Capstone Engagement

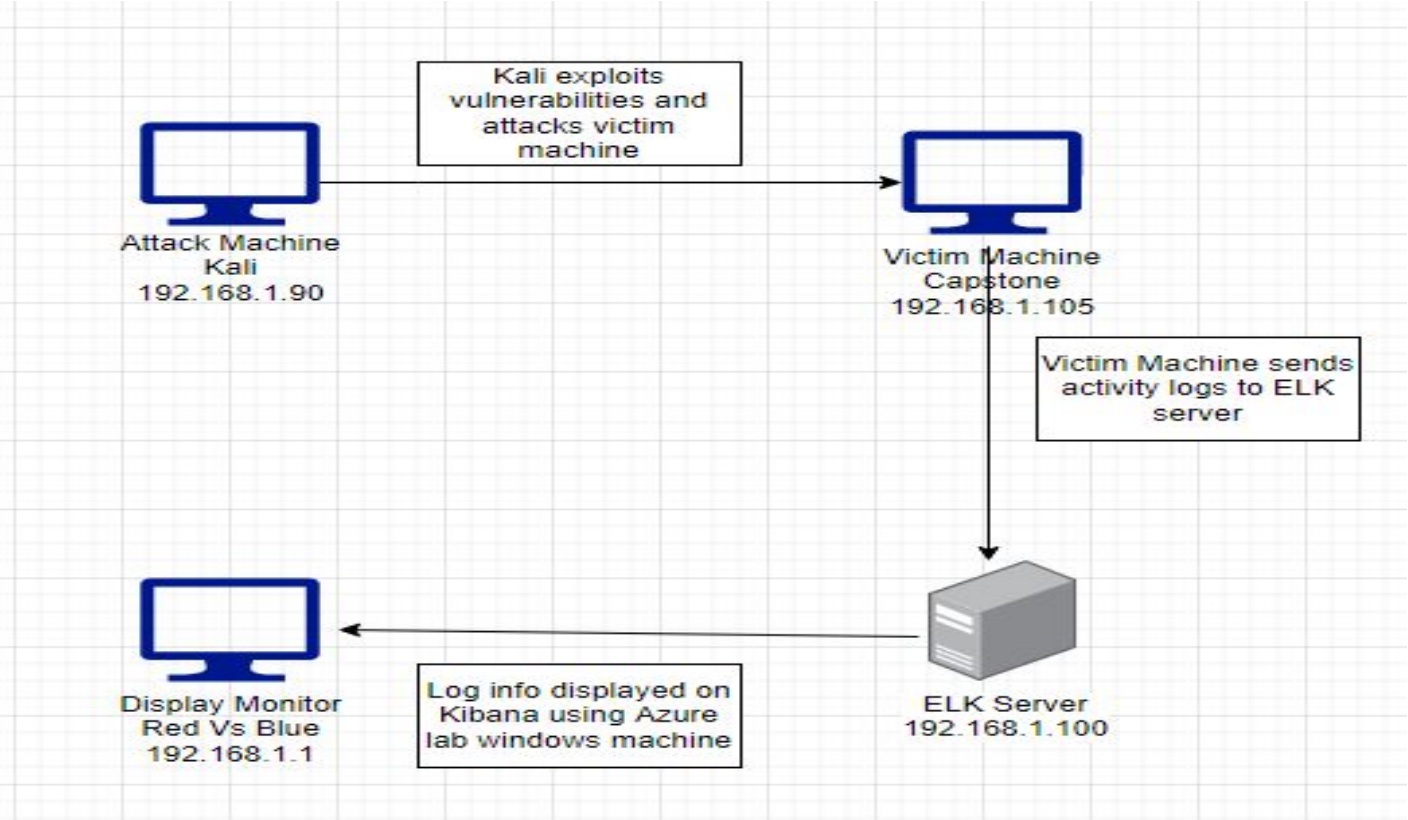
Assessment, Analysis, and Hardening of a Vulnerable System

