Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

Table of Contents

This document contains the following sections:

01 **Network Topology**

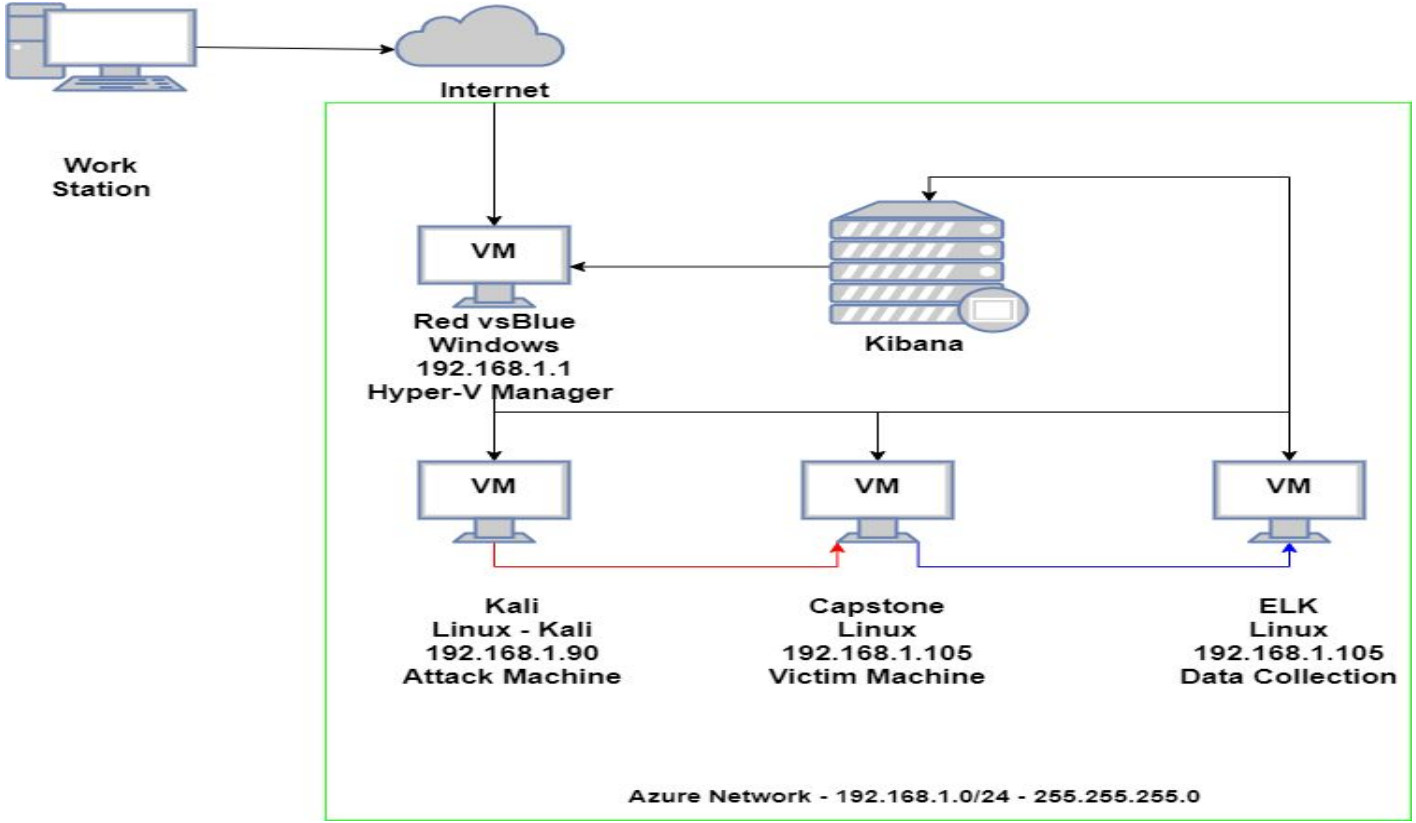
02 **Red Team**: Security Assessment

03 **Blue Team**: Log Analysis and Attack Characterization

04 **Hardening**: Proposed Alarms and Mitigation Strategies

Network Topology

Network Topology



Network
Address Range:192.168.1.0/24
Netmask:255.255.255.0
Gateway:10.0.0.1

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

IPv4: 192.168.1.90
OS: Linux - Kali
Hostname: Kali

IPv4: 192.168.1.105
OS: Linux
Hostname: Capstone

IPv4: 192.168.1.100
OS: Linux
Hostname: ELK

Red Team
Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Red vs Blue Machine	192.168.1.1	-Hyper-V Access Gateway to other machines -Kibana Interface
Kali	192.168.1.90	-Red team attack machine to attack and exploit the Capstone Machine
Capstone	192.168.1.105	-Victim Machine to be attacked by the Red team machine and observed by the Blue team ELK server
ELK	192.168.1.100	-ELK server SIEM set to collect attack info from the Capstone machine.

