

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



Traffic Profile



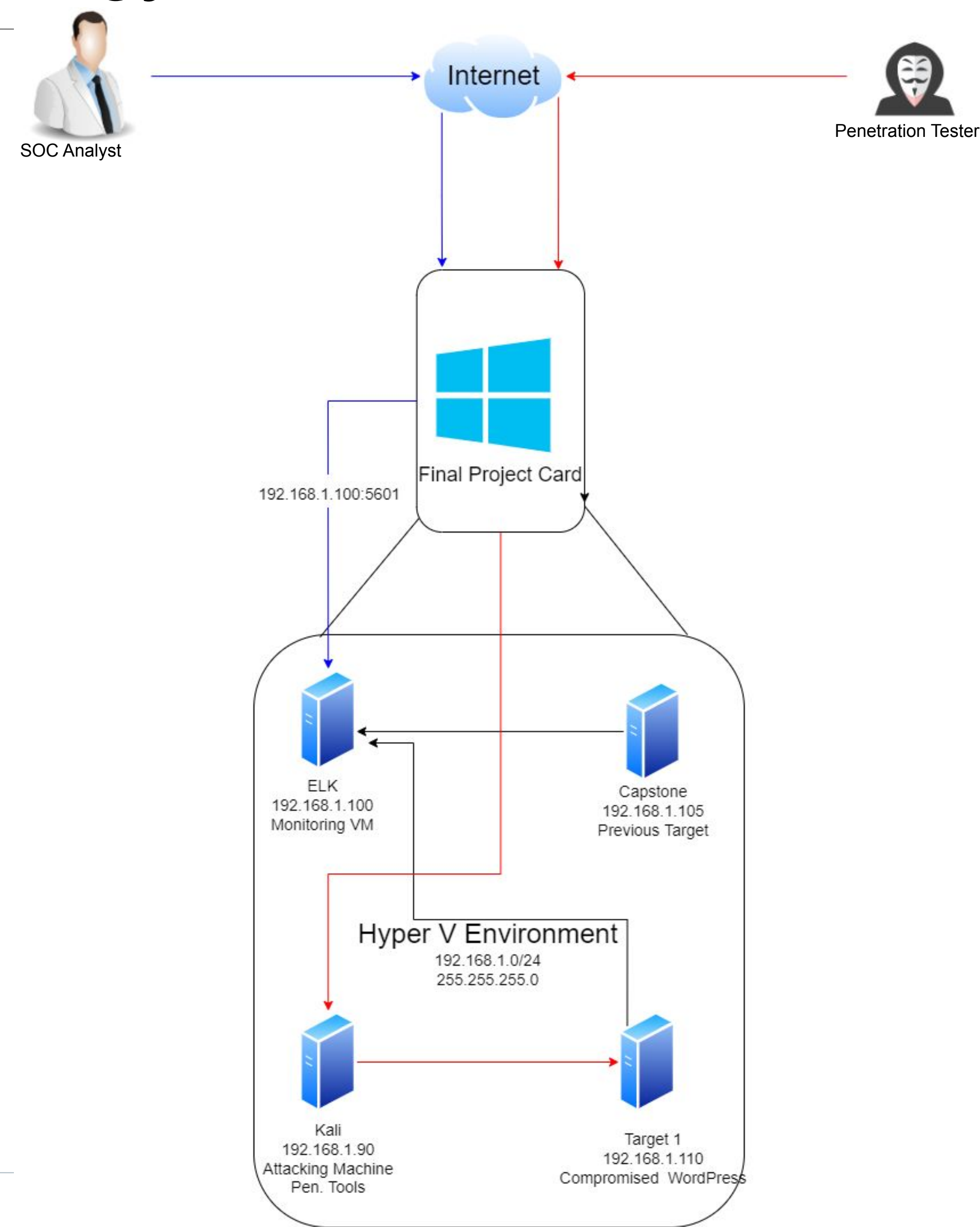
Normal Activity



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: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) "<R00T>" 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).

10329	2020-06-30	09:56:14.777321600	172.16.4.205	166.62.111.64	HTTP	386	GET /wp-content/uploads/2018/02/Beauty.jpg HT...
72525	2020-06-30	10:06:46.641627900	10.0.0.201	73.104.37.111	UDP	403	63448 → 55177 Len=361
69157	2020-06-30	10:06:26.338156800	50.18.44.131	10.0.0.201	TCP	54	80 → 49763 [ACK] Seq=186 Ack=722 Win=64240 Le...

Malicious Activity

Trojan Horse (Zloader)

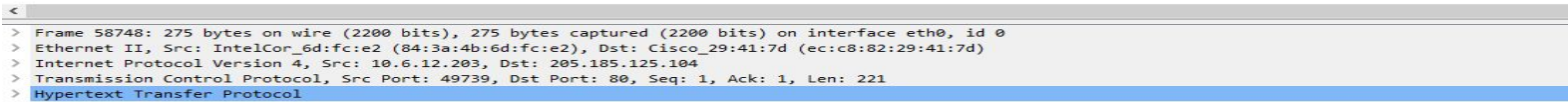
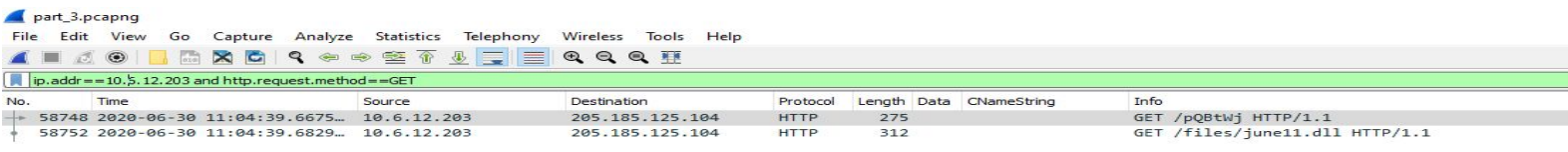
Summarize the following: Frank-n-ted.com(10.6.12.20) file was downloaded that was malicious

