Capstone Engagement

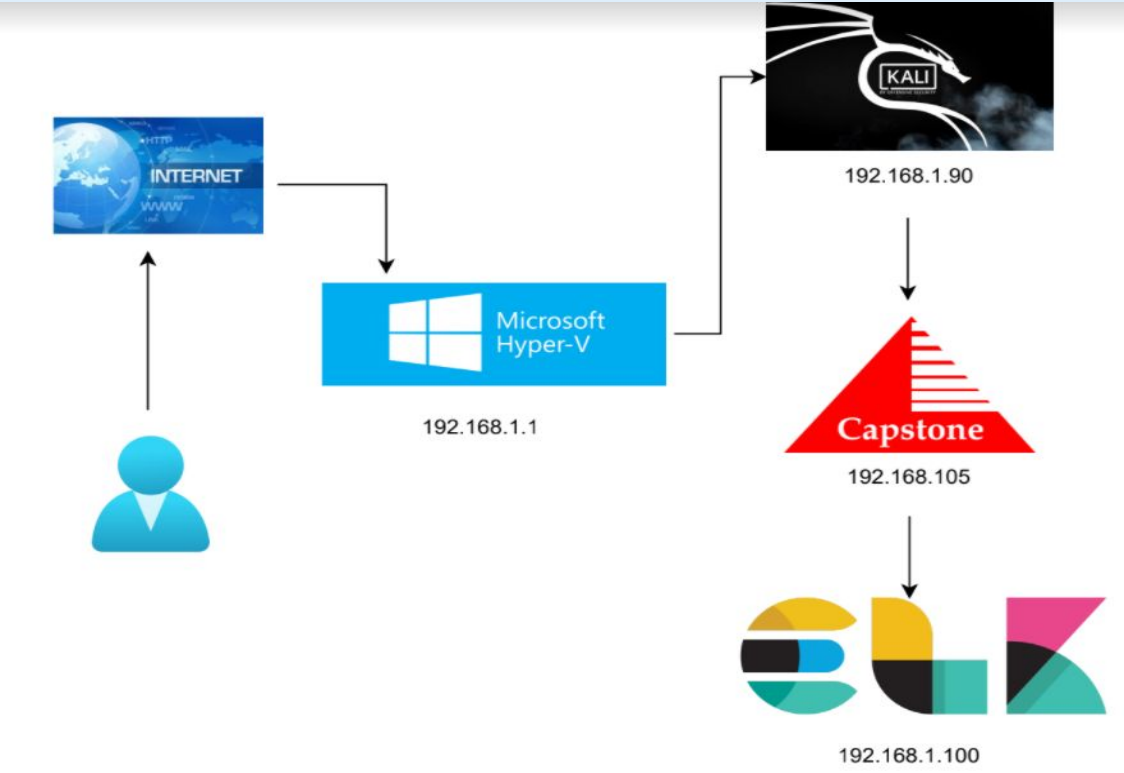
Assessment, Analysis, and Hardening of a Vulnerable System

Table of Contents

This document contains the following sections:

Network Topology

Network Topology



Network
Address Range:
192.168.1.0
Netmask:255.255.255.0
Gateway:10.0.0.76

Machines
IPv4:19.168.1.1
OS: Windows 10
Hostname: Azure -Hyper V

IPv4:192.168.1.100
OS:Linux
Hostname ELK:

IPv4:192.168.1.90
OS: Linux
Hostname: Kali

IPv4:192.168.1.105
OS:Linux
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 Host Machine	192.168.1.1	Host Machine
Kali Linux	192.168.1.90	Machines used to exploit
Capstone	192.168.1.105	Target Machine
ELK	192.168.1.100	Monitor and analyze data and logs

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Port 80 is open to public access.	Unsecured access to Port 80 from the public..	Sensitive files and folders can easily be located from the public
Hashed Passwords	When a password has been “hashed” it means it has been turned into a scrambled representation of itself	Hashed passwords can be cracked using many different websites.
WebDAV Configuration	Exploitation using shell access	Allows hackers to modify the website.
Brute Force	The use of several different credential logins in order to gain access..	System access easily gained by programs.

