Network Pivoting and Lateral Movement Using Metasploit

@ArunVedha07

CONTENTS

1. Exploitation Project Documentation

1.1 Objective

he objective of this assignment is to demonstrate network pivoting and lateral movement within a controlled lab environment. The assessment focuses on compromising an initial system, leveraging it as a pivot point, discovering additional hosts within an internal network, and exploiting a secondary target service to gain further access. This project highlights how an attacker can move beyond a single compromised host and expand access across a network when segmentation and monitoring controls are weak.

1.2 Requirements

This assessment was performed using the following setup and tools:

- Kali Linux – attacker system
- Metasploitable (UNIX-based) – pivot host
- Additional internal target system
- Metasploit Framework
- Virtualized lab environment with bridged and host-only networking

2. High-Level Summary

This project demonstrates a real world pivoting scenario where an initially compromised host is used to access and exploit systems located in a different network segment.

The workflow included:

- Gaining initial access to a UNIX-based system
- Configuring Metasploit routing to pivot through the compromised host
- Discovering internal network hosts via pivoted network scanning
- Identifying exposed services on internal systems
- Exploiting a vulnerable FTP service to compromise a second machine

This confirms that a single system compromise can lead to broader network exposure when internal trust boundaries are not properly enforced.

3. Client Side Exploitation Assignment

3.1 Internal Network Discovery

After configuring routing through the compromised system, a network sweep was performed through the pivot to identify reachable internal IP addresses. This step revealed multiple active devices connected within the internal network segment. This confirmed successful pivoting and demonstrated the ability to enumerate hosts beyond the initially compromised system.

3.2 Service Enumeration on Internal Host

One of the discovered internal hosts was selected for further analysis. Service enumeration identified an exposed FTP service running on the target system. Further inspection indicated that the FTP service version was outdated and potentially vulnerable, making it a suitable candidate for exploitation.

3.3 Vulnerability Identification

The detected FTP service was identified as vsftpd, a version known to be affected by a publicly documented backdoor vulnerability. This vulnerability allows unauthorized access under specific conditions and is commonly used to demonstrate lateral movement risks in lab environments. The presence of this vulnerable service confirmed that the internal host was exploitable through the established pivot.

3.4 Exploitation & Second Host Compromise

The vsftpd backdoor exploit was executed through the pivoted connection, resulting in successful access to the second system within the internal network. This validated full lateral movement from the initial compromised host to a secondary target. Access to the second system confirmed that the pivot configuration and exploit chain were successful.

3.5 Screenshot & Evidence

The following figures provide visual evidence of the pivoting and lateral movement workflow performed within a controlled lab environment:
01: Initial shell access obtained on the compromised UNIX-based system, confirming successful foothold establishment.
02: Meterpreter session upgraded and routing information configured within Metasploit, enabling access to the internal network segment through the compromised host.
03: Internal host discovery performed through the established route, identifying additional systems reachable within the internal network.

4: Port scanning conducted against an identified internal host to enumerate exposed services.
05: Service version detection performed on the discovered FTP service, identifying the running vsftpd version.
06: Successful exploitation of the vsftpd backdoor vulnerability, resulting in access to a second internal system and confirming effective lateral movement.
All screenshots are stored in the /screenshots directory as supporting documentation for the pivoting and lateral movement workflow.