Capstone Engagement

Assessment, Analysis,
and Hardening of a Vulnerable System

Bradley Lawler

Table of Contents

This document contains the following sections:

Network Topology

Network Topology
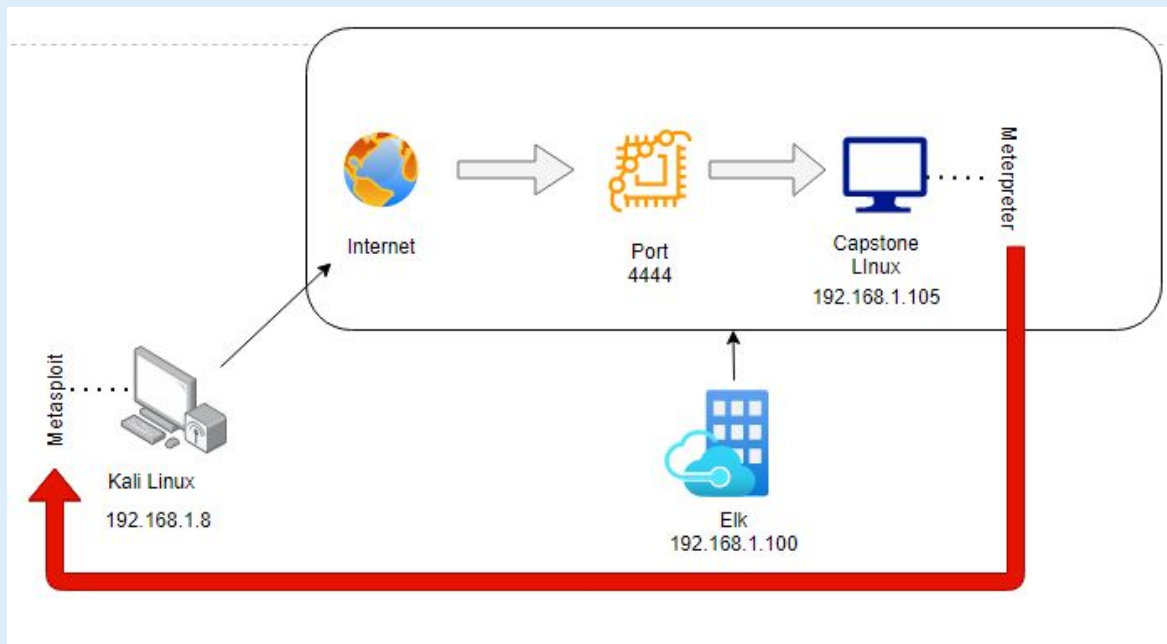
Network
Address Range:
192.168.0/24
Netmask: 255.255.255.0
Gateway: 1:1

Machines
IPv4: 192.168.1.8
OS: Kali Linux
Hostname: Kali

IPv4: 192.168.1.105
OS: Linux
Hostname: Capstone Linux

IPv4: 192.168.1.100
OS: Ubuntu
Hostname: Elk

Internet

Port
4444

Capstone
LInux
192.168.1.105

Meterpreter

Metasploit

Kali Linux
192.168.1.8

Elk
192.168.1.100

Red Team
Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

```
root@kali:~# arp-scan --localnet
Interface: eth0, datalink type: EN10MB (Ethernet)
Starting arp-scan 1.9.5 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.1.1      00:15:5d:00:04:03      Microsoft Corporation
192.168.1.100    00:15:5d:00:04:01      Microsoft Corporation
192.168.1.105    00:15:5d:00:04:02      Microsoft Corporation
```

Hostname	IP Address	Role on Network
Target (Capstone)	192.168.1.105	Machine we are attacking.
Windows Virtual Machine (Azure)	192.168.1.1	Host Machine
Logging (ELK)	192.168.1.100	Machine used to aggregate logs.
Kali Linux Machine	192.168.1.8	Machine we are using to attack.

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Unauthorized File Upload	This allows users to upload potentially malicious files to the server.	This allows an attacker the ability to use any malicious script by placing the file directly on the server.
Bruteforce SSH login	This allows an attacker the ability to get a legitimate users login password, and gain a shell of that user.	Another vulnerability I found was bruteforcing Ryans Username and Password in order to gain a shell of Ryan. This led to finding the flag.
Sensitive Data Exposure	This is a Top 10 OWSAP vulnerability.	This allowed the attacker access to the secret_folder directory. This access led to the compromised credentials needed to gain access to the WebDAV folder.

