

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

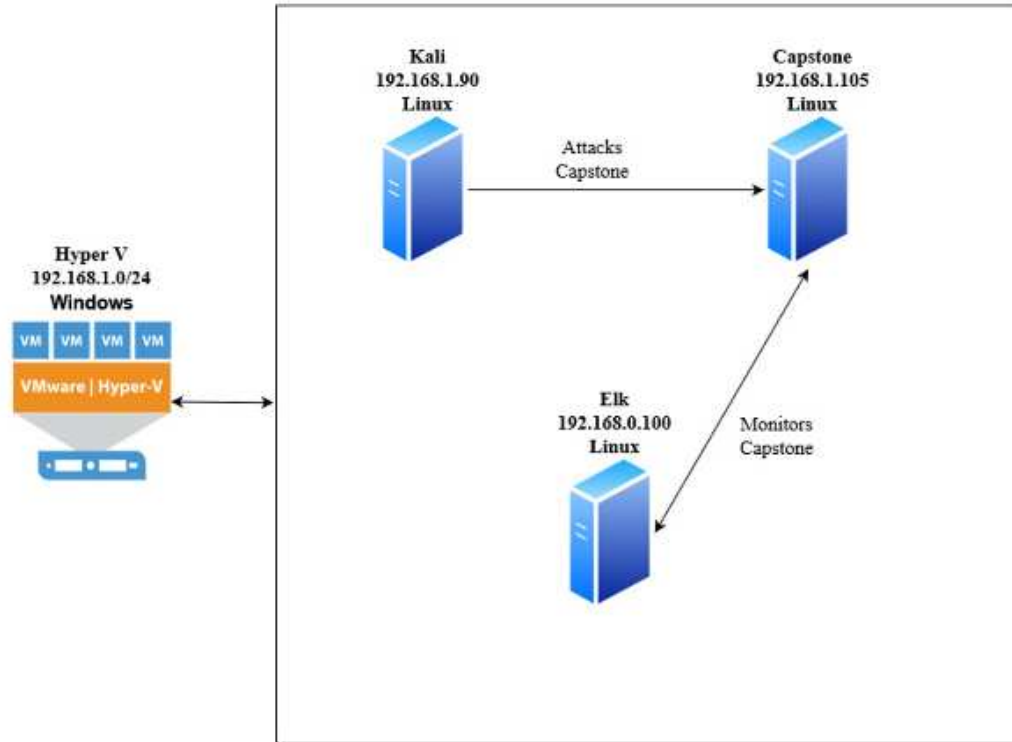
Blue Team: Log Analysis and Attack Characterization

04

Hardening: Proposed Alarms and Mitigation Strategies

Network Topology

Network Topology



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

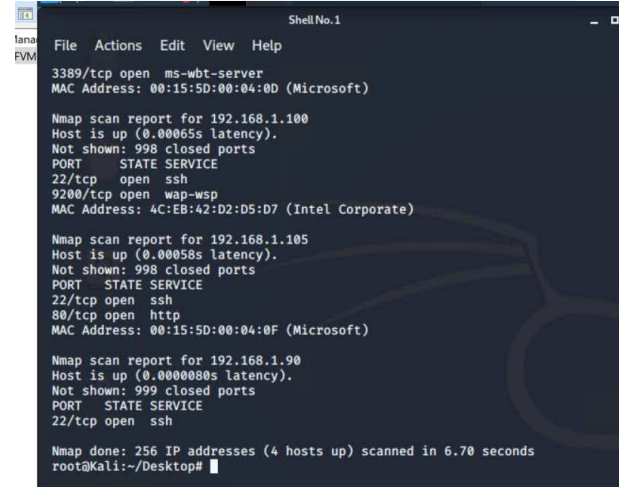
From the kali machine, I ran the nmap scan command on the target IP address.

