Capstone Engagement

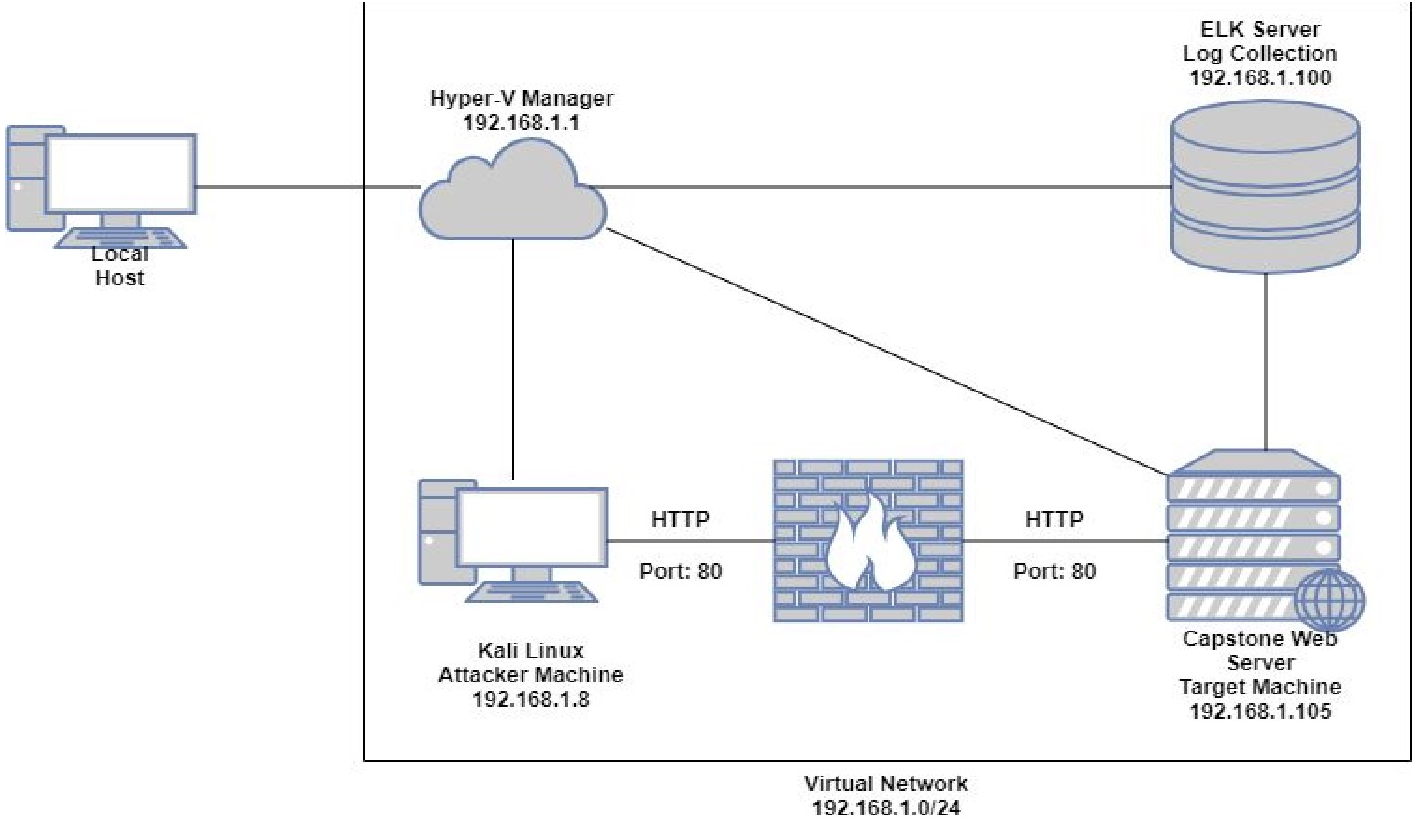
Assessment, Analysis, and Hardening of a Vulnerable System

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
Hostname: Hyper-V Manager

IPv4:192.168.1.8
OS: Kali Linux
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
Capstone	192.168.1.105	Because the web server Apache is installed on the targeted system, it is called the targeted machine.
Kali	192.168.1.8	The IP4 addresses of the Kali Linux system that is being utilized to launch the assault is revealed.
Elk	192.1.100	The service responsible for maintaining logs that may be utilized to identify and resolve server-related issues.
Hyper V Manager	192.168.1.1	The application program is responsible for remotely accessing the virtual server from the physical server.

