Capstone Engagement

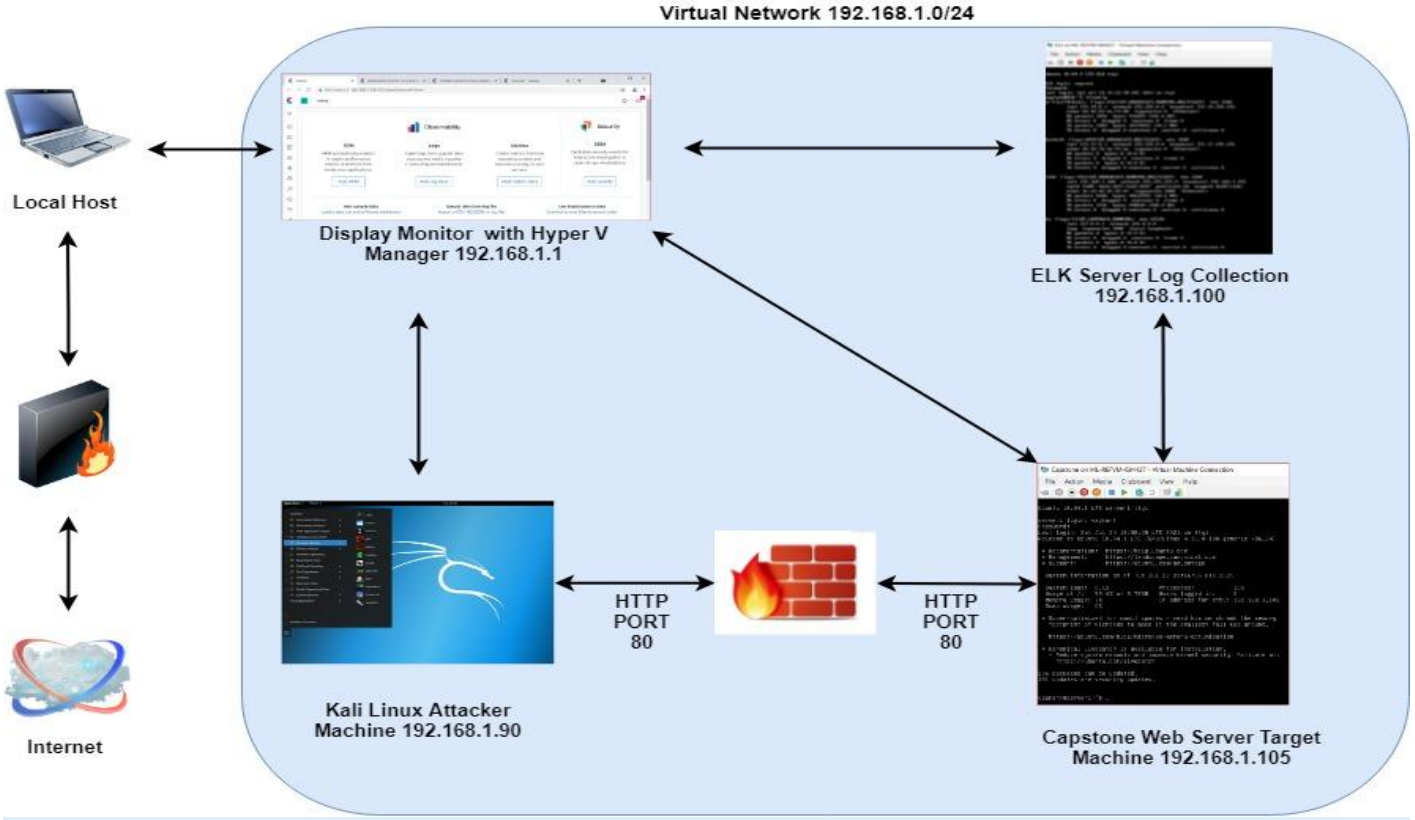
Assessment, Analysis, and Hardening of a Vulnerable System

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: 192.168.1.90
OS: Linux
Hostname: Kali

IPv4: 192.168.1.105
OS:Linux
Hostname:Capstone

IPv4:192.168.1.100
OS:Linux
Hostname: ELK

IPv4:198.168.1.1
OS:Windows
Hostname:ML-REfVm-684424

Red Team
Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Router - Hyper V Manager (ML-RefVM-684427)	192.168.1.1	Local Host Machine Software that virtualizes hardware into virtual machines or servers
Kali	192.168.1.90	Attacker Machine using kali machine
Capstone Web Server1	192.168.1.105	Victim / Target Machine using apache web server
Elk	192.168.1.100	Monitoring Machine - Log Collection service to identify problems in a server or application