Exploitation: Sensitive Data Exposure

01

Tools & Processes
- NMAP
- Hydra
- Crackstation
- Metasploit
- Meterpreter

02

Achievements
These combined allowed me to gain access to the WebDAV directory and upload a PHP script, also allowing a reverse TCP shell directly from the attackers computer. Then Metasploit was used to listen for the server and create a Meterpreter session. Once the session was created I was able to search and find the flag.

03
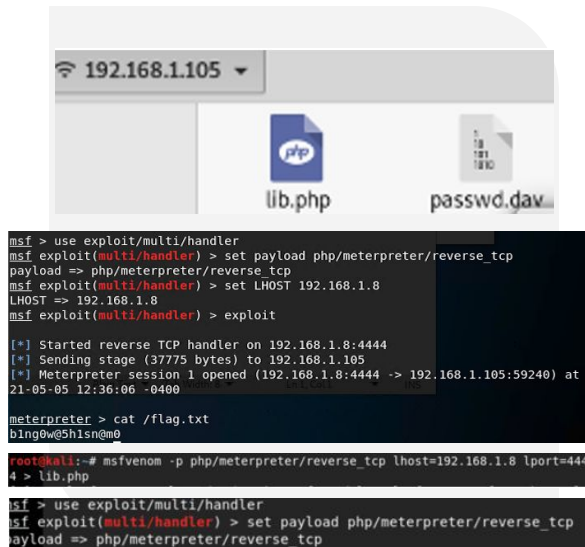
Blue Team
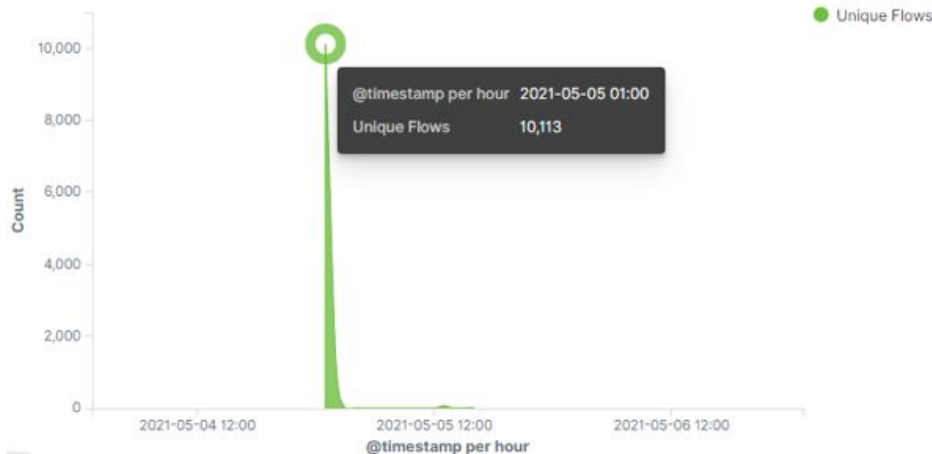Log Analysis and
Attack Characterization

Analysis: Identifying the Port Scan

Answer the following questions in bullet points under the screenshot if space allows. Otherwise, add the answers to speaker notes.
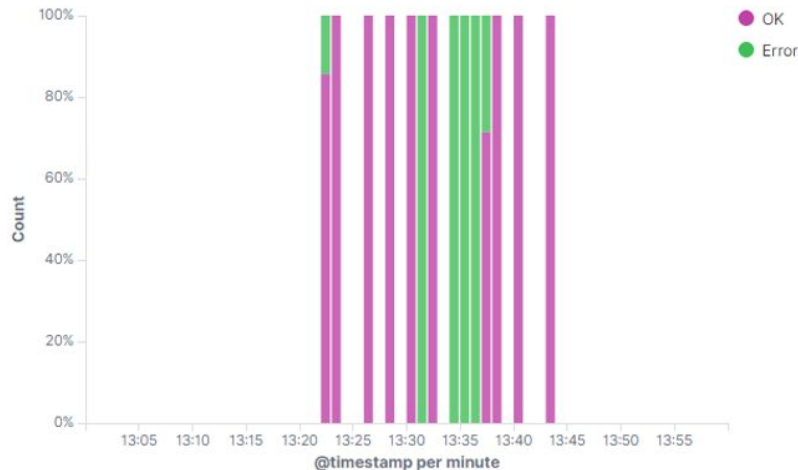
- What time did the port scan occur?
- How many packets were sent, and from which IP?
- What indicates that this was a port scan?

