Capstone Engagement

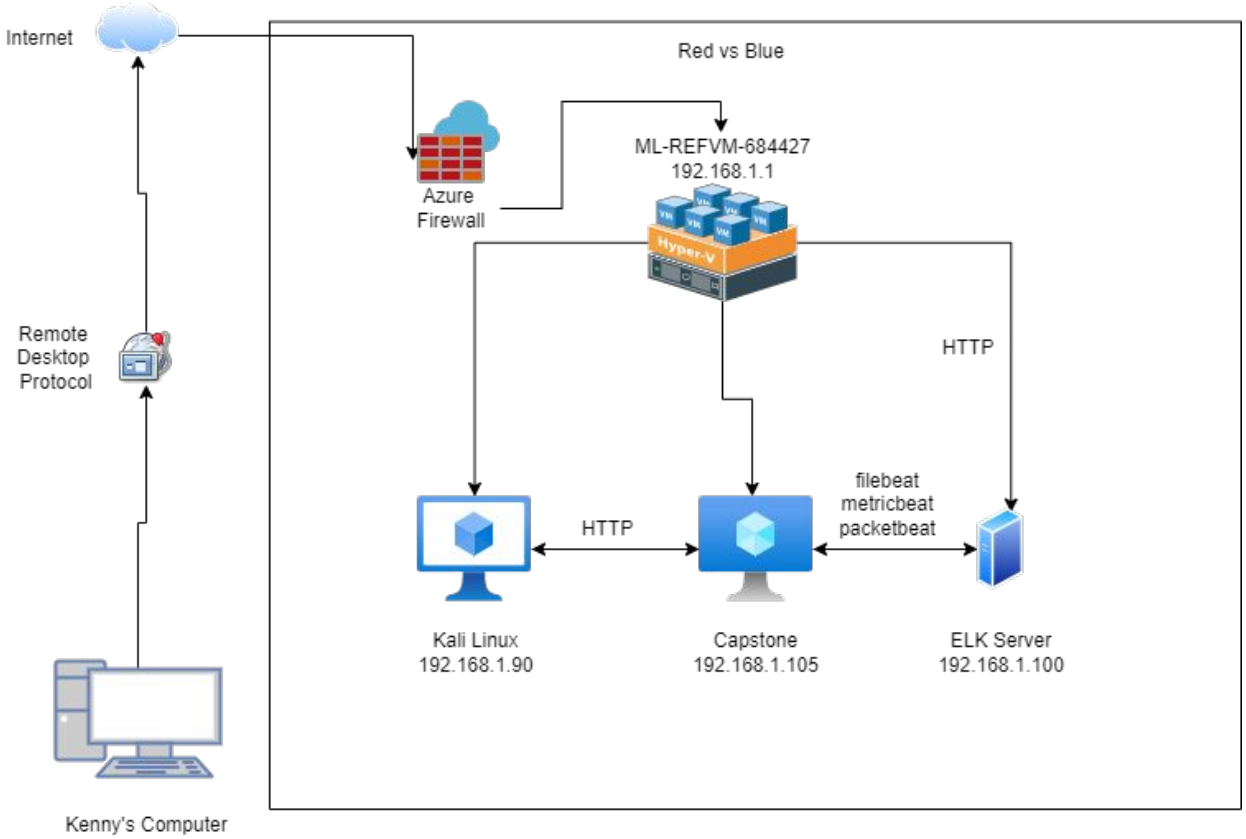
Assessment, Analysis, and Hardening of a Vulnerable System

Table of Contents

This document contains the following sections:

Network Topology

Network Topology



Network
Address Range: 192.168.1.0/24
Netmask: 255.255.255.0
Gateway: 192.168.1.1

