Final Engagement

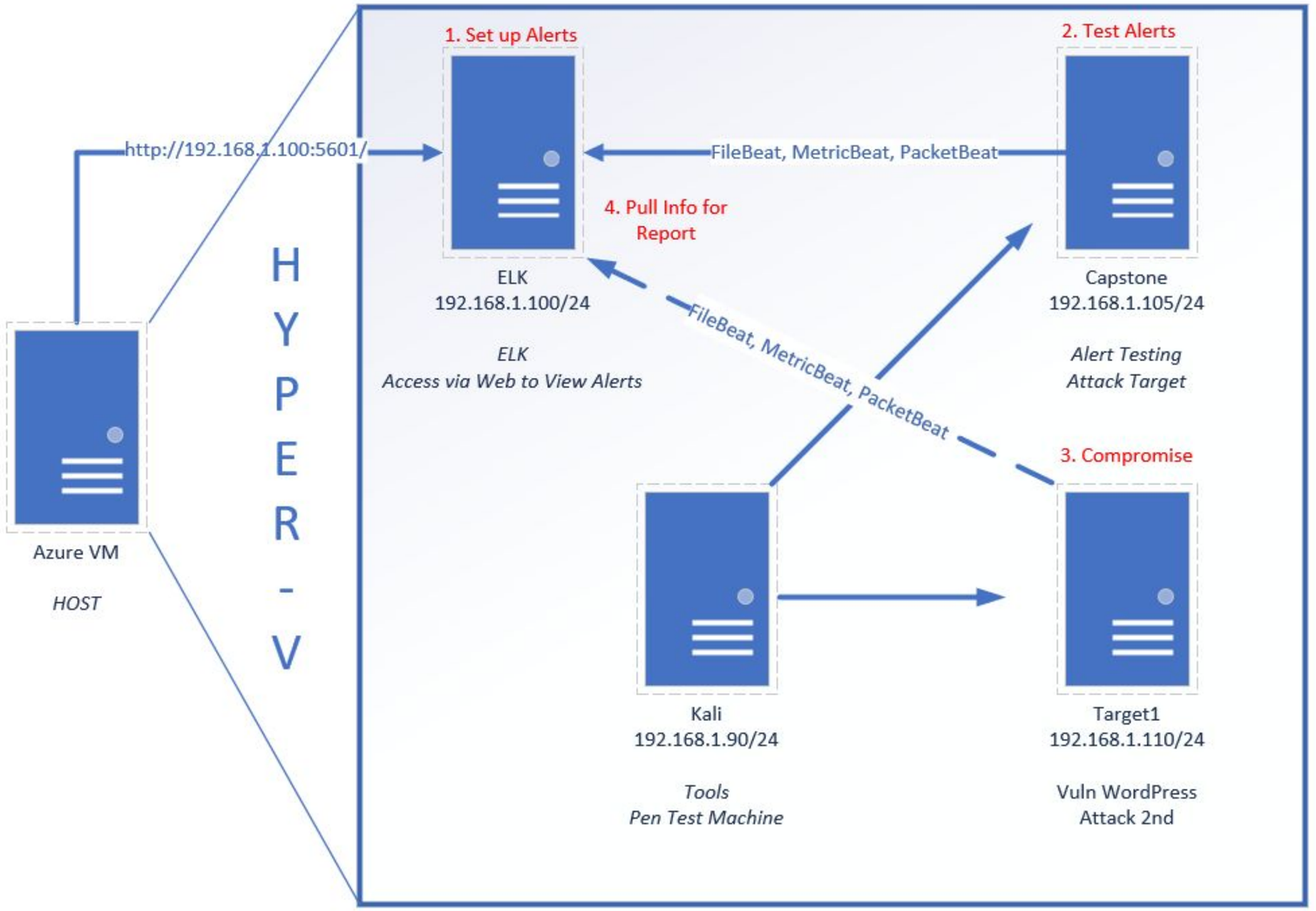
Attack, Defense & Analysis of a Vulnerable Network

Table of Contents

This document contains the following resources:

Network Topology
& Critical Vulnerabilities

Network Topology



Network
Address Range:192.168.1.0/24

Machines
IPv4: 192.168.1.90
OS: Kali Linux
Hostname: Kali

IPv4: 192.168.1.100
OS: Ubuntu 18.04.4 LTS
Hostname: ELK

IPv4: 192.168.1.105
OS: Ubuntu 18.04.4 LTS
Hostname: Capstone

IPv4: 192.168.1.110
OS: Debian Linux Jessie
Hostname: Target 1

IPv4: 192.168.1.115
OS: Debian Linux Jessie
Hostname: Target 2

Critical Vulnerabilities: Target 1

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

Vulnerability	Description	Impact
Insecure Password	User used their username as their password & password hashes were easily “cracked”	Allowed for SSH access to Target1 due to weak security.
Unrestricted User Rights	User (michael) was allowed into folders on Target1 that the user didn’t need access to.	Allowed for directory traversal and viewing of files that contained privileged passwords.
Privilege Escalation	User(steven) had sudo rights to Python which allowed scripts to run as Root	A python script was able to be run with sudo which was able to spawn a Root level bash shell.