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



```
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

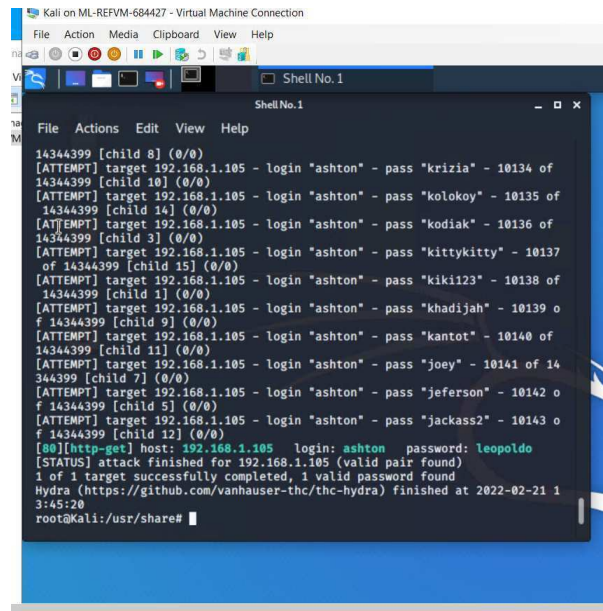
After finding the name of user "Ashton" as a likely login name. I ran the Hydra script with the rockyou.txt.gz wordlist in an attempt to brute force the user's password.

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. The final successful attempt shows the password "leopoldo" for the user "ashton". The terminal also shows the status of the attack and the time it took to complete.

```
File Actions Edit View Help
Shell No.1
File Actions Edit View Help
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 o
f 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 o
f 14344399 [child 5] (0/0)
[ATTEMPT] target 192.168.1.105 - login "ashton" - pass "jackass2" - 10143 o
f 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 page title is "Index of /company_folders/". Below the title is a table with 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	-	-

At the bottom of the page, it says "Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80".

Exploitation: Unrestricted File Upload

01

Tools & Processes

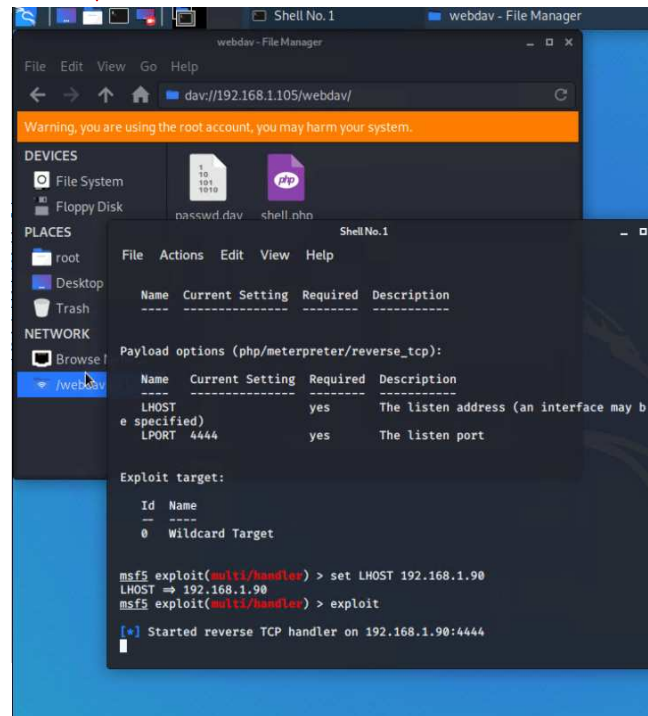
By using Metasploit and msvenom, I was able to upload a reverse shell to the target machine using the credentials I had uncovered previously.


