Capstone Engagement

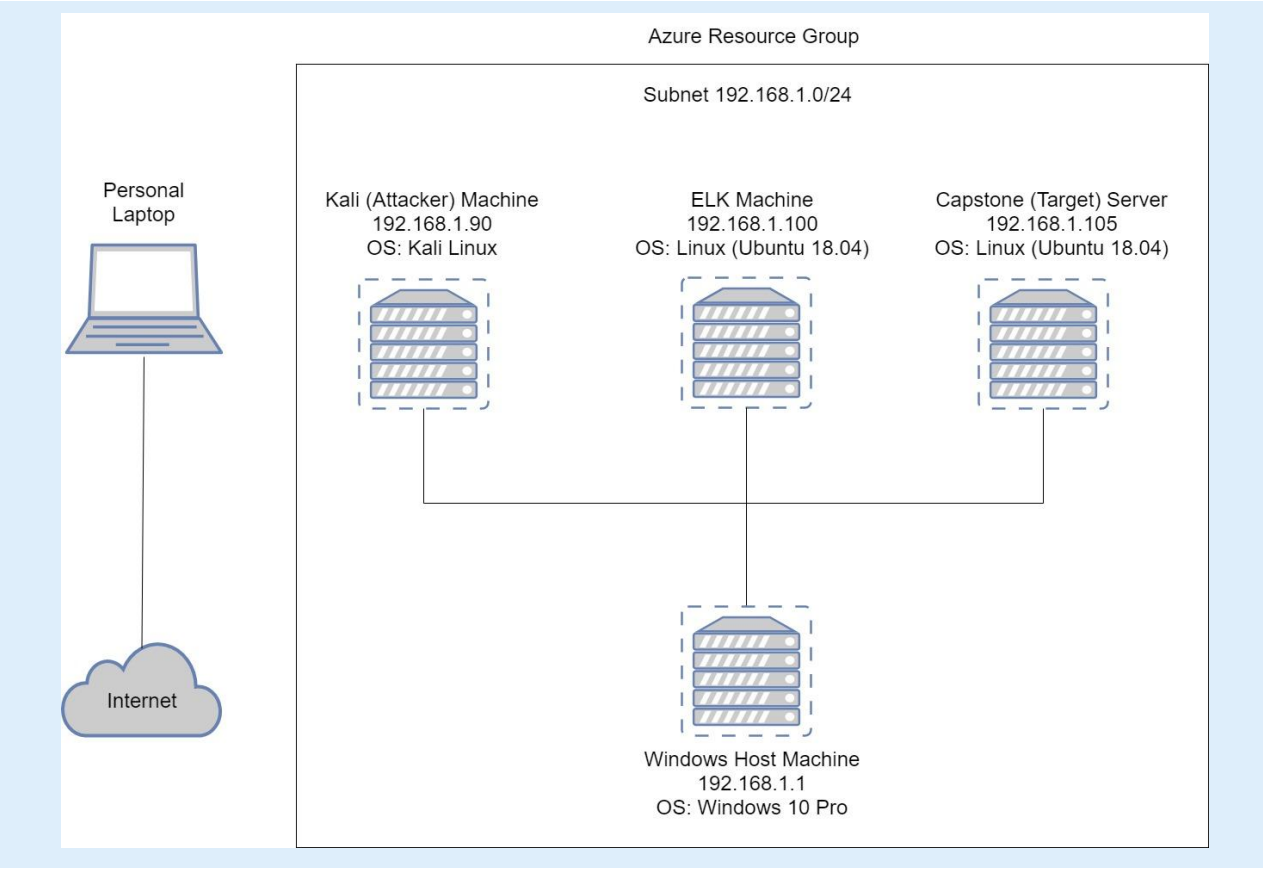
Assessment, Analysis, and Hardening of a Vulnerable System

Table of Contents

This document contains the following sections:

Network Topology

Network Topology



Network
Address Range: 192.168.1.0/24
Netmask: 255.255.240.0
Gateway: 10.0.0.1

Machines
IPv4: 192.168.1.90
OS: Kali Linux
Hostname: Kali VM

IPv4: 192.168.1.100
OS: Linux (Ubuntu 18.04)
Hostname: ELK

IPv4: 192.168.1.105
OS: Linux (Ubuntu 18.04)
Hostname: Capstone Server

IPv4: 192.168.1.1
OS: Windows 10 Pro
Hostname: Windows Host Machine

Red Team

Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Windows Host machine	192.168.1.1	Azure Cloud Environment
Kali VM	192.168.1.90	Red Team Attacking machine
ELK	192.168.1.100	Blue Team Defensive machine
Capstone Server	192.168.1.105	Target machine

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
CWE-548: Information Leak Through Directory Listing	A directory listing is inappropriately exposed, providing an attacker with potentially sensitive information.	Exposing directory lists provides attackers with useful information that allows them to devise exploits.
CWE-307: Improper Restriction of Authentication Attempts **CWE**-521: Weak Password Requirements	Software has insufficient measures to prevent multiple failed authentication attempts in a short time frame. The product does not require users to have strong passwords.	An attacker can perform any amount of authentication attempts and eventually gain access to an account. An attacker can easily guess user passwords and gain user access.
CWE-311: Missing encryption of sensitive data **CWE**-553: Command Shell in Externally Accessible Directory	The software does not encrypt sensitive or critical information before storage or transmission. A possible shell file exists in accessible directories.	An attacker with access to the network can attain sensitive data and use this to devise exploits. An attacker can execute unauthorised code or commands on the web server.

Exploitation: CWE-548

01

Tools & Processes

Used an Nmap scan to discover the IP address and the open port 80 of the target machine.
Entered the IP address on a web browser from the attacker machine.

Navigated through the directory lists to explore different directories and files.

02

Achievements

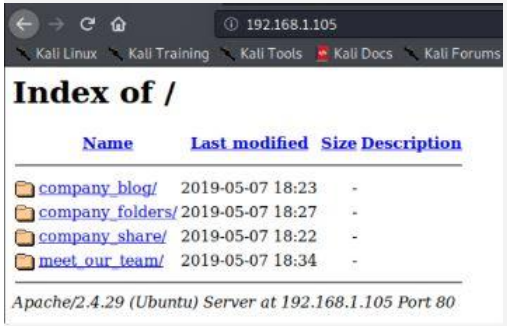
Gained access to the web server of the target machine from the attacker machine.

Discovered a recurring reference to a hidden directory “company_folders/secret_folder” on the web server.

Discovered the user managing the hidden directory.

03

```
Nmap scan report for 192.168.1.105
Host is up (0.00085s latency).
Not shown: 998 closed ports
PORT    STATE SERVICE
22/tcp open  ssh
80/tcp open  http
```




```
Ashton is 22 years young, with a masters
degreee in aquatic jousting. "Moving over
to managing everyone's credit card and
security information has been terrifying.
I can't believe that they have me managing
the company_folders/secret_folder! I
really shouldn't be here" We look forward
to working more with Ashton in the future!
```

Exploitation: CWE-307 & CWE-521

01

Tools & Processes

Used Hydra and the “rockyou.txt” word list to gain access via brute force into the secret_folder directory.

02

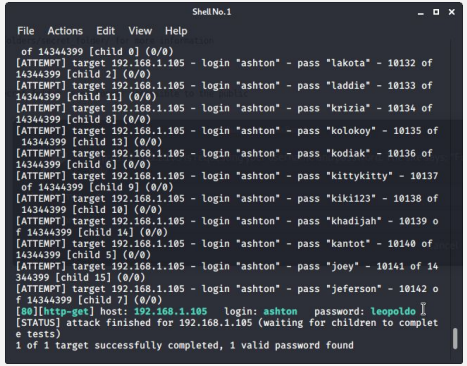
Achievements

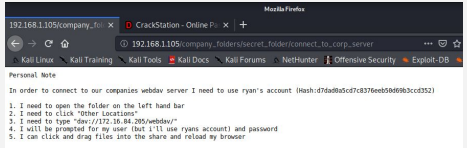
Gained access into the secret_folder directory.

Uncovered the following sensitive company information:

- Another users credentials in a password hash.
- Instructions on making changes to the WebDAV protocol in plaintext.