Critical Vulnerabilities: Target 2

Our assessment uncovered the following critical vulnerabilities in **Target 2**.

Vulnerability	Description	Impact
PHPMailer RCE: CVE 2016-10033	Allows extra parameters to the mail command	Allows execution of arbitrary code
Privilege Escalation	Obtained through default username and password for root	Grants root access
Directory Listing	Lists files and directories that exist on a Web server	Allows unapproved entry to directories and files

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 (33M) 10.0.0.201 (19M) 185.243.115.84 (16M)	Machines that sent the most traffic.
Most Common Protocols	TLS HTTP DNS	Three most common protocols on the network.
# of Unique IP Addresses	810	Count of observed IP addresses.
Subnets	192.168.1.0/24 172.16.4.0/24 10.6.12.0/24 10.0.0.0/24	Observed subnet ranges.

Behavioral Analysis

Purpose of Traffic on the Network

Users were observed engaging in the following kinds of activity.

“Normal” Activity

- Visiting a Blog Website - MySoCalledChaos.com
- Downloading and installing Desktop Background

Suspicious Activity

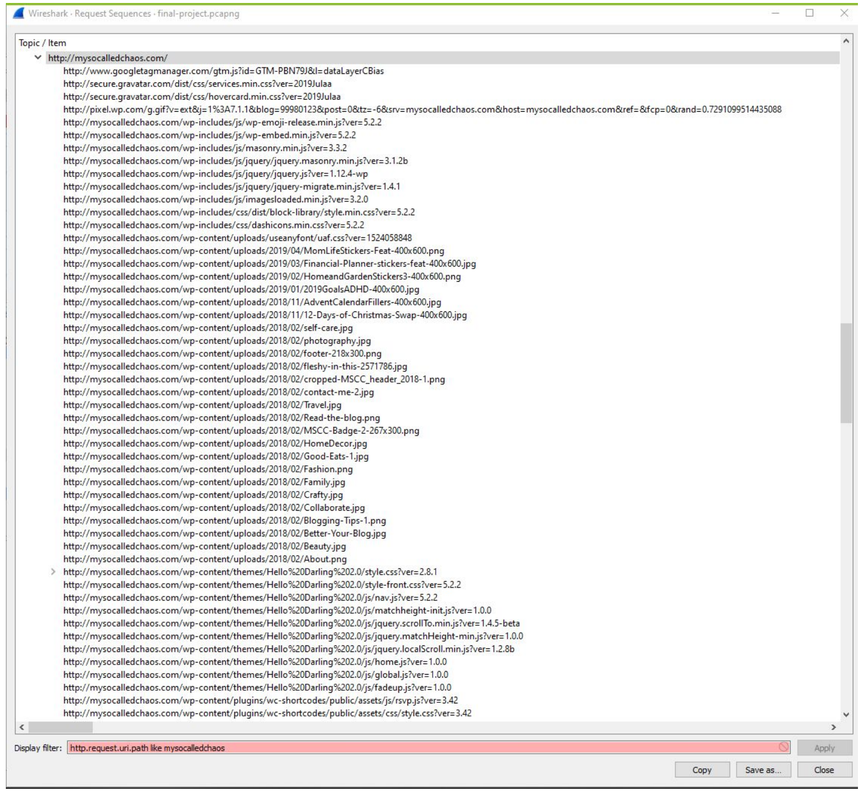
- Dropping Reverse Shell components
- SSH logins
- Downloading Torrents
- Setup AD network and Domain Controller

Normal Activity

Web Browsing

Summarize the following:

- HyperText Transfer Protocol
- The user appeared to be editing a WordPress Blog, mysocalledchaos.com, Viewing Sabetha Hospital's site.