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
A3:2017-Sensitive Data Exposure *CWE-23: Relative Path Traversal*	The software uses external input to construct a pathname that should be within a restricted directory, but it does not properly neutralize sequences such as ".." that can resolve to a location that is outside of that directory.	This allows attackers to traverse the file system to access files or directories that are outside of the restricted directory. *Ex. Internal secret folder*
A5:2017-Broken Access Control *CWE-307: improper Restriction of excessive authentication attempts Brute force*	The software does not implement sufficient measures to prevent multiple failed authentication attempts within in a short time frame, making it more susceptible to brute force attacks.	An attacker could perform an arbitrary number of authentication attempts using different passwords, and eventually gain access to the targeted account. Ex.hydra
A1:2017-Injection *CWE-98: Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion')*	The PHP application receives input from an upstream component, but it does not restrict or incorrectly restricts the input before its usage in "require," "include," or similar functions.	this can allow an attacker to Remote File Inclusion (RFI) to access files that contain previously-injected PHP code. Ex.webdav access

Relative Path Traversal

1

Tools & Processes

We used Nmap tool to choose target and view the open ports and services in our network. We used XSS or a path traversal technique to aim to look for existing and or hidden web objects.

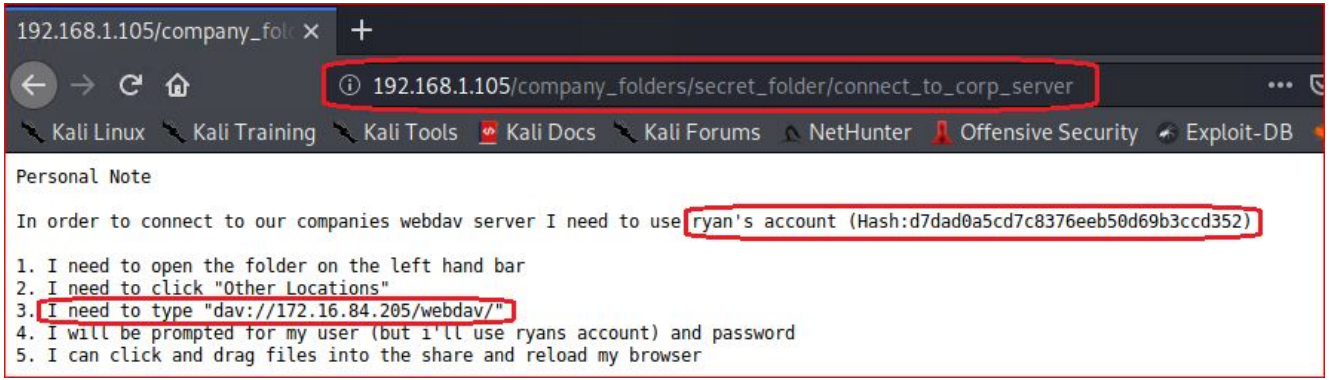
Path used:

`http://192.168.1.105/company_folders/secret_folder/`

2

Achievements

Using this path tool granted the knowledge of two hidden directories within the web server. The ‘secret_folder’ and ‘webdav’ were both uncovered.



Improper Restriction of Excessive Authentication Attempts Brute Force

01

Tools & Processes

The Hydra program was used to run a brute force attack on the credentials for ‘secret_folder’ directory.

