Capstone Engagement

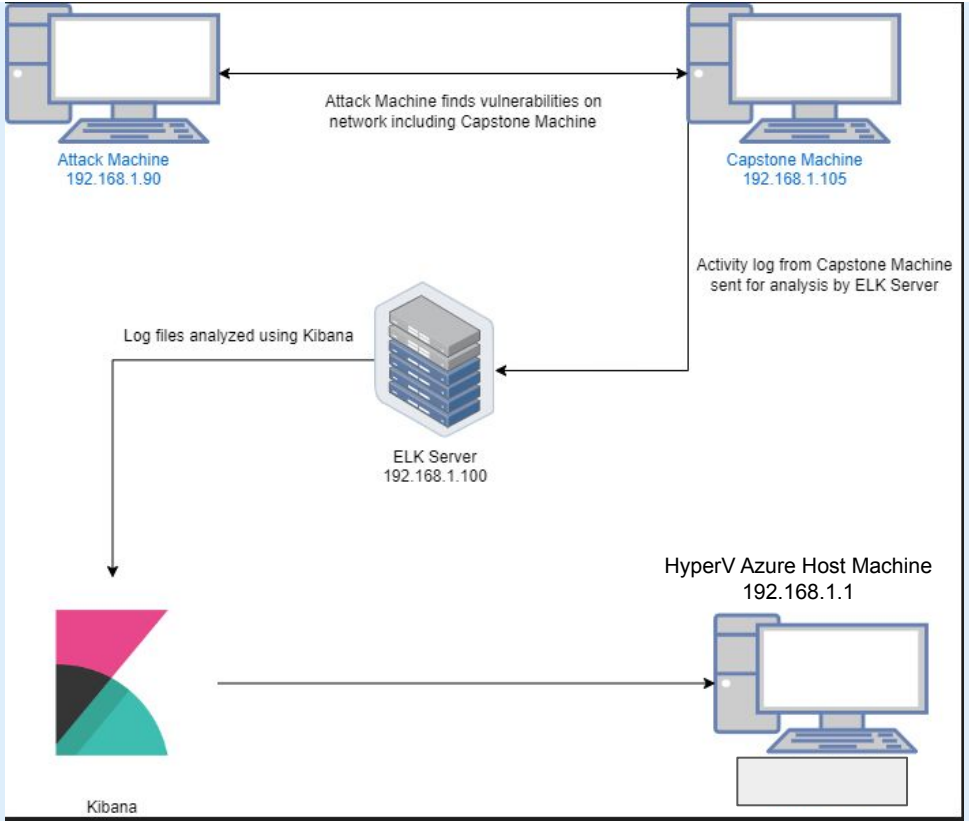
Assessment, Analysis, and Hardening of a Vulnerable System

Table of Contents

This document contains the following sections:

Network Topology

Network Topology



Network
Address Range: 192.168.1.0/24
Netmask: 255.255.255.0
Gateway: 10.0.0.76

Machines
IPv4: 192.168.1.1
OS: Windows 10
Hostname: Azure Hyper-V-ML-RefVm-684427

IPv4: 192.168.1.90
OS: Kali GNU/Linux
Hostname: Kali

IPv4: 192.168.1.100
OS: Ubuntu
Hostname: ELK

IPv4:192.168.1.105
OS: Ubuntu
Hostname: Capstone

Red Team

Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Hyper-V Azure machine ML-RefVm-684427	192.168.1.1	Host Machine Cloud Based
Kali	192.168.1.90	Attacking Machine
Elk Stack	192.168.1.100	Network Monitoring Machine running Kibana
Capstone	192.168.1.105	Target Machine that Replicates a vulnerable server

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Open port with public access CVE-2019-6579 (Port 80)	Unsecured access to anyone attempting entry using Port 80.	Sensitive (and secret) files and folders can be found.
WebDAV Vulnerability	Exploit WebDAV on a server and shell access is possible	A WebDAV that is not configured properly can allow hackers to remotely modify website contents.
Hashed Passwords	A password that is not salted can be easily cracked via online tools such as www.crackstation.com or programs such as hashcat.	A hacker can easily access system files if a username is already known and once they crack a password.
Root accessibility	Authorization to execute commands and access any resources on the vulnerable	Vulnerabilities can be leveraged. Extensive potential impact on any connected network.

