Capstone Engagement

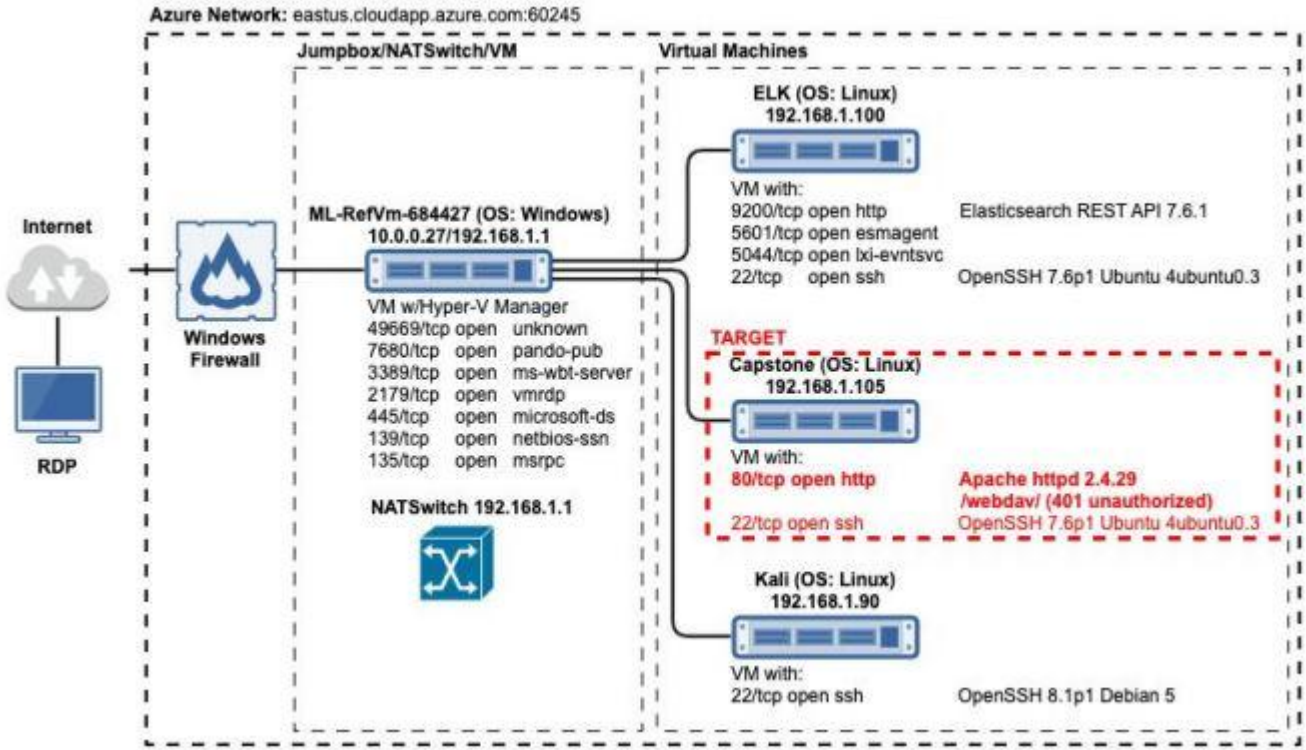
Assessment, Analysis, and Hardening of a Vulnerable System

Table of Contents

This document contains the following sections:

Network Topology

Network Topology



Network
Address Range:
Netmask:
Gateway:

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
Capstone	192.168.1.105	Web Server
ELK	192.168.1.100	SIEM System
ML-RefVm-684427	192.168.1.1	NATSwitch
Kali	192.168.1.90	Penetration Test System

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Directory listing enabled on Apache Web Server	*Allows for full read access of directories on Apache Web Server*	*Sensitive information exists in the directories. Shows that Ashton is the administrator for /company_folders/secret_folder/*
Weak Password with no Multi-Factor Authentication or Password Lockout	Password is able to be brute forced due to no lockout features due to failed logins or MFA	Brute force allowed access to /secret_folder/ and displayed a password has for Ryan @ dav://192.168.1.105/webdav/
Reverse Shell	Allows for a reverse shell exploit to gain access on web server. IPS/IDS/Firewall allow outbound ports and undetected reverse shell	Successfully achieved remote access via a backdoor reverse shell to Apache Web Server