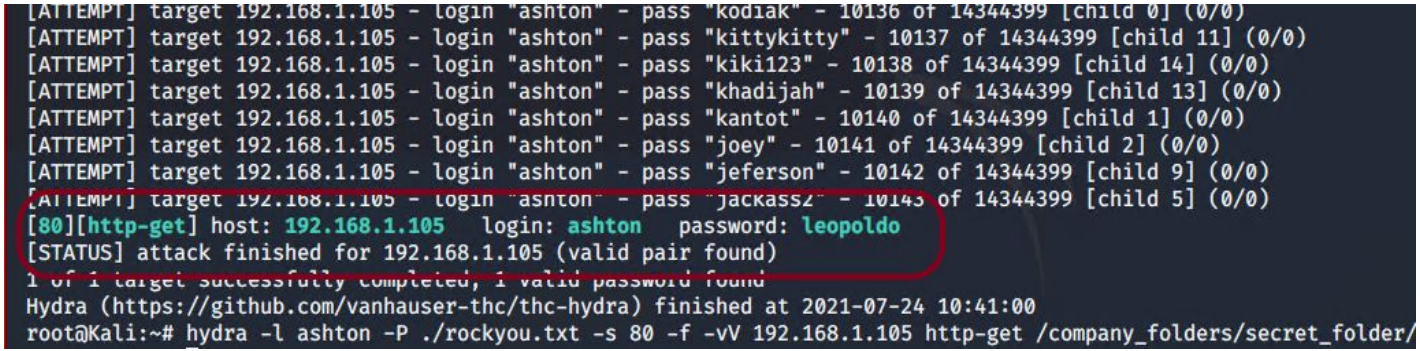
Command used:

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

02

Achievements

That command was able to produce the credentials “ashton:leopoldo” for access to the ‘secret_folder’



Improper Control of Filename for Include/Require Statement in PHP Program

01

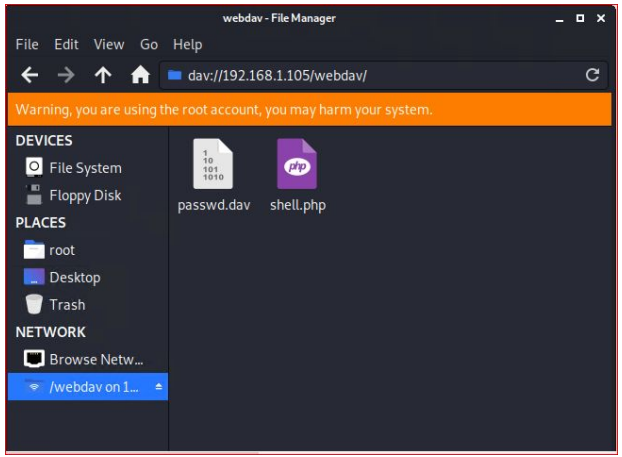
Tools & Processes

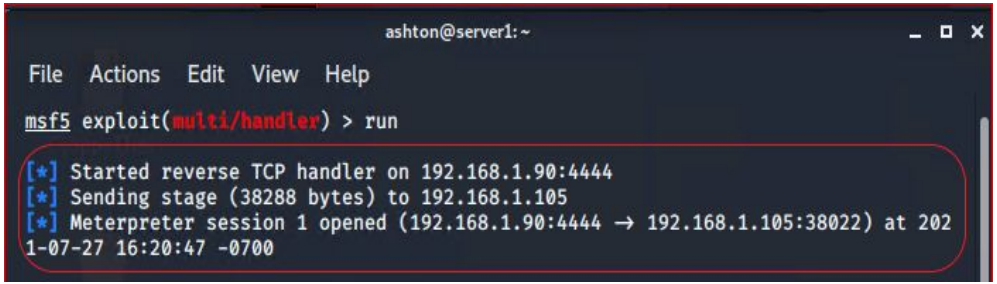
We were able to upload a reverse shell code without the server restricting the input before its usage. Once provisioning meterpreter to listen to port 4444 the attack was success.

02

Achievements

Once the code was executed this provided access to the target server using a reserve shell.

