethahospital.com	TCP	60	50185	→	80
46003	568.392242500	Gilbert-Win7-PC.oka...	www.vinylmeplease.com	TCP	66	49198	→	80
46005	568.394138300	Gilbert-Win7-PC.oka...	www.vinylmeplease.com	TCP	60	49198	→	80
46007	568.402173300	Gilbert-Win7-PC.oka...	www.vinylmeplease.com	HTTP	502	GET /magaz		
46030	568.629564100	Gilbert-Win7-PC.oka...	www.vinylmeplease.com	TCP	60	49198	→	80
46034	568.698238100	Gilbert-Win7-PC.oka...	www.vinylmeplease.com	TCP	60	49198	→	80
46035	568.699190200	Gilbert-Win7-PC.oka...	www.vinylmeplease.com	TCP	60	49198	→	80
46036	568.700400000	Gilbert-Win7-PC.oka...	www.vinylmeplease.com	TCP	60	49198	→	80
Flags: 0x018 (PSH, ACK) Window size value: 1024 [Calculated window size: 262144] [Window size scaling factor: 256] Checksum: 0x8fc5 [unverified] [Checksum Status: Unverified] Urgent pointer: 0 [SEQ/ACK analysis] [Timestamps] TCP payload (287 bytes)								
Hypertext Transfer Protocol								
GET /images/favicon.ico HTTP/1.1\r\n								
[Expert Info (Chat/Sequence): GET /images/favicon.ico HTTP/1.1\r\n] Request Method: GET Request URI: /images/favicon.ico Request Version: HTTP/1.1								
0030	04 00 8f c5 00 00 47 45	54 20 2f 69 6d 61 67 65GE T /image					
0040	73 2f 66 61 76 69 63 6f	6e 2e 69 63 6f 20 48 54	s/favicon.ico HT					
0050	54 50 2f 31 2e 31 0d 0a	41 63 63 65 70 74 3a 20	TP/1.1.. Accept:					
0060	2a 2f 2a 0d 0a 41 63 63	65 70 74 2d 45 6e 63 6f	/*..Acc ept-Enco					
0070	64 69 6e 67 3a 20 67 7a	69 70 2c 20 64 65 66 6c	ding: gz ip, defl					
0080	61 74 65 0d 0a 55 73 65	72 2d 41 67 65 6e 74 3a	ate..Use r-Agent:					
0090	20 4d 6f 7a 69 6c 6c 61	2f 35 2e 30 20 28 57 69	Mozilla /5.0 (Wi					
00a0	6e 64 6f 77 72 20 4e 54	20 21 20 2e 20 2b 20 57	ndows NT 10.0. W					

