Capstone Engagement

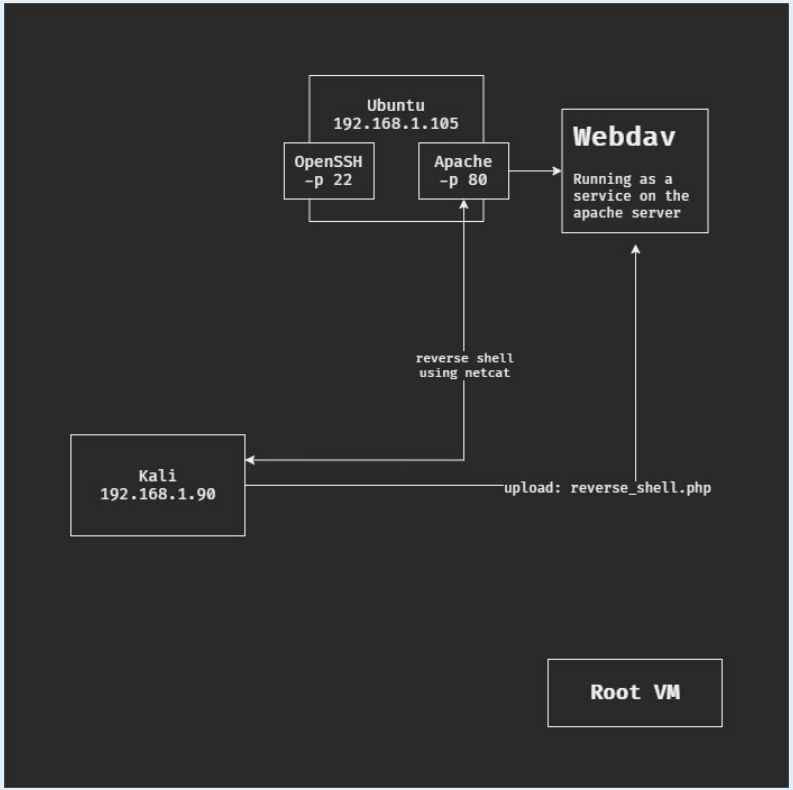
Assessment, Analysis, and Hardening of a Vulnerable System

Table of Contents

This document contains the following sections:

Network Topology

Network Topology



Network
Address Range: 192.168.1.0/24
Netmask: 172.17.196.209
Gateway: 10.0.0.1

Machines
IPv4: 192.168.1.1
OS: Windows XP
Hostname: ML-RefVm-684427

IPv4: 192.168.1.90
OS: Kali
Hostname: Kali

IPv4: 192.168.1.100
OS: Ubuntu
Hostname:

IPv4: 192.168.1.105
OS:Ubuntu
Hostname: Server1

Red Team
Security Assessment

Recon: Describing the Target

Nmap identified the following hosts on the network:

Hostname	IP Address	Role on Network
ML-RefVm-684427	192.168.1.1	Base Machine hosting the 3 VMs below
Kali	192.168.1.90	Box used for penetration testing
Ubuntu	192.168.1.100	Hosting a Kibana server and capturing activity on 192..168.1.105.
Server1	192.168.1.105	Box we are attempting to pop - hosting an apache and ssh server

Vulnerability Assessment

The assessment uncovered the following critical vulnerabilities in the target:

Vulnerability	Description	Impact
Use the CVE number if it exists. Otherwise, use the common name.	*Describe the vulnerability.*	*Describe what this vulnerability allows the attacker to do.*
For example: LFI Vulnerability	LFI allows access into confidential files on a site.	An LFI vulnerability allows attackers to gain access to sensitive credentials

Exploitation: [Name of First Vulnerability]

01

Tools & Processes
How did you exploit the vulnerability? Which tool (Nmap, etc.) or techniques (XSS, etc.) did you use?

02

Achievements
What did the exploit achieve? For example: Did it grant you a user shell, root access, etc.?

03

[INSERT: screenshot or command output illustrating the exploit.]

Exploitation: [Name of Second Vulnerability]

01

Tools & Processes
How did you exploit the vulnerability? Which tool (Nmap, etc.) or techniques (XSS, etc.) did you use?

02

Achievements
What did the exploit achieve? For example: Did it grant you a user shell, root access, etc.?

03

[INSERT: screenshot or command output illustrating the exploit.]

Exploitation: [Name of Third Vulnerability]

01

Tools & Processes
How did you exploit the vulnerability? Which tool (Nmap, etc.) or techniques (XSS, etc.) did you use?

02

Achievements
What did the exploit achieve? For example: Did it grant you a user shell, root access, etc.?

03

[INSERT: screenshot or command output illustrating the exploit.]

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