Capstone Engagement

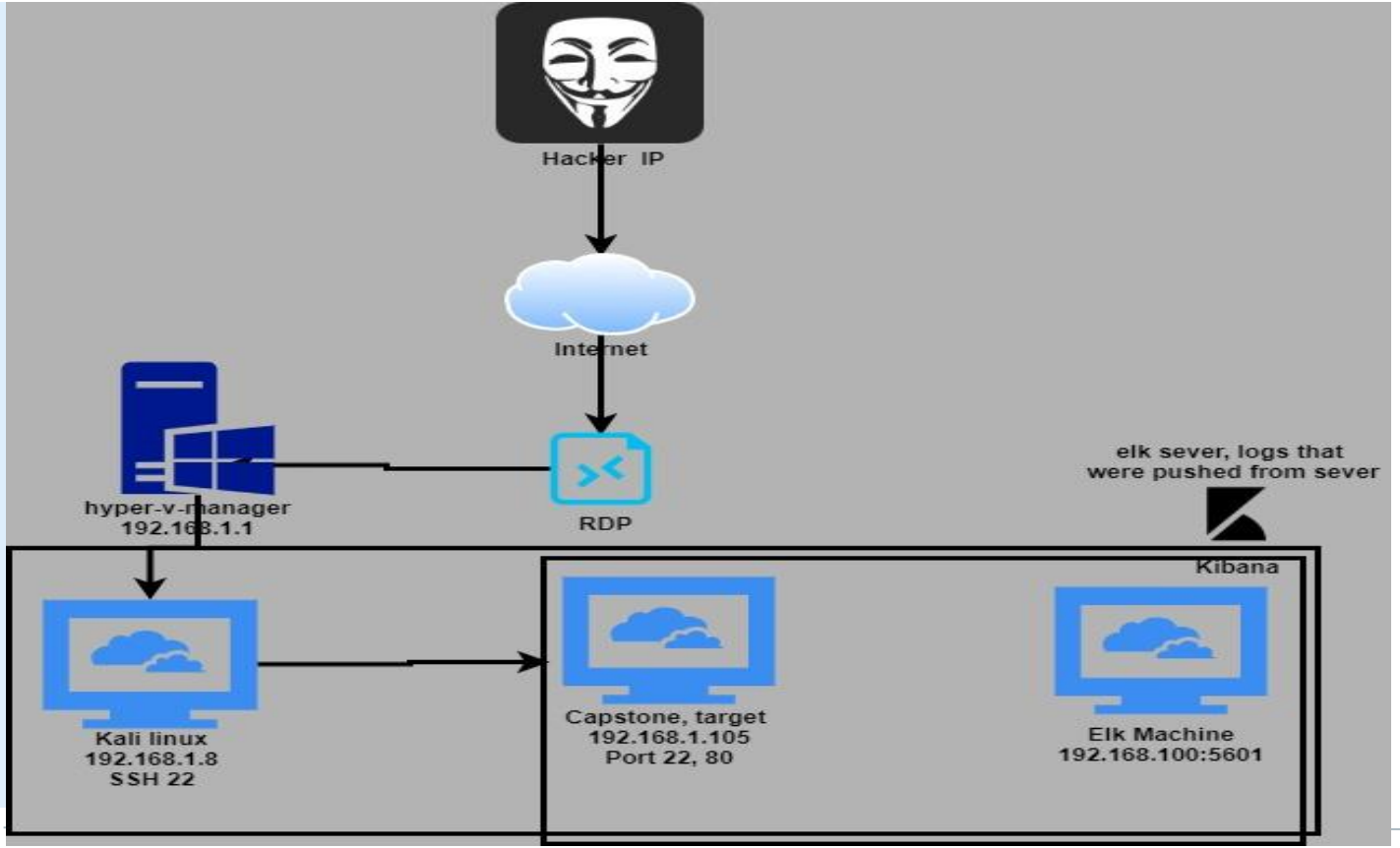
Assessment, Analysis, and Hardening of a Vulnerable System