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





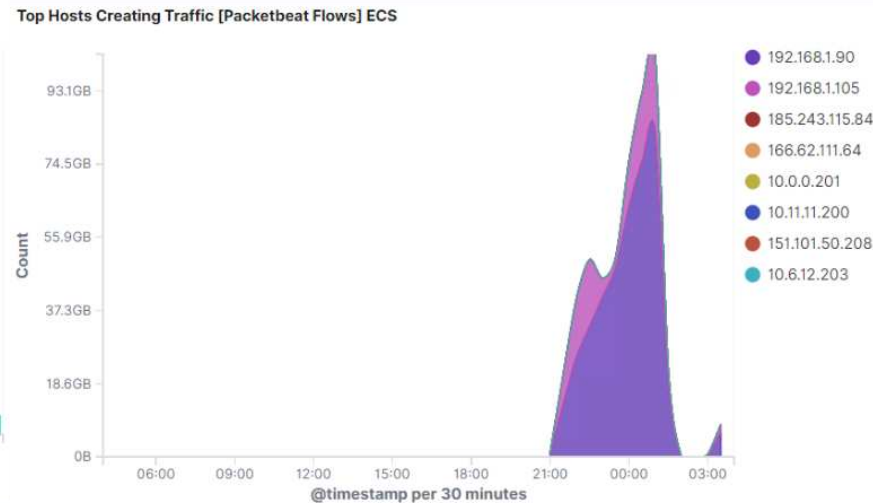
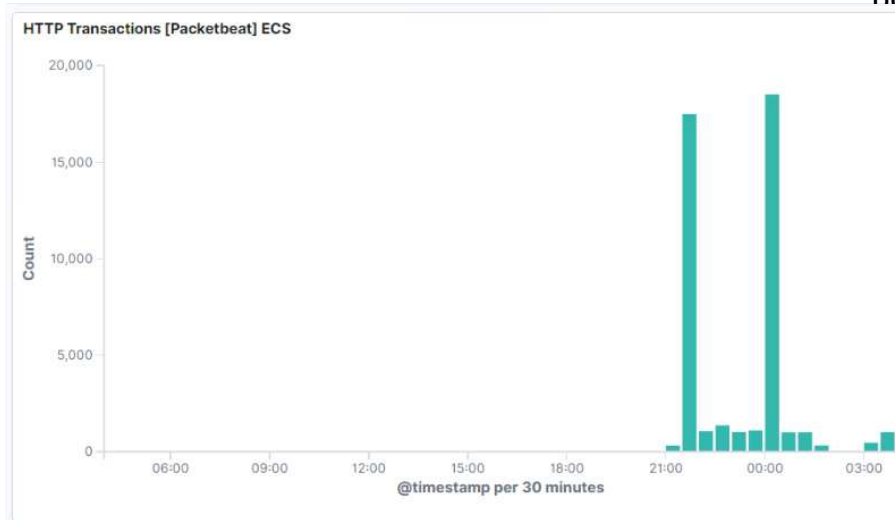
Blue Team

Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan



- The port scan began around 2130.
- 7,289 packets were sent from 192.168.1.90.
- A sudden burst of packets from the same source via the same port is strongly suggestive of a port scan



Analysis: Finding the Request for the Hidden Directory

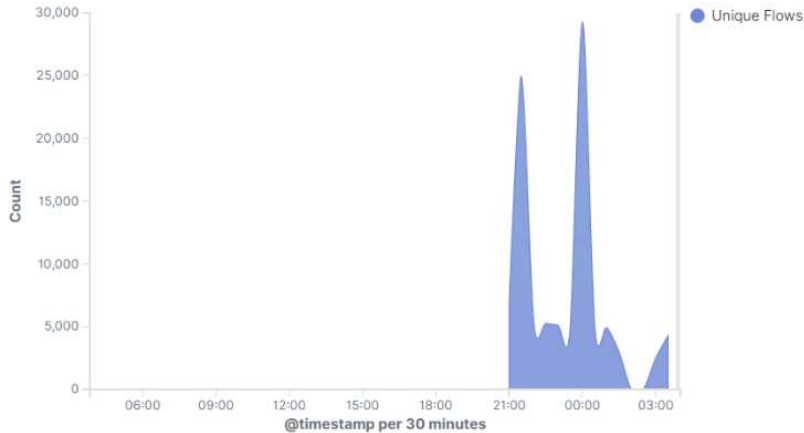


- 16,326 requests occurred at around 2145.
- The connect_to_corp_server file was accessed containing instructions on accessing webdav.