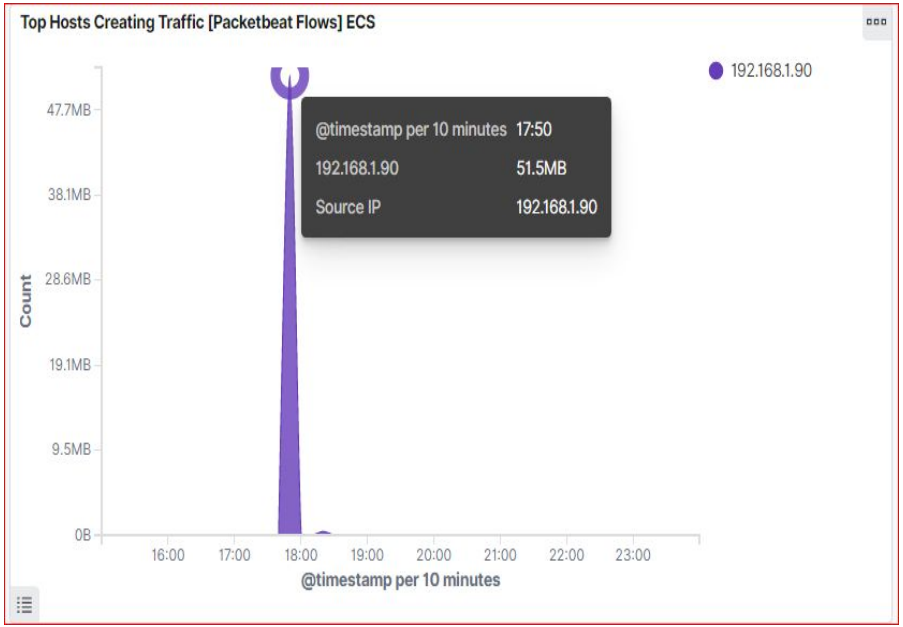


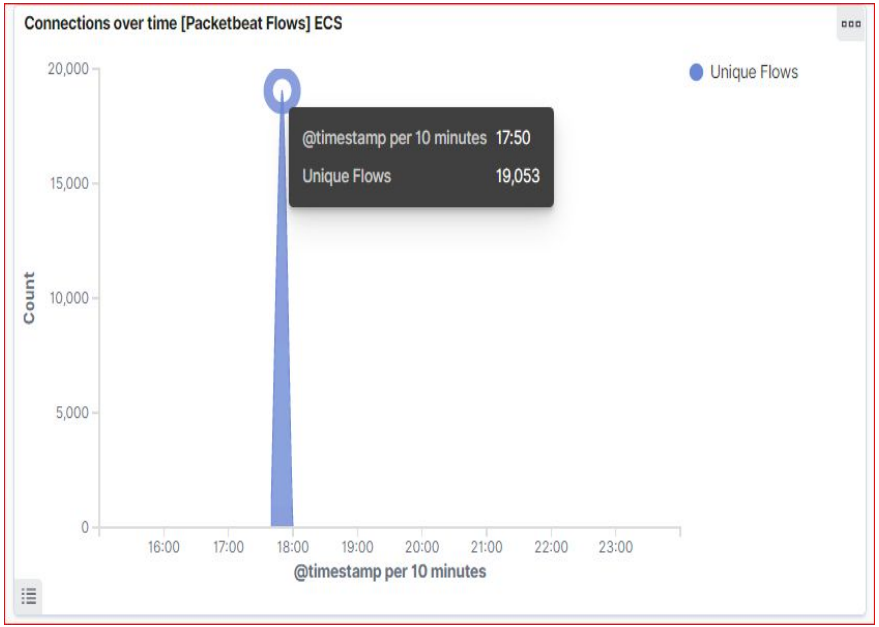


Blue Team
Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

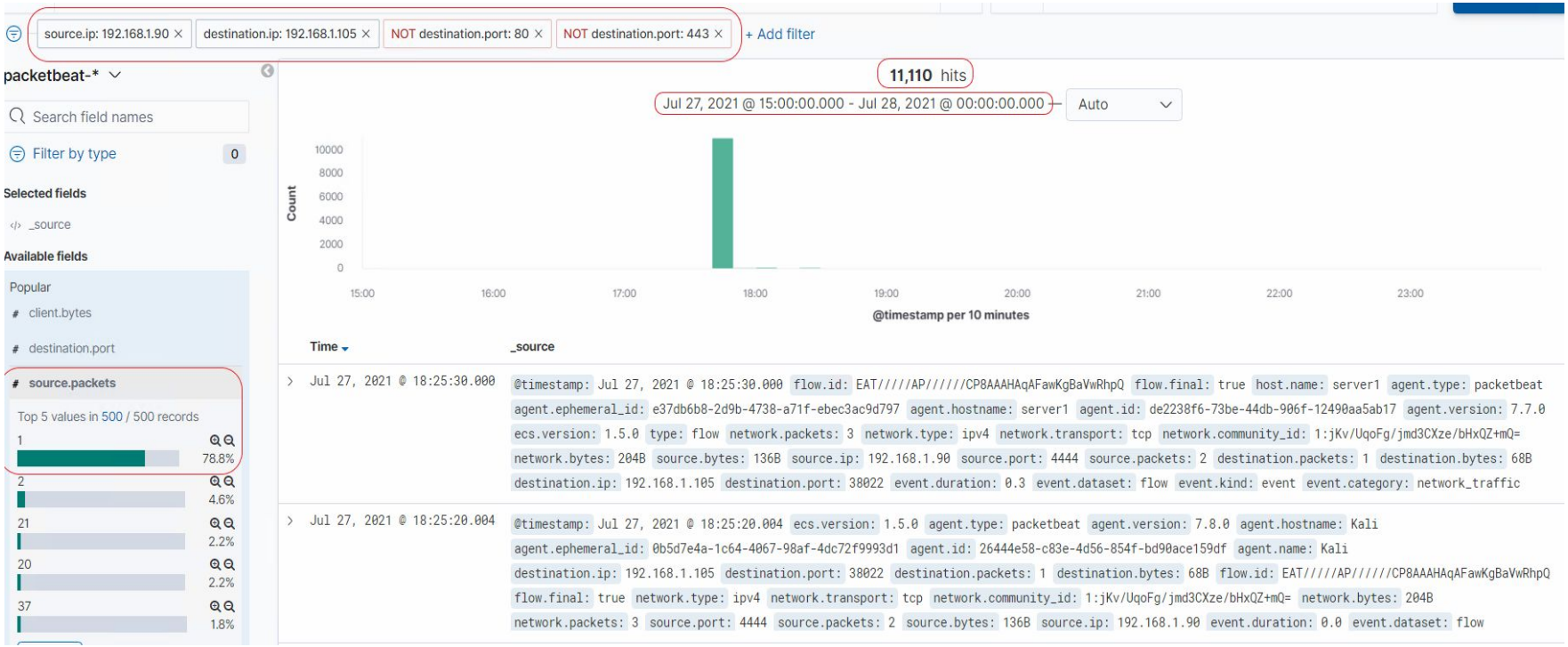
- The Port scan occurred approximately 17:50:00
- 19,053 hits were sent from the attacker machine 192.168.1.90





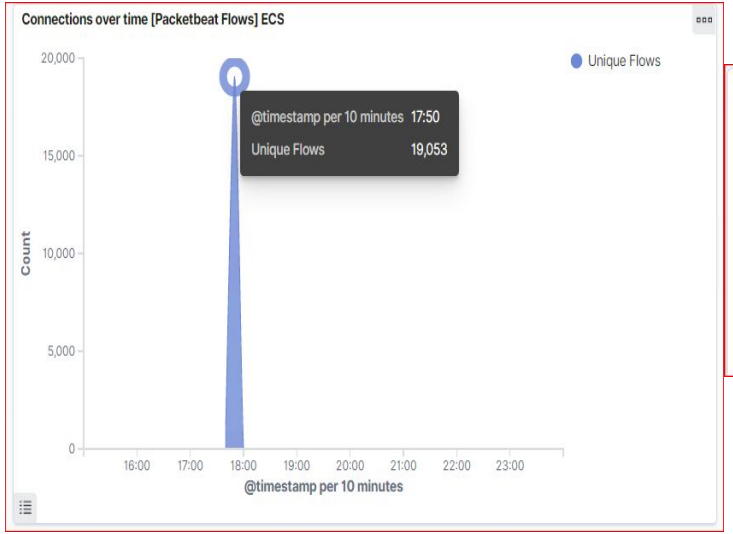
Analysis: Identifying the Port Scan (Cont.)

- In below screenshot, we can observe that total requests of 11,110 scan all for different port numbers apart from port 80 and 443.



Analysis: Finding the Request for the Hidden Directory

- In the first screenshot we can observe that the attack started at 17:50:00 with 19,053 requests.
- The top three hits for directories and files that were requested were:
  - http://192.168.1.105/company_folder/secret_folder
  - http://192.168.1.105/company_folder/webdav
  - http://192.168.1.105/webdav/shell.php