Connections over time [Packetbeat Flows] ECS

Unique Flows

| @timestamp per hour | 2021-05-05 01:00 |
| Unique Flows | 10,113 |

Errors vs successful transactions [Packetbeat] ECS

- OK
- Error

- The port scan occurred May 5th, 2021 at 13:20.
- There were 10,113 packets.
- The number of hits in such a short amount of time indicates this was a port scan.
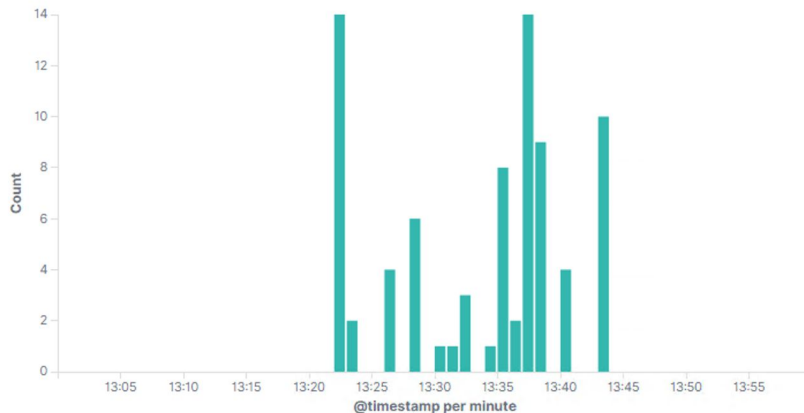
Analysis: Finding the Request for the Hidden Directory

Answer the following questions in bullet points under the screenshot if space allows. Otherwise, add the answers to speaker notes.

- What time did the request occur? How many requests were made?
- Which files were requested? What did they contain?

HTTP Transactions [Packetbeat] ECS

Index of /company_folders/secret_folder

Name	Last modified	Size	Description
Parent Directory		-	
connecting_to_webdav	2019-04-30 15:40	416	

Apache/2.4.29 (Ubuntu) Server at 172.16.84.205 Port 80

url.full: Descending ⇳	Count ⇳
http://192.168.1.105/company_folders/secret_folder	21,431

- It looks like the original request started about 13:21, and had 21,431 requests
- The company_folders/secret_folder was the file requested. It contained instructions on how to connect to WebDav.
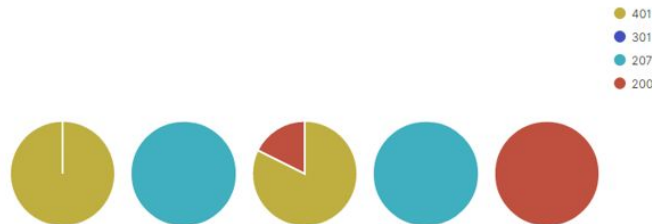
Analysis: Uncovering the Brute Force Attack

Answer the following questions in bullet points under the screenshot if space allows. Otherwise, add the answers to speaker notes.

- How many requests were made in the attack? .
- How many requests had been made before the attacker discovered the password?

HTTP status codes for the top queries [Packetbeat] ECS

- 401
- 301
- 207
- 200

Connections over time [Packetbeat Flows] ECS

@timestamp per hour 2021-05-05 01:00
Unique Flows   10,113

s over time [Packetbeat Flows] ECS

- Unique Flows

- I had 10,113 requests during my attack.
- It doesn't seem like I had any requests leading up to the attack.

Analysis: Finding the WebDAV Connection

Answer the following questions in bullet points under the screenshot if space allows. Otherwise, add the answers to speaker notes.
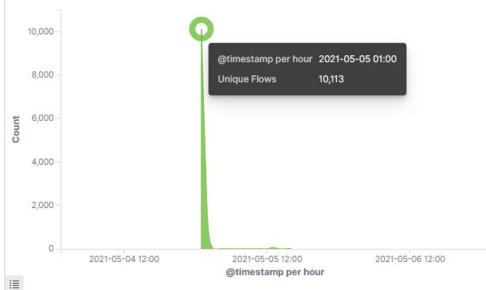
- How many requests were made to this directory?
- Which files were requested?

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/webdav	26
http://192.168.1.105/webdav/passwd.dav	10
http://192.168.1.105/webdav/	8
http://192.168.1.105/	6
http://192.168.1.105/icons/back.gif	6

- *I had a total of 44 requests to the WebDav directory*
- *WebDAV, WebDAV/passwd.dav, and WebDAV/ were the files requested.*

Blue Team
Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

What kind of alarm can be set to detect future port scans? I would set an alarm to detect multiple hits per second, especially from a Script Kiddie.

