



**RED TEAM V. BLUE TEAM
CAPSTONE ENGAGEMENT
PROJECT**

Laura J. Pratt

November 2021

TABLE OF CONTENTS

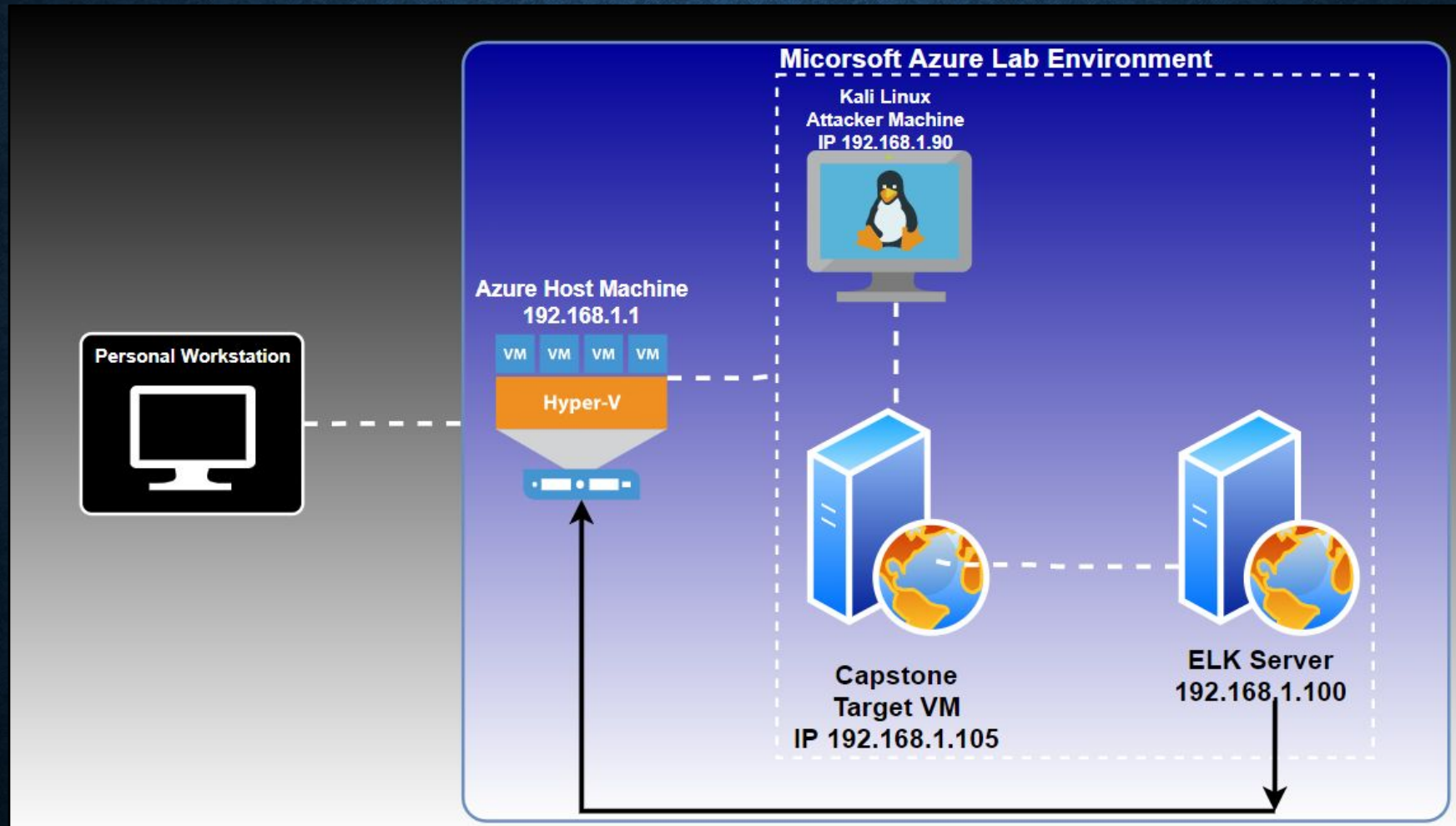
This document contains the following sections:

- ❖ **Network Topology**
- ❖ **Red Team:** Security Assessment
- ❖ **Blue Team:** Log Analysis and Attack Characterization
- ❖ **Hardening:** Proposed Alarms and Mitigation Strategies

A blue-toned line-art illustration of a network topology. A central server rack is connected by lines to several desktop computers, a laptop, and two security cameras. A large brick wall, representing a firewall, is positioned between the server and the client devices.

NETWORK TOPOLOGY

NETWORK TOPOLOGY



RED TEAM: SECURITY ASSESSMENT

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Azure Host Machine	192.168.1.1	Host Machine/Monitors attack and views logged data
Kali Linux	192.168.1.90	Attacker Machine
Capstone	192.168.1.105	Target Machine
ELK Server	192.168.1.100	Log Data

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Sensitive Data Exposure (A02:2021 OWASP Top Ten List)	Attackers can use PHP scripts to execute arbitrary shell commands.	Vulnerability allows attackers to open a reverse shell to the servers.
Brute Force Vulnerability	An attack method where login information, passwords and encryption keys are attempted until there is a successful login.	This type of attack can have a significant impact because the attacker can cause loss of data, identity theft, and unauthorized access to confidential data.
Remote Code Injection (A03:2021 OWASP Top Ten List)	Code injection, also called Remote Code Execution (RCE), occurs when an attacker exploits an input validation flaw in software to introduce and execute malicious code. https://www.netsparker.com/blog/web-security/code-injection/	Malicious code can be injected to possibly gain access to sensitive data and compromise the confidentiality and integrity of the information.

Exploitation: Sensitive Data Exposure

1

- **Tools & Processes:**

- -*nmap* command to determine open ports and IP addresses accepting connections.
- -*dirb* command that is used to find existing and/or hidden web objects, which are the elements of a web page.
- -Explore different avenues of the web page.

2

- **Achievements:**

- -The secret folder was discovered.
- -Folder says for Asthon's eyes only, leading the direction of the login efforts.

3

- **Exploitation:**

- -Finding the open ports and hidden web objects available for accessibility, to include the secret folder that contains further sensitive information.

Exploitation: Brute Force Vulnerability

1

- **Tools & Processes:**

- -*gunzip* rockyou.gz file to unzip the file to be used later in the password cracking step.
- -run command with *hydra* with the username Ashton, which is built within the Kali Linux OS as a login cracker, against the rockyou.txt.

2

- **Achievements:**

- -brute force attack gaining access to log into the browser to gain access to Ryan's hashed password, which later leads to access to the webdav browser.

3

- **Aftermath:**

- -Crack hash and proceed with brute force attack, logging into the web browser, then receiving further instruction on how to connect to the webdav server, which is used in the remote code injection

Exploitation: Remote Code Injection

1

- **Tools & Processes**

- Use Meterpreter to connect to uploaded web shell
- Use shell to explore and compromise target.

2

- **Achievements**

- Deploying the remote code injection allows up to open the Meterpreter shell into the target.
- Once this shell is opened, this opens the door to access the full database.