03





Exploitation: CWE-311 & CWE-553

01

Tools & Processes

Used “crackstation.net” to crack the password hash for new user ‘Ryan’ provided in secret_folder.

Created and uploaded an msfvenom payload and used metasploit to establish a remote listener.

Executed a reverse shell to open a backdoor on the webserver.

02

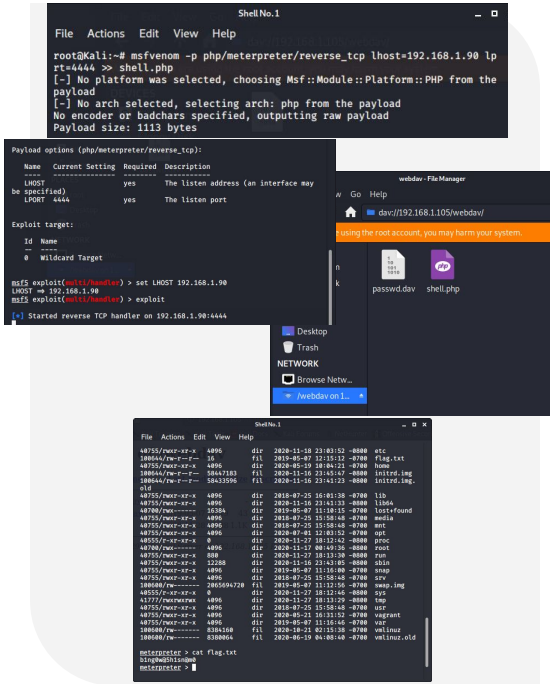
Achievements

What did the exploit achieve? For example: Did it grant you a user shell, root access, etc.?

Ryan’s credentials granted access to the WebDAV.

Opening a backdoor granted access to the root directory on the capstone server and retrieve the “flag.txt” file.

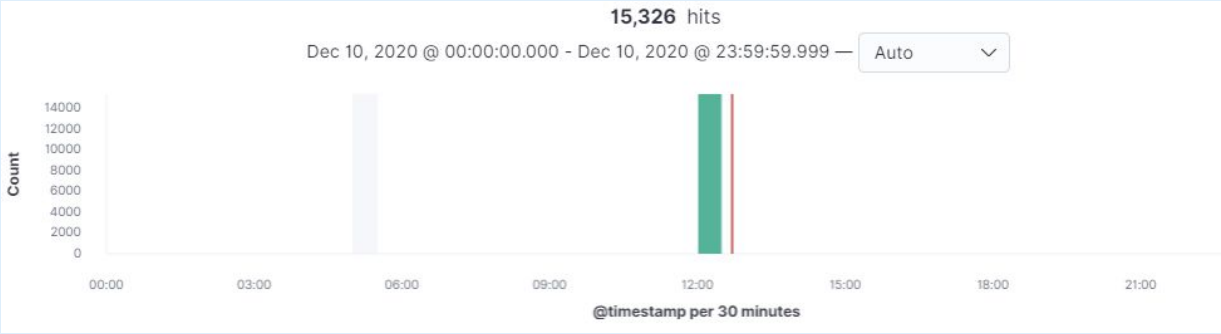
03



Blue Team

Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan



- The port scan occurred at 12:04pm
- 15326 packets were sent from the IP address 192.168.1.90

Top Source Ports [Filebeat Netflow]

Source	Bytes	Packets	Flow Records
32768	0B	0	1
32770	0B	0	1
32772	0B	0	1
32774	0B	0	1
32776	0B	0	1
32778	0B	0	1
32780	0B	0	1
32782	0B	0	1

- The fact that there were multiple ports requested at the same time indicates this was a port scan.