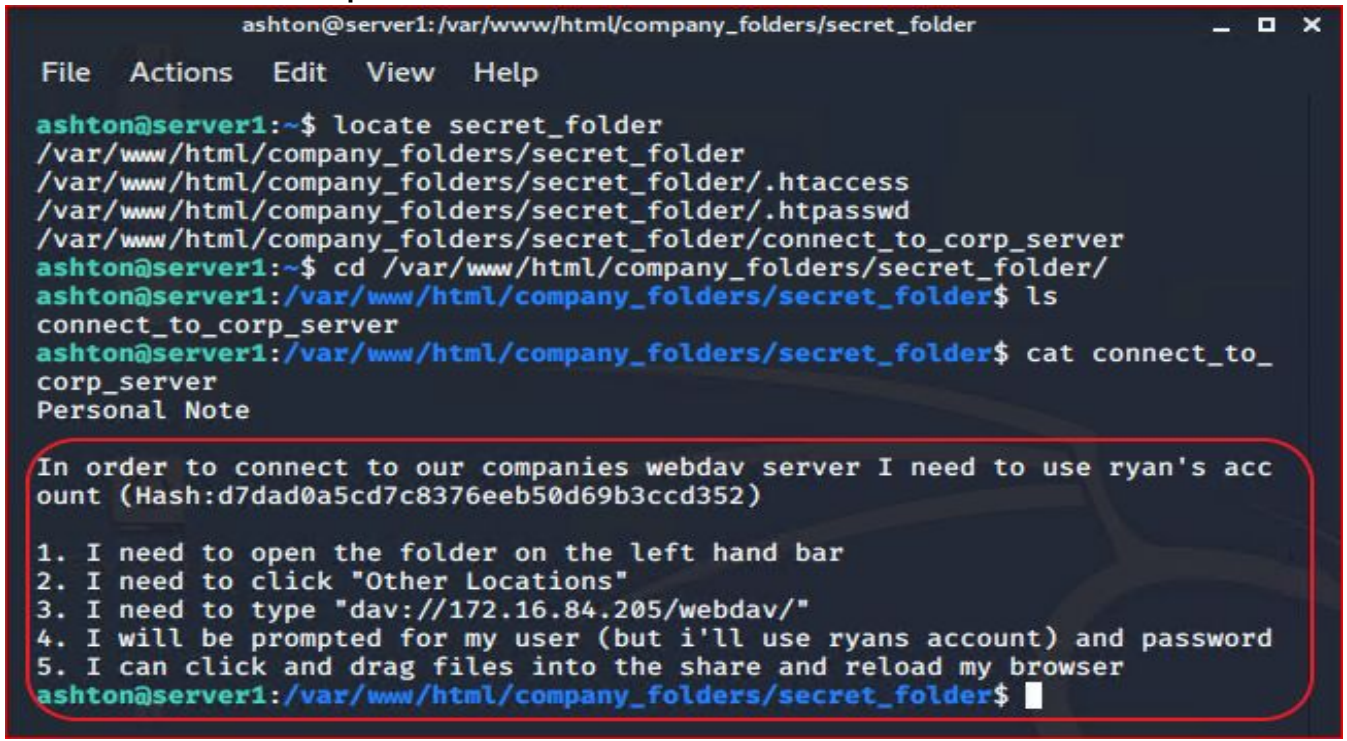


Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder/	16,245
http://192.168.1.105/webdav	70
http://192.168.1.105/webdav/shell.php	40
http://192.168.1.105/	12
http://192.168.1.105/company_folders/secret_folder	8