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
CWE-23: Traversing across the relative path	External input is used to generate a directory structure that must be inside one protected subdirectory, but it does not correctly defuse patterns such as ".." that really can translate to a destination that's outside the folder in which it is being used.	The hacker will be able to gain information of any hidden folders on the system at the moment of this.
CWE-307: Validation Attempts that are excessive are not properly restricted.	Because the program does not have adequate safeguards to prevent many unsuccessful authentication attempts within a short period of time, it is more vulnerable to brute force assaults than it should be.	This will provide the attacker the ability to conduct dictionary-based attacks in order to gain credentials.
CWE-98: 'PHP Remote File Inclusion' has an incorrect control of the filename for the Include/Require statement in the PHP program.	It is possible that the PHP program gets input from an originating component, but that the PHP program does not limit, or erroneously limits, the input information before it is used in "require," "include," or similar methods.	This will provide the attacker the ability to employ remote file inclusion in order to run code on a server as a result.

Exploitation: CWE-23: Relative Path Traversal

01

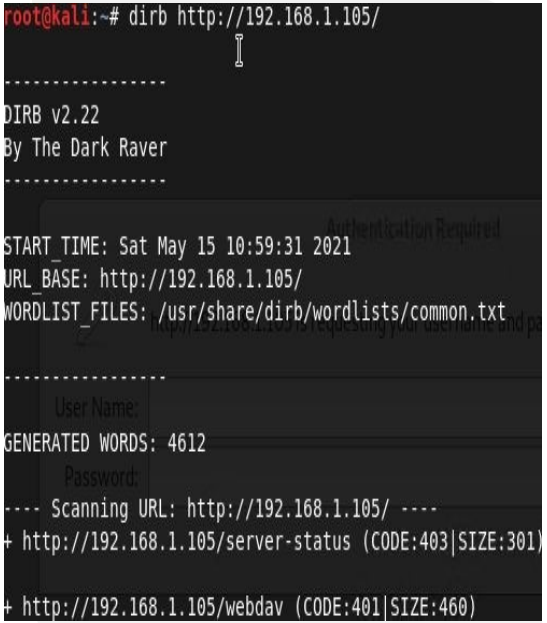
Tools & Processes
The "dirb" command was used to conduct a dictionary-based exploit against the web server, which was successful. DIRB searches for web items that are already present and/or hidden.

Command used:
Dirb http://192.168.1.105

02

Achievements
Using this program provided access to two secret folders on the web server, which were previously unknown. Both the'server-status' and 'webdav' folders were found by utilizing the dirb tool.

03



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

01

Tools & Processes

It was necessary to utilize the Hydra software in order to conduct a brute force assault on the credential for the directory containing the 'secret folder.

Command used:

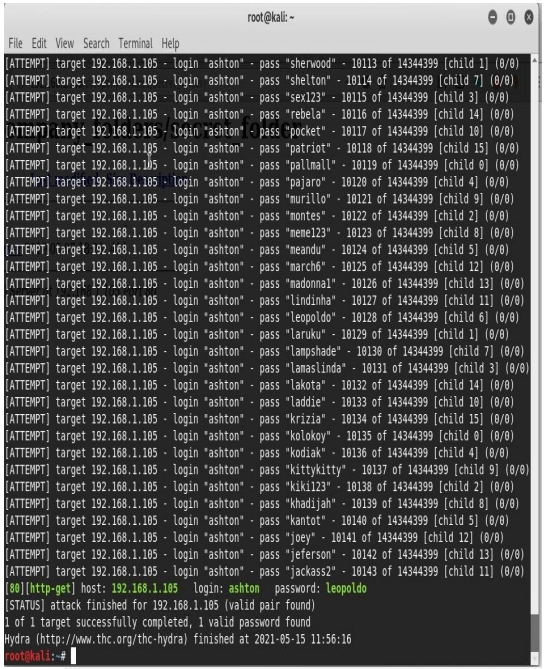
hydra -l ashton -P rockyou.txt -s 80 -f -vV 192.168.1.105 http-get /company_folders/secret_folder

02

Achievements

This was successful in generating the credentials "ashton:leopoldo" for accessing to the folder containing the secret folder.