Analysis: Finding the Request for the Hidden Directory

Time	_source
> Dec 10, 2020 @ 12:03:58.084	url.path: /company_folders/secret_folder @timestamp: Dec 10, 2020 @ event.kind: event event.category: network_traffic event.dataset: ht 10, 2020 @ 12:03:58.084 event.end: Dec 10, 2020 @ 12:03:58.085 url.full: http://192.168.1.105/company_folders/secret_folder url.sch client.ip: 192.168.1.90 client.port: 53016 client.bytes: 163B serve

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	15,326

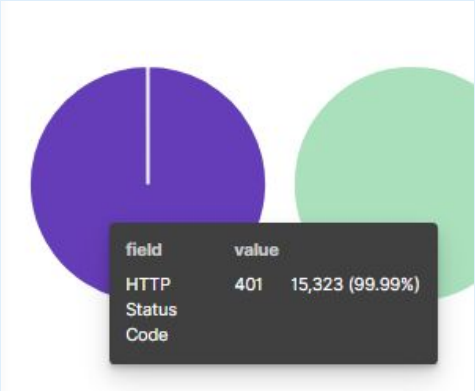
- The request occurred at 12:04pm and 15326 requests were made

```
Personal Note

In order to connect to our companies webdav server I need to use ryan's account (Hash:d7dad0a5cd7c8376eeb50d69b3ccd352)

1. I need to open the folder on the left hand bar
2. I need to click "Other Locations"
3. I need to type "dav://172.16.84.205/webdav/"
4. I will be prompted for my user (but i'll use ryans account) and password
5. I can click and drag files into the share and reload my browser
```

- The company_folders/secret_folder file was requested and contained the information depicted above.

Analysis: Uncovering the Brute Force Attack

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	15,326



- A total of 15326 requests were made during the brute force attack
- 15323 requests received an error 401 HTTP code indicating only 3 requests were successful.

Analysis: Finding the WebDAV Connection

url.full: Descending	Count
http://192.168.1.105/webdav	72

- 72 requests were made to the webdav directory

url.full: Descending	Count
http://192.168.1.105/webdav/shell.php	50
http://192.168.1.105/webdav/passwd.dav	8

- The webdav/shell.php file was requested 50 times and the webdav/passwd.dav file was requested 8 times.

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?

An alarm that alerts if a certain number of ports from any IP address that is not 192.168.1.105 reaches higher than a set threshold.

What threshold would you set to activate this alarm?

3 ports accessed per source IP per second.

System Hardening

What configurations can be set on the host to mitigate port scans?

- Enable filters that sweep for port scans from other IP addresses.
- Log TCP connection attempts.
- Firewall blocking all nonessential access to ports.

Mitigation: Finding the Request for the Hidden Directory

Alarm

What kind of alarm can be set to detect future unauthorized access?

An alarm that allows only internal IP addresses to request access to the hidden directory.

What threshold would you set to activate this alarm?

A single attempt from an external IP must activate the alarm. (Threshold: 0)

System Hardening

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

- Stronger authentication
- Encrypted data inside hidden directory
- Configure filebeat to monitor access to hidden directory
- Deny access to the folder from external IP addresses

Mitigation: Preventing Brute Force Attacks

Alarm

What kind of alarm can be set to detect future brute force attacks?

An alarm that is activated if the number of 401 HTTP status codes issued in 10 second intervals reaches a threshold.
A second alarm that is activated if the “user_agent.original” field detects “hydra” in its result.

What threshold would you set to activate this alarm?
3

System Hardening

What configuration can be set on the host to block brute force attacks?

- Strong password policy
- Account lockout after 5 attempts
- Implement CAPTCHA to ensure the user is human

Mitigation: Detecting the WebDAV Connection

Alarm

What kind of alarm can be set to detect future access to this directory?

An alarm that is activated any time the directory is accessed by a non-specified IP address.

What threshold would you set to activate this alarm?

A single attempt from a non-specified IP must activate the alarm. (Threshold: 0)

System Hardening

What configuration can be set on the host to control access?

- Multi-factor authentication
- Whitelist essential IP's

Mitigation: Identifying Reverse Shell Uploads

Alarm

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

An alert when a PUT request is made by any non-specified machine and an alert for any traffic over port 4444 or 5555.

What threshold would you set to activate this alarm?

A single attempt from any non-specified IP must activate the alarm. (Threshold: 0)

System Hardening

What configuration can be set on the host to block file uploads?

- Authentication required for file uploads
- An upload filter the inhibits users from uploading files with executable code

the End