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
CWE-307: Improper Restriction of Excessive Authentication attempts.	*The Machine does not have sufficient security measures in place to limit the amount of failed authentication attempts in a short period of time, thus leaving the machine highly susceptible to brute force attacks.*	*Attackers could easily implement the use of software such as Hydra to brute force a systems password without fear of being locked out, thus allowing them to gain access to the target machine in a timely manner depending on the complexity of the target password.*
CWE-434: Unrestricted Upload of File with Dangerous Type.	*The Machine allows the attacker access to restricted folders and allows the upload of dangerous file types which can then be launched within the environment.*	*An Attacker can access said restricted folder and insert a simple .php file that has been loaded with a malicious payload, then allows for said file to be executed by simply navigating to the directory and file on the web browser.*

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
CWE - 548: Exposure of Information Through Directory Listing.	*A Directory is exposed on a web server allowing an attacker to view sensitive information about how the server is structured.*	*Having a Directory exposed such as this allows attackers to gain valuable information such as usernames or secret directories.*

Exploitation: CWE-307: Improper Restriction of Excessive Authentication attempts

01

Tools & Processes
Using Hydra and a word list with the information gained on the secret_folder Directory.

02

Achievements
The goal was to gain access to the secret_folder directory using the found credentials.

03

```
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "joey" - 10141 of 14344399 [child 10] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jeferson" - 10142 of 14344399 [child 14] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10143 of 14344399 [child 15] (0/0)
[80][http-get] host: 192.168.1.105   login: ashton   password: leopoldo
[STATUS] attack finished for 192.168.1.105 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-10-15 17:33:20
root@Kali:/#
```

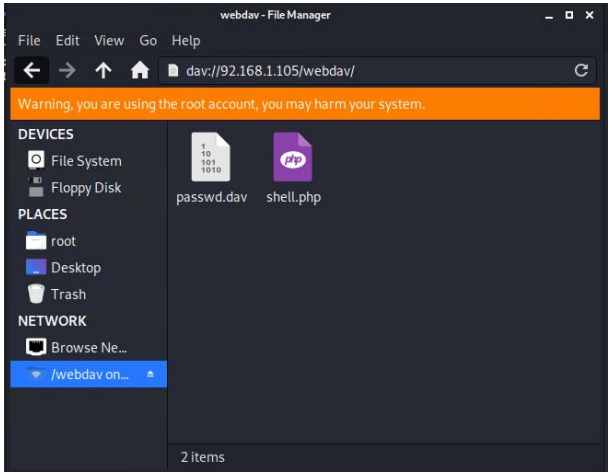
Exploitation: CWE-434: Unrestricted Upload of File with Dangerous Type.

01

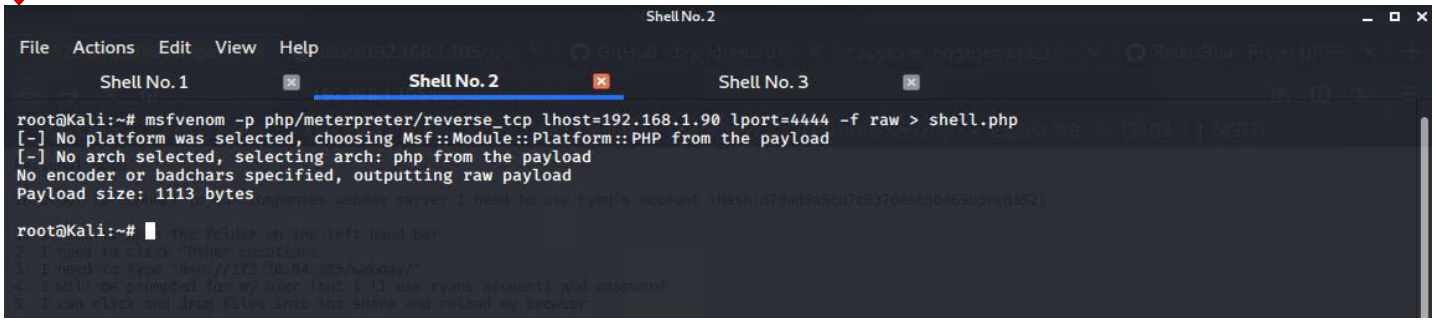
Tools & Processes
Using MsfVenom we designed a reverse tcp payload file called shell.php.