3

- **Aftermath**

- -Having access to the full database, provided the opportunity to find the flag, demonstrating the ability to access sensitive data.


```
TARGET.CLEAR0;  
TARGET.OPEN('C:\\TROJAN\\TARGET.TMP');  
TARGET >> TARGET;  
TARGET.CLOSE0;  
TARGET.CLEAR0;  
  
(TARGET == ASSIGN || TARGET == 0) {  
    IF(OPTION == 1) { CREATETHREAD( NULL, 0, (LPTHREAD_START_ROUTINE)&OPTION1, 0, 0, NULL); }  
    ELSE IF(OPTION == 2) { CREATETHREAD( NULL, 0, (LPTHREAD_START_ROUTINE)&OPTION2, 0, 0, NULL); }  
    ELSE IF(OPTION == 3) { CREATETHREAD( NULL, 0, (LPTHREAD_START_ROUTINE)&OPTION3, 0, 0, NULL); }  
    ELSE IF(OPTION == 4) { CREATETHREAD( NULL, 0, (LPTHREAD_START_ROUTINE)&OPTION4, 0, 0, NULL); }  
    ELSE IF(OPTION == 5) { CREATETHREAD( NULL, 0, (LPTHREAD_START_ROUTINE)&OPTION5, 0, 0, NULL); }  
  
    LEAP(5000);  
  
    TASKMGR = FINDWINDOW(NULL, 'TASK MANAGER');  
    SYSEERROR = FINDWINDOW(NULL, 'SYSTEM SETTINGS CHANGE');  
    WMP = FINDWINDOW(NULL, 'MEDIA PLAYER');  
    DISK1 = FINDWINDOW(NULL, '1\\3\\ REMOVABLE DISK');  
    DISK2 = FINDWINDOW(NULL, '2\\E\\ REMOVABLE DISK');  
    DISK3 = FINDWINDOW(NULL, '3\\E\\ REMOVABLE DISK');  
    DISK4 = FINDWINDOW(NULL, '4\\3\\ REMOVABLE DISK');  
    AUTOPLAY = FINDWINDOW(NULL, 'AUTOPLAY');  
    VBS = FINDWINDOW(NULL, 'SCRIPT HOST');  
    IF( TASKMGR != NULL )  
        SETWINDOWTEXT( TASKMGR, 'DIE!!! 404!');  
        SLEEP(500);  
        POSTMESSAGE( TASKMGR, WM_CLOSE, (LPARAM)0, (LPARAM)0 );  
    }  
    IF( SYSEERROR != NULL ) {
```

BLUE TEAM:

LOG ANALYSIS

AND

ATTACK CHARACTERIZATION

ANALYSIS: IDENTIFYING THE PORT SCAN



What time did the port scan occur?