Table of Contents

This document contains the following sections:

Network Topology

Network Topology



Network
Address Range:192.168.1.8/100
Netmask: 255.555.255.0
Gateway: 0.0.0.0

Machines
IPv4: 192.168.1.8
OS: linux
Hostname: Kali

IPv4: 192.168.1.105
OS: linux
Hostname: Capstone

IPv4: 192.168.1.1
OS: Windows
Hostname: RefVM

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	VUlNERABILITY MACHINE
KALI	192.168.1.8	ATTACKING VIRTUAL MACHINE
ELK	192.168.1.100	SIEM, KIBANA Logs
Hyper V manager,	192.168.1.1	JumpBox

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
The password was found using hydra was easily found. Lack of strong passwords and also there was nothing put in place to stop the brute force attack. Ex. too many attempts,	*Brute forcing the attack with hydra, we was able to locate the passwords using a file that stores commonly using passwords in a file called Rockyou.txt*	*The impact of the vulnerability allowed me to gain access to the credentials and login to the secret folder with ashton credentials*
The Apache web server was vulnerable	*The web server for the company was available for me to easily navigate to. There wasn't any form of authentication required until i had to go inside of a secret folder.*	*The impact of the vulnerability allowed me to see public information which led me to the secret folder to find more vital information*
The server was vulnerable to a reverse shell payload. A backdoor using root privileges.	*A revershell payload can exploit a vulnerable system that hasn't been patched and ports closed*	*The impact of the vulnerability allowed me to create a reverse payload and access the server from a back door and implement a shell.php*

Exploitation: Brute Force attack using HYDRA

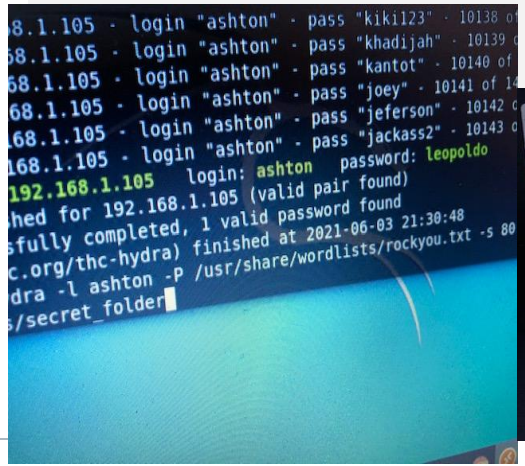
01

First, I was able to brute force ashtons account using hydra.After finding out his credentials, I was able to log into a secret folder that his exposed himself of having on the companies website. After logging into the secret folder, was able to see webdav/ information that contains a hashed. That hashed was ryan's password credentials