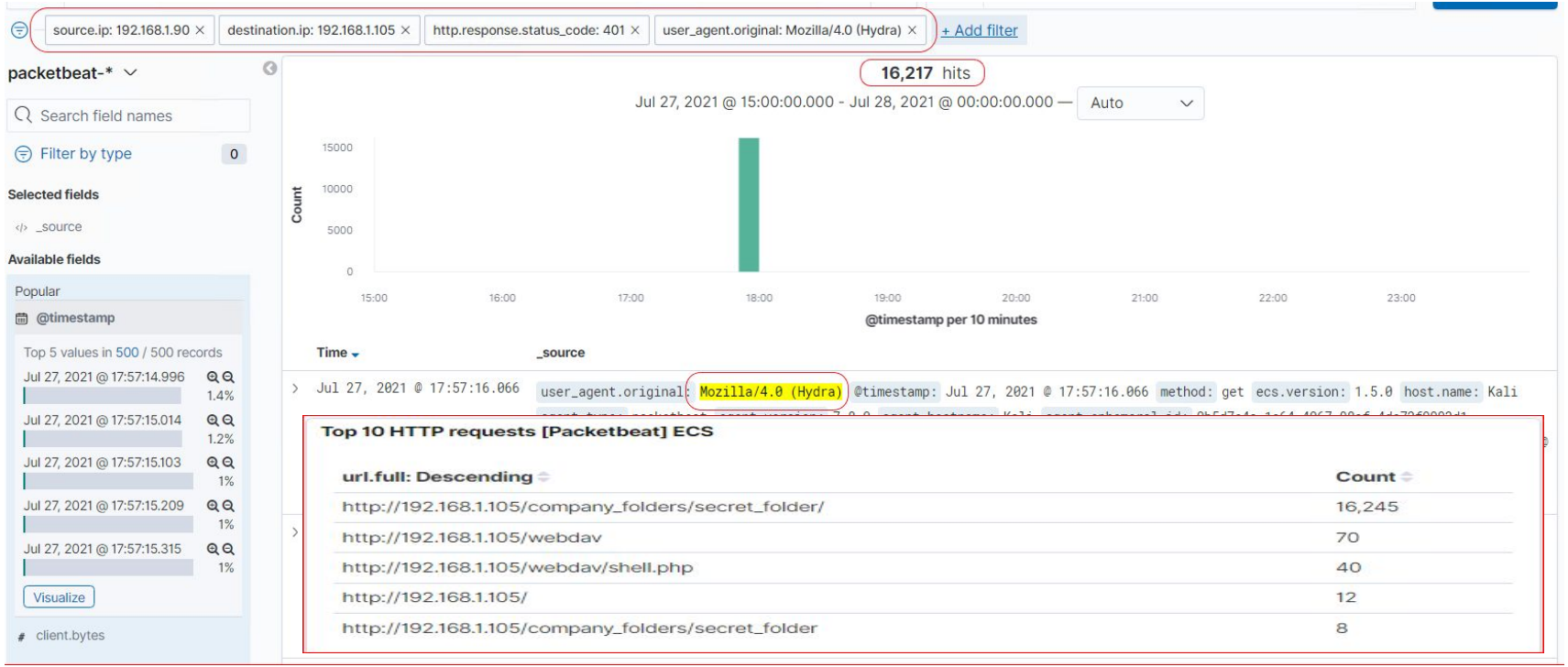
Analysis: Finding the Request for the Hidden Directory

- The directory requested was a internal secret folder hidden within the company folders.
- The secret folder contained instructions on how to access the webdav server using Rayn's Account.
- It also included a hashed password.



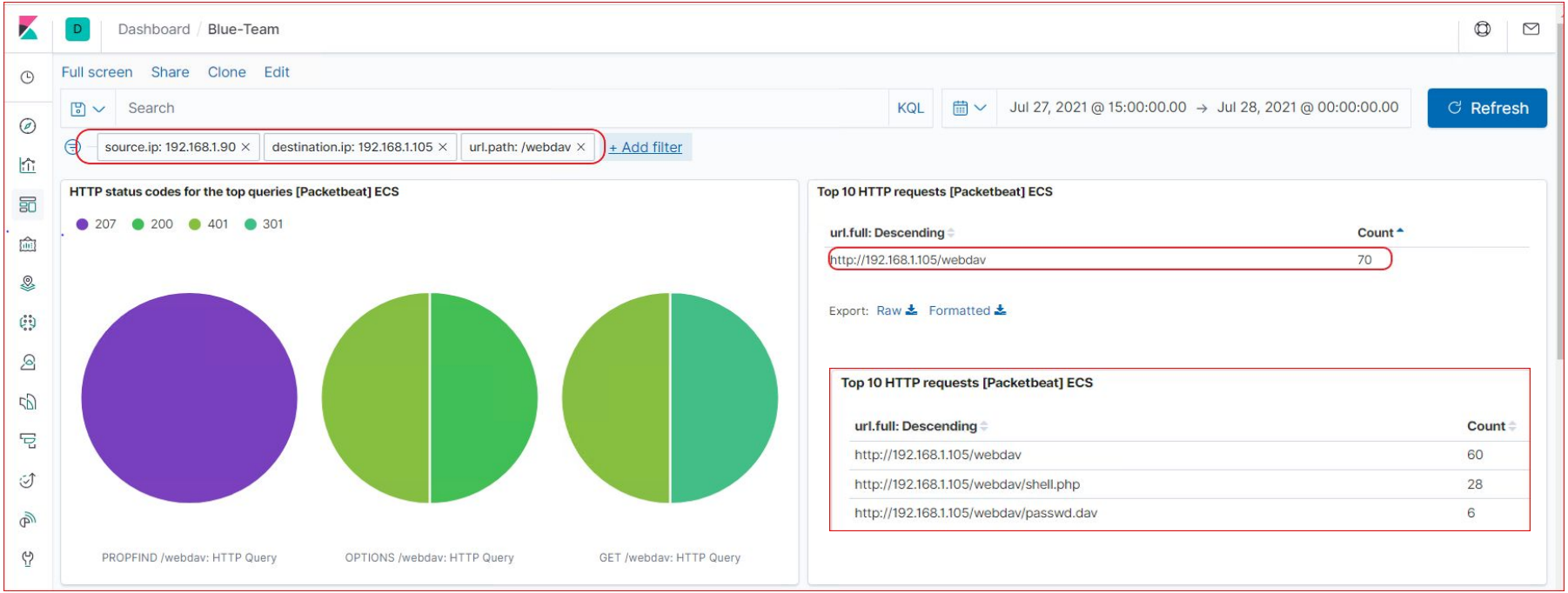
Analysis: Uncovering the Brute Force Attack