Exploitation: [Port 80 Open to Public Access]

01

Tools & Processes

I used nmap to scan for open ports on the target machine

02

Achievements

Nmap scanned 256 IP addresses and found 4 hosts and the 2 open ports that peaked my interest was port 22 and port 80

03

Shell No.1

File Actions Edit View Help

```
root@Kali:~/Desktop# nmap 192.168.1.90/24
Starting Nmap 7.80 ( https://nmap.org ) at 2022-01-22 04:40 PST
Nmap scan report for 192.168.1.1
Host is up (0.00055s latency).
Not shown: 995 filtered ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
2179/tcp open  vmrdp
3389/tcp open  ms-wbt-server
MAC Address: 00:15:5D:00:04:0D (Microsoft)

Nmap scan report for 192.168.1.100
Host is up (0.00053s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
9200/tcp open  wap-wsp
MAC Address: 4C:EB:42:D2:D5:D7 (Intel Corporate)

Nmap scan report for 192.168.1.105
Host is up (0.00054s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
```

Exploitation: [Brute Force Password]

01

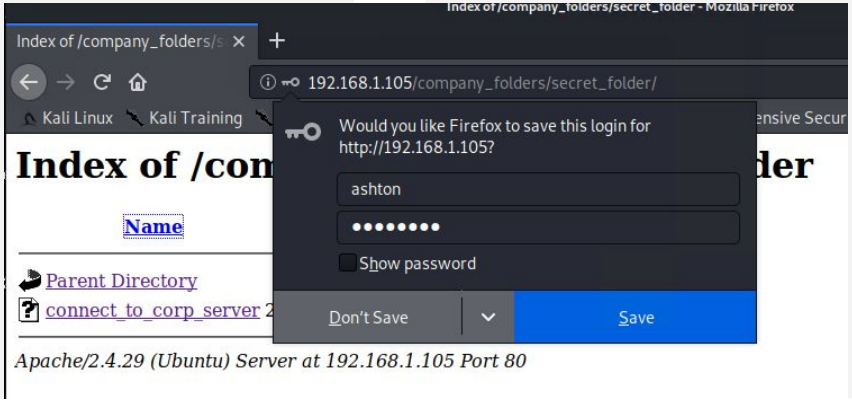
Tools & Processes

I used Hydra which is preinstalled on Kali Linux. I also used rockyou.txt as it also required a password list.

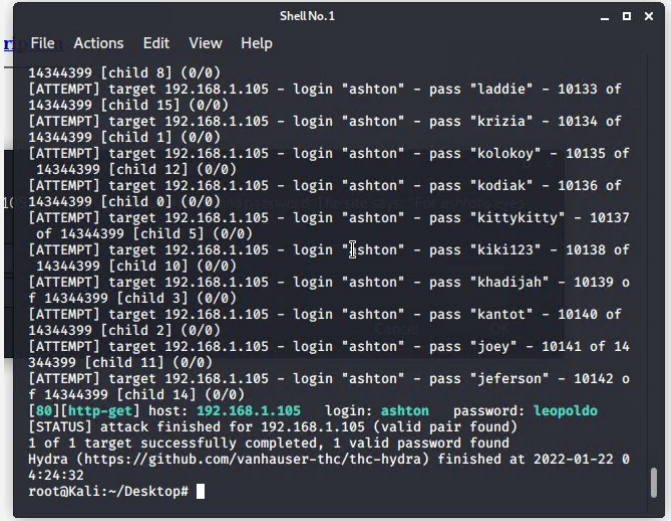
02

Achievements

This exploit confirmed the username “ashton” with the password “leopoldo”



03



Exploitation: [Hashed Password]

