



Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

Table of Contents

This document contains the following sections:

01

Network Topology

02

Red Team: Security Assessment

03

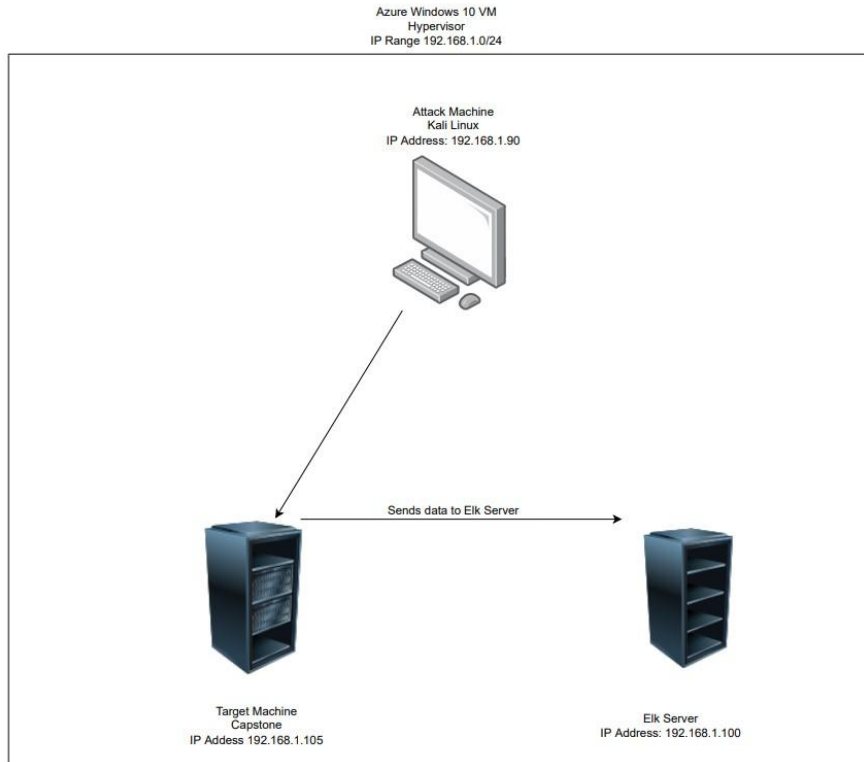
Blue Team: Log Analysis and Attack Characterization

04

Hardening: Proposed Alarms and Mitigation Strategies

Network Topology

Network Topology



Network

Address Range:
192.168.1.0/24
Netmask: 255.255.255.0
Gateway: 192.168.1.1

Machines

IPv4: 192.168.1.90
OS: Linux
Hostname: Kali

IPv4: 192.168.1.105
OS: Linux
Hostname: Capstone

IPv4: 192.168.1.100
OS: Linux
Hostname: Elk

The background of the slide is a dark red, almost black, field filled with a complex, repeating geometric pattern of triangles and polygons in various shades of red and maroon, creating a textured, crystalline effect.

Red Team Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Red vs Blue Azure Cloud Environment	192.168.1.1	Provide virtual environment to conduct offensive operations and defensive analysis.
Kali VM	192.168.1.90	Machine utilized for penetration test of vulnerable web server
Capstone	192.168.1.105	VM used to provide vulnerable server
Elk	192.168.1.100	Web application that logs traffic and allows for analysis

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
<i>Use the CVE number if it exists. Otherwise, use the common name.</i>	<i>Describe the vulnerability.</i>	<i>Describe what this vulnerability allows the attacker to do.</i>
Weak Credentials	Weak Credentials are susceptible to Brute Force Attacks.	A successful Brute Force Attack on weak credentials can allow for unauthorized access to sensitive information and implementation of malicious payloads.
Sensitive Data Exposure	Simple and or weak hashes are stored on web server.	Simple hashes can be cracked using tools such as crackstation to discover user credentials .
Unauthorized File Upload	Attackers can upload files to server.	Attacker can upload malicious files to the web server such as PHP scripts.

