Capstone Engagement

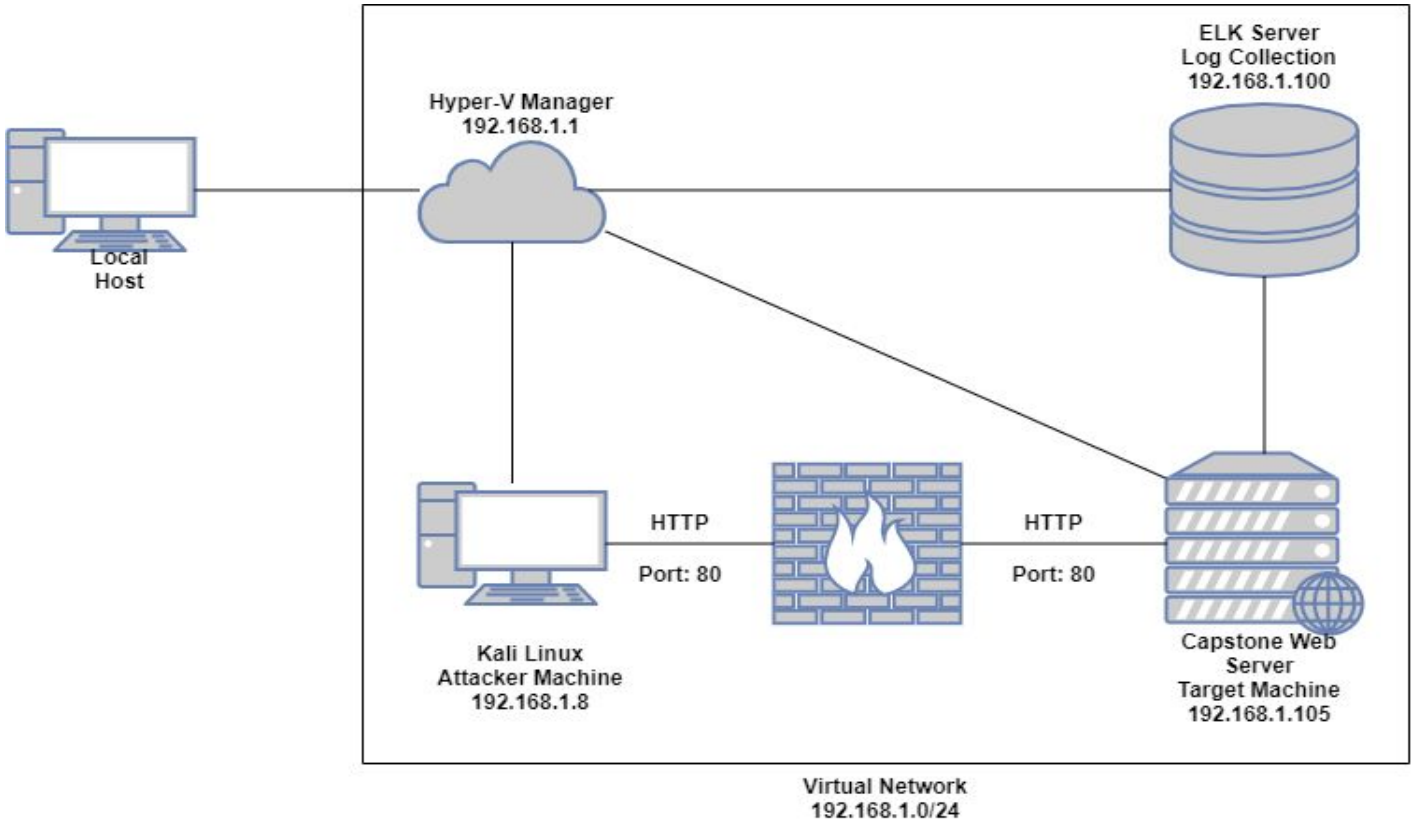
Assessment, Analysis, and Hardening of a Vulnerable System

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	This is the target machine using the apache web server.
Kali	192.168.1.8	This is the attacking machine using the Kali Linux.
Elk	192.1.100	Centralized logging service to identify problems in a server or application
Hyper V Manager	192.168.1.1	Software that virtualizes hardware into virtual machines/servers

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
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 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," "include," or similar functions	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