03



Exploitation: CWE-98: Improper Control of Filename for Include/Require Statement in PHP Program

01

Tools & Processes

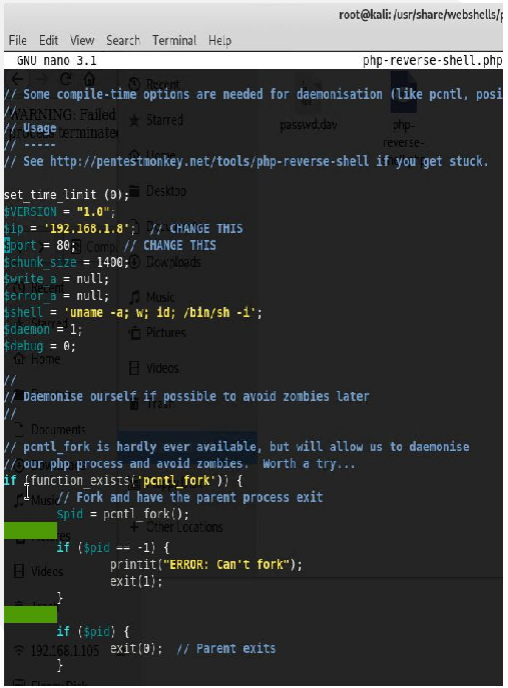
A reverse shell code may be uploaded without the server controlling what can be uploaded before it is used. Once netcat was configured to listen on port 80, the attack was a complete and resounding success.

02

Achievements

Once the malware had been executed, it allowed access to the target server through the use of a reverse shell protocol.