Exploitation: Weak Credentials

01

Tools & Processes

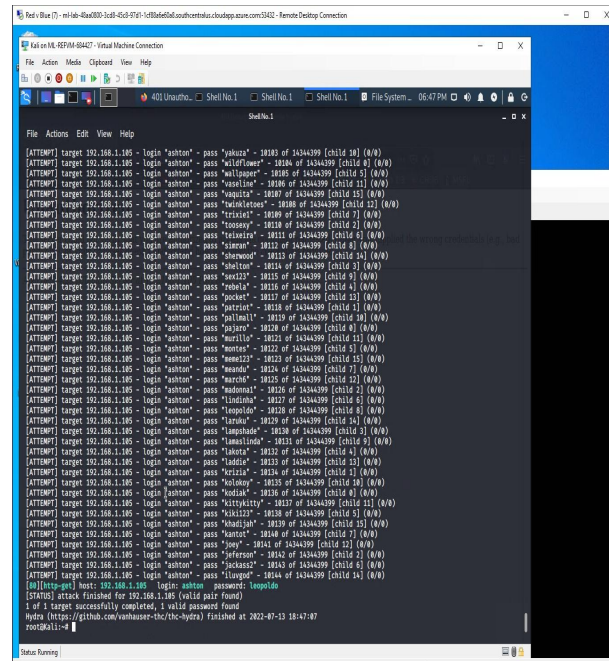
- Conducted a brute force attack
- Used Hydra to crack the password in conjunction with the rockyou.txt password list

02

Achievements

- This gave me Ashton's password
- With Ashton's credentials I was able to gain access to the /company_folders/secret_folder/

03



```
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-07-13 18:47:07
root@kali:~#
```


Exploitation: Sensitive Data Exposure

01

Tools & Processes

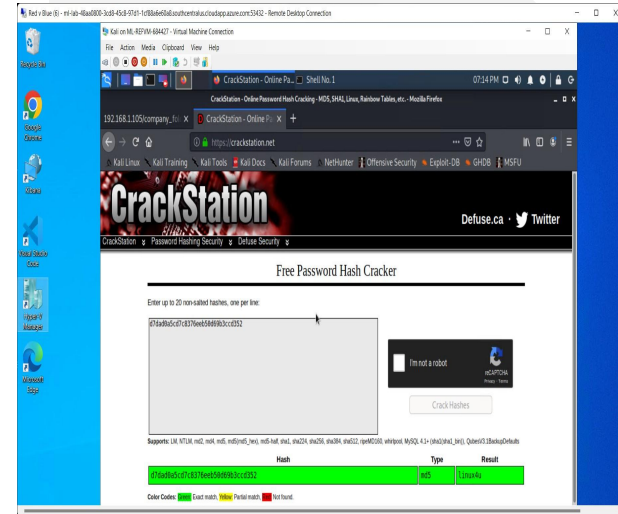
- Used crackstation.net to crack password hash

02

Achievements

- Able to crack Ryan's password hash
- Gained access to the Webdav thus allowing me the ability to upload and move files

03



Exploitation: Unauthorized File Upload

01

Tools & Processes

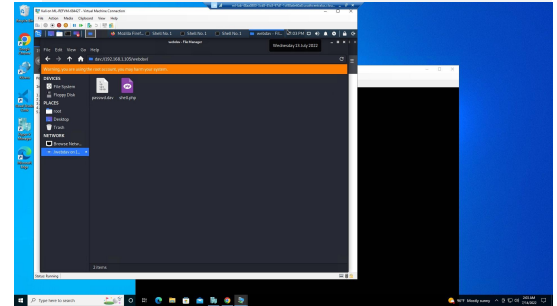
-Use WebDav to upload shell created with msfconsole on Kali machine.

02

Achievements

-Able to upload a Reverse TCP shell on the target machine
- With the shell uploaded I could now establish a remote connection to the target machine.