HTTP Transactions [Packetbeat] ECS



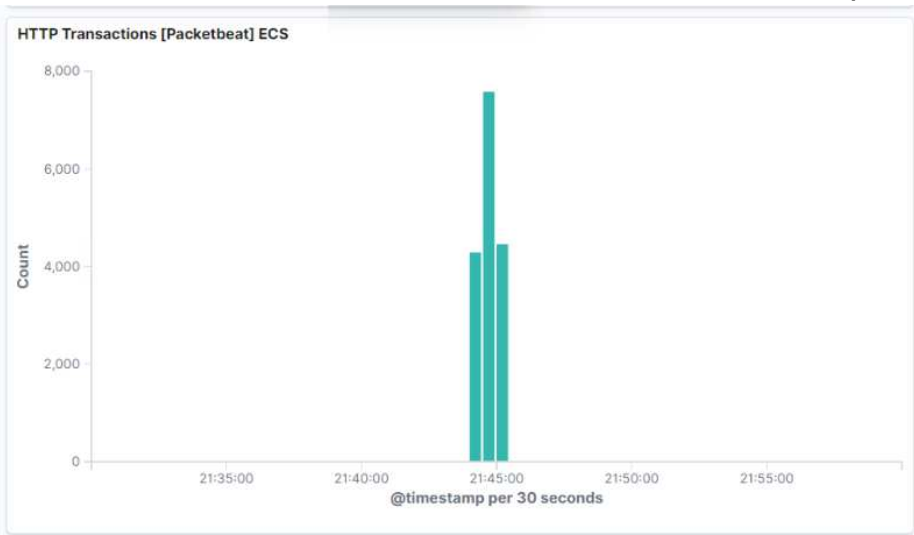
Connections over time [Packetbeat Flows] ECS



Analysis: Uncovering the Brute Force Attack



- 16,326 requests occurred in a very short space of time.
- Requests dropped off substantially once the attacker presumably obtained the password.



Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	16,327

Export: [Raw](#) [Formatted](#)

Analysis: Finding the WebDAV Connection



- 130 requests were made to the webdav directory.
- A PUT record was found indicating when the shell.php file was placed into the compromised directory.

Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder	31,948
http://127.0.0.1/server-status?auto=	1,766
http://snnmnkxdhflwgthqismb.com/post.php	279
http://www.gstatic.com/generate_204	146
http://192.168.1.105/webdav	130

```
t query PUT /webdav/shell.php
# server.bytes 533B
# server.ip 192.168.1.105
# server.port 80
# source.bytes 1.3KB
# source.ip 192.168.1.90
# source.port 38068
t status OK
```




Blue Team

Proposed Alarms and Mitigation Strategies

Mitigation: Blocking the Port Scan

Alarm

Port scanning can be easily mitigated by blocking traffic from a particular source after a certain threshold has been met. To that end, an alarm should be triggered if more than 2000 requests are detected from a particular source within a relatively short timeframe.

System Hardening

A properly configured firewall can easily protect against potentially malicious port scanning by dropping filtered requests and not sending any reply to ping attempts.

Mitigation: Finding the Request for the Hidden Directory

Alarm

A huge number of unfulfilled GET requests were sent to the `secret_folder` directory before it was successfully accessed by the intruder. An alarm should be triggered should more than a small number (5 or so) of failed requests be detected to this directory.

System Hardening

The hidden directory could be better protected through a wide variety of means. The sensitive data should be encrypted, or even moved to another machine that isn't globally accessible via the internet. Multi-factor authentication and the use of internal software firewalls would also help to protect this sensitive directory.

Mitigation: Preventing Brute Force Attacks

Alarm

Since this kind of brute force attack necessarily involves huge numbers of failed login attempts, thwarting them simply requires us set up an alarm that will trigger if more than 3 failed login requests or 401 errors occur involving the same account or IP address within a set span of time. I would begin by locking the account and/or blocking the source IP after 3 failed login attempts within the span of 1 hour, and adjust from there as needed.

System Hardening

Brute force dictionary attacks can be resisted in a number of ways. Stronger passwords and two factor authentication is always a good idea to increase system security. Limiting the number of failed login attempts before a user account is locked is also a widely used measure to prevent such attacks.

Mitigation: Detecting the WebDAV Connection

Alarm

The easiest and most straightforward way to protect against unauthorized WebDAV access would be to create a whitelist of authorized IPs and set an alarm to trigger any time an unauthorized IP attempts to access the WebDAV.

System Hardening

A firewall should be put in place to block any non-whitelisted IP addresses. Stronger password policies and multifactor authentication should also be considered. In addition, a more secure alternative to WebDAV should be considered as WebDAV is inherently quite insecure.

Mitigation: Identifying Reverse Shell Uploads

Alarm

Alarms should be set to trigger if any traffic is detected along port 4444 or if there is any attempt to upload arbitrary or executable code to the system.

System Hardening

Attempted file uploads should require their own separate authorization, and the uploading of certain file extensions should be blocked using multiple layers of firewall filters.

*The
End*