- 16,245 - 16,217 Approx. requests were made during the attack.
- Out of 16,217 requests for password protected `secret_folder` only 8 were successful considering the file inside the directory.



Analysis: Finding the WebDAV Connection

- 70 total requests were made to the webdav directory.
- The `shell.php` file was requested 28 times
- The `passwd.dav` file was requested 6 times.



Blue Team
Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

What kind of alarm can be set to detect future port scans?

- A filter can be activated if detected traffic from a single source IP address is connecting to different ports 100 of requests per second.

What threshold would you set to activate this alarm?

- if a sny given IP address sends more than 100 requests per minute for more than 5 minute to access closed ports should have the filter activate.

System Hardening

What configurations can be set on the host to mitigate port scans?

- Install local firewall, an IPS can detect port scans.
- ICMP traffic can be filtered
- An IP allowed list can be enabled.

Describe the solution. If possible, provide required command lines.

- Filtering traffic from an IP address triggered by the IPS can effectively mitigate port scans.

Mitigation: Finding the Request for the Hidden Directory

Alarm

What kind of alarm can be set to detect future unauthorized access?

- Allow authorized IP addresses
- An Alarm could be set to go off for any IP address not on the whitelist that attempts to access.

What threshold would you set to activate this alarm?

- The threshold for this alarm would be 1, for any machine accessing it.

System Hardening

What configuration can be set on the host to block unwanted access?

- This directory should not allowed to exist on the server.

Describe the solution. If possible, provide required command lines.

- `# rmdir -r`
- this can be used to the remove all files and directories itself from the server.

Mitigation: Preventing Brute Force Attacks

Alarm

What kind of alarm can be set to detect future brute force attacks?

- An Alert can be created if 401 unauthorized is returned from the server over a threshold.

What threshold would you set to activate this alarm?

- Start with 5 over a 30 minute period to allow forgotten or mistyped passwords and refine.

System Hardening

What configuration can be set on the host to block brute force attacks?

- Limit failed login attempts
- Limit logins to whitelist of IP addresses.

Describe the solution. If possible, provide the required command line(s).

- Configure Account policies on your server to limit failed login attempts.

Mitigation: Detecting the WebDAV Connection

Alarm

What kind of alarm can be set to detect future access to this directory?

- Set an alert for any blacklisted IP attempting to access this directory
- All IPS outside the server range should be blacklisted.

What threshold would you set to activate this alarm?

- The threshold for this alarm be one, any attempt to access should trigger alarm.

System Hardening

What configuration can be set on the host to control access?

- Connections to this shared folder should not be accessible from the web and restricted by a machine using a black list firewall rule.

Describe the solution. If possible, provide the required command line(s).

- Blocklisting ports 80 and 443
- Blacklisting all external IPs

Mitigation: Identifying Reverse Shell Uploads

Alarm

What kind of alarm can be set to detect future file uploads?

- Set an alert for any .php file that is uploaded.
- Set firewall to block traffic to the shared folder on ports 80, 443 and 4444.

What threshold would you set to activate this alarm?

- Any traffic on these ports would warrant a alarm trigger.

System Hardening

What configuration can be set on the host to block file uploads?

- Remove the ability to upload files from over the web, all file uploads should be from a local source.

Describe the solution. If possible, provide the required command line.

- Block port 80,443, and 4444


The End