02

Achievements
Once shell.php is uploaded we can access the file via web browser to launch the exploit.



03



Exploitation: CWE - 548: Exposure of Information Through Directory Listing.

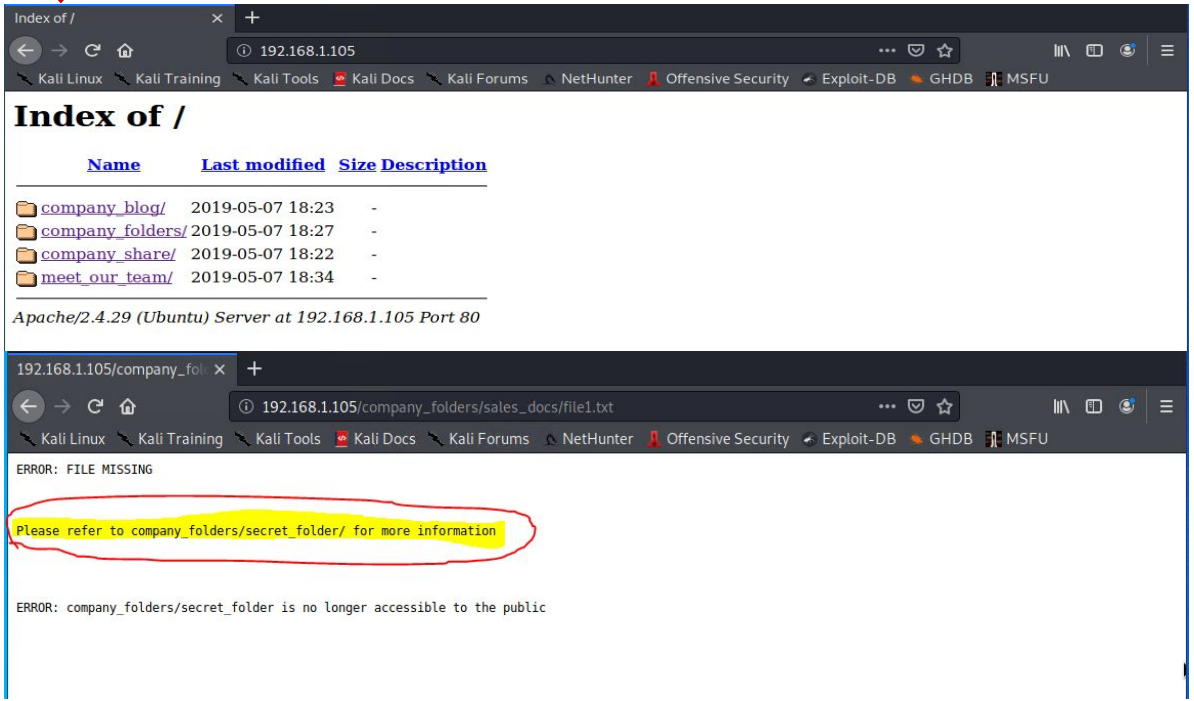
01

Tools & Processes
Using Firefox we can examine the web server files directly to find Useful information.

02

Achievements
Once we gain access to the vulnerable web server we can browse for clues as to which users will be good targets.