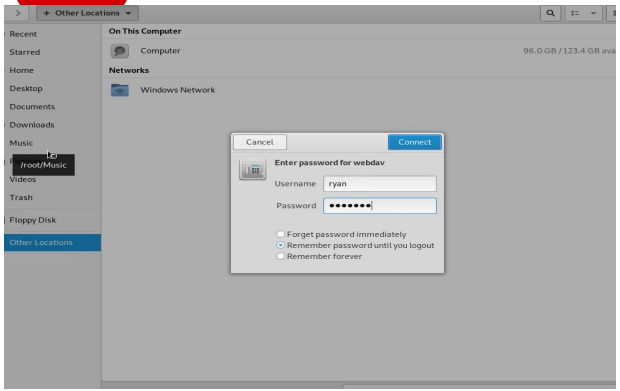
02

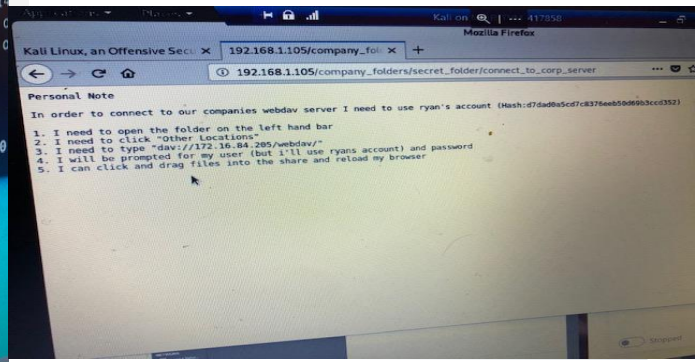
USER:Ashton
PW: leopoldo

USER: ryan
PW: linux4u



03





Exploitation: Expose Ashton files on apache website

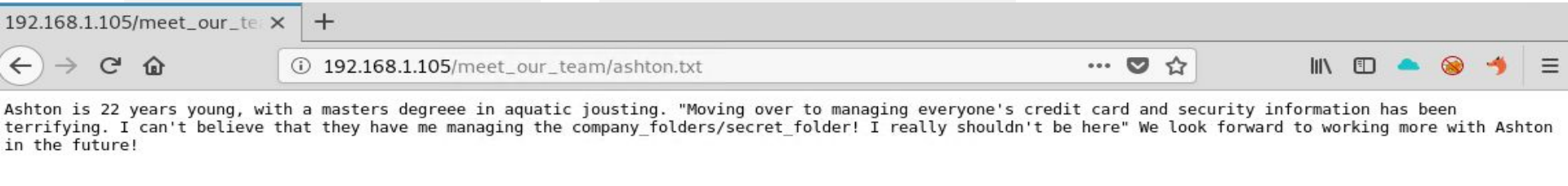
01

First, I was able to navigate to apache web server 192.168.1.105:5601. The files were listed of all the employees. There were valuable information in the company folders. Also, inside one of the folders were root privileges for Ashtons account.

02

When I was inside of ashtons account, he was responsible for the company secret folder. It was listed as, /company_folders/secret_folder/. Inside of the folder was more valuable information. I was able to log into ashtons secret folders with credentials ASHTON and LEOPOLDO

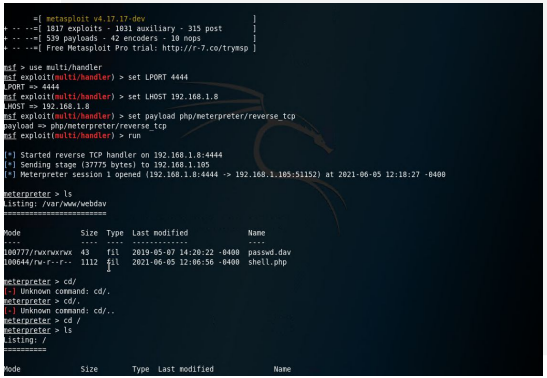
03



Exploitation: reverse shell payload backdoor

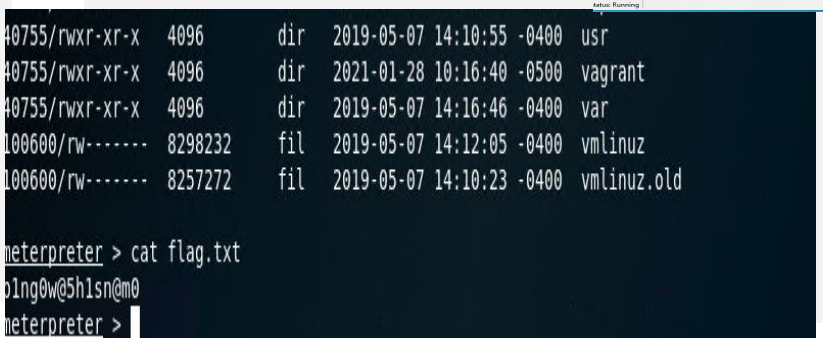
01

On the Victim's machine, we were able to execute a custom reverse shell payload. I also was able to upload a shell on the backend of the root .