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: 192.168.1.1

Machines
IPv4: 192.168.1.1
OS: Windows
Hostname: Hyper-V Manager

IPv4: 192.168.1.90
OS: Kali Linux
Hostname: Linux

IPv4: 192.168.1.105
OS: Linux
Hostname: Capstone

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
Kali	192.168.1.8	The attacking machine used against Capstone
Capstone	192.168.1.105	Target machine using the apache web server
Elk	192.1.100	Logs the info of attack from capstone machine
Hyper-V Manager	192.168.1.1	Software that virtualizes hardware into Virtual machines/ Virtual Servers

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Open port 80	*An open HTTP port is a vulnerability that allows attackers to access private information such as credentials which may allow them to do further damage.*	*This allowed the red team to find the hidden directories and making the files in those directories accessible.*
CWE-307: Improper Restriction of Excessive Authentication Attempts	The software did not restrict login attempts within a short time frame making it vulnerable to brute force attacks	This enabled the red team access to Ashton's password using Hydra.
Hashed Password	A hashed password can be cracked through different tools such as CrackStation	This enabled the red team to use Crackstation to identify the password for ryans account

Exploitation: Open port 80

01

Tools & Processes

Red Team used nmap to scan for any open ports and services in the network

02

Achievements

We found that the capstone IP 192.168.1.105 had an open port 22 and 40

03

```
root@Kali:~# nmap 192.168.1.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2022-07-25 16:26 PDT
Nmap scan report for 192.168.1.1
Host is up (0.00061s latency).
Not shown: 995 filtered ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
2179/tcp open  vmrdp
3389/tcp open  ms-wbt-server
MAC Address: 00:15:5D:00:04:0D (Microsoft)

Nmap scan report for 192.168.1.100
Host is up (0.00055s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
9200/tcp open  wap-wsp
MAC Address: 4C:EB:42:D2:D5:D7 (Intel Corporate)

Nmap scan report for 192.168.1.105
Host is up (0.00078s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
```

Exploitation: CWE-307

01

Tools & Processes

The Hydra software was able to run a brute force attack on the crediants for the secret_folder directory

Command: 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 allowed me to attain ashtons password which was leopoldo and allowed me access to the secret_folder directory

03

Exploitation: Hashed Password

01

Tools & Processes

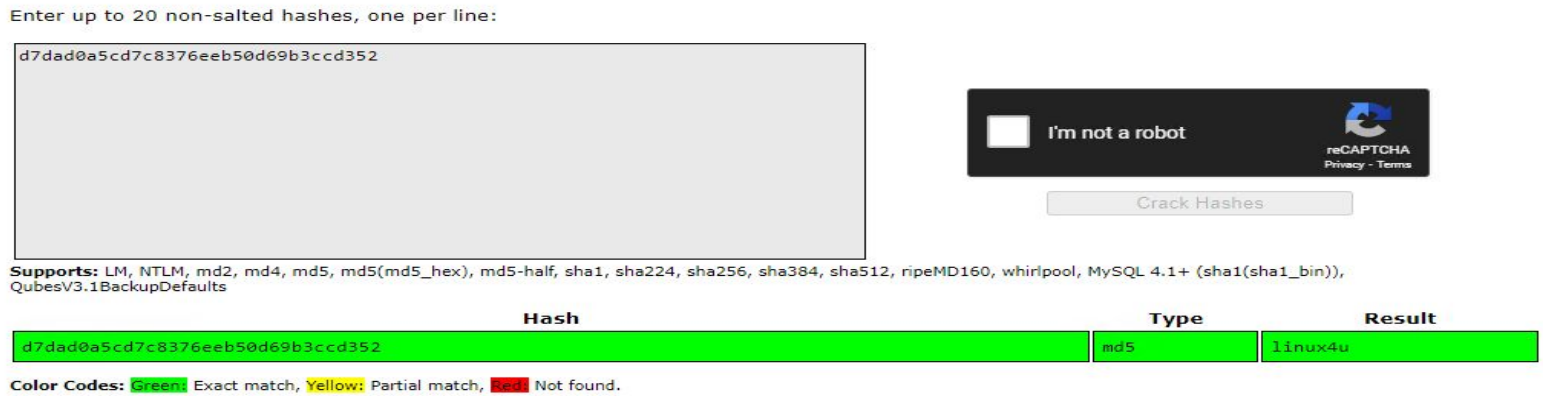
Using CrackStations i was able to find the plaintext of the hashed password for Ryan