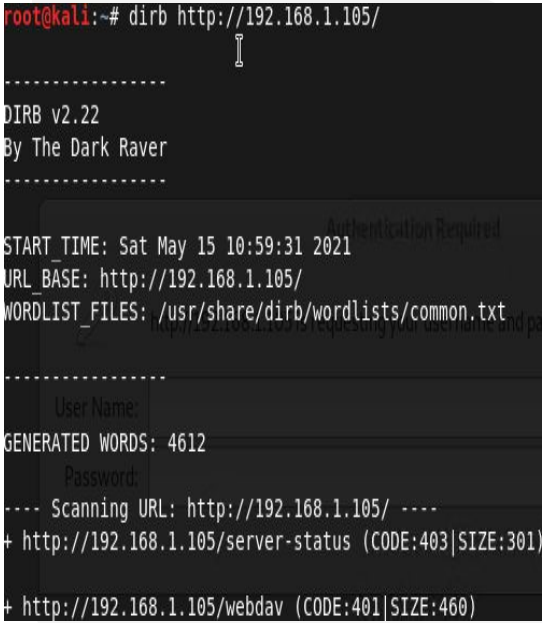
Tools & Processes
Used the “dirb” command to launch a dictionary based attack against the web server. DIRB looks for existing and/or hidden web objects.

Command used:
Dirb http://192.168.1.105

02

Achievements
Using this tool granted the knowledge of two hidden directories within the web server. The ‘server-status’ and ‘webdav’ directories were both uncovered using dirb.

03



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

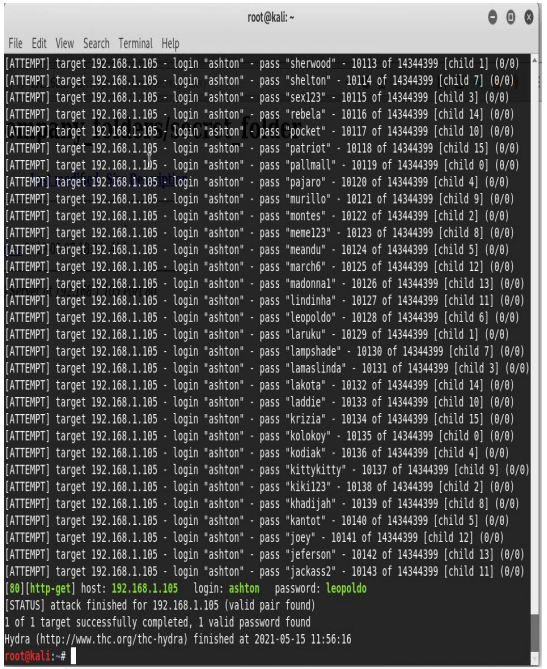
Command used:
hydra -l ashton -P rockyou.txt -s 80 -f -vV 192.168.1.105 http-get /company_folders/secret_folder

02

Achievements

This was able to produce the credentials “ashton:leopoldo” for access to the ‘secret_folder’ directory.

03



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

01

Tools & Processes

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

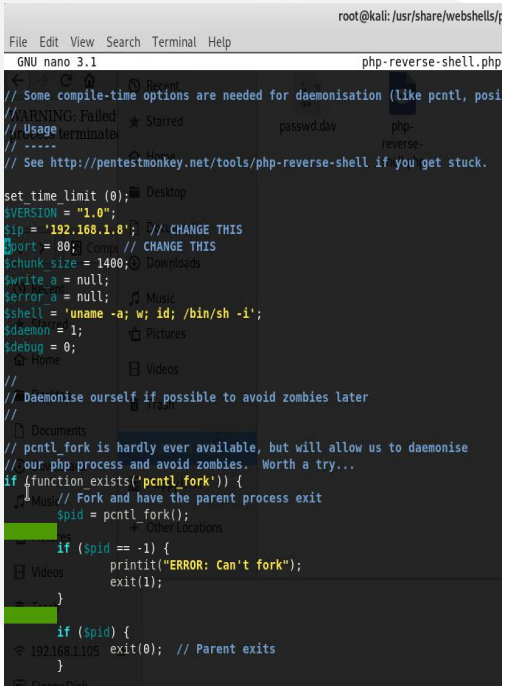
Once provisioning netcat to listen on port 80 the attack was a success.