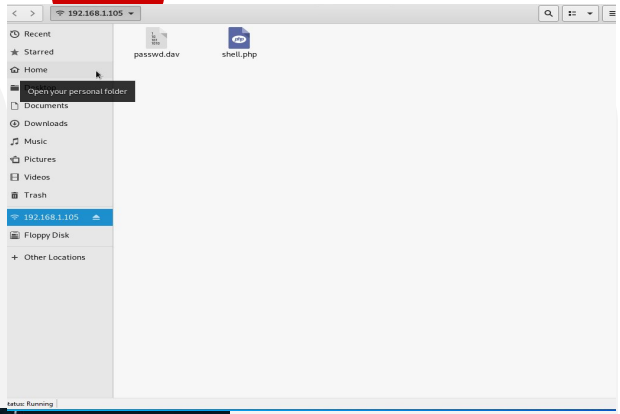


02

After being able to access the victim's machine from the payload, I was able to gain root privileges and search for the flag.



03



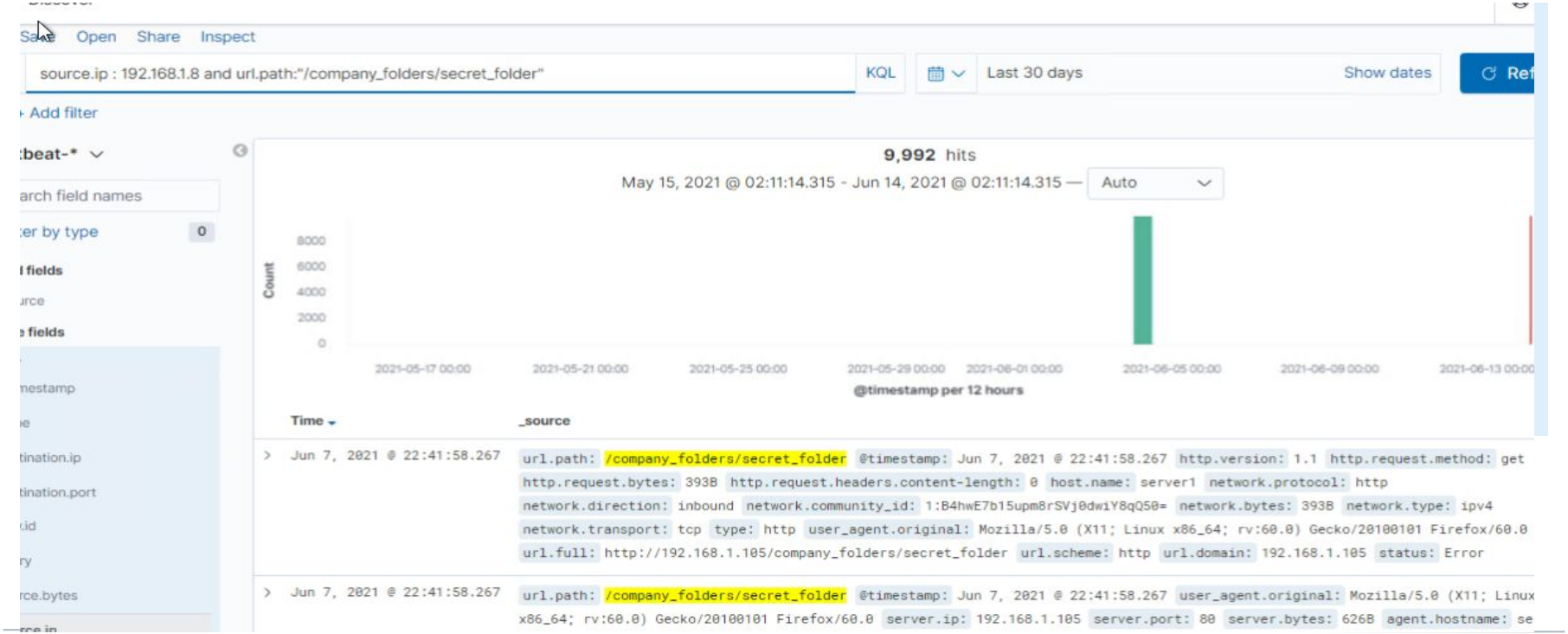
Blue Team
Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