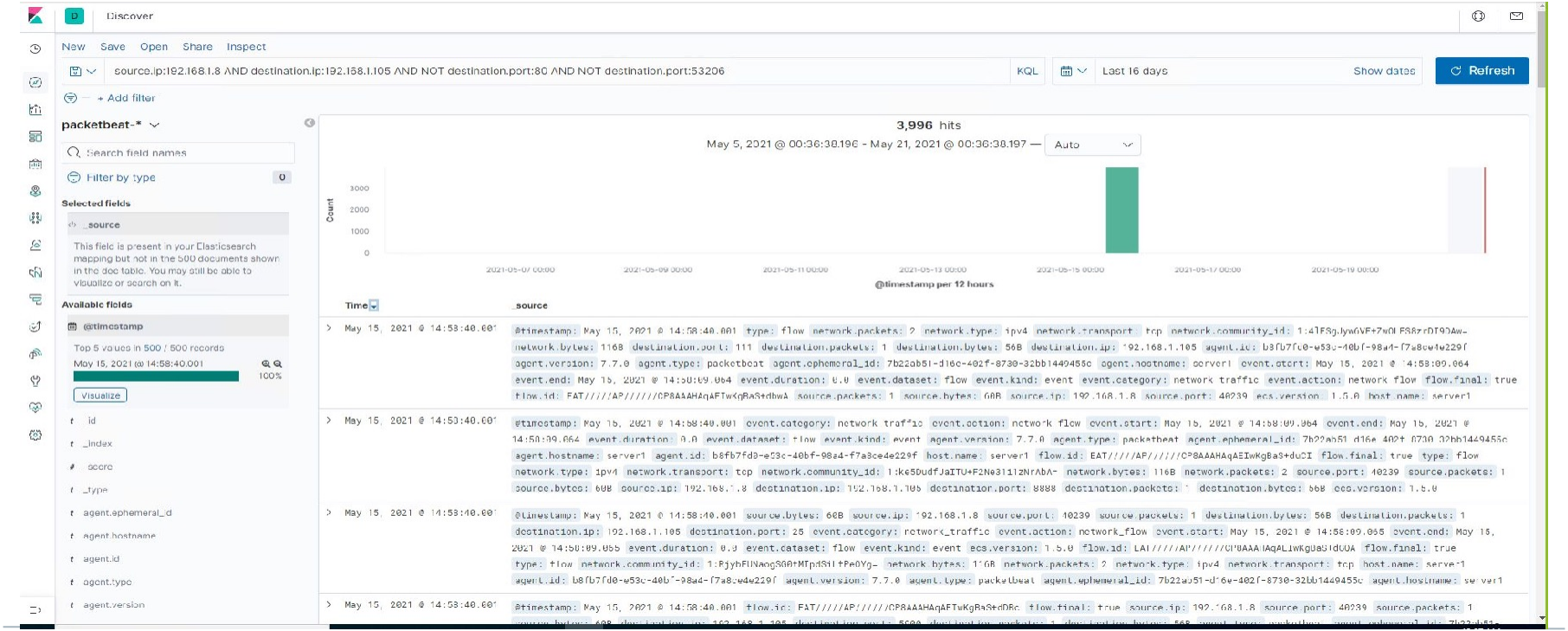
03



Blue Team
Log Analysis and Attack Characterization

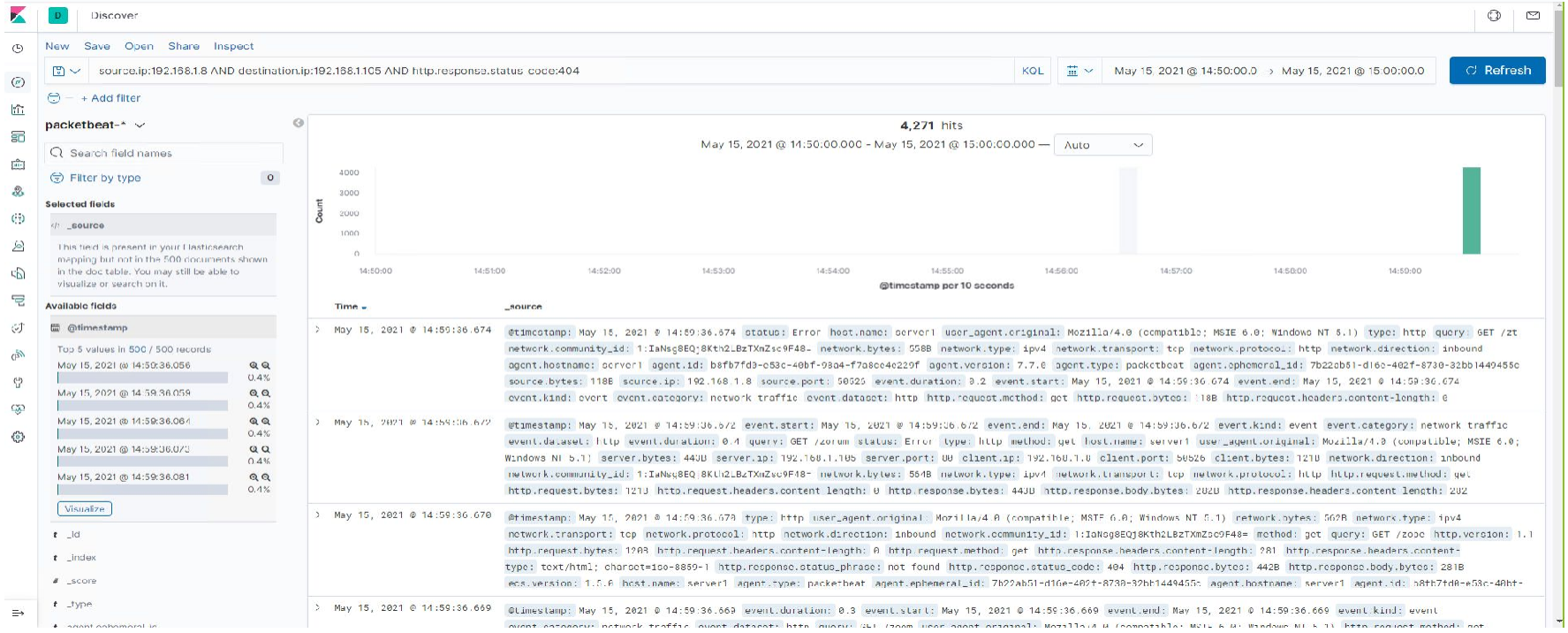
Analysis: Identifying the Port Scan

- The Port scan occurred at 6:13pm
- There were 4,120 packets sent from the IP address 192.168.1.8
- A few thousand requests all for different port numbers