Exploitation: Directory Listing on Apache Web Server

01

Tools & Processes

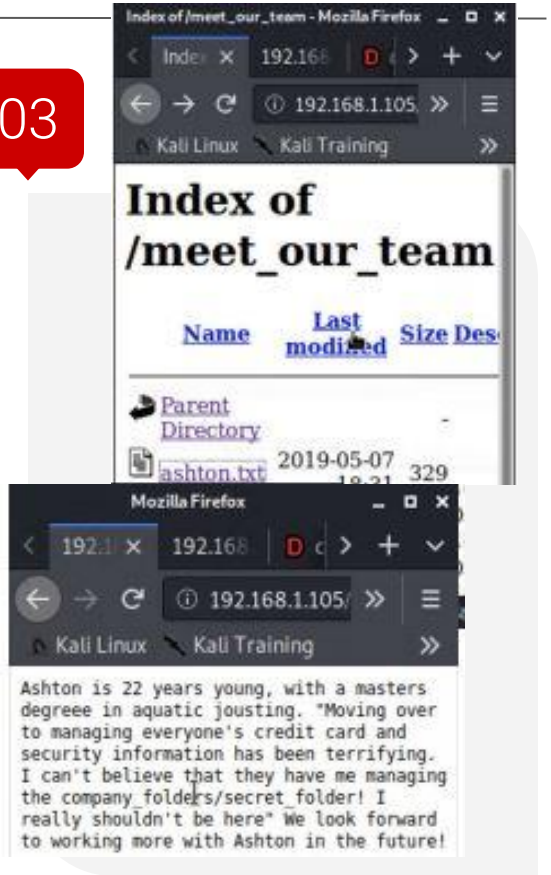
Navigate to 192.168.1.105/ on any web browser

02

Achievements

Searched through files on web server and quickly discovered Ashton is the administrator for /company_folders/secret_folder/

03



Exploitation: Weak Password & No Lockout or MFA

01

Tools & Processes

Use Hyrda to execute a brute force dictionary attack to get Ahston's password

hydra -t 4 -V -f -l ashton -P /usr/share/wordlists/rockyou.txt http-get://192.168.1.105/company_folders/secret_folder/

02

Achievements

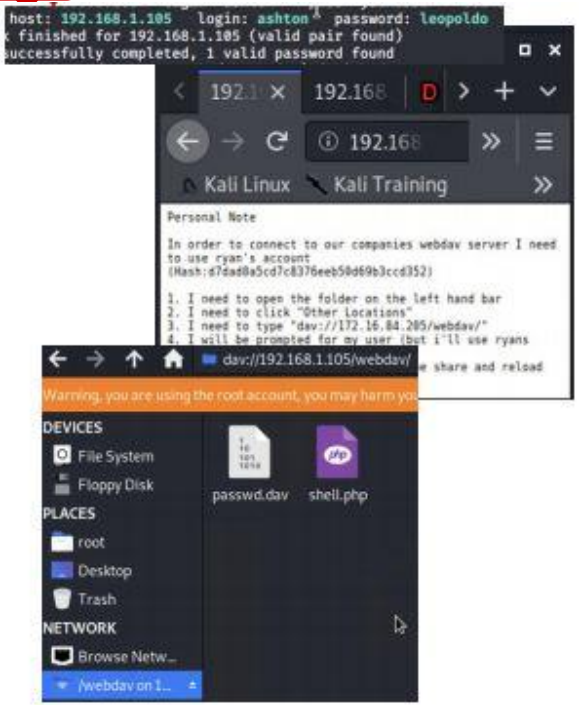
Password for Ashton was found in "rockyou.txt" dictionary

Achieved access to /secret_folder/

Access to /webdav/ system was discovered

A password hash was found for Ryan. Password was cracked using online tool

03



Exploitation: Reverse Shell

01

Tools & Processes
Uploaded reverse shell payload using php/meterpreter/reverse_tcp

Created remote listener on port 1234

Executed reverse shell backdoor on Capstone Apache server

02

Achievements
Opened a remote backdoor shell to the Capstone Apache Server and gained access to root directory.

03

Meterpreter > shell find / -name flag.txt 2>/dev/null

Output: /flag.txt

cd /
cat flag.txt

Output: b1ng0w@5h1sn@m0

Blue Team
Log Analysis and Attack Characterization

Analysis: Finding the Request for the Hidden Directory

- There were 6, 319 requests made. The “connect_to_corp_server” file was requested which holds instructions as to how to connect to the server

File/Folder Accessed	Attacker IP Address	Access Count
http://192.168.1.105/company_folders/secret_folder/	192.168.1.90	6,319
http://192.168.1.105/company_folders/secret_folder/connect_to_corp_server	192.168.1.90	1

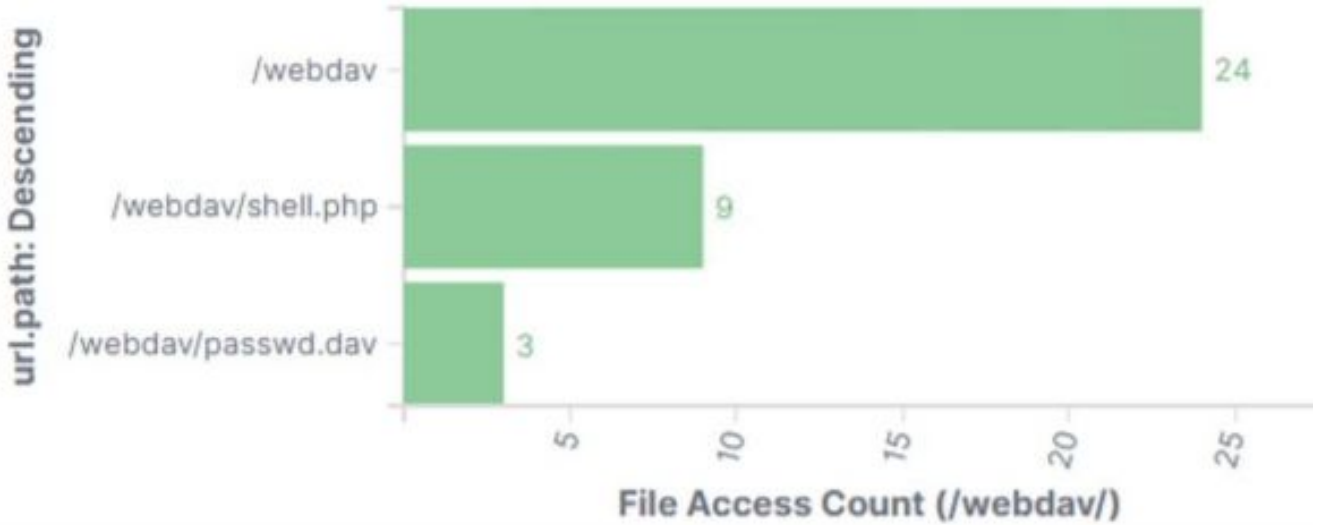
Analysis: Uncovering the Brute Force Attack