- What time did the port scan occur? **The scan occured 2:00pm on JUNE 5th**
- How many packets were sent, and from which IP? **546 packets were being sent**
- What indicates that this was a port scan? **Multiple ports were scan around the same time**

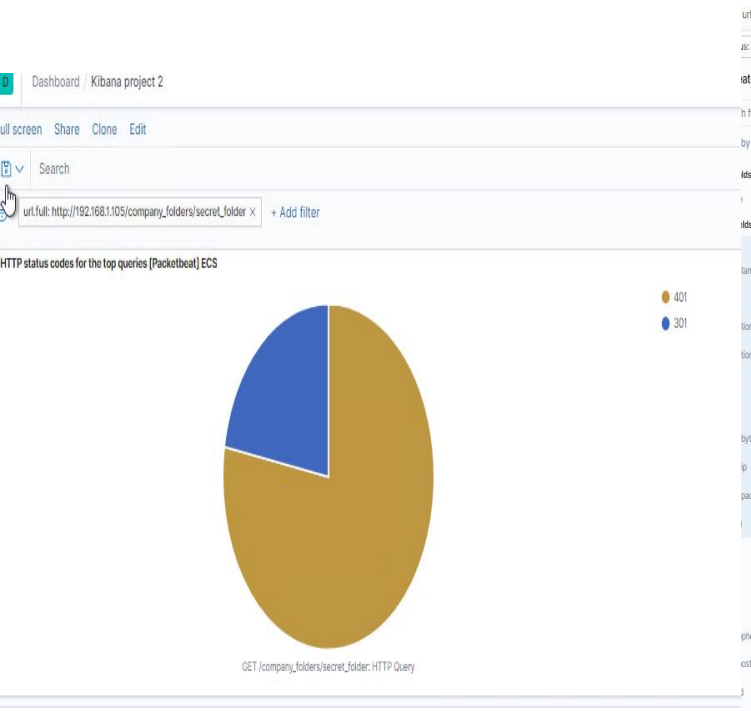
Analysis: Finding the Request for the Hidden Directory

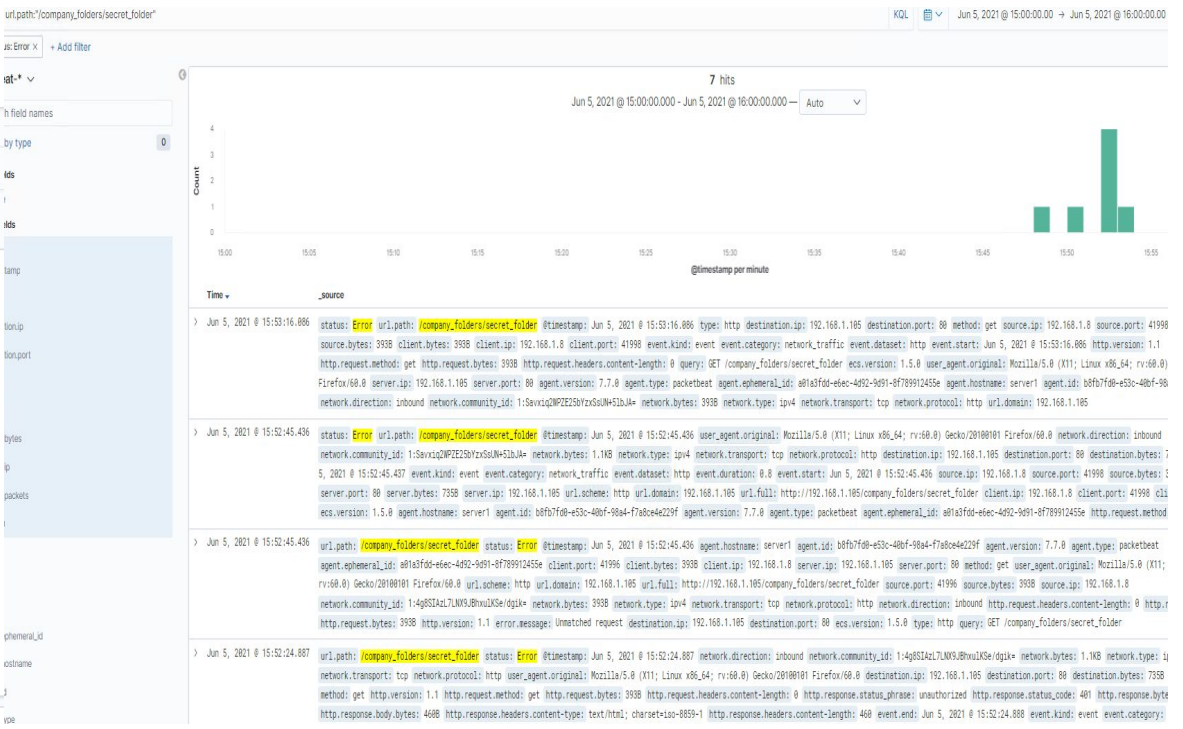
- What time did the request occur? **JUNE 5th** How many requests were made? **9,992 packets**
- Which files were requested? **company_folders/secret_folder What did they contain**? **The hashes for ryans PW account**



