

Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

Tyler Gill

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

[Insert Here]

Use draw.io to create a diagram of the network.

Add your diagram to this slide and fill out the data in the sidebar.

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: 192.168.0.100
OS: Linux
Hostname: Elk

IPv4: 192.168.1.1
OS: Windows
Hostname: Hyper-V

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
Hyper V	192.168.11	Virtual gateway and VM manager
kali	192.168.1.90	Attacking machine
Elk	192.168.0.100	Monitors and logs activity on target Capstone machine
Capstone	192.168.1.105	Target machine

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Open Ports	Open and unfiltered ports were detected via an nmap scan.	These open ports could potentially allow an attacker to access the target machine through a variety of means.
Brute Force Vulnerability	There is no mechanism for protecting against dictionary and other brute force attacks.	Any login credentials stored on the target machine are vulnerable to attackers.
Data Exposure	Sensitive files are not properly indexed and are easily accessible to any intruder on the system.	An attacker can obtain free access to the system's directory structure and easily find any sensitive data.
Unrestricted File Upload	There were no measures in place to prevent the injection of arbitrary code onto the system.	This allows an attacker to upload a variety of malicious code onto the target machine.

Exploitation: Open Ports

01

Tools & Processes

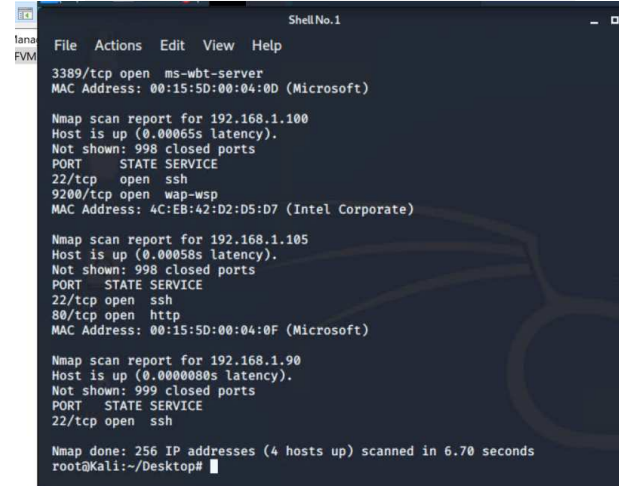
From the kali machine, I ran the nmap scan command on the target IP address.

02

Achievements

The nmap scan found that port 80 on the machine located at IP address 192.168.1.105 was open and vulnerable. This allowed me to access the machine's file directory via a web browser and ultimately access sensitive data on the machine.

03



```
ShellNo.1
File Actions Edit View Help

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 (0.00065s 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 (0.00058s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
MAC Address: 00:15:5D:00:04:0F (Microsoft)

Nmap scan report for 192.168.1.90
Host is up (0.000080s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh

Nmap done: 256 IP addresses (4 hosts up) scanned in 6.70 seconds
root@Kali:~/Desktop#
```


Exploitation: Brute Force Vulnerability

01

Tools & Processes

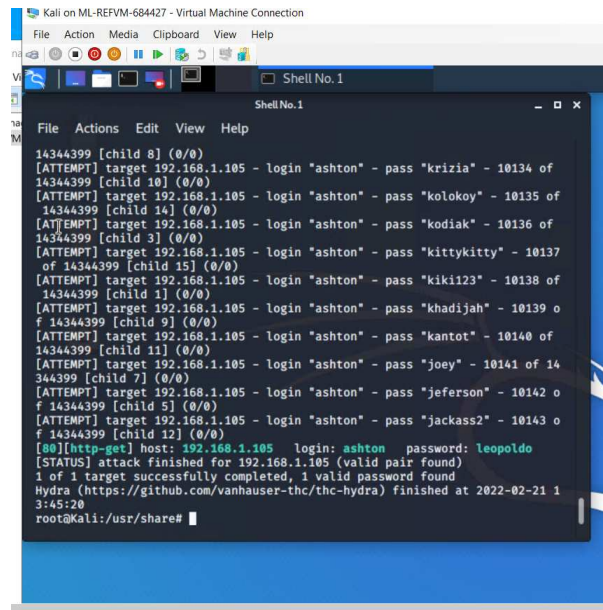
After finding the name of user "Ashton" as a likely login name. I ran the Hydra script with the rockyou.txt.gz wordlist in an attempt to brute force the user's password.

02

Achievements

Hydra was able to crack the user's password and allowed me access to secret file folder located on the target machine.