01

Tools & Processes

I used crackstation.com to crack the hashed password

02

Achievements

Used the username “Ryan” to access the /webdav folder with the password “linux4u”

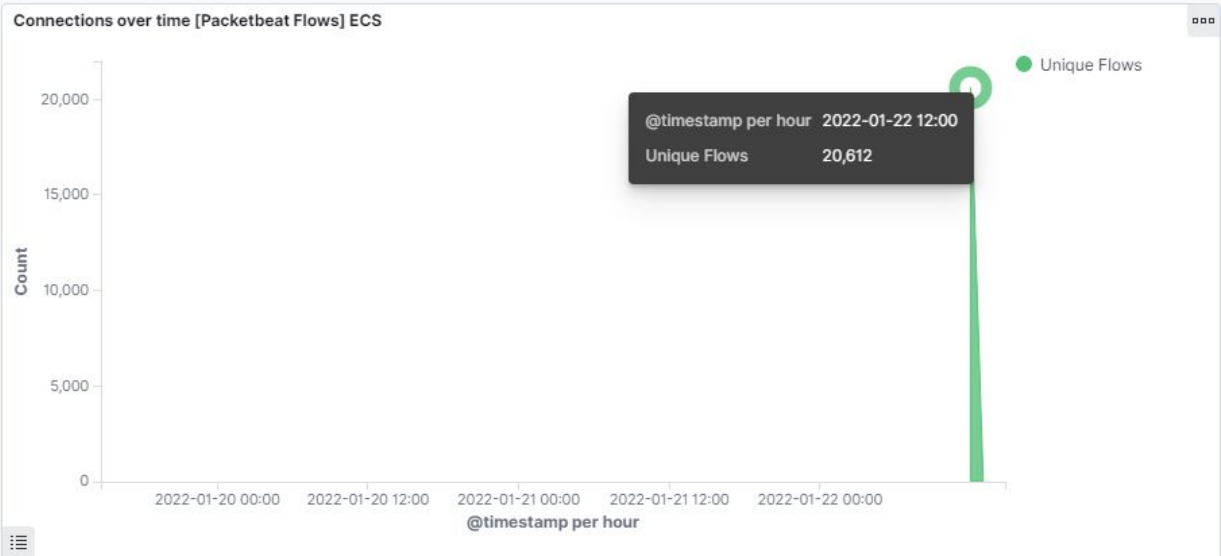
03

Blue Team

Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

- The port scan started on 22nd of January 2022.
- 20,612 connections occurred a the peak, the source IP was 192.168.1.90
- The sudden peaks in network traffic indicate that this was a port scan.



Analysis: Finding the Request for the Hidden Directory

- The request started on the 22nd of January 2022.
- There were 15,868 requests made to access the /secret_folder.
- The /secret_folder contained a hash that could be used to access the system using another Ryan's credentials
- The secret folder also allowed me to upload a payload which can be used to exploit other vulnerabilities.