Analysis: Uncovering the Brute Force Attack

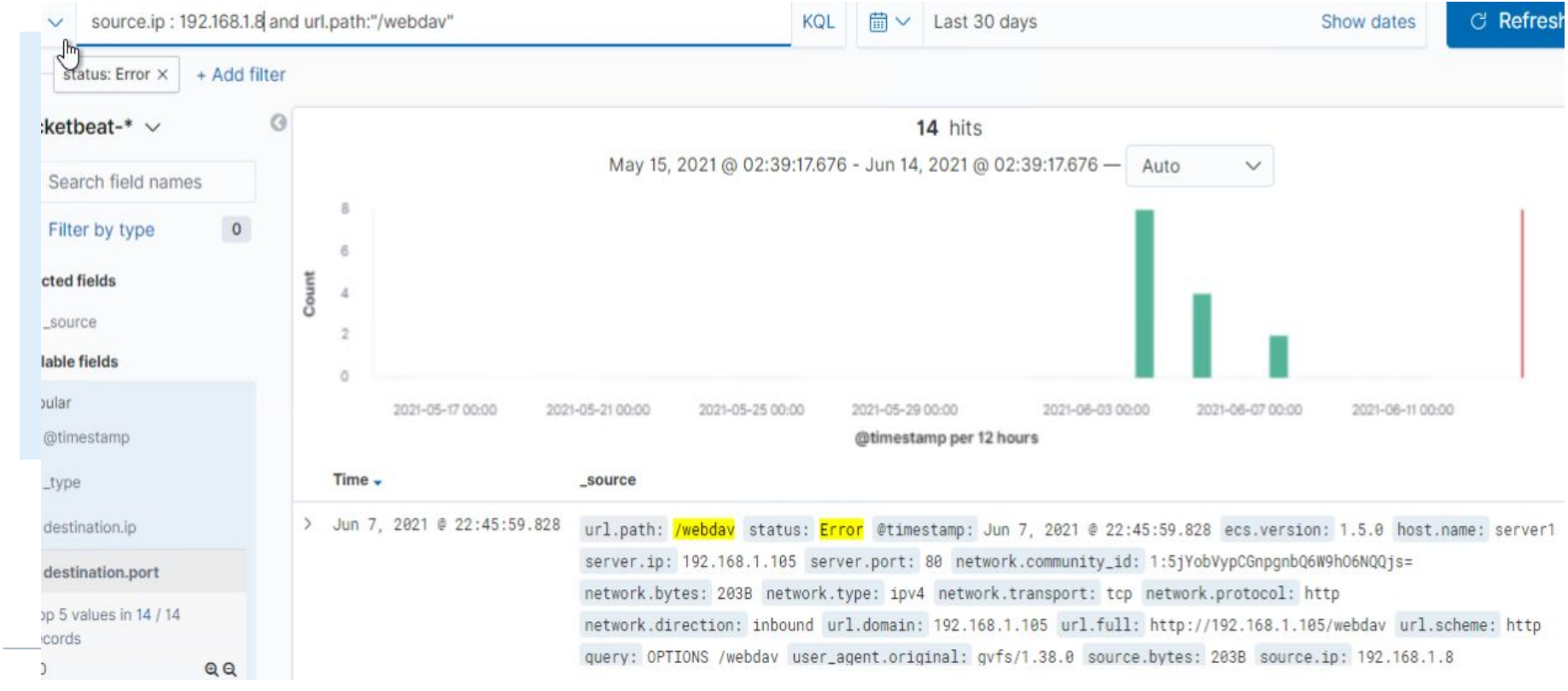
- How many requests were made in the attack? **7 hits were connected**
- How many requests had been made before the attacker discovered the password?