Machines
IPv4: 192.168.1.1
OS: Windows 10 Pro
Hostname: Red vs Blue

IPv4: 192.168.1.90
OS: Kali Linux 5.4.0
Hostname: Kali

IPv4: 192.168.1.105
Hostname: Capstone

IPv4: 192.168.1.100
Hostname: ELK Server

Red Team
Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Kali	192.168.1.90	Attacker/ Used to exploit Capstone vulnerabilities
ELK Sever	192.168.1.100	Monitoring and logging traffic on Capstone server
Capstone	192.168.1.105	Target
Azure Hyper-V	192.168.1.1	Hosting Kali, ELK Server and Capstone

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Brute Force Vulnerability	No password protocol to prevent rapid multiple login entries.	Easy to crack users and passwords can increase the likelihood of being breached.
Sensitive Data Exposure	Usernames and password hashes were available to view.	Leaks and possible credentials being compromised which attackers can use for other malicious activity.
Unauthorized File Upload	Attackers can upload malicious files onto the web servers.	PHP scripts can be uploaded to the server.
Remote Code Execution	Attackers can use PHP scripts to open a reverse shell.	Attackers can execute malicious commands to gain access to sensitive data.

Exploitation: Nmap and Brute Force Attack

Tools & Processes

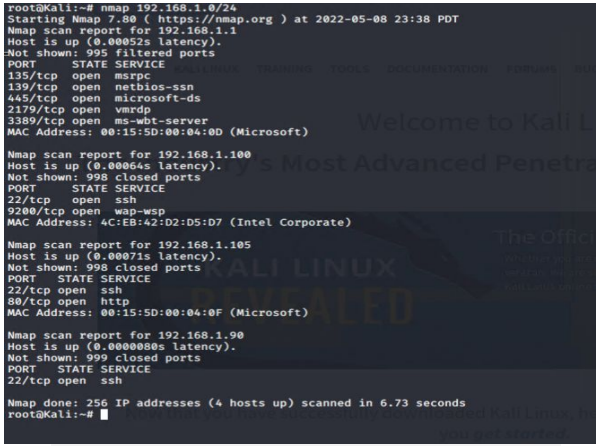
Used Nmap to scan networks for the target's IP and to view open ports which can lead to known vulnerabilities. Target IP was found with an open port 80 which allows for HTTP. This lead to finding a hidden directory which was password protected but vulnerable to brute force attacks. The login authentication gave information that user is Ashton.