Desktop Background

Summarize the following:

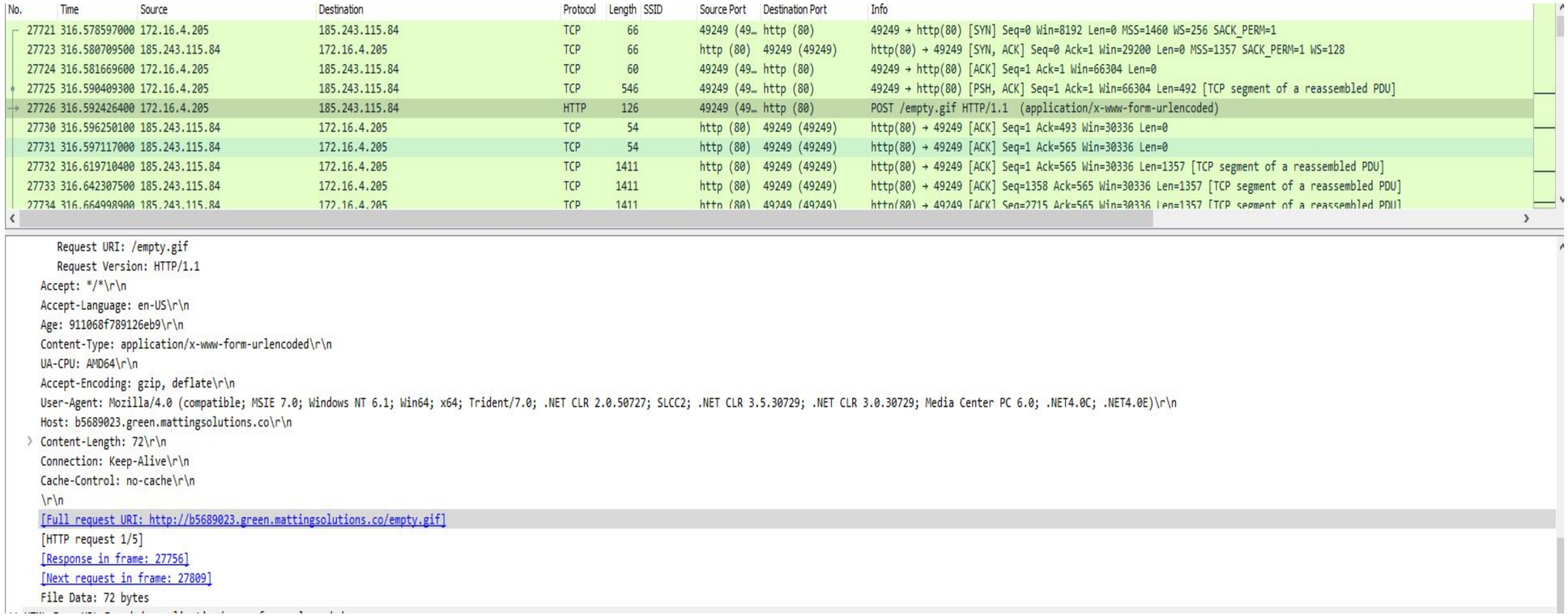
- Protocols Used: HTTP
- Img downloaded from green.mattingsolutions.co
- empty.gif?ss&ss1img

Malicious Activity

Reverse Shell

Summarize the following:

- Use of HTTP to place a reverse shell script on a web server
- The user was visiting http://b5689023.green.mattingsolutions.co/empty.gif