03



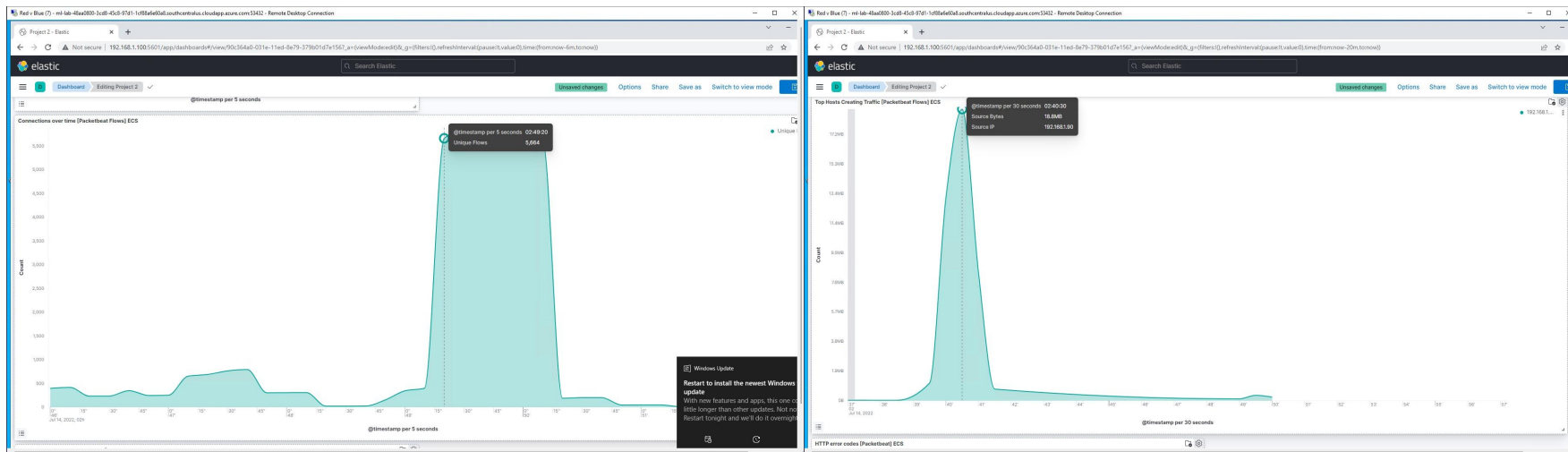


Blue Team

Log Analysis and Attack Characterization

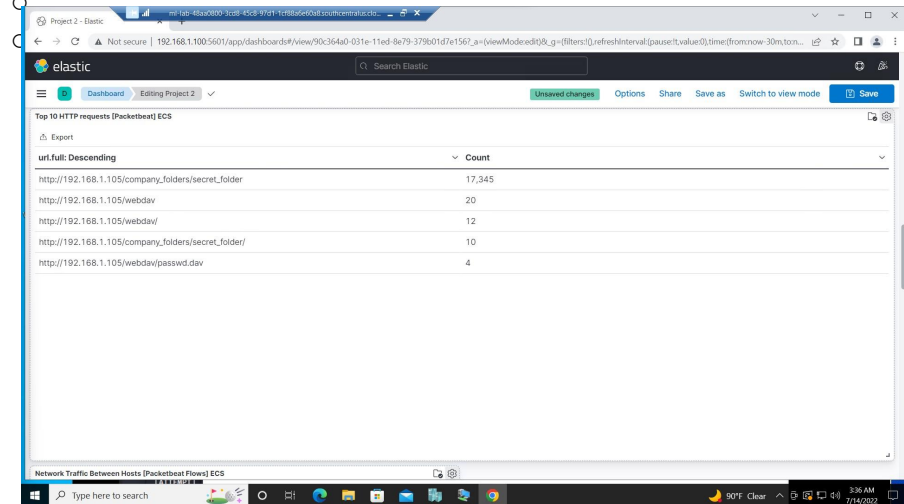
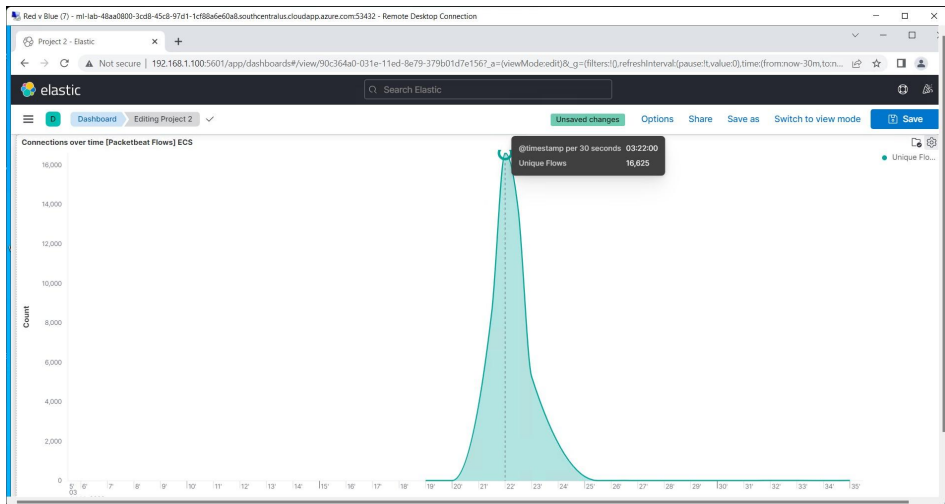
Analysis: Identifying the Port Scan