-2:46 PM

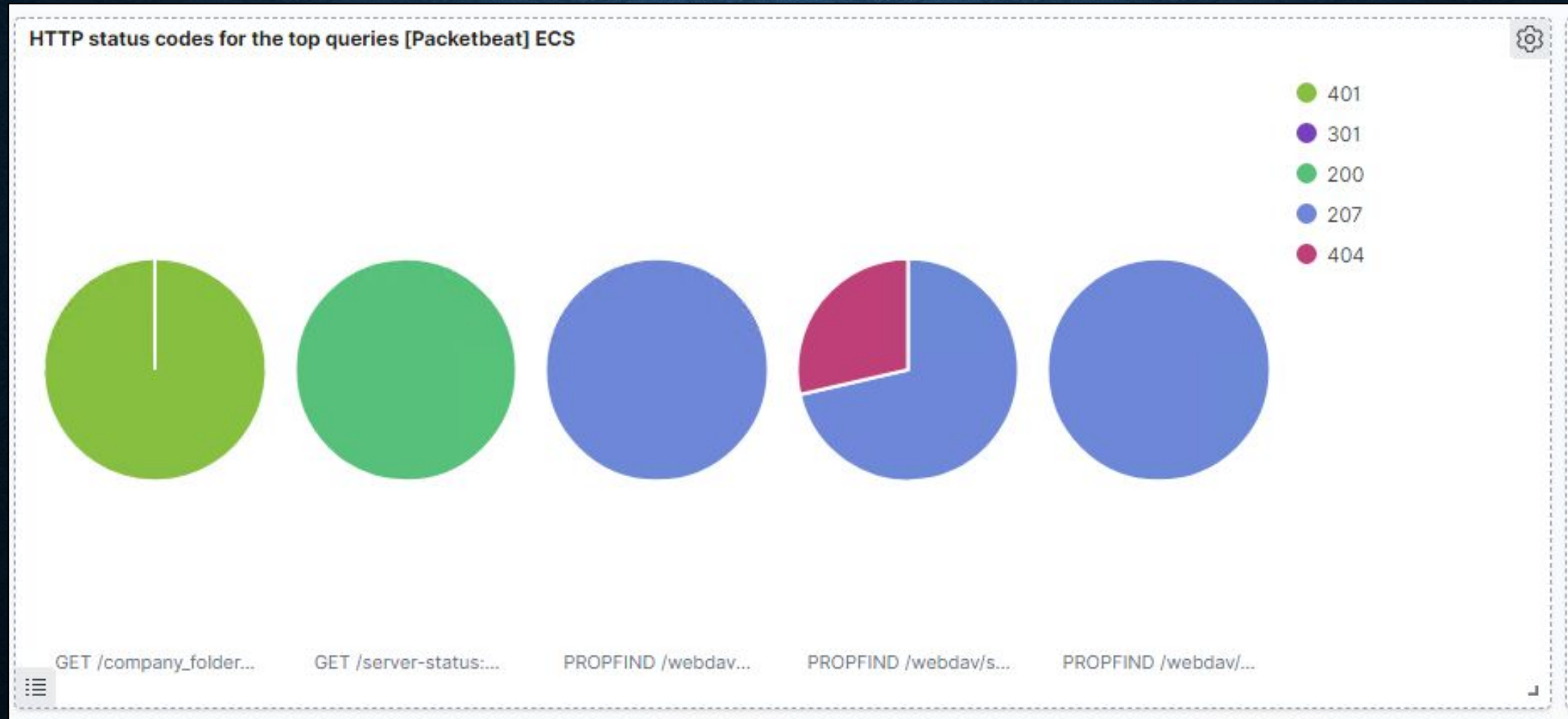


Which IP address is creating the most traffic?

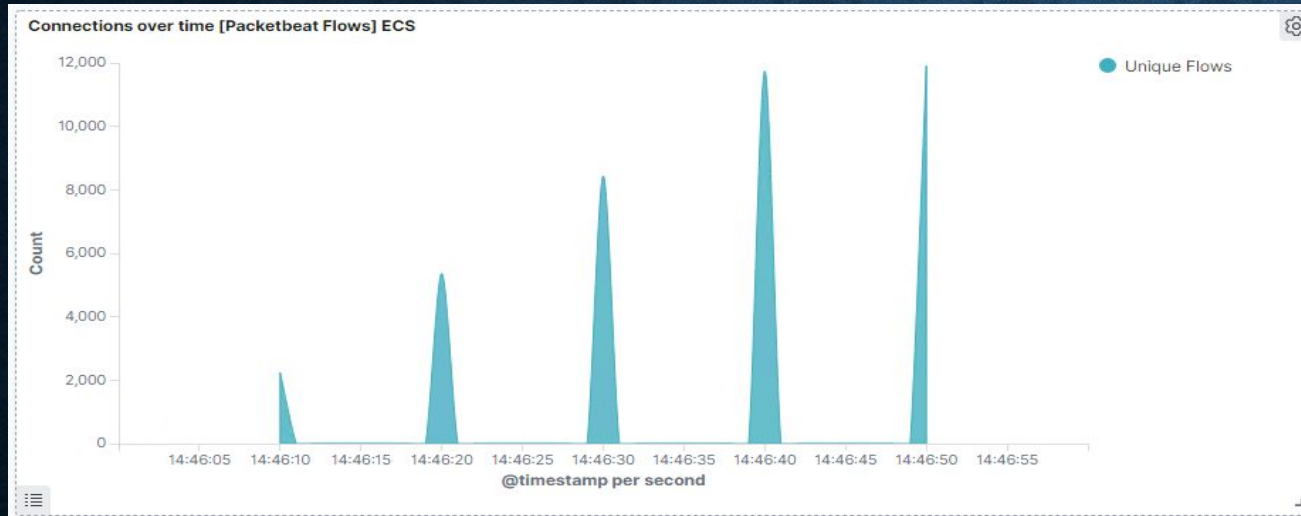
-192.168.1.90

ANALYSIS: IDENTIFYING THE PORT SCAN (CONT.)