No.	Time	Source	Destination	Protocol	Length	SSID	Source Port	Destination Port	Info
27721	316.578597000	172.16.4.205	185.243.115.84	TCP	66		49249 (49…	http (80)	49249 → http(80) [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
27723	316.580709500	185.243.115.84	172.16.4.205	TCP	66		http (80)	49249 (49249)	http(80) → 49249 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1357 SACK_PERM=1 WS=128
27724	316.581669600	172.16.4.205	185.243.115.84	TCP	60		49249 (49…	http (80)	49249 → http(80) [ACK] Seq=1 Ack=1 Win=66304 Len=0
27725	316.590409300	172.16.4.205	185.243.115.84	TCP	546		49249 (49…	http (80)	49249 → http(80) [PSH, ACK] Seq=1 Ack=1 Win=66304 Len=492 [TCP segment of a reassembled PDU]
27726	316.592426400	172.16.4.205	185.243.115.84	HTTP	126		49249 (49…	http (80)	POST /empty.gif HTTP/1.1 (application/x-www-form-urlencoded)
27730	316.596250100	185.243.115.84	172.16.4.205	TCP	54		http (80)	49249 (49249)	http(80) → 49249 [ACK] Seq=1 Ack=493 Win=30336 Len=0
27731	316.597117000	185.243.115.84	172.16.4.205	TCP	54		http (80)	49249 (49249)	http(80) → 49249 [ACK] Seq=1 Ack=565 Win=30336 Len=0
27732	316.619710400	185.243.115.84	172.16.4.205	TCP	1411		http (80)	49249 (49249)	http(80) → 49249 [ACK] Seq=1 Ack=565 Win=30336 Len=1357 [TCP segment of a reassembled PDU]
27733	316.642307500	185.243.115.84	172.16.4.205	TCP	1411		http (80)	49249 (49249)	http(80) → 49249 [ACK] Seq=1358 Ack=565 Win=30336 Len=1357 [TCP segment of a reassembled PDU]
27734	316.664998900	185.243.115.84	172.16.4.205	TCP	1411		http (80)	49249 (49249)	http(80) → 49249 [ACK] Seq=2715 Ack=565 Win=30336 Len=1357 [TCP segment of a reassembled PDU]

```
    Request URI: /empty.gif
    Request Version: HTTP/1.1
Accept: */*\r\n
Accept-Language: en-US\r\n
Age: 911068f789126eb9\r\n
Content-Type: application/x-www-form-urlencoded\r\n
UA-CPU: AMD64\r\n
Accept-Encoding: gzip, deflate\r\n
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/7.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)\r\n
Host: b5689023.green.mattingsolutions.co\r\n
Content-Length: 72\r\n
Connection: Keep-Alive\r\n
Cache-Control: no-cache\r\n
\r\n
[Full request URI: http://b5689023.green.mattingsolutions.co/empty.gif]
[HTTP request 1/5]
[Response in frame: 27756]
[Next request in frame: 27809]
File Data: 72 bytes
```

Downloading Torrents

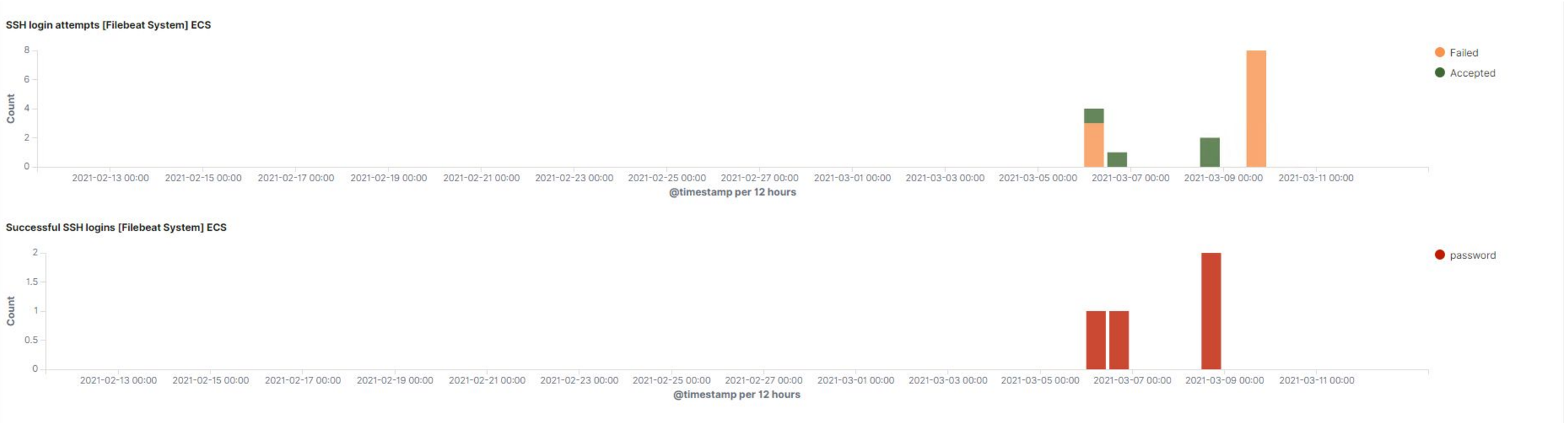
Summarize the following:

- Use of HTTP to download a torrent file
- The user was accessing www.mypublicdomaintorrents.com
- Include screenshots of packets justifying your conclusions.
- Downloaded torrent file: Betty_Boop_Rhythm_on_the_Reservation.avi.torrent

SSH Logins

Summarize the following:

- The only SSH traffic observed by the SIEM was during the actual attacks, no other SSH logins were logged.
- SSH was used for infiltration of the Target1 & Target2.



The End