Exploitation: Ports open to public access

01

Tools & Processes

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

02

Achievements

Located both ports 80 and 22 were open.

03

```
Nmap scan report for 192.168.1.100
Host is up (0.00087s 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 (0.00075s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 00:15:5D:00:04:0F (Microsoft)

Nmap scan report for 192.168.1.90
Host is up (0.0000080s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
```

Exploitation: Hashed Passwords

01

Tools & Processes
Crackstation.net allowed access to translate the hashed password.

02

Achievements
The password ‘linux4u’ was used in conjunction with username Ryan to access the /webdav folder.

03

Exploitation: Brute Force

01

Tools

1.Hydra attack used against directory in order to brute force password.

2.Command: $ *hydra –l ashton –P /usr/share/wordlists/rockyou.txt –s 80 –f –vV 192.168.1.105 http-get /company_folders/secret_folder*

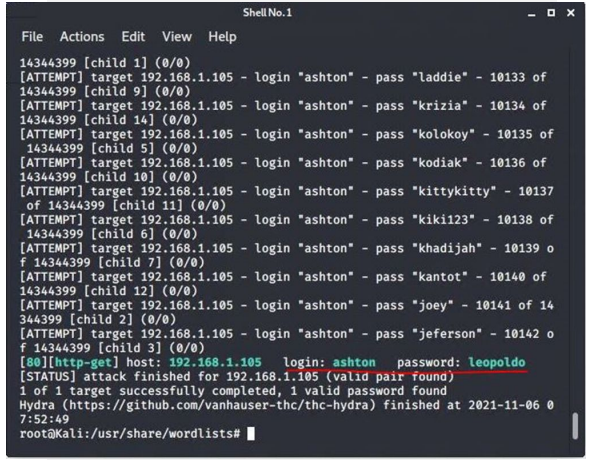
3.Once the attack is complete the username *ashton* and password *leopoldo* are returned.

02

Achievements

The exploit provided me with confirmation of the login name ‘ashton’ as well as the password ‘leopoldo’.