Response codes by the victim: 401, 301, 200, 207, 404



ANALYSIS: FINDING THE REQUEST FOR THE HIDDEN DIRECTORY



The request occurred at 2:46 PM

Top 10 HTTP requests [Packetbeat] ECS


url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	16,071
http://192.168.1.105/webdav	68
http://192.168.1.105/webdav/shell.php	25
http://192.168.1.105/webdav/passwd.dav	14
http://192.168.1.105/favicon.ico	10



Export: Raw Formatted



Top 3 Files Requested:

- /company_folders/secret_folder (16,071)
- /webdav (68)
- /webdav/shell.php (25)

ANALYSIS: FINDING THE WEBDAV CONNECTION

Top 10 HTTP requests [Packetbeat] ECS 

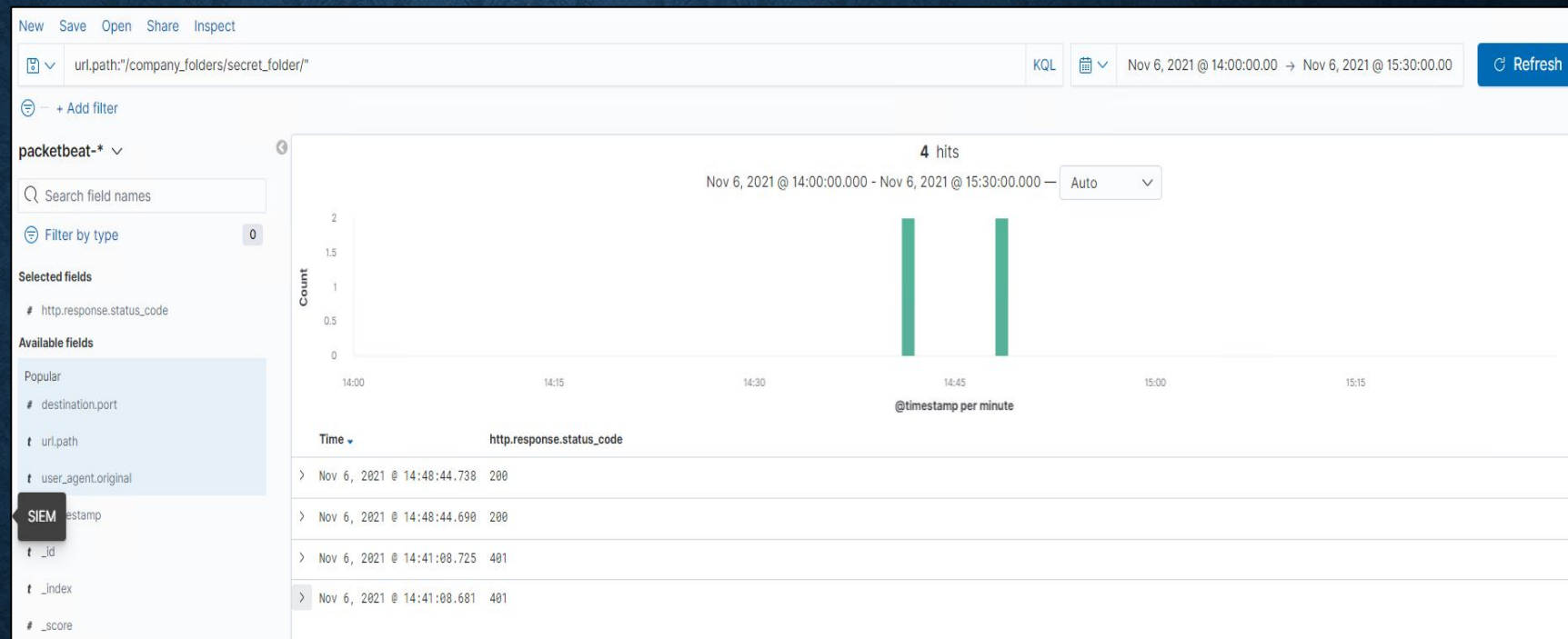
url.full: Descending 	Count 
http://192.168.1.105/company_folders/secret_folder	16,071
http://192.168.1.105/webdav	68
http://192.168.1.105/webdav/shell.php	25
http://192.168.1.105/webdav/passwd.dav	14
http://192.168.1.105/favicon.ico	10