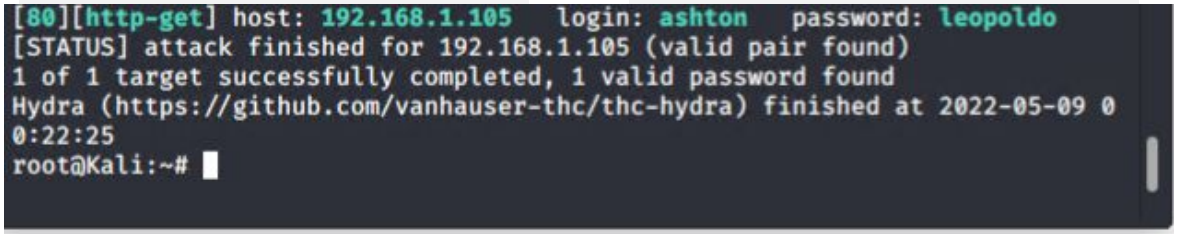
Achievements

Target IP found: 192.168.1.105

Open Port: 80

Hidden Directory Found: /company_folders/secret_folder

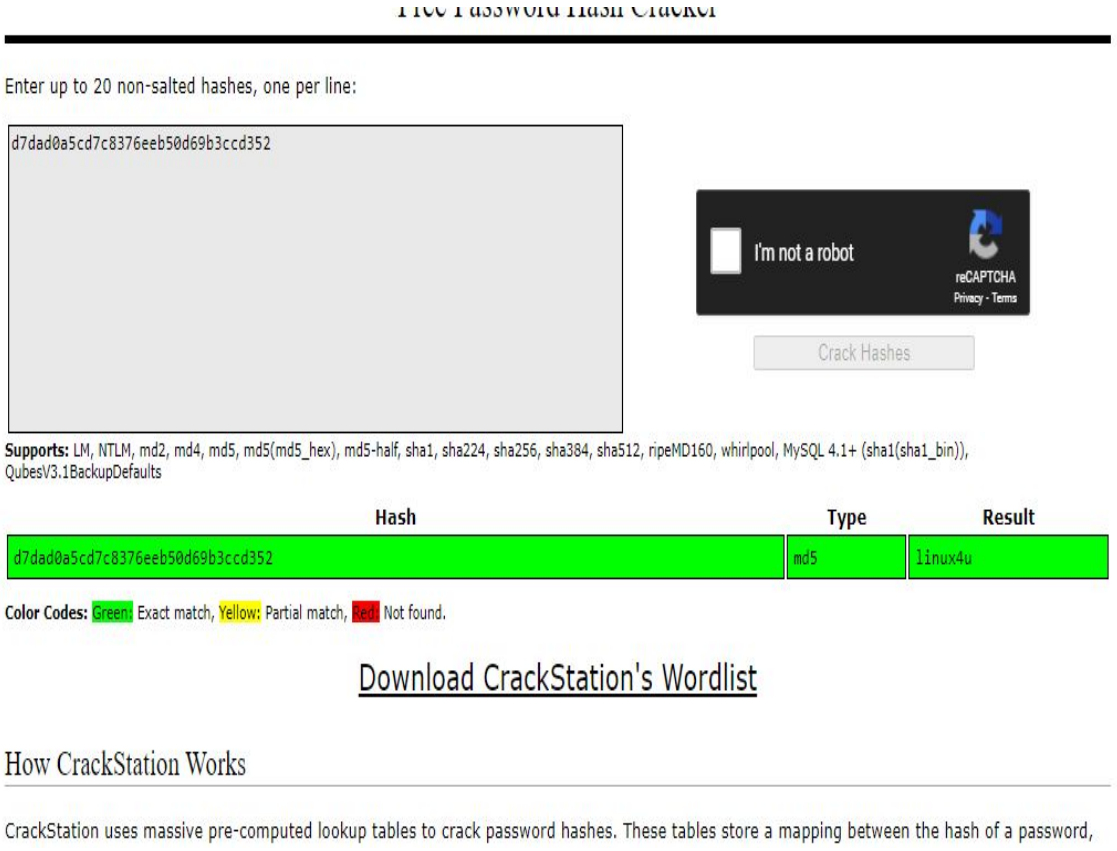




Exploitation: Password Hash Crack

Tools & Processes
Once access was gained on the secret folder, there was a hash for a different account given. Using crackstation.net, the hash was cracked within a second.