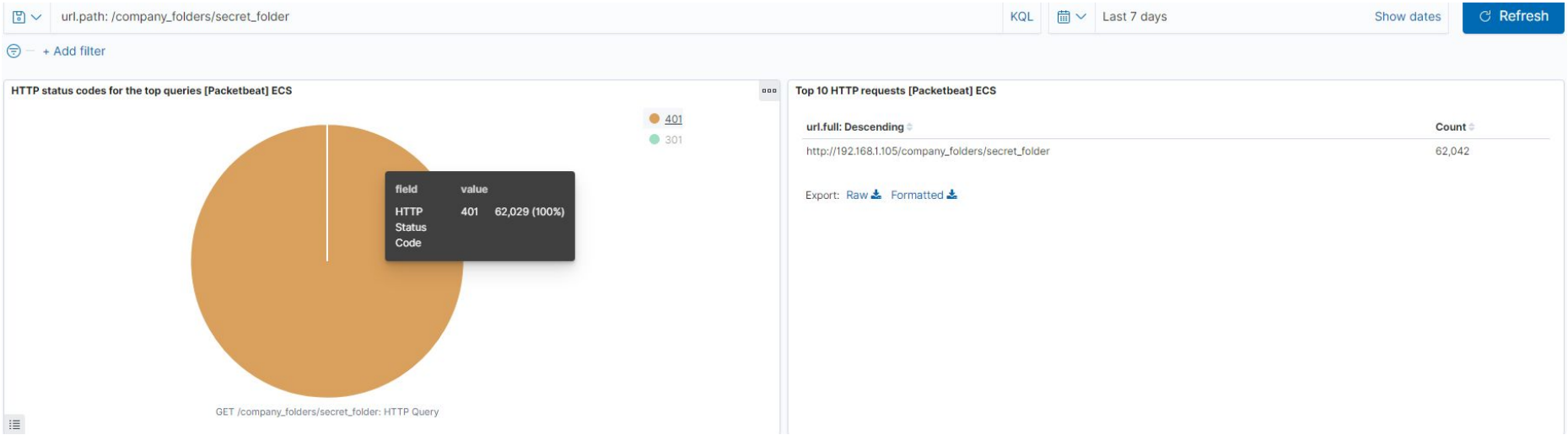
Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	15,868
http://192.168.1.105/webdav	18
http://192.168.1.105/	4
http://192.168.1.105/company_folders/secret_folder/	4
http://192.168.1.105/company_folders/secret_folder/connect_to_corp_server	2

Export: Raw Formatted

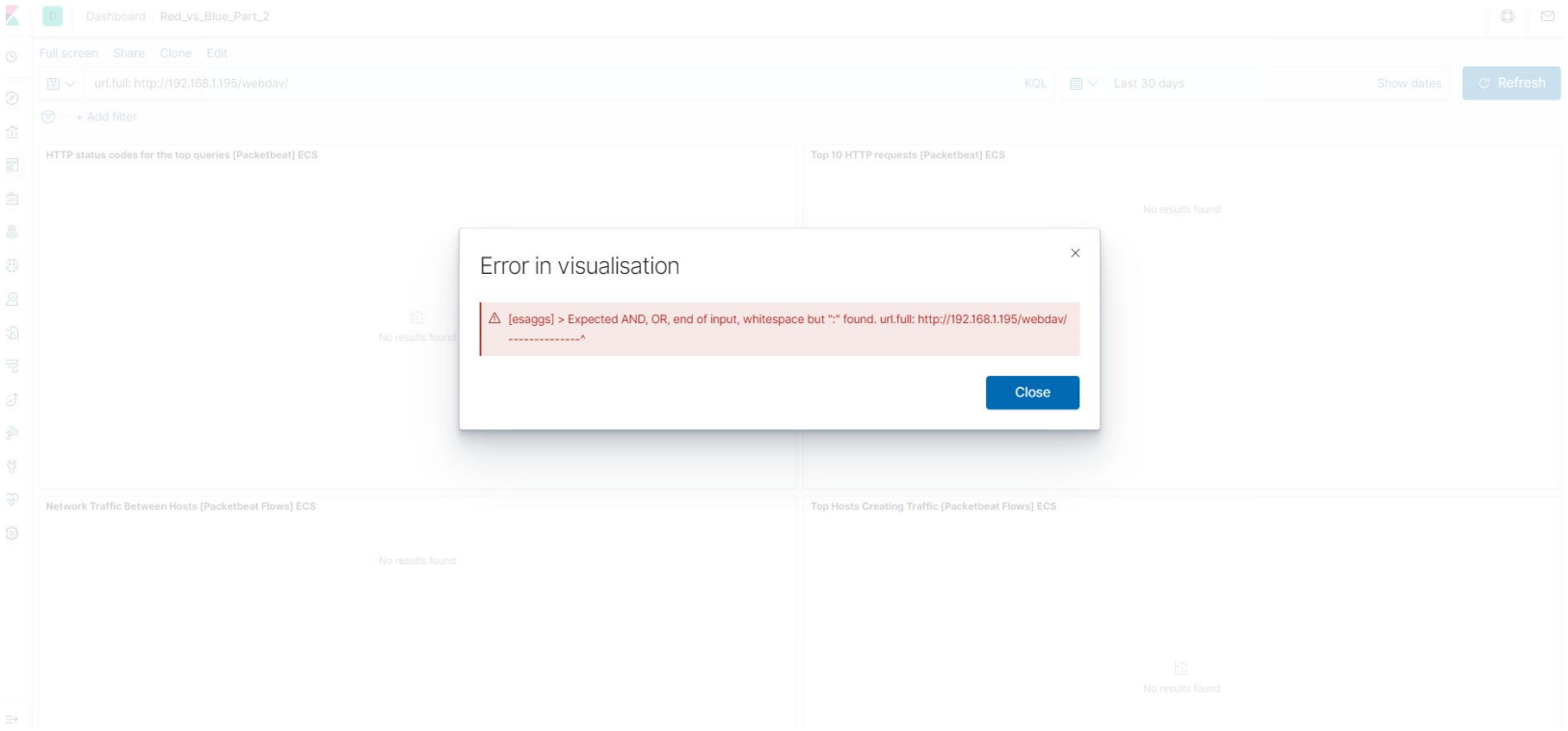
Analysis: Uncovering the Brute Force Attack