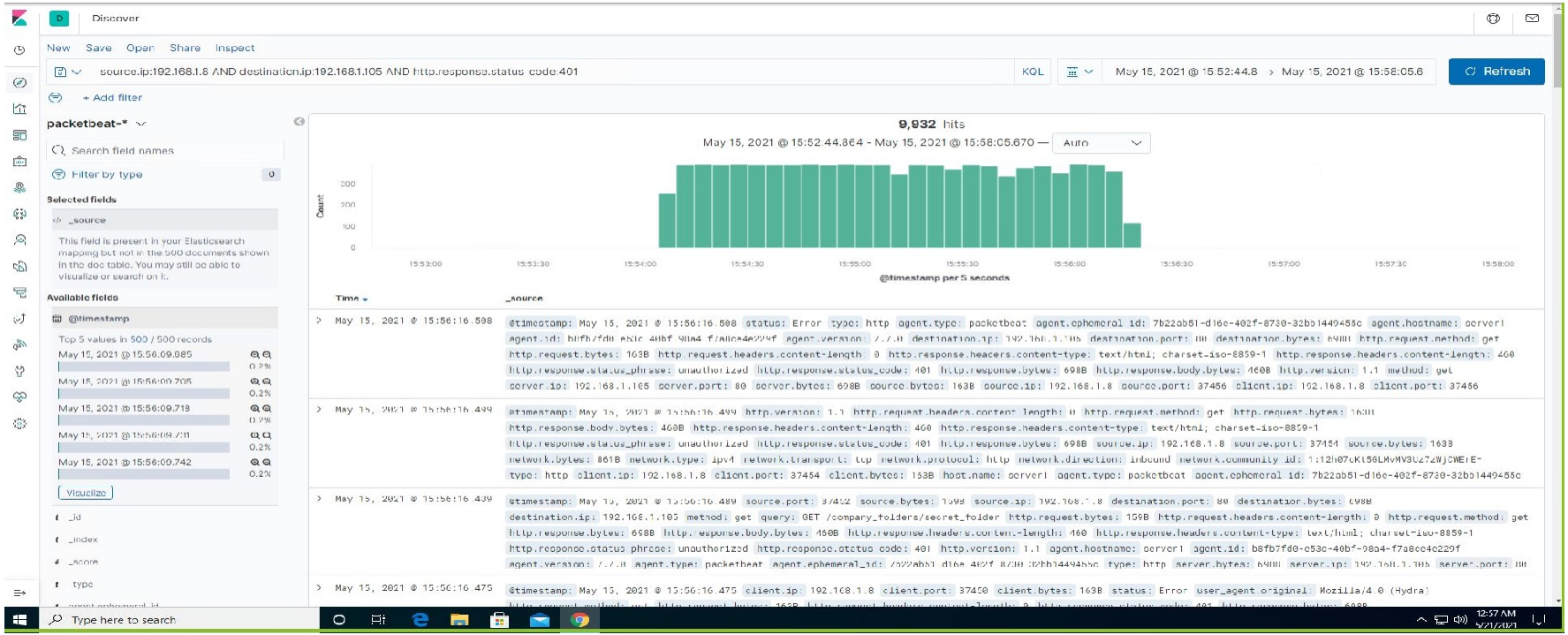
Analysis: Finding the Request for the Hidden Directory

- At 6:41pm 4, 850 requests were made
- Each request was for a different directory from the DIRB wordlist, it identified two directories, server-status and webdav.