- Port Scan occurred at 2:40 am
- 14,449 packets were sent. The IP address is 192.168.1.90
- The high volume of packets sent by the source IP is an indication of a port scan



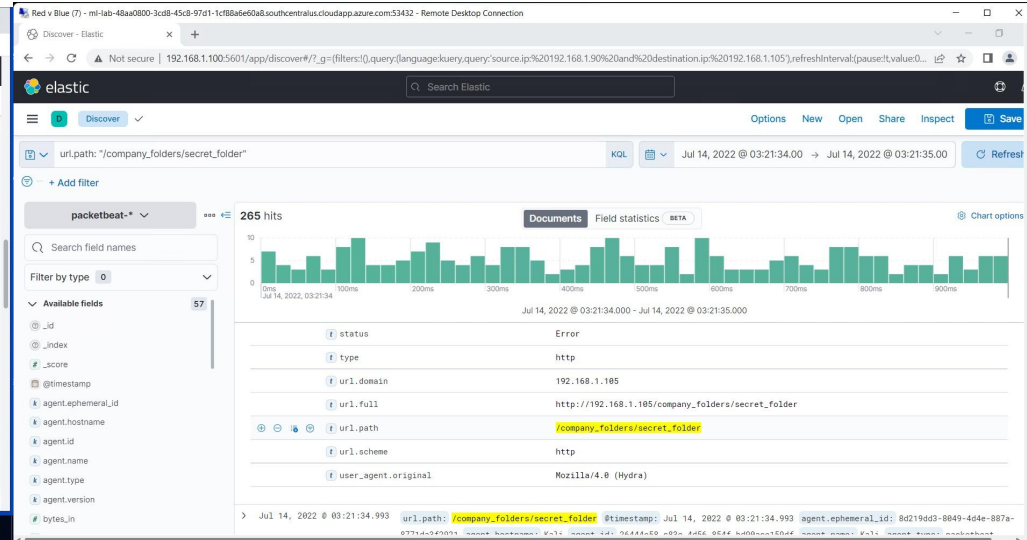
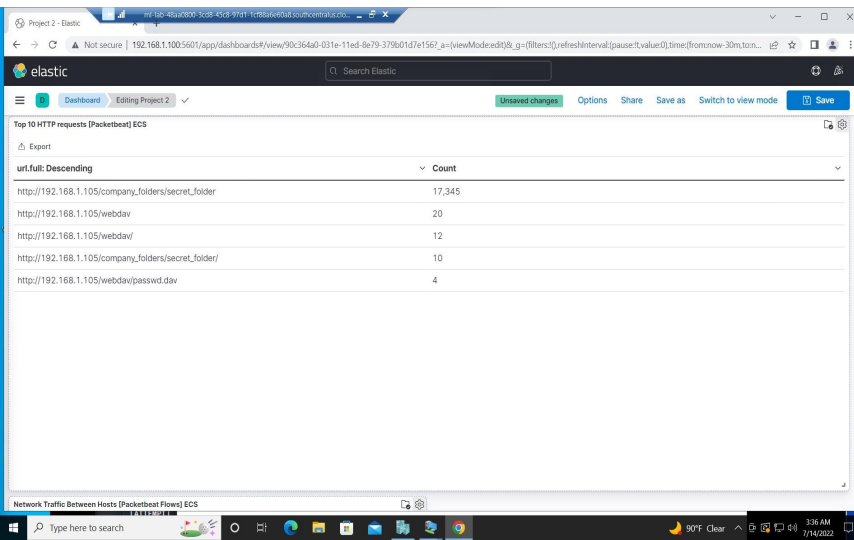
Analysis: Finding the Request for the Hidden Directory

- The Request occurred at 3:22 am
- There were a total of 16,625 requests
- File requested were
 - http://192.168.1.105/company_folders/secret_folder
 - <http://192.168.1.105/webdav>
 - <http://192.168.1.105/webdav/passwd.dav>