03



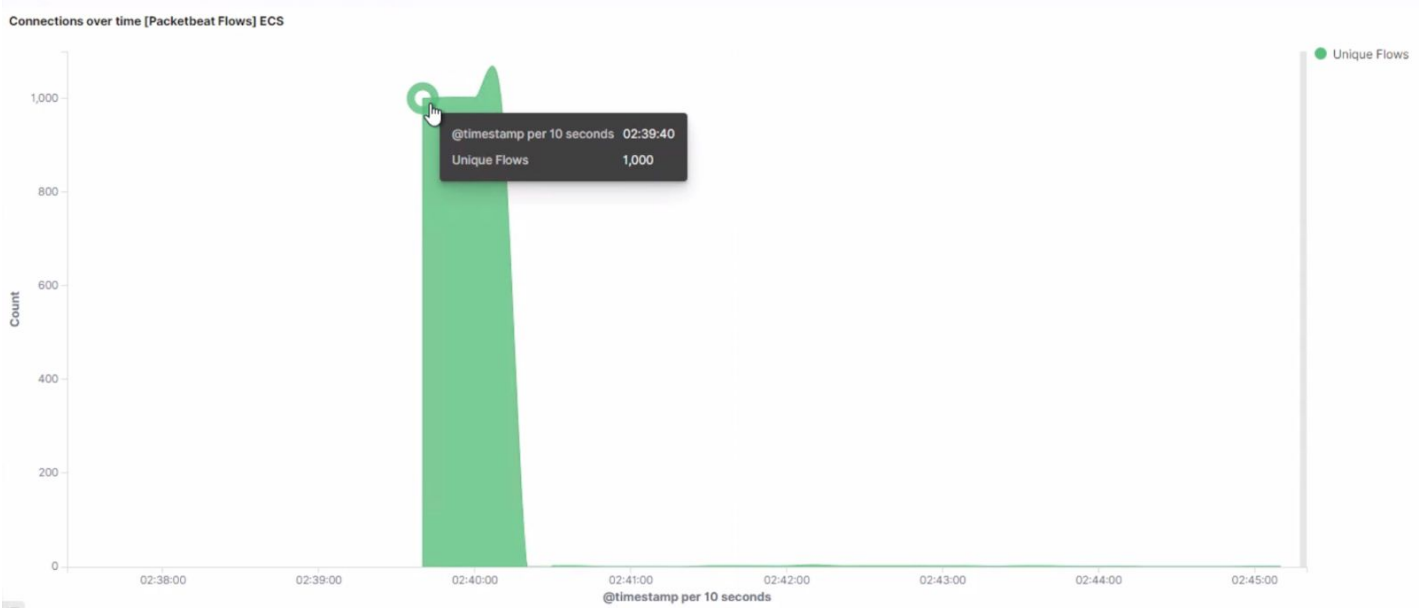
Blue Team

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?



- 2:40
- 1,000 from 192.168.1.8
- Increased connections

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?

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	10,003

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder/connect_to_corp_server	1

- At 2:50 the requests began for a total of 10,003
- The file ‘connect_to_corp’ was the requested which contained server directions and usernames with hashed passwords.

Analysis: Uncovering the Brute Force Attack

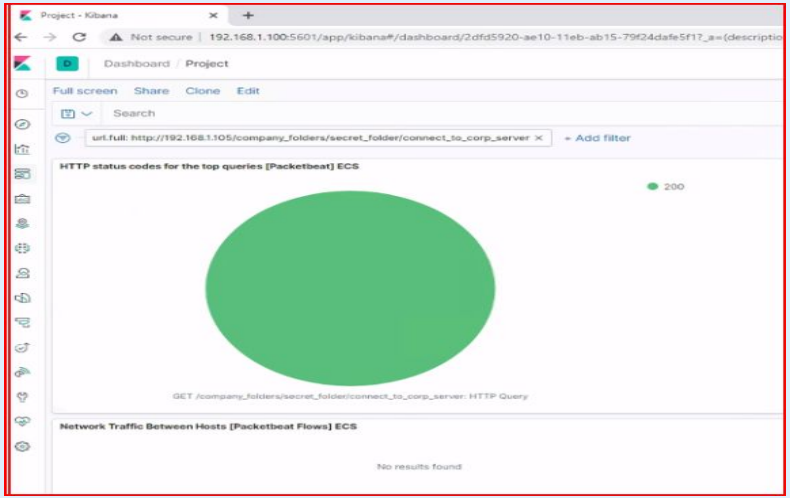
Answer the following questions in bullet points under the screenshot if space allows. Otherwise, add the answers to speaker notes.

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

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	10,003
http://127.0.0.1/server-status?auto=	3,582
http://192.168.1.105/webdav	70
http://192.168.1.105/webdav/shell.php	17
http://192.168.1.105/	9

