Capstone Engagement

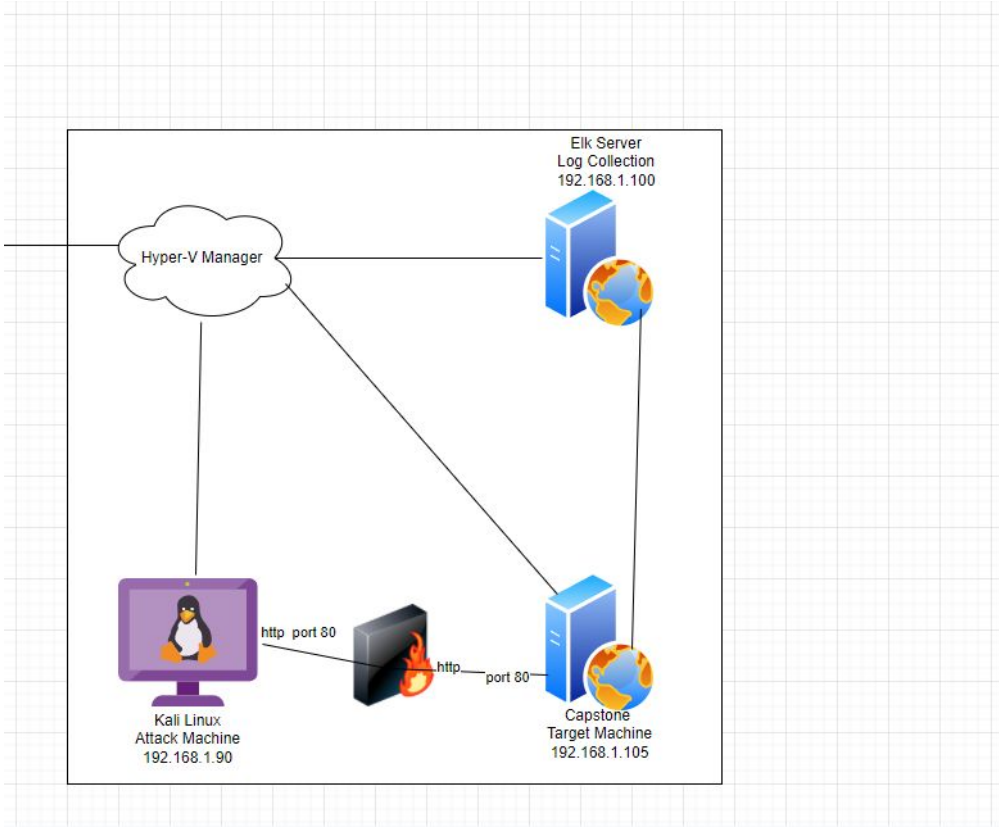
Assessment, Analysis, and Hardening of a Vulnerable System

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: 192.168.1.90
OS: Linux 2.6.32
Hostname: kali

IPv4: 192.168.1.105
OS: Linux
Hostname: Capstone

IPv4: 192.168.0.100
OS: Linux
Hostname: ELK

IPv4: 192.168.1.1
OS: Windows
Hostname: Red vs Blue - ML-REFVM

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	Server
ELK	192.168.1.100	SIEM System (traffic monitoring)
RED VS BLUE ML-REFVM	192.168.1.1	NATSWITCH (HYPER V)
Kali Linuxx	192.168.1.90	Attacking System (Penetration Testing)

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Use the CVE number if it exists. Otherwise, use the common name.	*Describe the vulnerability.*	*Describe what this vulnerability allows the attacker to do.*
Directory Listening Available on Apache Web Server	Malicious users can use the browser to read full contents of directories on Capstone Apache web server	Sensitive information let's attackers know user "Ashton" has administrative privileges for the directory: /company_folders/secret_folder/
No Failed Password Lockouts/ Weak Passwords	Weak passwords were found and there was no rule in place to limit false login attempts (resulting in a brute force attack).	Brute force attack gave access to /secret_folder/Password hash for Ryan via Webdav (dav://192.168.1.105/webdav/)
Persistent Reverse Shell Backdoor	Reverse shell payload exploit on web server is possible because the ids/firewall allows outbound ports	This exploit gives the attacker backdoor access to the Capstone Server