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



49 / 67

Community Score

49 security vendors and 1 sandbox flagged this file as malicious

d36366666b407fe5527b96696377ee7ba9b609c8ef4561fa76af218ddd764dec

Googleupdate.exe

invalid-signature overlay pedll signed spreader

549.84 KB

2022-06-07 01:35:13 UTC

5 minutes ago

DLL

DETECTION

DETAILS

RELATIONS

BEHAVIOR

COMMUNITY

Security Vendors' Analysis

Ad-Aware	Trojan.Mint.Zamg.O	AhnLab-V3	Malware/Win32.RL_Generic.R346613
Alibaba	TrojanSpy:Win32/Yakes.0454a340	ALYac	Trojan.Mint.Zamg.O
Arcabit	Trojan.Mint.Zamg.O	Avast	Win32:DangerousSig [Trj]
AVG	Win32:DangerousSig [Trj]	Avira (no cloud)	TR/AD.ZLoader.ladbd
BitDefender	Trojan.Mint.Zamg.O	BitDefenderTheta	Gen:NN.ZedlaF.34712.lu9@aul70Qgi
Bkav Pro	W32.AIDetect.malware2	CrowdStrike Falcon	Win/malicious_confidence_100% (W)

13

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://publicdomianstorrents.info/grabs/bettybooprythmonthereservationgrab.jpg> to download a photo, this ended up being a torrent file

```
0 10.0.0.201 172.217.9.2 HTTP 434 GET /pagead/show_ads.js HTTP/1.1
0 10.0.0.201 50.18.44.131 HTTP 412 GET /tools/diggthis.js HTTP/1.1
0 10.0.0.201 168.215.194.14 HTTP 500 GET /grabs/bettybooprythmonthereservationgrab.jpg HTTP/1.1
0 10.0.0.201 168.215.194.14 HTTP 465 GET /divxi.jpg HTTP/1.1
0 10.0.0.201 52.94.240.125 HTTP 415 GET /s/ads.js HTTP/1.1
0 10.0.0.201 168.215.194.14 HTTP 531 GET /usercomments.html?movieid=513 HTTP/1.1
0 10.0.0.201 52.94.240.125 HTTP 427 GET /s/ads-common.js HTTP/1.1
0 10.0.0.201 72.21.202.62 HTTP 885 GET /e/cm?t=publicdomai0f-20&o=1&p=48&l=op1&pvid=40C236A13FDD0B68&ref-ur...
0 10.0.0.201 52.94.233.131 HTTP 1067 GET /1/associates-ads/1/OP/?cb=1531628232887&p=%7B%22program%22%3A%221%2...
0 10.0.0.201 168.215.194.14 HTTP 589 GET /bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reserv...
0 10.0.0.201 140.211.166.134 HTTP 195 GET /version-1.0 HTTP/1.1
0 10.0.0.201 91.189.95.21 HTTP 423 GET /announce?info_hash=%e4%be%9eM%b8v%e3%e3%17%97x%b0%3e%90b%97%be%5c%8...
0 10.0.0.201 168.215.194.14 HTTP 434 GET /bt/announce.php?info_hash=%1d%da%0dH%a8%98%bd%81%5c%7d2%ee%836o%03%...
0 10.0.0.201 168.215.195.227 HTTP 434 GET /announce?info_hash=%1d%da%0dH%a8%98%bd%81%5c%7d2%ee%836o%03%09y%60%...
0 10.0.0.201 168.215.194.14 HTTP 253 GET /bt/scrape.php?info_hash=%1d%da%0dH%a8%98%bd%81%5c%7d2%ee%836o%03%09...
0 10.0.0.201 168.215.195.227 HTTP 253 GET /scrape?info_hash=%1d%da%0dH%a8%98%bd%81%5c%7d2%ee%836o%03%09y%60%fe...
0 10.0.0.201 72.21.91.29 HTTP 288 GET /MFEwTzBNMEswSTAJBgUrDgMCGGUABBSAUQYBMq2awn1Rh6Doh%2FsBYgFV7gQUA95QN...
0 10.0.0.201 72.21.91.29 HTTP 290 GET /MFEwTzBNMEswSTAJBgUrDgMCGGUABBTBL0V27RVZ7LBduom%2FnYB45SPUEwQU5Z1ZM...
0 10.0.0.201 72.21.91.29 HTTP 292 GET /MFEwTzBNMEswSTAJBgUrDgMCGGUABBTnvAI%2FnN49qPTJY2qTtfkLxjvEAQUo53mH...

.... ..0. .... = LG bit: Globally unique address (factory default)
.... ..0 .... = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 10.0.0.201, Dst: 168.215.194.14
Transmission Control Protocol, Src Port: 49834, Dst Port: 80, Seq: 1, Ack: 1, Len: 535
Hypertext Transfer Protocol
GET /bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent HTTP/1.1\r\n
Referer: http://publicdomaintorrents.info/nshowmovie.html?movieid=513\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36 Edge/17.17134\r\n
Accept-Language: en-US\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
Upgrade-Insecure-Requests: 1\r\n
Accept-Encoding: gzip, deflate\r\n
Host: www.publicdomaintorrents.com\r\n
Connection: Keep-Alive\r\n
\r\n
[Full request URI: http://www.publicdomaintorrents.com/bt/btdownload.php?type=torrent&file=Betty_Boop_Rhythm_on_the_Reservation.avi.torrent]
[HTTP request 1/1]
[Response in frame: 69719]
```



(Look of Disapproval)

The End