- 62,042 requests were made during the attack to access the secret folder.
- 62,029 requests were made before the attacker discovered the password.



Analysis: Finding the WebDAV Connection

- Getting an error when querying url.full: http://192.168.1.105/webdav
- Getting blank results when querying url.full: “http://192.168.1.105/webdav”



Blue Team

Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

Set pings every time there are 1000 connections within an hour.

System Hardening

- Make sure the firewall is always updated to minimize new zero-day attacks
- The firewall should be able to cut off the scan attempts in real time.
- Set server iptables to drop packet traffic when thresholds are exceeded
- Run a system port scan regularly to detect and record any open ports.

Mitigation: Finding the Request for the Hidden Directory

Alarm

I will set an alert when there are requests to for the secret folders and files to detect any unauthorized access.

I would recommend a threshold of maximum 5 attempts per hour that would trigger an alert to be sent.

System Hardening

- Any highly confidential folders should not be shared for public access.
- Make sure data contained within confidential folders are encrypted.
- Review IP addresses that cause an alert to be sent: either whitelist or block the IP addresses.
- Do not use any obvious naming conventions for sensitive/company critical data/private folders

Mitigation: Preventing Brute Force Attacks

Alarm

A HTTP 401 Unauthorised client error indicates that the requests has not been applied because it lacks valid authentication credentials for the target source.

By setting an alarm that alerts if a 401 error is returned we can detect any future brute force attacks.

I would set a threshold of 5-10 errors returned to activate this alarm.

System Hardening

- Create a policy that locks out accounts for 30 minutes after 5 unsuccessful attempts
- Create a policy that requires password complexity. This passwords will be compared to common password lists and prevent users from reusing historical passwords.

Mitigation: Detecting the WebDAV Connection

Alarm

Create a whitelist of trusted IP addresses and review this list every 6 months.

I would set an alarm on the HTTP GET request that activates on any IP addresses trying to access the webDAV directory outside of those trusted IP addresses.

When any HTTP PUT request are made this will activate this alarm.

System Hardening

- Creating a whitelist of all trusted IP addresses and making sure that my firewall security policy blocks all other access.
- I would also ensure that any access to the webDAV folder is only permitted to users with complex username and password.

Mitigation: Identifying Reverse Shell Uploads

Alarm

Alerts will need to be set for any traffic attempting to access port 4444.

I will set the threshold for this alert to activate whenever one or more attempts are made.

System Hardening

- Make sure that only the necessary ports are open.
- Block any IP address other than the whitelisted IP addresses as reverse shell can be created over DNS this action will only limit the risks of reverse shell connections, not eliminate the risk.
- Set the access to the /webDAV folder to read only to prevent payloads from being uploaded.

the End