Exploitation: Directory Listing Enabled on Apache

01

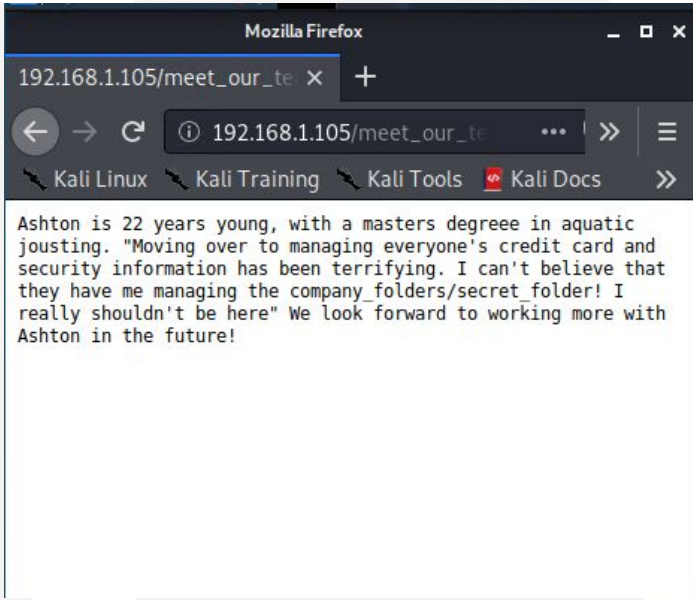
Tools & Processes
Navigated to 192.168.1.105/ on Kali web browser, perused some files, and quickly found damaging information in Ashton's profile

02

Achievements
Created a file containing all directories and file locations

Found Ashton is the administrator of /company_folders/secret_folder/

03



Exploitation: Easily Cracked Passwords and No PW Lockouts

01

Tools & Processes

At this point the attacker can use Hydra to execute a brute force dictionary attack to gain the password to Ashton's Account

02

Achievements

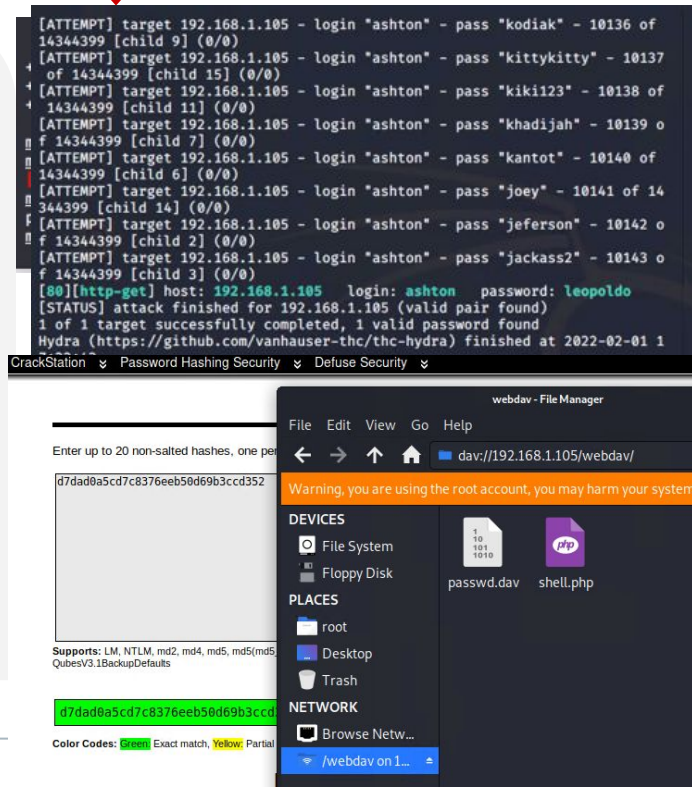
Password for Ashton was found in 'rockyou' dictionary.

Access to /secret_folder/ was achieved.

Access info for /webdav/ was secured.

Ryan's hash was able to be decrypted into a password allowinig webdav access

03



Exploitation: Persistent Reverse Shell Backdoor

01

Tools & Processes

Created and uploaded a php payload using msfvenom: php/meterpreter/reverse_tcp

This established a remote listener.

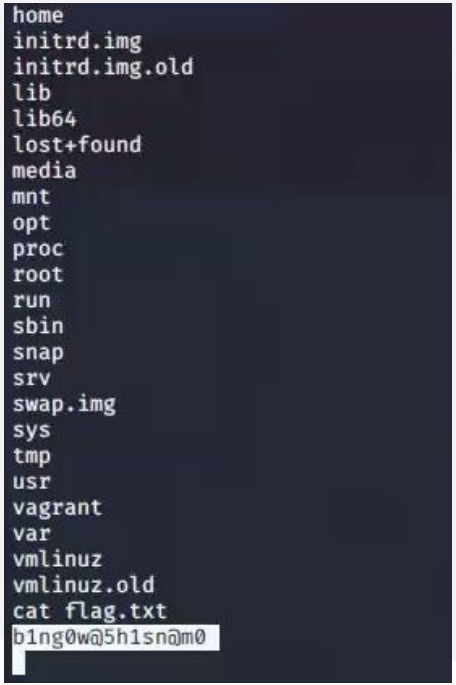
A reverse shell backdoor was placed in the Capstone apache server.