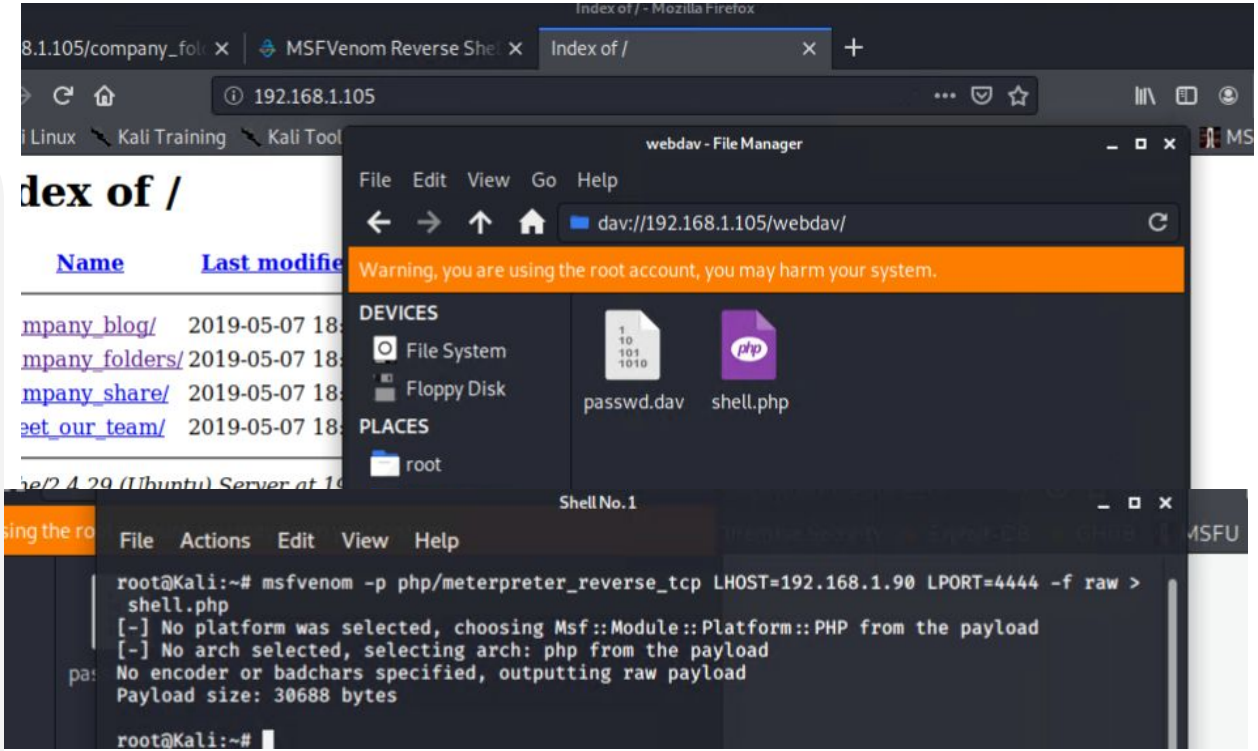
Achievements
Password to Ryan's account: linux4u



Exploitation: Uploading Reverse Shell onto Server

Tools & Processes
After gaining access to Ryan's account, I was able to upload any file I wanted onto the server. Using msfvenom, a reverse shell that allowed meterpreter was uploaded.

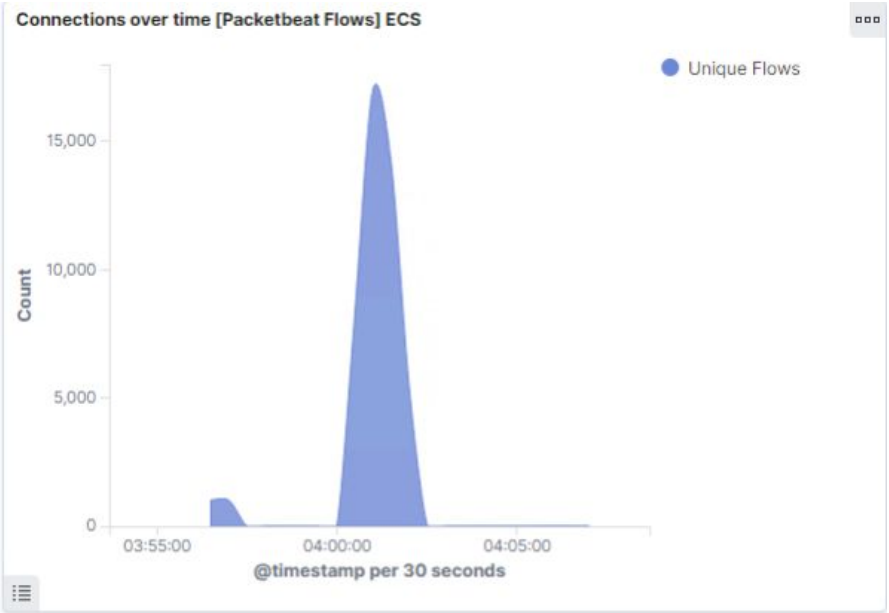
Achievements
Uploaded reverse shell to establish a connection to target's PC.