03



The screenshot shows a terminal window titled "Kali on ML-REFVM-684427 - Virtual Machine Connection". Inside the terminal, a Hydra brute force attack is shown in progress. The output displays multiple failed login attempts for the user "ashton" with various passwords like "krizia", "kolokoy", "kodiak", "kittykitty", "kiki123", "khadijah", "kantot", "joey", "jeferson", and "jackass2". Finally, a successful login is achieved with the password "leopoldo". The terminal output includes the following text:

```
14344399 [child 8] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "krizia" - 10134 of
14344399 [child 10] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kolokoy" - 10135 of
14344399 [child 14] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kodiak" - 10136 of
14344399 [child 3] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kittykitty" - 10137 of
14344399 [child 15] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kiki123" - 10138 of
14344399 [child 1] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "khadijah" - 10139 of
14344399 [child 9] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "kantot" - 10140 of
14344399 [child 11] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "joey" - 10141 of 14
344399 [child 7] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jeferson" - 10142 of
14344399 [child 5] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10143 of
14344399 [child 12] (0/0)
[80][http-get] host: 192.168.1.105 login: ashton password: leopoldo
[STATUS] attack finished for 192.168.1.105 (valid pair found)
1 of 1 target successfully completed. 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-02-21 1
3:45:20
root@Kali: /usr/share#
```

Exploitation: Data Exposure

01

Tools & Processes

Sensitive files and folder were improperly indexed and exposed to any trespasser. I was able to explore the file system and find my way to sensitive folders using only a web browser.

02

Achievements

I was able to find my way to the "secret folder" directory and was then able to discover the names of various users and clues as to what level of access said users might have.

03



The screenshot shows a web browser window with the address bar displaying "Not secure | 192.168.1.105/company_folders/". The main content area is titled "Index of /company_folders/" and contains a table with the following columns: "Name", "Last modified", "Size", and "Description". The table lists the following items:

Name	Last modified	Size	Description
Parent Directory	-	-	-
company_culture/	2019-05-07 18:25	-	-
customer_info/	2019-05-07 18:26	-	-
sales_docs/	2019-05-07 18:27	-	-
secret_folder/	2019-05-07 19:25	-	-

Below the table, the text "Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80" is visible.

Exploitation: Unrestricted File Upload

01

Tools & Processes

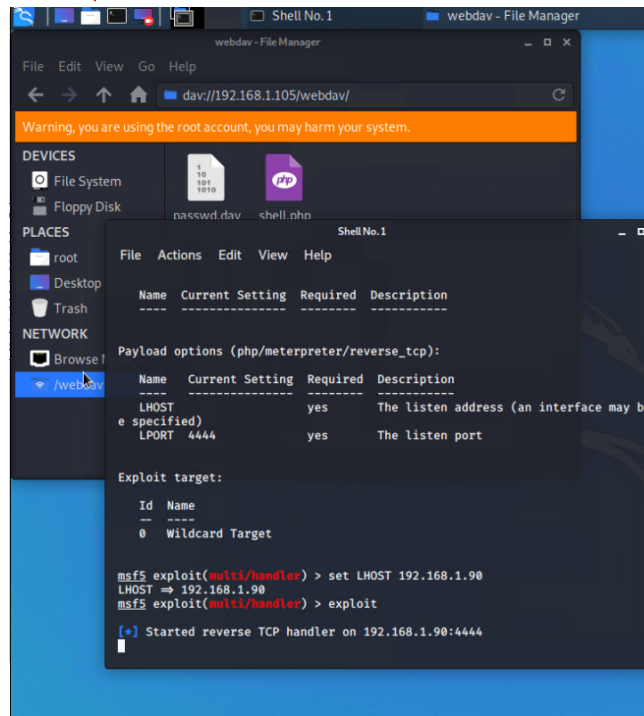
By using Metasploit and msvenom, I was able to upload a reverse shell to the target machine using the credentials I had uncovered previously.


02

Achievements

The reverse shell was used as a backdoor that allowed for full access to the target system. From there, it was a simple matter to find and capture the target flag using basic linux search commands.

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?

[Insert Here]

Include a screenshot of Kibana logs depicting the 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?

[Insert Here]

Include a screenshot of Kibana logs depicting the request for the hidden directory.

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

[Insert Here]

Include a screenshot of Kibana logs depicting the brute force attack.

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?
- Which files were requested?

[Insert Here]

Add a screenshot of Kibana logs depicting the WebDAV connection.



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?

What threshold would you set to activate this alarm?

System Hardening

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

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

Mitigation: Finding the Request for the Hidden Directory

Alarm

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

What threshold would you set to activate this alarm?

System Hardening

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

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

Mitigation: Preventing Brute Force Attacks

Alarm

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

What threshold would you set to activate this alarm?

System Hardening

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

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

Mitigation: Detecting the WebDAV Connection

Alarm

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

What threshold would you set to activate this alarm?

System Hardening

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

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

Mitigation: Identifying Reverse Shell Uploads

Alarm

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

What threshold would you set to activate this alarm?

System Hardening

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

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

*The
End*