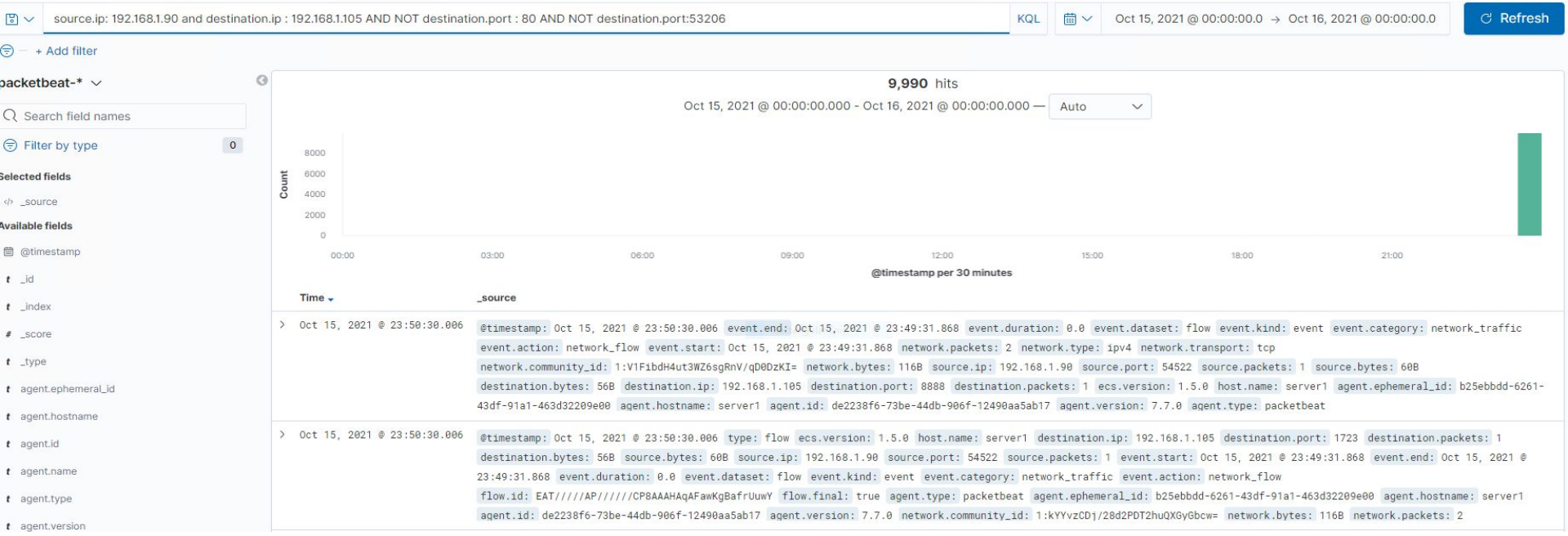
03



Blue Team
Log Analysis and Attack Characterization

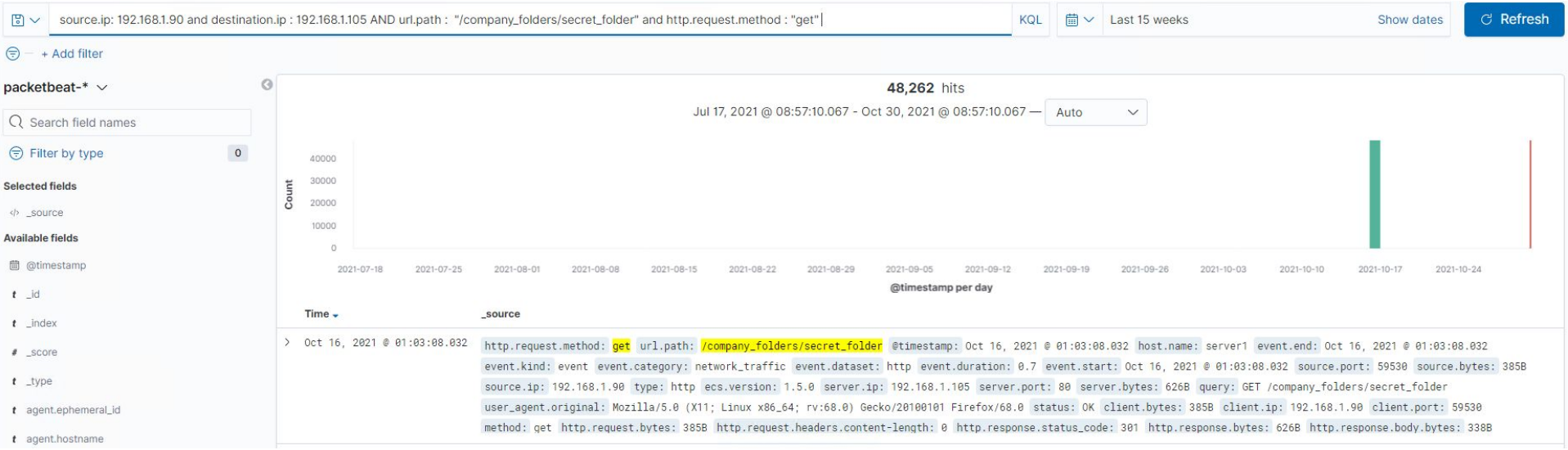
Analysis: Identifying the Port Scan

- The Port scan Occured at 23:50
- There was 9990 packets sent from the IP 192.168.1.90 (several attempts)
- We can see this is a port scan due to the several thousand packets being sent across several ports.