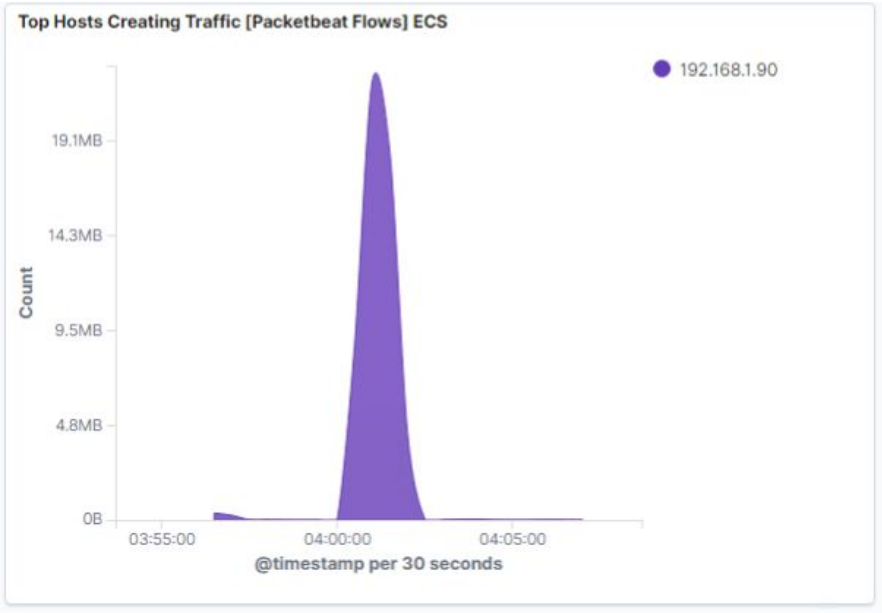


Blue Team
Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

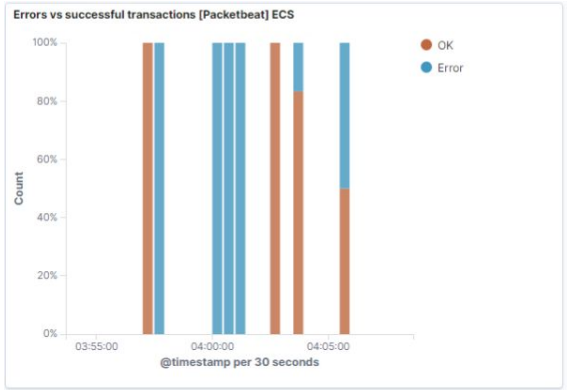
At around 3:56:00, there was a potential port scan being done due to a small influx of connections. A total of 1,016 packets were sent from the IP: 192.168.1.90. Usually, if a user detects a high number of connections within a short time period, this may be an indicator that a port scan has been done. However, further analysis will be needed to make sure.





Analysis: Finding the Request for the Hidden Directory

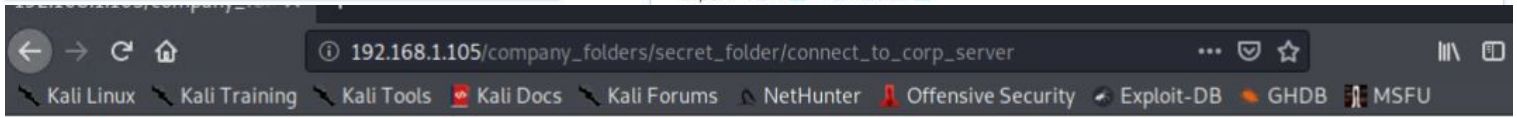
The requests for the hidden directory “secret_folder” were made at approximately 4:00:00. A total of 4 requests were made. The file contained the password hash as well as the directions to gain access to another authorized user’s account(ryan) which allowed the attacker to gain to their webdav.



Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	17,144
http://192.168.1.105/webdav	18
http://192.168.1.105/	4
http://192.168.1.105/company_folders/secret_folder/	4
http://192.168.1.105/webdav/	4

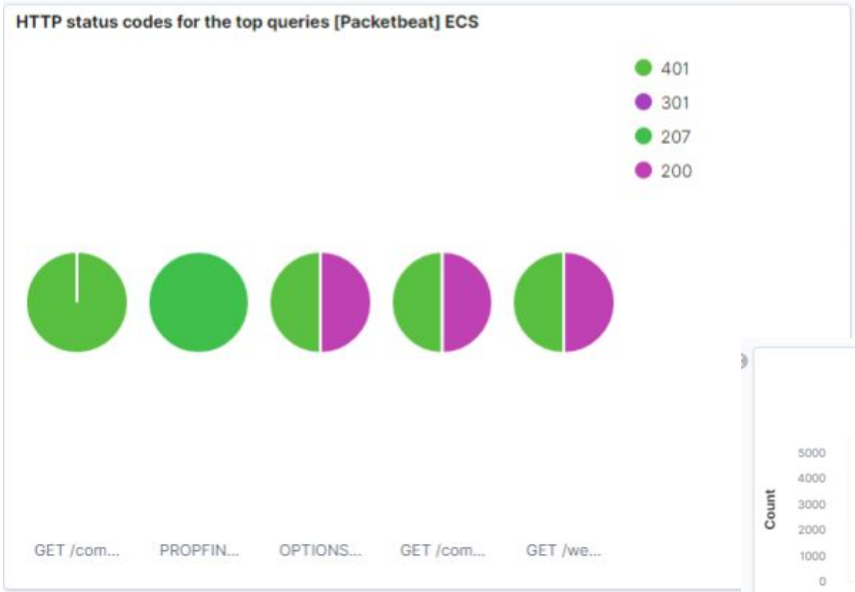
Export: Raw Formatted

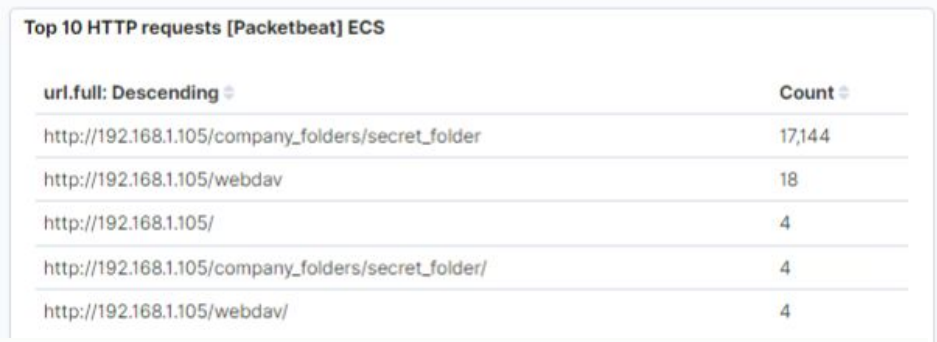


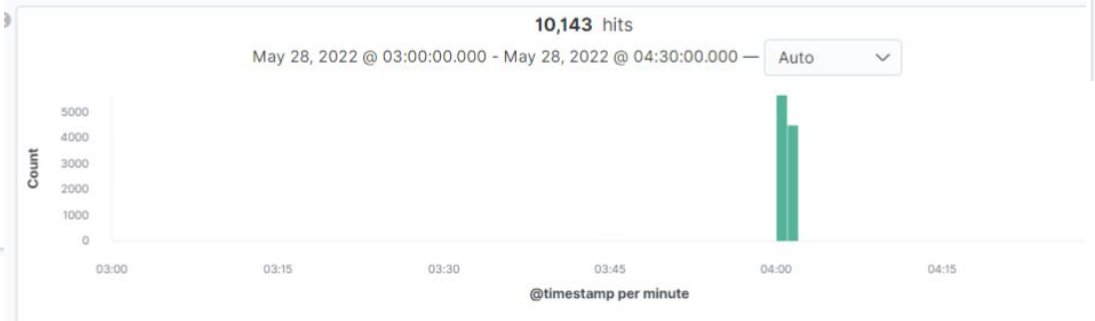

```
Personal Note

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
```