02

Achievements

This password allowed me access to the system through the WebDav connection enabling me to upload a shell script to attack

03

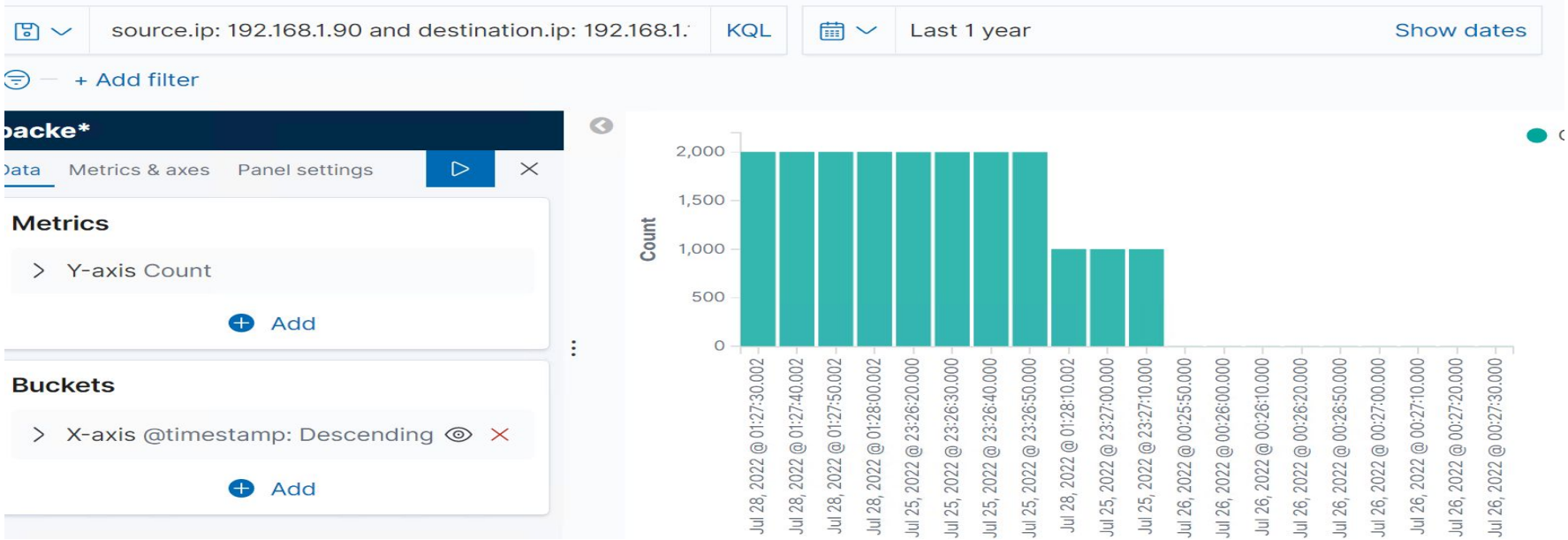


Blue Team
Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

Answer the following questions in bullet points under the screenshot if space allows. Otherwise, add the answers to speaker notes.