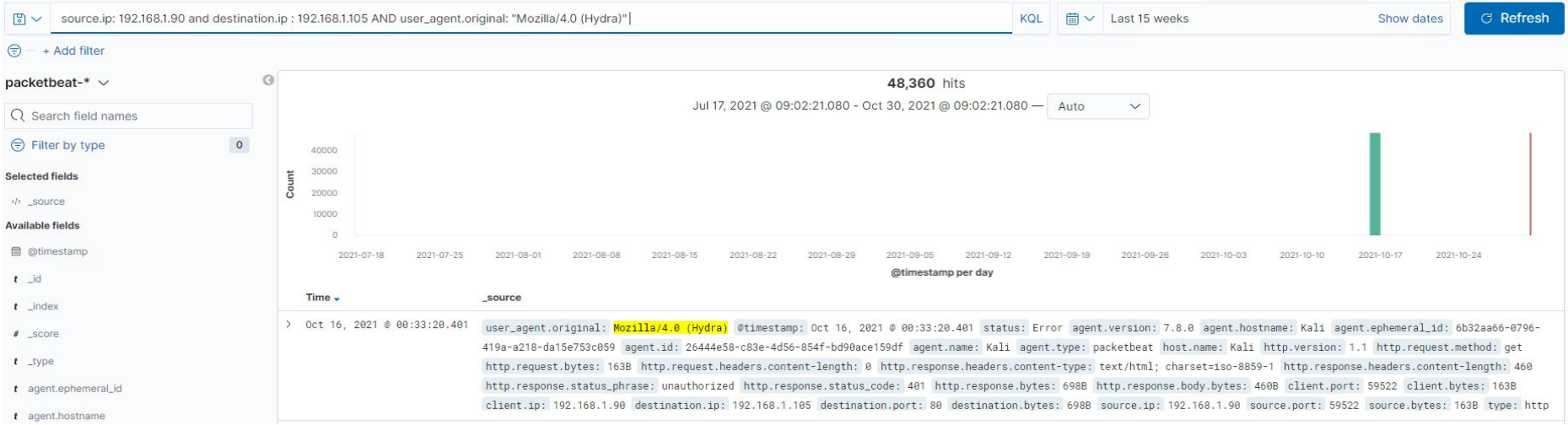
Analysis: Finding the Request for the Hidden Directory

- This request occurred at 01:03
- This is a request to enter the secret folder which contains a file with instructions to access the webdav including the CEO password that is Hashed.



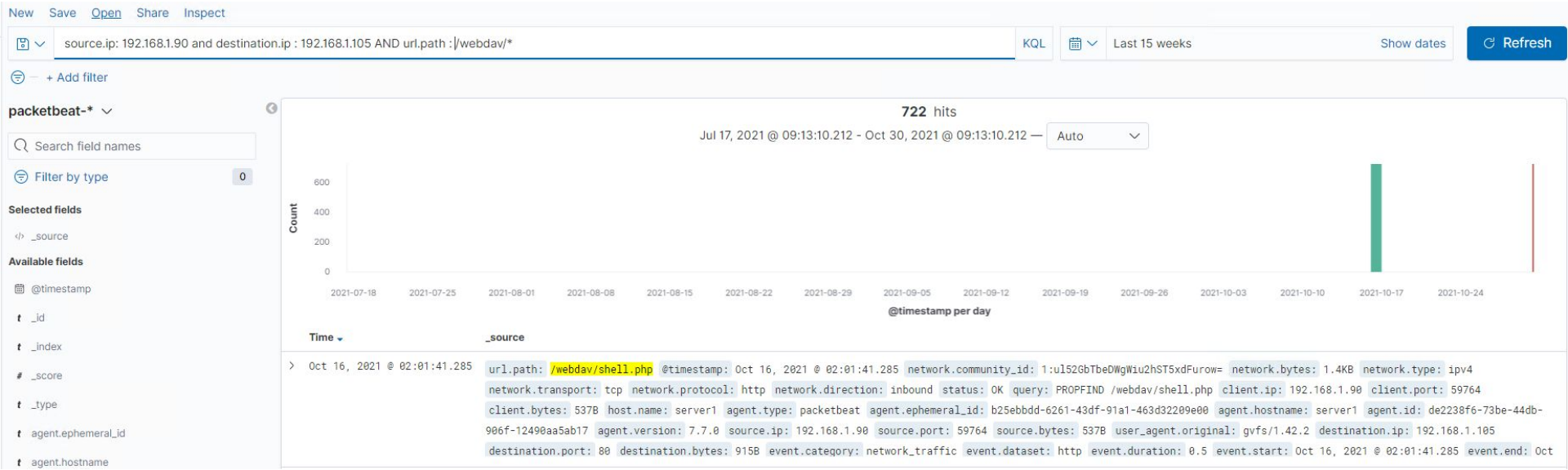
Analysis: Uncovering the Brute Force Attack