Analysis: Uncovering the Brute Force Attack

There were 17,000 requests made during the attack. 10,143 request were made before the attacker found out the password.







Analysis: Finding the WebDAV Connection

A total of 24 requests were made to WebDav. The files that were requested were shell.php(24 request) and passwd.dav(30 request)

Network Traffic Between Hosts [Packetbeat Flows] ECS

Source IP	Destination IP	Source Bytes	Destination Bytes
192.168.1.90	192.168.1.105	55.1MB	347.8MB

Export: Raw Formatted

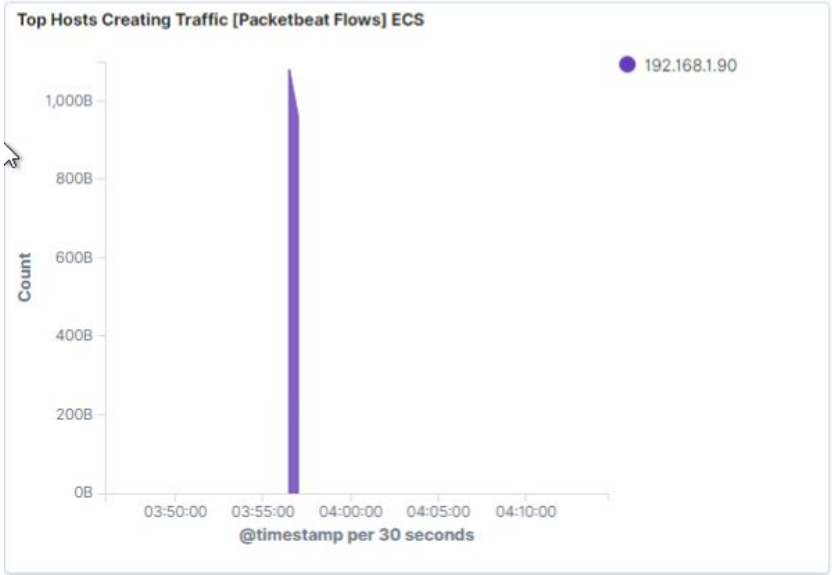
Top 10 HTTP requests [Packetbeat] ECS

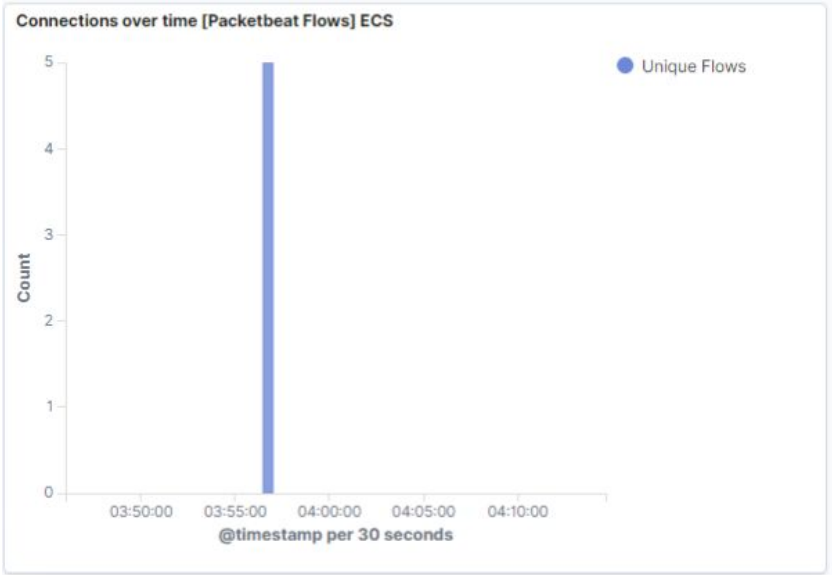
url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	17,144
http://192.168.1.105/webdav/passwd.dav	30
http://192.168.1.105/webdav/shell.php	24
http://192.168.1.105/webdav	18
http://192.168.1.105/webdav/	6