What threshold would you set to activate this alarm? I would start my baseline at 100 packets per second.

System Hardening

What configurations can be set on the host to mitigate port scans? I would enable filters 7000 - 7004 and also 7016. This will catch TCP, UDP, ICMP, and ICMPv6 sweeps.

Describe the solution. If possible, provide required command lines. User education is where I would start. Education will stop most users from clicking on random links and shells. Education will also allow users to be clued in to slowdowns and other abnormalities.

Mitigation: Finding the Request for the Hidden Directory

Alarm

What kind of alarm can be set to detect future unauthorized access? I would set an alarm that would notify of any access to the folder. My dashboard showed 21,431 attempts at the secret_folder

What threshold would you set to activate this alarm? I would set the threshold at 1, this would notify you of any access.

System Hardening

What configuration can be set on the host to block unwanted access? I would utilize a white list only allowing access to certain user groups or levels

Describe the solution. If possible, provide required command lines. When I first ran my dashboard I didn't show any hits. I determined my Azure machine shut down, when I restarted it I didn't reconfigure the Capstone machine. I reran the activity to show access to the secret_folder. This will explain the difference in numbers.

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	21,431

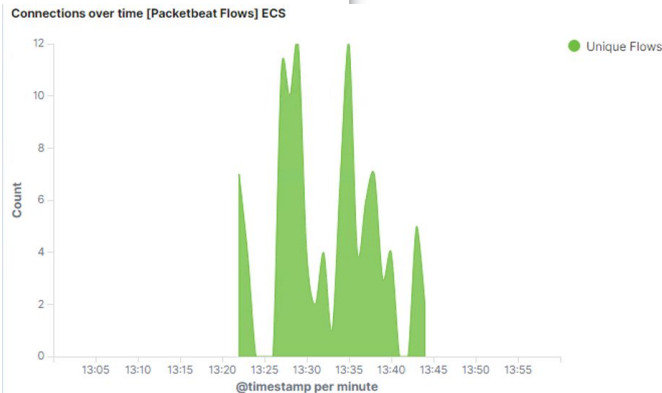# Mitigation: Preventing Brute Force Attacks

Alarm

What kind of alarm can be set to detect future brute force attacks? I would set my alarm for 401 Unauthorized Client codes. This would show people trying to gain access but getting denied.

What threshold would you set to activate this alarm? Using my data I had 35 HTTP hits in one minute, I would set it to trigger at 5 attempts.

System Hardening

What configuration can be set on the host to block brute force attacks? I recommend a better file structure and 2 Factor Identification for logins.

Describe the solution. If possible, provide the required command line(s). Lock out after 5 unsuccessful attempts.

Connections over time [Packetbeat Flows] ECS

● Unique Flows

Count

12
10
8
6
4
2
0

13:05 13:10 13:15 13:20 13:25 13:30 13:35 13:40 13:45 13:50 13:55

@timestamp per minute

Mitigation: Detecting the WebDAV Connection

Alarm

What kind of alarm can be set to detect future access to this directory? I would create an alarm that will notify of any requests to the WebDAV folder.

What threshold would you set to activate this alarm? I had 44 total hits to the WebDAV folder, with that information I would either set it at 0 if we didn't want any access or with my baseline set it at 40

System Hardening

What configuration can be set on the host to control access? I would create a white list of allowed IP address, and lock out all others.

Describe the solution. If possible, provide the required command line(s). I used my dashboard to provide me with how many hits the WebDAV folder had.

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/webdav	26
http://192.168.1.105/webdav/passwd.dav	10
http://192.168.1.105/webdav/	8
http://192.168.1.105/	6
http://192.168.1.105/icons/back.gif	6

Export: Raw ⬇ Formatted ⬇

Mitigation: Identifying Reverse Shell Uploads

Alarm

What kind of alarm can be set to detect future file uploads?
I would set an alarm to notify of any traffic directed to port

What threshold would you set to activate this alarm? Using a baseline from my dashboard I would set my threshold at 25 to start.

System Hardening

What configuration can be set on the host to block file uploads? User education will play a big part. Teaching users to not click on random links and access files they are not sure what they are will limit what shells get loaded to the system.

Describe the solution. If possible, provide the required command line. To get my dashboard to show this I used source.ip : 192.168.1.8 and port : 4444