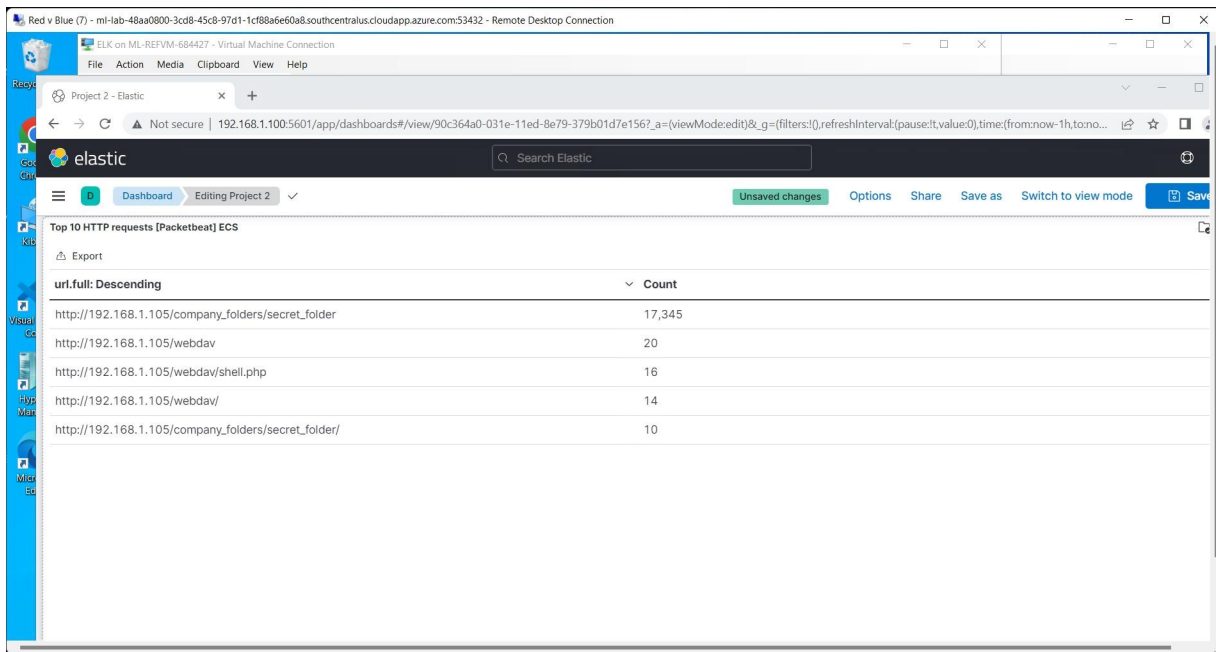
Analysis: Uncovering the Brute Force Attack

- There were 17,345 requests in the attack
- 17,335 requests were made before the attack discovered the password. There were only 10 successful times the attacker was able to log into the folder.



Analysis: Finding the WebDAV Connection

- There were 20 requests made to the WebDav directory
- The only file requested from that directory was the shell.php file. It was requested 16 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?

- Alarm is triggered after a large volume of requests in a short time frame from a single IP address

What threshold would you set to activate this alarm?

- Threshold is set for 500 requests in 10 minutes

System Hardening

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

- Close port 22 to outside traffic

Mitigation: Finding the Request for the Hidden Directory

Alarm

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

- Allow access to only authorized IP addresses.

What threshold would you set to activate this alarm?

- If a request comes from an unauthorized IP address the alarm is triggered

System Hardening

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

- Generate a list of acceptable IP addresses that can access the hidden directory
- Multi Factor Authentication and regular password updates to prevent the compromise of credentials from Brute Force Attacks.

Mitigation: Preventing Brute Force Attacks

Alarm

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

- High volume of requests from a single IP address in a short time frame

What threshold would you set to activate this alarm?

- 200 requests in 5 minutes

System Hardening

What configuration can be set on the host to block brute force attacks?

- Multi Factor Authentication
 - Regular Password Updates
-

Mitigation: Detecting the WebDAV Connection

Alarm

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

- All WebDav access is limited to specific IP addresses

What threshold would you set to activate this alarm?

- Alert is activated anytime a file is altered, deleted, copied, or moved to ensure it was done by authorized IP address

System Hardening

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

- Create a list of authorized users that can access WebDav
- List of acceptable IP address that can be used to access WebDav

Mitigation: Identifying Reverse Shell Uploads

Alarm

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

- Alarm is created to alert of the uploading of web shells

What threshold would you set to activate this alarm?

- Anytime a web shell is uploaded the alarm is triggered

System Hardening

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

- Limit outbound traffic from WebDav to only known IP addresses
- Use web application permissions to limit access WebDav

*The
End*