02

Achievements

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

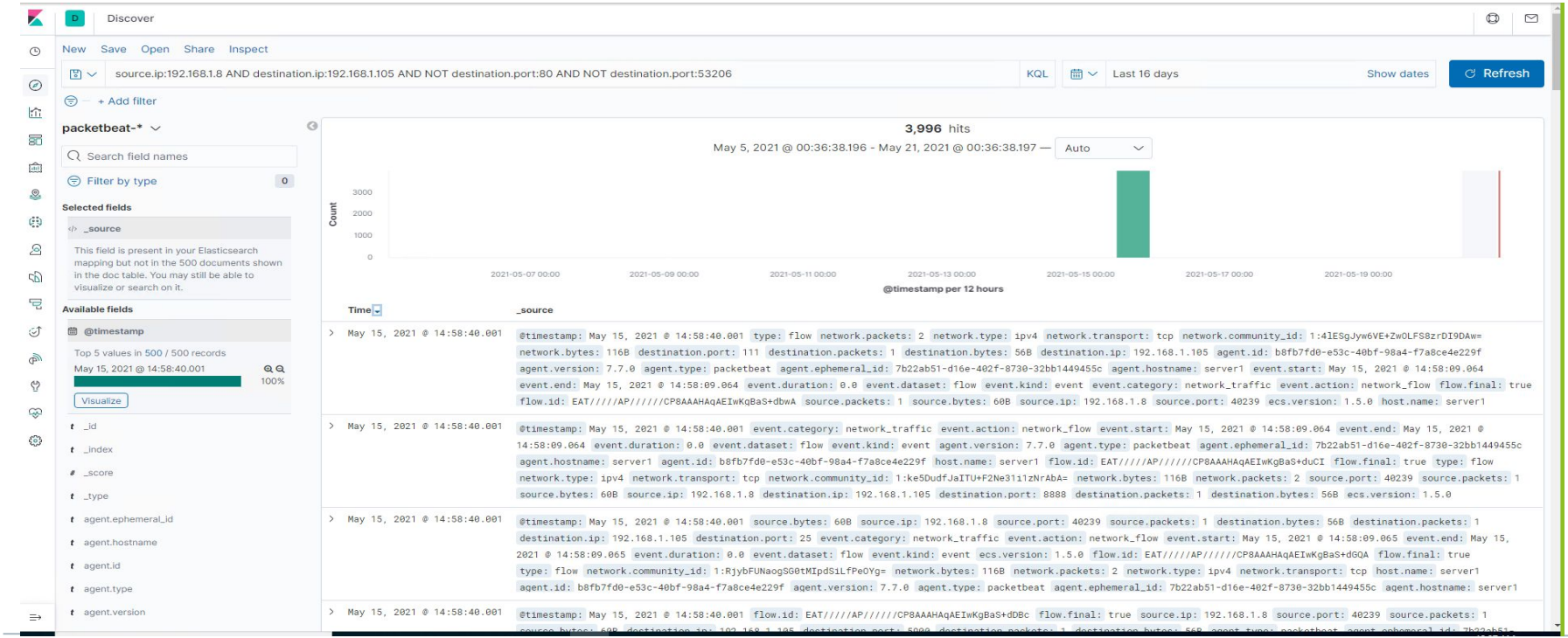
03



Blue Team
Log Analysis and Attack Characterization

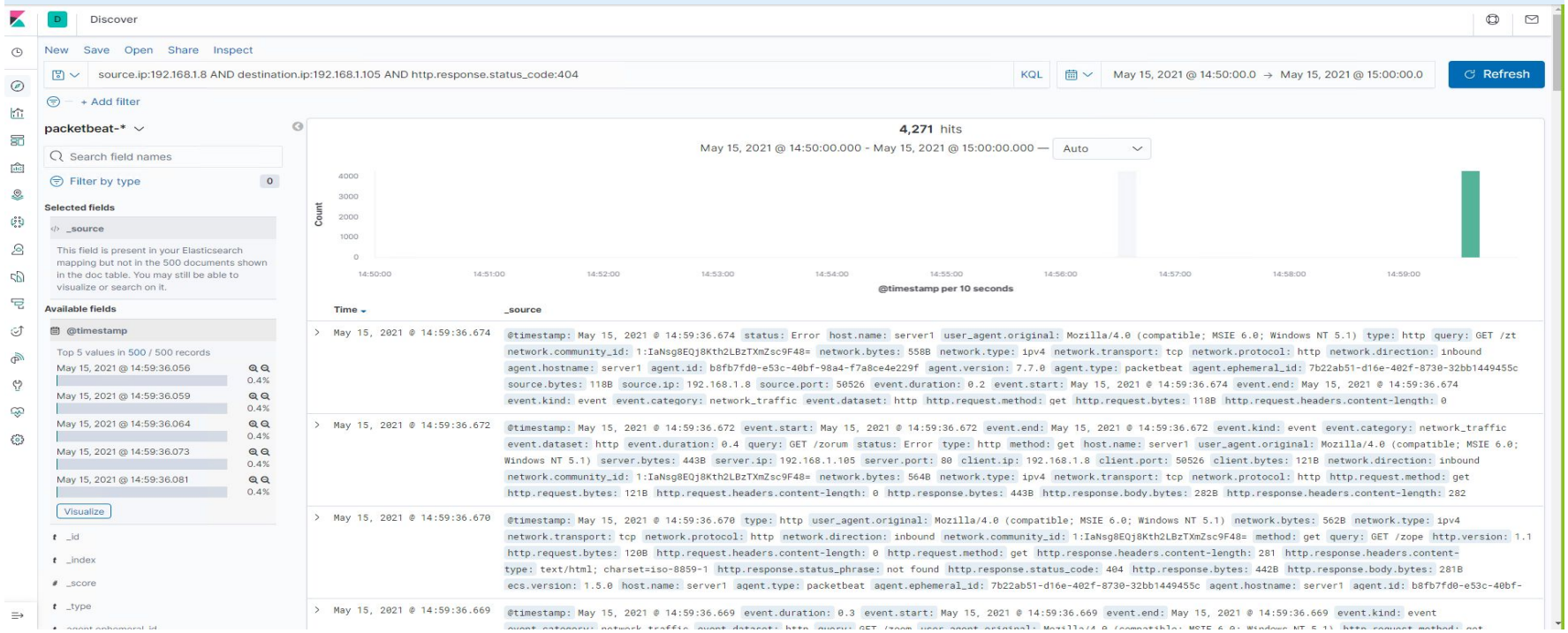
Analysis: Identifying the Port Scan