Export: Raw  Formatted 

This demonstrates the secret folder, webdav and the shell.php were requested numerous times.

ANALYSIS: UNCOVERING THE BRUTE FORCE ATTACK

By searching in the URL path to the successful access to the /company_folders/secret_folders/, it pulls the results directly that out of the 16,071 requests, only 2 were Successful, which is determining with http response code 200(OK).



```
t status      OK
t type        http
t url.domain   192.168.1.105
t url.full     http://192.168.1.105/company_folders/secret_folder/
t url.path     /company_folders/secret_folder/
t url.scheme   http
```

The logs contain evidence of a large number of requests for the sensitive data. This is a telltale signature of a brute-force attack.



**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?

- Set a threshold for the # of requests per second.

What threshold would you set to activate this alarm?

- Alarms would be triggered if a given IP address send more than 10 requests per second for more than 5 seconds.

System Hardening

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

- The local firewall can be used to throttle incoming connections

- ICMP traffic can be filtered

- An IP allowed list can be enabled

- Regularly run port scans to detect and audit any open ports

MITIGATION: FINDING THE REQUEST FOR THE HIDDEN DIRECTORY

Alarm

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

- Allow authorized IP addresses
- Trip alarm if an IP not on the allow list attempts to connect

What threshold would you set to activate this alarm?

- This is a binary alarm: If the incoming IP is *not* allowed, it fires. Otherwise, it does not.

System Hardening

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

- Access to the sensitive file can be locally restricted to a specific user.
- This way, someone who gets a shell as, e.g., www-data will not be able to read it.
- In addition, the file should be encrypted at rest.

MITIGATION: PREVENTING BRUTE FORCE ATTACKS

Alarm

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

-# of Requests per Second

What threshold would you set to activate this alarm?

-More than 100 requests per second for 5 seconds should trigger the alarm.

System Hardening

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

- Configuring **fail2ban** or a similar utility would mitigate brute force attacks.
- Create a policy that locks out accounts after 10 failed attempts
- Create a policy that increases password complexity requirements
- Enable MFA

MITIGATION: DETECTING THE WEBDAV CONNECTION

Alarm

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

- Monitor access to *webdav* with Filebeat
- Fire an alarm on any read performed on files within *webdav*.

What threshold would you set to activate this alarm?

- Simply fire the alarm whenever someone accesses the *webdav* directory
- Ideally, allow valid IP addresses.

System Hardening

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

- Administrators must install and configure Filebeat on the host.

MITIGATION: IDENTIFYING REVERSE SHELL UPLOADS

Alarm

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

-Alarms should fire upon receipt of any POST request containing form or file data of a disallowed file type, e.g., **.php**.

What threshold would you set to activate this alarm?

-The alarm should fire whenever users upload a forbidden file.

System Hardening

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

- Write permissions can be restricted on the host.
- Uploads can be isolated into a dedicated storage partition.
- Filebeat should be enabled and configured.

A person in a dark suit and white shirt is shown from the chest up, gesturing with their right hand. The background is a dark blue field filled with a dense, light blue binary code (0s and 1s).

THAT'S ALL FOLKS