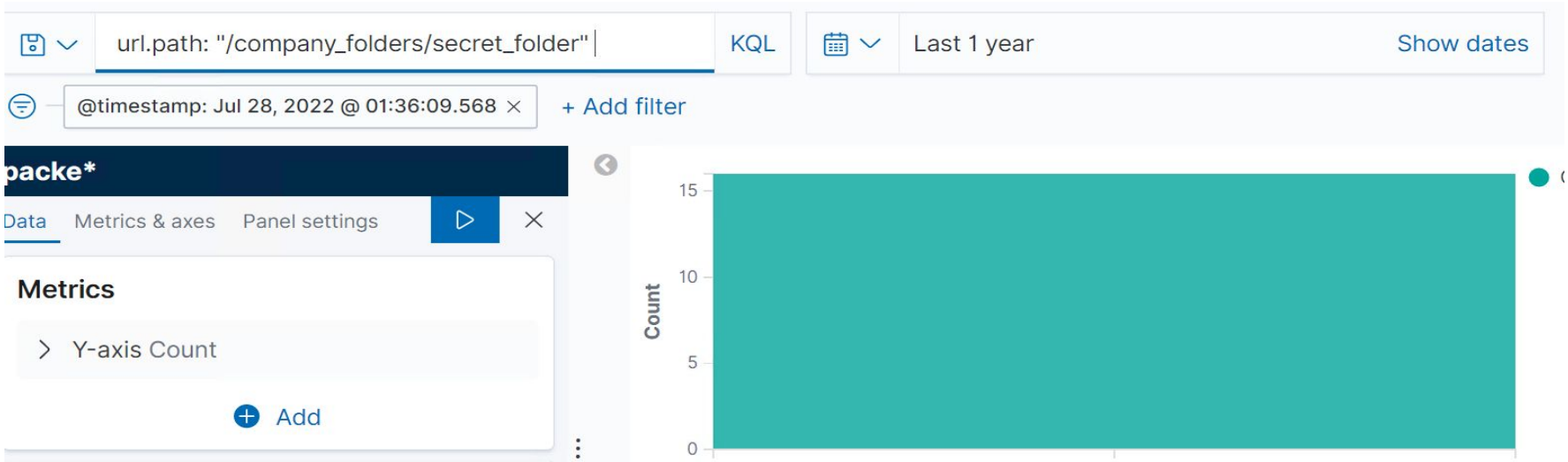
- The port scan occurred on July 28 at 1:27 AM
- 2,002 packets were sent from 192.168.1.90
- A few thousand requests all for different ports



Analysis: Finding the Request for the Hidden Directory

Answer the following questions in bullet points under the screenshot if space allows. Otherwise, add the answers to speaker notes.

- The request occurred at 1:36 AM and 15,567 hits
- company_folders/secret_folder was requested which contained the credentials for ashton



Analysis: Uncovering the Brute Force Attack

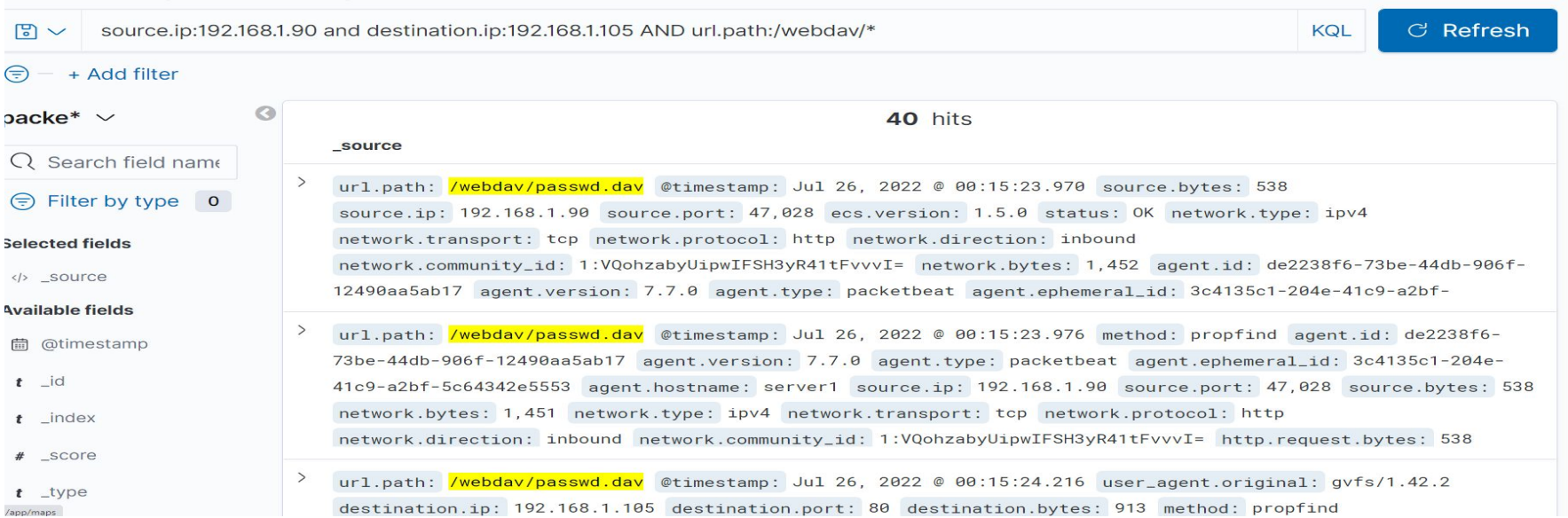
Answer the following questions in bullet points under the screenshot if space allows. Otherwise, add the answers to speaker notes.