Export: Raw Formatted

Analysis : Identifying the Meterpreter Session (Reverse Shell)

By isolating port 4444, which is commonly used for eavesdropping on traffic, around 3:56:00, there was a huge influx of traffic. This can be a indication that a connection was made.





Blue Team
Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

A threshold alarm can be set to help indicate whether an attack is happening. A threshold of more than 10 in 5 seconds will activate the alarm which can allow the defenders to monitor anything over more closely to see if there was any other indicators of an attack.

System Hardening

Adjusting the firewall settings so that only ports that need to be accessible from outside of the network are the only ones open, all other should be closed. For the ones that needs to be open, applying patches to those ports consistently will help mitigate attackers.

Redirecting open ports to honeypots which will slow attackers down is another mitigation which does not require much work.

Mitigation: Finding the Request for the Hidden Directory

Alarm

As a hidden directory should only be accessible to authorized users only, an alarm that alerts whenever any unauthorized user attempts to gain access should be implemented.

Establishing a threshold that every attempt an alert is sent will help monitor traffic.

System Hardening

Implementing a strict allowed user list to allow allow access to those that are authorized. Taking out any information that may lead or give away authorize users information.
Encrypting the data that contains sensitive/confidential information.

Mitigation: Preventing Brute Force Attacks

Alarm

Create an alarm that alerts when 401 status codes are being detected. Setting a threshold of 100 failed login attempts every 5 seconds and is triggered if that threshold is reached.

If an authorized user fails more than 100 attempts within a 5 second time frame, then they will have to report to their IT department for close monitoring .

System Hardening

What configuration can be set on the host to block brute force attacks?
Limiting failed login attempts to a reasonable number. Limiting login attempts to a range of IPs and if attempted more than threshold, apply a temporary lockout. Apply CAPTCHA during the login period to ensure it is a human interaction. Regularly change passwords with complex passwords that requires the use of special characters, capitals, etc.

A program called fail2ban is also a great mitigation tool that monitor the log files for malicious activity.

Mitigation: Detecting the WebDAV Connection

Alarm

An alarm that triggers with there are any request being made from an unrecognizable IP. Monitoring access with Filebeat and capturing the IPs that had multiple failed login attempts.

Applying a threshold of 15 failed attempts to trigger an alert to closely monitor that IP's activity.

System Hardening

Denying access to IPs that has passed the threshold of failed login attempts. This will help mitigate attackers from brute forcing their way into WebDAV.
Adding encryption to the traffic by setting up WebDAV with HTTPS services. The WebDAV used before did not have any encryption to the traffic which leads to it being vulnerable is accessed by an attacked. Setting up HTTPS with WebDAV ensures that it is more secure with the use of encryption.

Mitigation: Identifying Reverse Shell Uploads

Alarm

Setting an alarm for that monitors access to Port 444 and is triggered when any file is being uploaded to WebDAV through an outside connection.

Capturing and blocking the IPs that are uploading files from an outside source. Only allow in-network IPs to upload files.

System Hardening

Setting permissions to out-of-network IPs to read-only to prevent any file upload. Allow allow authorized users within the network to upload files to the server. Require a two factor or multi-factor authentication for users that are required to upload files to verify their identity to proceed. Only allow specific IPs through the firewall to access WebDAV.


The End