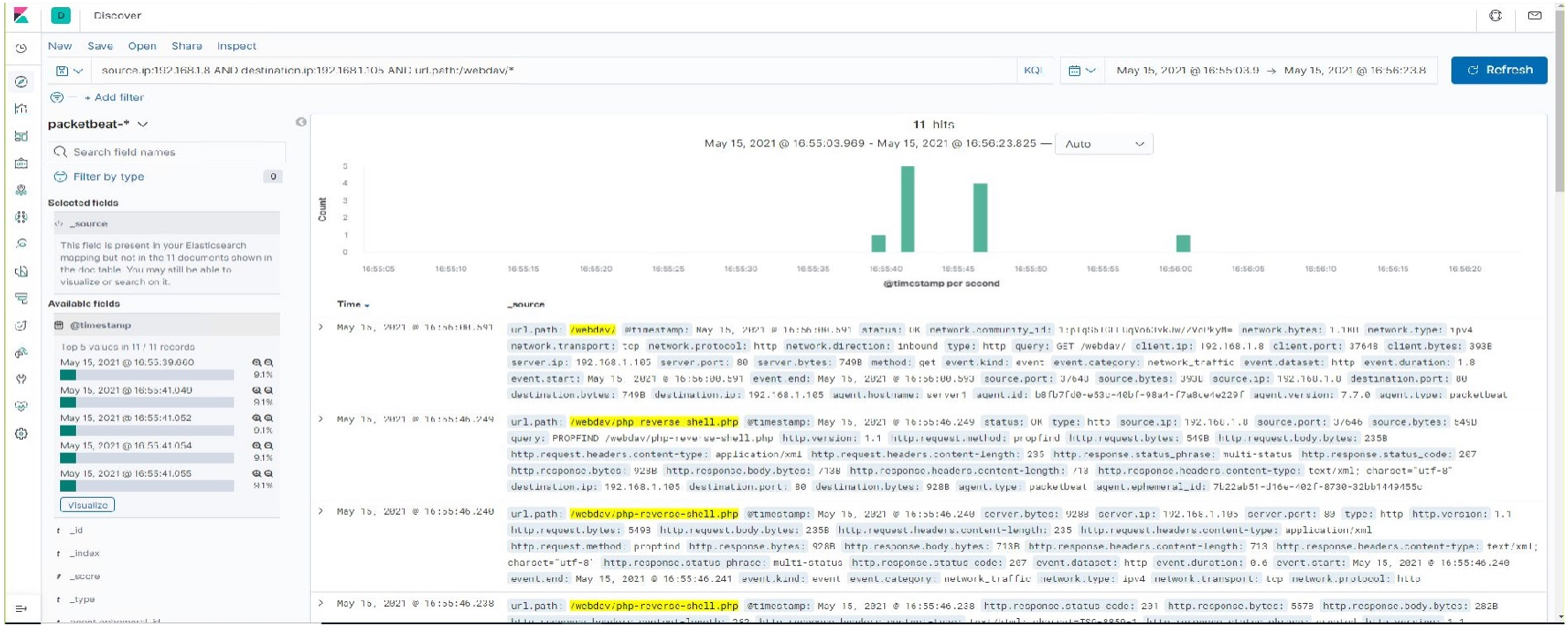
Analysis: Uncovering the Brute Force Attack

- 10,293 requests were made during the attack.
- Once the credentials were found the hydra application stopped sending requests, so they were all needed



Analysis: Finding the WebDAV Connection

- 18 total requests were made to the webdav directory.
- The php-reverse-shell.php file was requested several 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?

- If traffic from a particular source IP address is found to be listening to several ports, a filter can be set to block the traffic.

What threshold would you set to activate this alarm?

- Attempting IP address trying to should have activated filters in case it tries to make a connection.

System Hardening

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

- Installing a firewall together with an IPS that can detect and shutdown scans.

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

- Traffic originating from IP should effectively be filtered.

Mitigation: Finding the Request for the Hidden Directory

Alarm

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

- Setting an alarm that will send a notification incase of an login attempt of an IP that is not whitelisted.

What threshold would you set to activate this alarm?

- 1 should be the threshold for the alarm to be activated incase of any machine connection attempt.

System Hardening

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

- Removing the directory from the server.

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

- *rmdir -r* – command for deleting a directory together with its files from the server.

Mitigation: Preventing Brute Force Attacks

Alarm

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

- 401 request should send a notification incase of an server login attempt.

What threshold would you set to activate this alarm?

- Inorder to refine and allow mistyped password, your timing should start with 10 over a period of 40

System Hardening

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

- Limiting the unsuccessful login attempts
- Limiting access to only whitelisted IPs

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

- Configuring Account conditions on the server to restrict unsuccessful login attempts

Mitigation: Detecting the WebDAV Connection

Alarm

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

- Set an notification for the blacklisted IP that attempt to reach this directory
- Blacklisting All IPs not reachable within the server range area.

What threshold would you set to activate this alarm?

- The alarm should be triggered when an attempt is noticed even if its 1 attempt

System Hardening

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

- Restrict connections to shared folder to only whitelisted Ips.

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

- Port 80 should be blocked together with port 443
- All external Ips should be blacklisted.

Mitigation: Identifying Reverse Shell Uploads

Alarm

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

- Triggering notification incase of file.php file upload.
- Shared folder should be blocked from traffic originating from ports 80, 443 or 4444

What threshold would you set to activate this alarm?

- Either of the ports should have an alarm trigger warrant.

System Hardening

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

- Managing upload file ability to the web from any local file folder.

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

- Block port 80, 443, and 4444