- The Port scan occurred at 2:58pm
- There were 3,996 packets sent from the IP address 192.168.1.8
- A few thousand requests all for different port numbers



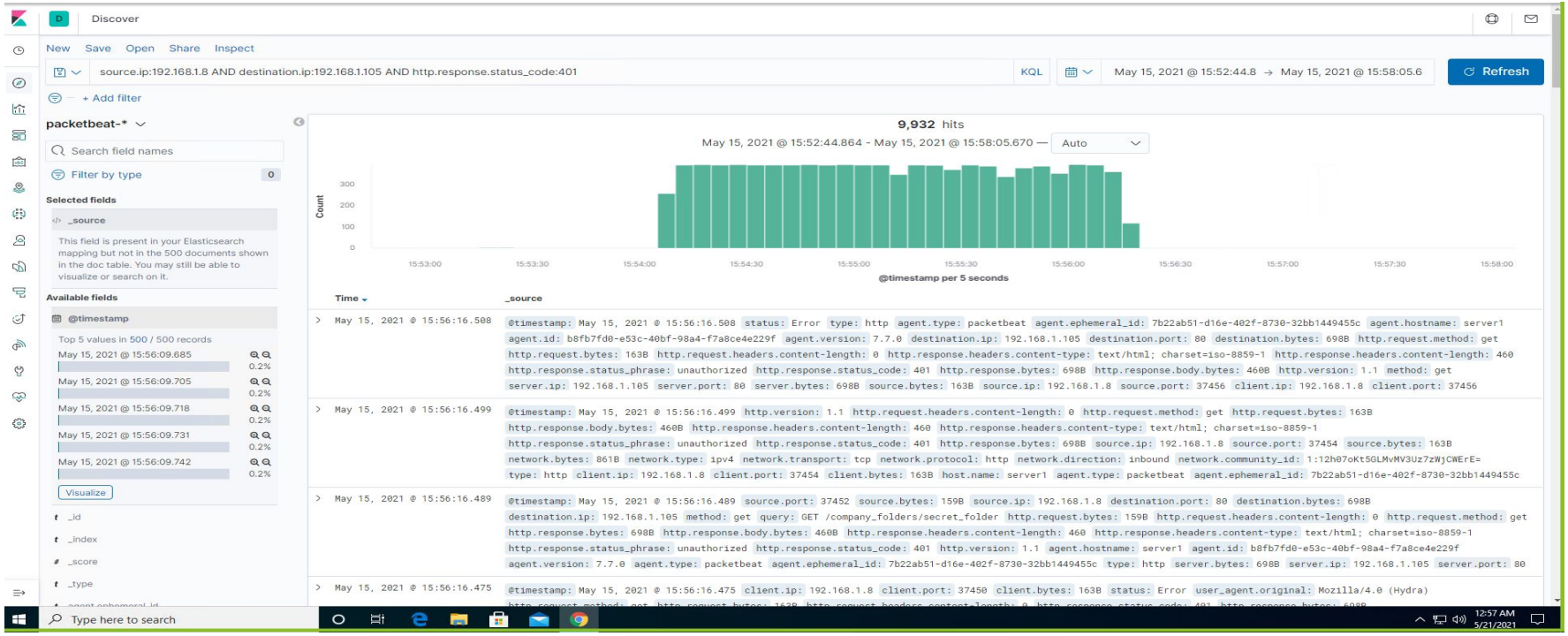
Analysis: Finding the Request for the Hidden Directory