02

Achievements

Once the backdoor was opened a number of secure folders were compromised and the root directory of the Capstone machine was vulnerable to the attacker

03



Blue Team
Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan

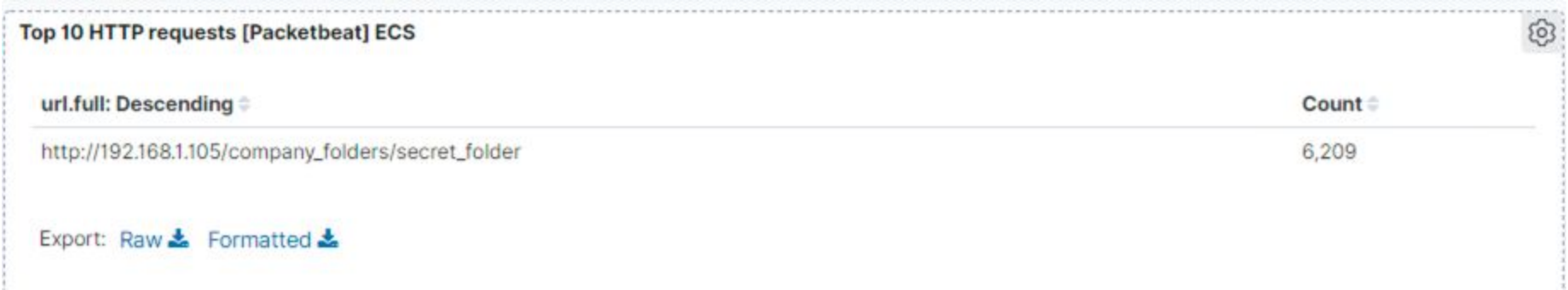
Answer the following questions in bullet points under the screenshot if space allows. Otherwise, add the answers to speaker notes.

- What time did the port scan occur?
- How many packets were sent, and from which IP?
- What indicates that this was a port scan?

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.

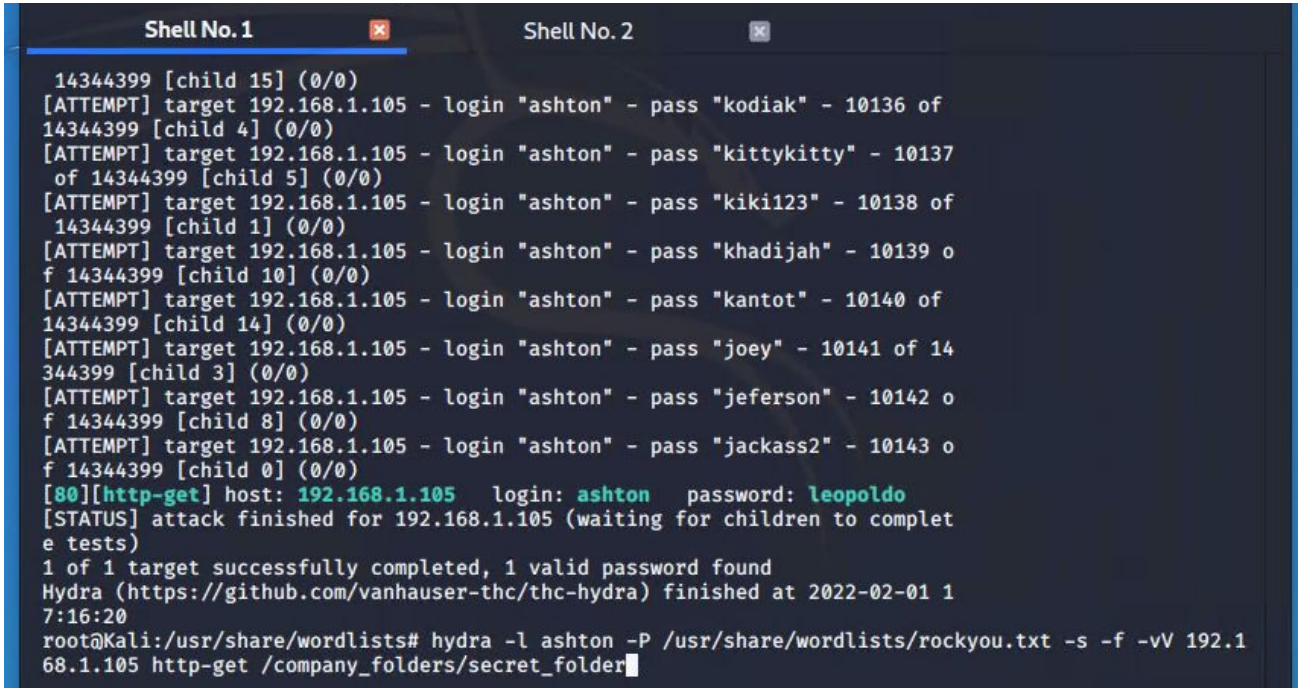
- What time did the request occur? How many requests were made?
- Which files were requested? What did they contain?