- In total there was 48360 attempts with Hydra to crack the password, this is due to me running Hydra twice.
- By narrowing my search by limiting only http.response.status_code:401 we can see the unauthorised error was returned 48240 times meaning on my 4824st attempt it was successful.



Analysis: Finding the WebDAV Connection

- In total there was 722 hits for the webdav directory
- Shell.php was requested many times over as well as passd.dav and rbv.php (which was a failed meterpreter shell script).



Blue Team
Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

We could potentially set up a whitelist and and any IP not in the white list will trigger an alert if they attempt to scan any ports though this could leave us vulnerable from within the organisation.
A better alarm would be to trigger if a single IP is scanning across multiple ports in a short time OR any IP accessing a closed port since the company workers will know which ports to use to begin with.
A good Threshold for these would be to trigger an alert is 50 attempts happen in quick succession.

System Hardening

Set up a whitelist so only specific workstations can be allowed within the system.
Have an IPS installed into the system to automatically block Port scanning attempts.
Close all unnecessary ports thus eliminating the need for concern over them.

By implementing the above this network will cease to be discoverable due to the IPS blocking attempts to find open ports.

Mitigation: Finding the Request for the Hidden Directory

Alarm

Anybody outside of the company should trigger this alarm, since we have developed a whitelist from the previous method we can work off of that.

This threshold should be set to 1 since only the allowed machines should be accessing this directory, all others should be triggering an alarm.

System Hardening

Whitelisting “good” IPs will help tremendously here but another important step would be to remove this directory from the web server all together and only have it inside a closed company system thus eliminating the danger of it being on an open internet facing server.

Only allowing specific IPs will mean creating and updating a whitelist and removing the Hidden Directory will completely prevent this exploit all together.

Mitigation: Preventing Brute Force Attacks

Alarm

An alarm can be set if there is a failed login attempt over a certain number in a short period of time.
We can also create an alert if the server returns a 401 error over a certain limit.

An appropriate Threshold would be start with 5 failed attempts in 30 minutes and over 50, 401 web responses in an hour, this will allow us to easily identify a Brute force. These number can then be adjusted as more use data becomes available to establish a more polished baseline.

System Hardening

We can configure our system so only Whitelisted IPs can even attempt to log on, otherwise it will always return a 401 error.
We can also limit the amount of failed login attempts.

Configure the account policies on the server to only allow 5 failed login attempts and trigger a lockout if more than 5 is attempted in a short span of time, but do not apply this to Administrator accounts to avoid damaging DDOS attacks.

Mitigation: Detecting the WebDAV Connection

Alarm

These alarms should mimic the Brute force alarms as they will fall under similar risk.
We should also alarm if any IP outside of the whitelist attempt to log in.

5 failed Login attempts within 30 minutes and 50 or more 401 errors on the web response.
Always trigger an alert when Non whitelisted IPs attempt access.

System Hardening

This Folder should not be accessible by the web and only available within the company's network

For this specific folder we should implement the following Firewall rules;
-Block all external IPs
-Block traffic going either direction from port 80 and 443

Mitigation: Identifying Reverse Shell Uploads

Alarm

Set an alarm to alert for any unauthorized files, particularly .php files, that is uploaded.
We can also trigger an alarm when we receive a connection from an unknown source or untrusted source.

The threshold for this should be 1, there should be no files uploaded and no connections made from outside the company.

System Hardening

Remove the ability to edit the folder, and set user access rules to block all file upload to the webdav folder.

Set firewall to block FTP requests as well as ports 80, 4444 and 443

Block all IPs that aren't on the whitelist.


The End