Analysis: Finding the WebDAV Connection

- How many requests were made to this directory? **14 hits were made for the webdav**
- Which files were requested? **/webdav/shell.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? **I would implement a intrusion detection systems for network and port scans.**

What threshold would you set to activate this alarm? **The threshold would be any ping requests greater then 2**

System Hardening

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

1. **You can install a firewall to blow traffic from unwanted request.**
2. **Install a TCP Wrapper, flexibility to permit or deny access to the servers based on IP addresses or domain names.**

Describe the solution. If possible, provide required command lines. **I will set a snort tool as well that will stop and prevent port scanning**

Mitigation: Finding the Request for the Hidden Directory

Alarm

What kind of alarm can be set to detect future unauthorized access? **I will set an alert for the secret folder that was brute forced and accessed. Also any 401 error codes.**

What threshold would you set to activate this alarm? **The threshold would be 3 attempts per hour**

System Hardening

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

1. **For starters, I wouldn't have the secret folder on the company website.**
2. **I will have a lockout policy for brute force attacks.**
3. **I will a firewall for unwanted internet access.**

Describe the solution. If possible, provide required command lines. **A defense in depth module put in place with these rules and techniques for layers of security**

Mitigation: Preventing Brute Force Attacks

Alarm

What kind of alarm can be set to detect future brute force attacks? **I will set a alarm just for 401 error codes.**

What threshold would you set to activate this alarm? **50 per hour**

System Hardening

What configuration can be set on the host to block brute force attacks? **I will set two factor authentications. Lock up the account, once there are so many attempts**

Describe the solution. If possible, provide the required command line(s). **Once a attacker tries to brute force, or even if they get in. They will to go through another authentication before they can get in. After many login attempts, teh account becomes locked.**

Mitigation: Detecting the WebDAV Connection

Alarm

What kind of alarm can be set to detect future access to this directory? **Have a alert set to trigger connections attempted to that file.**

What threshold would you set to activate this alarm? **10 attempts per hour**

System Hardening

What configuration can be set on the host to control access? **I will set a rule to have all deny to the webdav with firewall**

Describe the solution. If possible, provide the required command line(s). **This will prevent all unwanted traffic away from webdav**

Mitigation: Identifying Reverse Shell Uploads

Alarm

What kind of alarm can be set to detect future file uploads? **A alert that monitors port 4444 or any attempts and failed connections. Also, configure a netcat tool to listen for open connections.**

What threshold would you set to activate this alarm?**The threshold would be 2 per hour. In addition to the webdav folder as well.**

System Hardening

What configuration can be set on the host to block file upload**s? Configure a netcat tool to, this will give the ability to bind outbound listening connections.**

Describe the solution. If possible, provide the required command line. **NC -1 -p 4444 -e cmd.exe. You will be prompted to a host connecting you to the connection.**


The End