Export: Raw Formatted

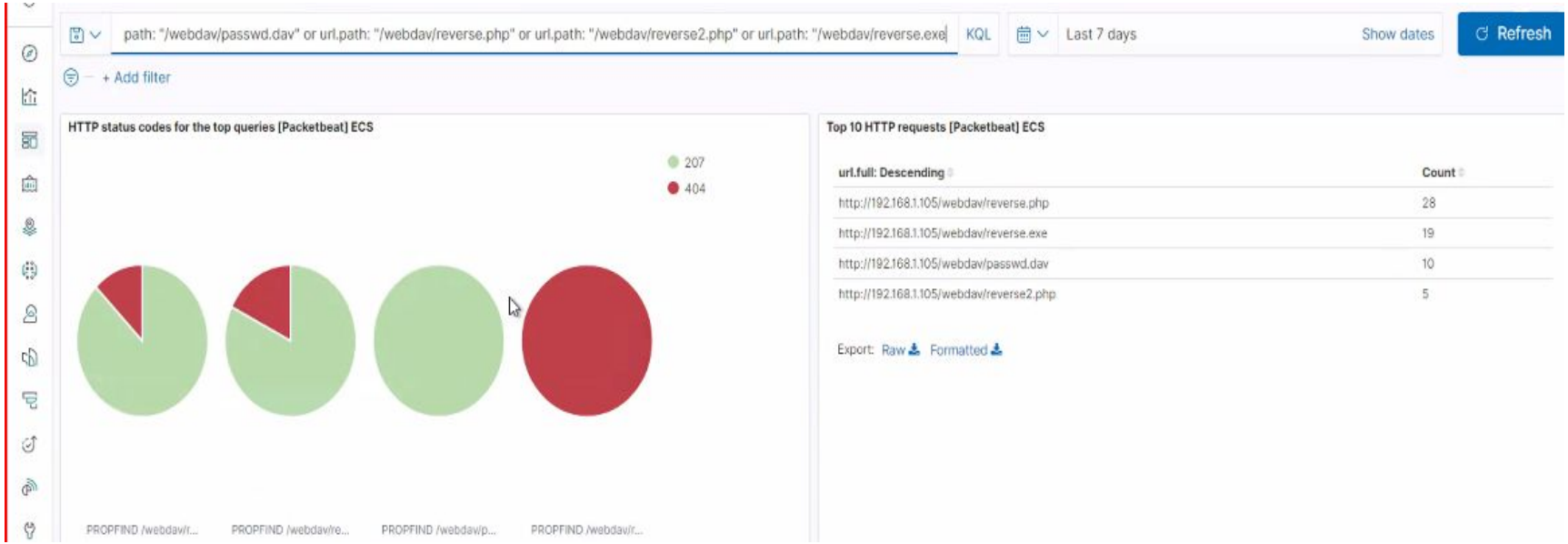


- 10,003 requests were made
- It took the attacker 9 attempts to reveal the password

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?



- 126 requests were made
- 4 files were requested: reverse.php, reverse.exe, passwd.dav, reverse2.php

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?
Alert

What threshold would you set to activate this alarm?
Alerts should be sent when there are 1000 connections every 60 minutes.

System Hardening

What configurations can be set on the host to mitigate port scans?
Limit port availability to only those ports considered necessary for system operations.
An IP allowed list can be enabled.
ICMP traffic can be filtered.
Enable alert triggers to communicate when thresholds have been exceeded.

Describe the solution. If possible, provide

Mitigation: Finding the Request for the Hidden Directory

Alarm

What kind of alarm can be set to detect future unauthorized access?
Alert set when an unauthorized IP addresses attempt to access any hidden files within the server.

What threshold would you set to activate this alarm?
A threshold of 3 attempts per hour should be made.

System Hardening

What configuration can be set on the host to block unwanted access?

Create an IP whitelist
Remove confidential files from server
Encrypt the data

Mitigation: Preventing Brute Force Attacks

Alarm

What kind of alarm can be set to detect future brute force attacks?
Alert for error code 401.

What threshold would you set to activate this alarm?
Ten 401 error codes per second.

System Hardening

What configuration can be set on the host to block brute force attacks?
Password complexity requirements.
Timed lockouts after 3 attempts in thirty minutes
CAPTCHA tool
Second Authentication

Mitigation: Detecting the WebDAV Connection

Alarm

What kind of alarm can be set to detect future access to this directory?
Alert for requests made from non-whitelisted IP address to access the WebDav.

What threshold would you set to activate this alarm?
Any attempt to access the files from an IP address not on the whitelist will trigger alarm.

System Hardening

What configuration can be set on the host to control access?
Whitelist IP address
Restriction and privileges strictly monitored
Remove sensitive information from WebDav

Mitigation: Identifying Reverse Shell Uploads

Alarm

What kind of alarm can be set to detect future file uploads?
Alert

What threshold would you set to activate this alarm?
Alert for when POST requests are made to unauthorized files.

System Hardening

What configuration can be set on the host to block file uploads?
Make sure only necessary ports are open
Remove and restrict .php files from being on WebDav.
Restrict file types that allowed to be uploaded.

the End