- 15,577 hits were made during the attack
- Out of all the 15,577 requests only one was successful

Analysis: Finding the WebDAV Connection

Answer the following questions in bullet points under the screenshot if space allows. Otherwise, add the answers to speaker notes.

- 40 requests were made for this directory
- The passwd.dav and shell.php were requested



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? An alarm can be set to notify the admin everytime HTTP requests reach a certain threshold

What threshold would you set to activate this alarm? Over 1000 mark

System Hardening

What configurations can be set on the host to mitigate port scans?
Constant monitoring via private port scans is a good means of mitigation.

Describe the solution. If possible, provide required command lines.
Filtering traffic from an IP triggered by the IPS can effectively mitigate port scans

Mitigation: Finding the Request for the Hidden Directory

Alarm

What kind of alarm can be set to detect future unauthorized access?
Restricting access to an account once reaching a certain amount of failed authentications.

What threshold would you set to activate this alarm? Around 5-7 failed authentications should be enough to alert the admin

System Hardening

What configuration can be set on the host to block unwanted access?
This directory should not be allowed to exist on the server. Should only be allowed access through a private VPN through the company.

Describe the solution. If possible, provide required command lines.
Rmdir -r can be used to remove all files and the directory itself from the server

Mitigation: Preventing Brute Force Attacks

Alarm

What kind of alarm can be set to detect future brute force attacks?
An alarm can be created if a 401 error is returned to the server over a certain threshold

What threshold would you set to activate this alarm?
Around 5-7 over 45 minutes, this is with human error such as typos.

System Hardening

What configuration can be set on the host to block brute force attacks?
Limiting failed login attempts and limit login attempts to only specified certified IP addresses

Describe the solution. If possible, provide the required command line(s).
Configure account policies on the server to limit failed login attempts

Mitigation: Detecting the WebDAV Connection

Alarm

What kind of alarm can be set to detect future access to this directory?
Set an alert for blacklisted IP's attempting to access the directory
Any IP outside the server range should be blacklisted

What threshold would you set to activate this alarm?
Any attempt to access should trigger the alarm

System Hardening

What configuration can be set on the host to control access?
This shared folder should not be accessible from the web and restricted by a firewall rule.

Describe the solution. If possible, provide the required command line(s).
Blocking ports 80 and 443 and blacklisting external IP's

Mitigation: Identifying Reverse Shell Uploads

Alarm

What kind of alarm can be set to detect future file uploads?
Set an alert for any .php file that is uploaded
Set firewall to block traffic to the shared folder on ports 80, 443 and 4444

What threshold would you set to activate this alarm?
Any traffics on these ports from an external IP should trigger an alarm

System Hardening

What configuration can be set on the host to block file uploads?
All file uploads should be done locally and remove the ability to upload files from all over the web

Describe the solution. If possible, provide the required command line.
Block ports 80,443 and 4444


The End