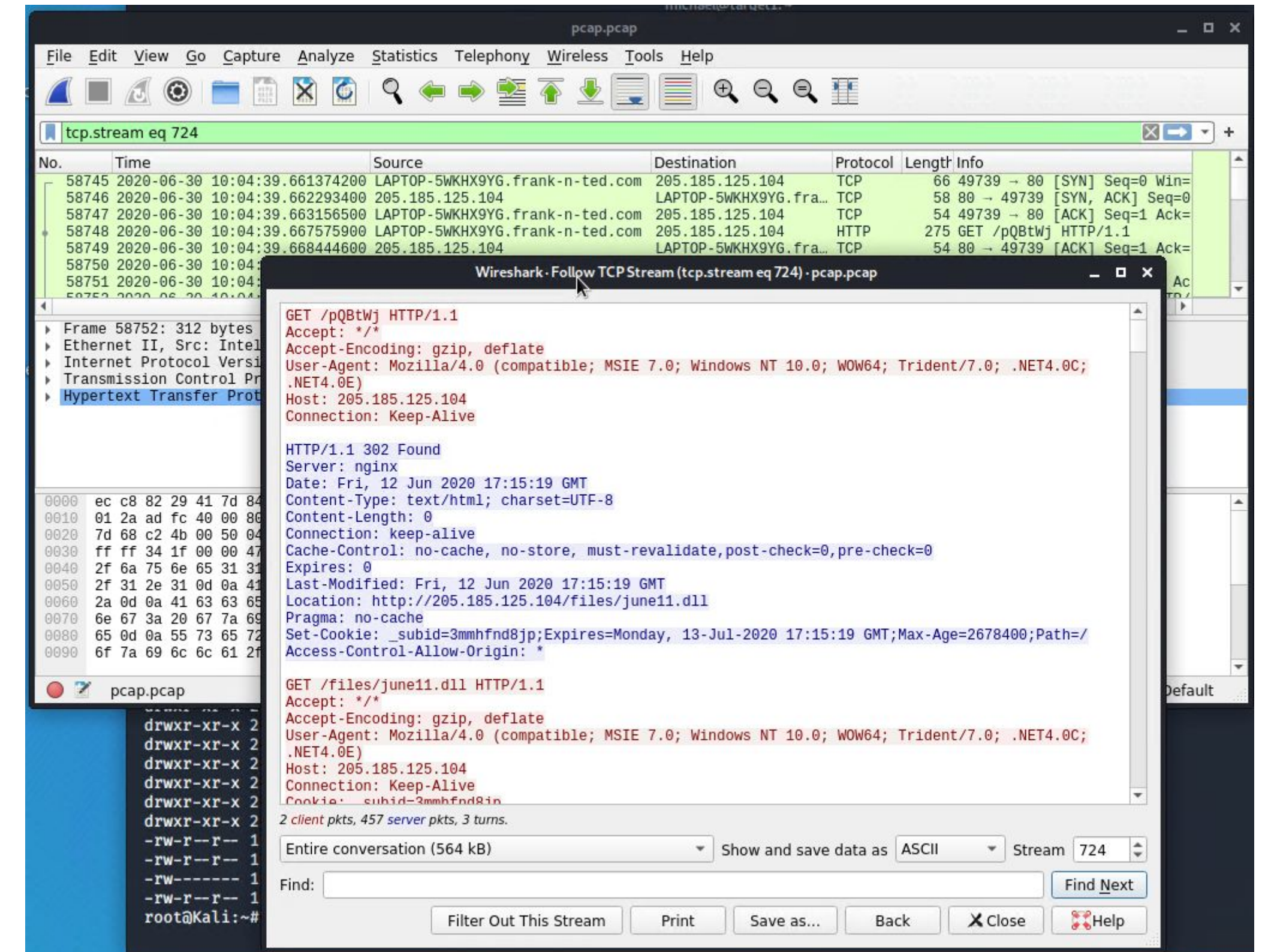
Malicious Activity

Trojan Infection

Summarize the following:

- Which protocol(s)?
 - HTTP
- What, specifically, was the user doing?
 - A trojan file was downloaded by the end user while browsing from `http://205.185.125.104`.
- Include a description of any interesting files.
 - The file downloaded with the trojan payload was named **june11.dll**.
 - Reference:

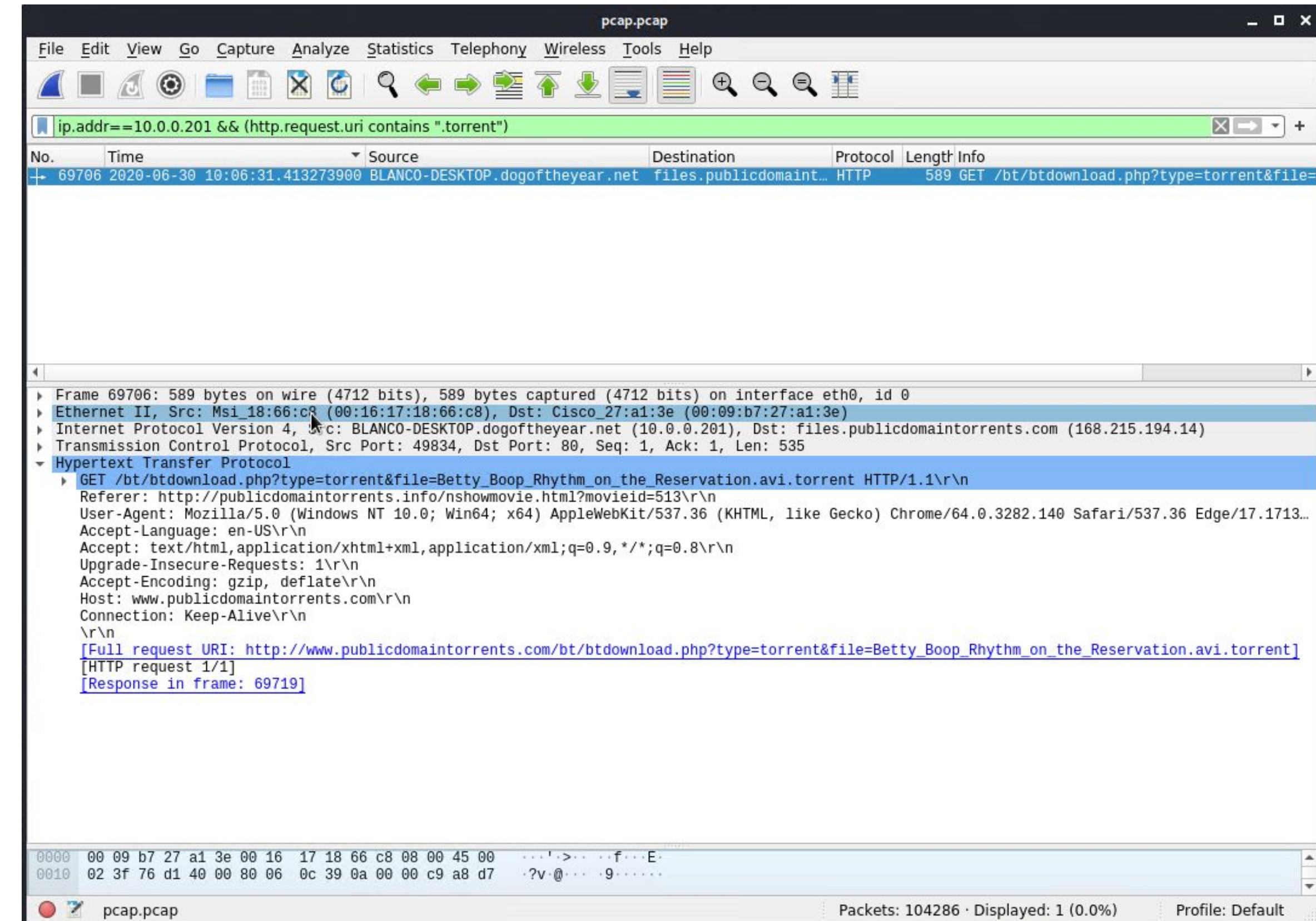
<https://www.virustotal.com/gui/file/d36366666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec>



Torrent Download

Summarize the following:

- Which protocol(s)?
 - HTTP
 - TCP/Bittorrent Protocol
- What, specifically, was the user doing?
 - User was browsing and searching public domain videos on www.publicdomaintorrents.com. We can also see bittorrent traffic to and from the end user.
- Include a description of any interesting files.
 - Betty_Boop_Rhythm_on_the_Reservation.avi.torrent was downloaded.



71764	779.991610800	node-257.pool-1-0.d...	BLANCO-DESKTOP.dogofth...	BitTorrent	122	Handshake
71765	779.997981300	BLANCO-DESKTOP.dogo...	node-257.pool-1-0.dyna...	BitTorrent	395	Extended Have All Allowed Fast, Pi
71777	780.018518100	BLANCO-DESKTOP.dogo...	ns327210.ip-37-187-109...	BitTorrent	122	Handshake
71804	780.296526200	node-257.pool-1-0.d...	BLANCO-DESKTOP.dogofth...	BitTorrent	375	Extended Have All Port Extended
71806	780.299337700	ns327210.ip-37-187-...	BLANCO-DESKTOP.dogofth...	BitTorrent	122	Handshake



The End