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.

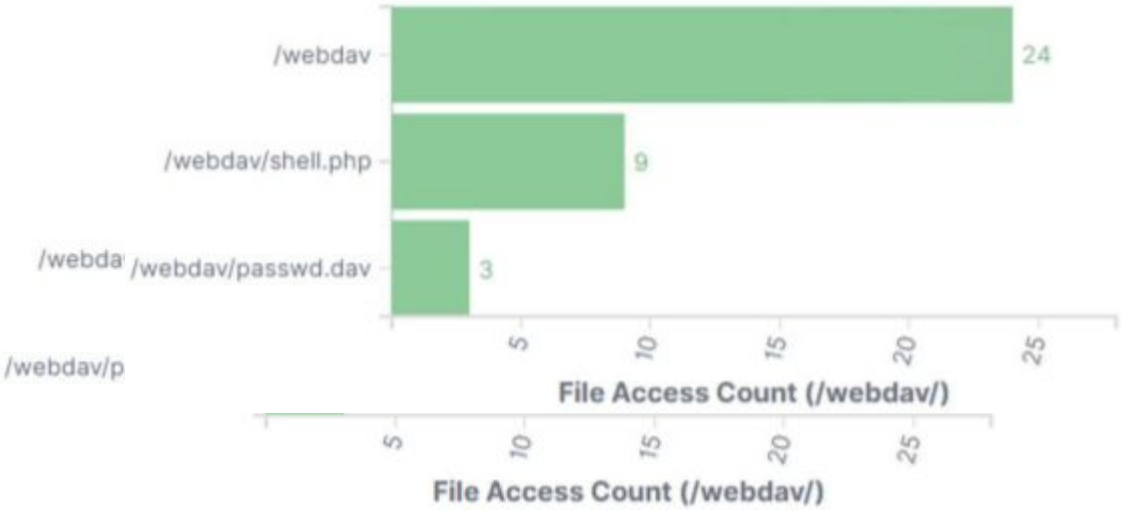
- How many requests were made in the attack? **6,314**
- How many requests had been made before the attacker discovered the password? **6,693**



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? **36 requests**
- Which files were requested? **Passwd.dav and 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?
Destination.ip: 192.168.1.105 and source.ip (not 192.168.1.105) and destination.port (not 443 or 80)
Report: # of Ports accessed per source IP per second

What threshold would you set to activate this alarm? Alert email and log when over three (non 443 or 80) port scans are detected at the same time

System Hardening

What configurations can be set on the host to mitigate port scans?
Block IP addresses, deploy port scans

Describe the solution. If possible, provide required command lines.

A firewall is necessary to block all incoming and outgoing ports except for 80 and 443 (which are necessary for the function of the site)

Mitigation: Finding the Request for the Hidden Directory

Alarm

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

source.ip: (not 192.168.1.105 or 192.168.1.1) and url.path : *secret_folder*

Report: # of times secret_folder is accessed from external IP

What threshold would you set to activate this alarm?
Alert email immediately when any IP outside the network logs into the folder

System Hardening

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

Httpd.conf file can be edited to only allow traffic from certain IPs and to deny others

Describe the solution. If possible, provide required command lines. **Hidden Indexes are not a secure idea and should be kept offline or not at all.**

Mitigation: Preventing Brute Force Attacks

Alarm

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

http.request.method : "get" and user_agent.original :"Mozilla/4.0 (Hydra)" and url.path :"/company_folders/secret_folder/" and status :(Error or OK)

What threshold would you set to activate this alarm?

Alrt email and log when over five 401 errors occur or when any 200 responses occur from outside IPs

System Hardening

What configuration can be set on the host to block brute force attacks? Multilayered login can be implemented as simply as using captcha.

Describe the solution. If possible, provide the required command line(s). Catcha. 2FA. Rotating password policy. Complex Password Policy

Mitigation: Detecting the WebDAV Connection

Alarm

What kind of alarm can be set to detect future access to this directory?
http.request.method : * and url.path: *webdav* and source.ip: (not 192.168.1.150 or 192.168.1.1)

Detects: **# of times webdav directory is accessed by outside IPs**

What threshold would you set to activate this alarm?
Alert email and log when any request is made

System Hardening

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

httpd.conf

Describe the solution. If possible, provide the required command line(s).

Allow only access from 192.168.1.1 and 192.168.1.105

Mitigation: Identifying Reverse Shell Uploads

Alarm

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

Count “puts” from unknown IPs

What threshold would you set to activate this alarm?

-When a file is uploaded an email should be sent to the SOC team
-File types like php can set off extra flags if necessary

System Hardening

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

-Don’t allow any IPs to (GET POST HEAD)

Describe the solution. If possible, provide the required command line.

- Require specific file types for upload. Require authentication from uploaders.


The End