- 6,314 requests were made in the brute force attack
- 6313 requests were made before the password was discovered

http.response.status_code: Descending	source.ip: Descending	destination.ip: Descending	user_agent.original: Descending	url.path: Descending	Count
401	192.168.1.90	192.168.1.105	Mozilla/4.0 (Hydra)	/company_folders/secret_folder/	6,313
200	192.168.1.90	192.168.1.105	Mozilla/4.0 (Hydra)	/company_folders/secret_folder/	1

Analysis: Finding the WebDAV Connection

- 36 requests were made to this directory
- The files that were requested were shell.php and passwd.dav



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?

destination.ip: 192.168.1.105 and source.ip: (not 192.168.1.105) and destination.port: (not 443 or 80) Report criteria: Number of ports accessed per source IP per second.

What threshold would you set to activate this alarm?

When more than 3 non port 403 or port 80 scans are detected at the same timestamp from the same IP

System Hardening

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

Firewall block on all ingress and egress communication on all ports except for 80 and 443

Describe the solution. If possible, provide required command lines.

IPtables/Firewall port blocking:
iptables -A INPUT -p tcp -m multiport! -dports,80,443 -j DROP

Mitigation: Finding the Request for the Hidden Directory

Alarm

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

source.ip: (not 192.168.1.105 or 192.168.1.1) and url.path : *secret_folder*

Number of times “secret_folder” accessed from external IP

What threshold would you set to activate this alarm?

Alert email and log when > 0 access is detected on “secret_folder” from IPs other than 192.168.1.105 or 192.168.1.1.

System Hardening

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

Configure the file to block unauthroized access from any IP other than what is explicitly allowed

Describe the solution. If possible, provide required command lines.

> nano /etc/httpd/conf/httpd.conf

* Locate directory section (/var/www/) and set it as follows:

Order allow,deny
Allow from 192.168.1.1
Allow from 192.168.1.105
Allow from 127
Deny from 192.168.1.90
*Disable directory listing in apache remove Indexes:

Mitigation: Preventing Brute Force Attacks

Alarm

What kind of 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)

What threshold would you set to activate this alarm?

Alert email and log when protected files and folders > 5 Error(401) responses occur

Any OK (2002) responses occur from non trusted IPs

System Hardening

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

A stronger password and MFA. If MFA is not possible, require security questions to be answered after a few failed attempts

Describe the solution. If possible, provide the required command line(s).

A stronger password is always a good place to start. Adding MFA when possible nearly entirely eliminates any chance of a Brute Force from happening. If MFA isn't possible, requiring security questions after a certain number of failed attempts would also be a good additional layer of security.

Mitigation: Detecting the WebDAV Connection

Alarm

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

Search criteria:
http.request.method : * and url.path: *webdav* and source.ip: (not 192.168.1.150 or 192.168.1.1)

Report criteria: Number of times the directory is requested from non-trusted IPs

What threshold would you set to activate this alarm?

Alert email and log when requests are made, on protected files and folders, from non-trusted IPs

System Hardening

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

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

Open your httpd.conf file:
> nano /etc/httpd/conf/httpd.conf

Locate directory section (/var/www/) and set it as follows:

```
<Directory /var/www/webdav/>
        Order allow,deny
        Allow from 192.168.1.1
        Allow from 192.168.1.105
        Allow from 127
        Deny from all
</Directory
```

Mitigation: Identifying Reverse Shell Uploads

Alarm

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

http.request.method : “put” and url.path: *webdav* and source.ip: (not 192.168.1.1 or 192.168.1.105)

What threshold would you set to activate this alarm?

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

System Hardening

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

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

Open your httpd.conf file:
> nano /etc/httpd/conf/httpd.conf (location may vary)

Locate directory section (/var/www/) and set it as follows:

```
<Directory /var/www/webdav/>
        Order allow,deny
        Allow from 192.168.1.1
        Allow from 192.168.1.105
        Allow from 127
        Deny from all
        <LimitExcept GET POST HEAD>deny from all
        </LimitExcept>
</Directory>
```


The End