- At 2:59pm 4,271 requests were made
- Each request was for a different directory from the DIRB wordlist, it identified two directories, server-status and webdav.



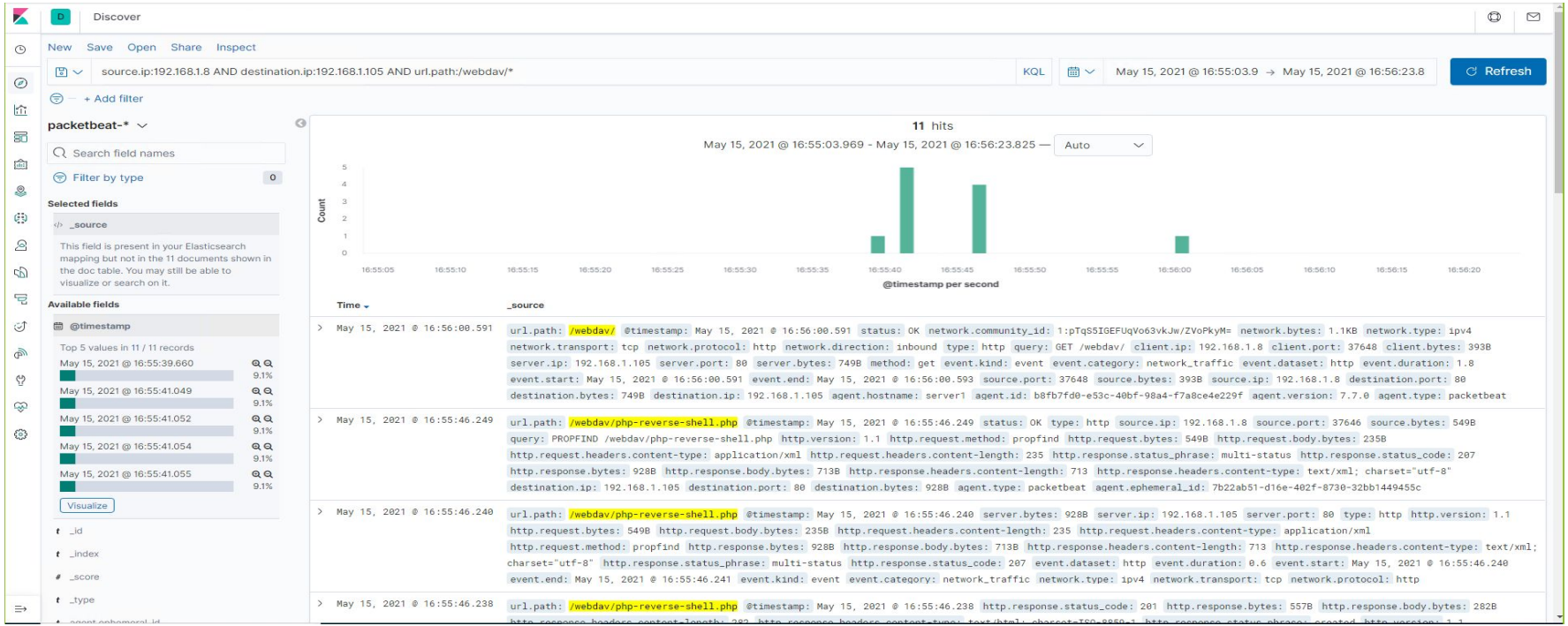
Analysis: Uncovering the Brute Force Attack

- 9,932 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

- 11 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?

- 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?

- 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?

- Install a firewall, an IPS can detect port scans and shut them down.

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

- 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?

- 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 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?

- 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 a 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 should be 1, 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 the machine using a blacklist firewall rule

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

- Blocking 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