Network Pivoting and Lateral Movement Using Metasploit

@ArunVedha07

CONTENTS

1. Exploitation Project Documentation

1.1 Objective

The objective of this assignment is to perform pivoting and lateral movement using a SOCKS proxy within a controlled lab environment. This assessment demonstrates how an attacker can leverage an initially compromised system to route traffic into an internal network and perform enumeration and exploitation from a separate terminal using proxy based access. This exercise highlights the effectiveness of SOCKS based pivoting for internal network assessment and lateral movement when direct access to the target network is restricted.

1.2 Requirements

This assessment was carried out using the following tools and environment:

- Kali Linux – attacker system
- Windows System (Primary) – initial compromised host
- Windows System (Clone) – internal target system
- Metasploit Framework
- SOCKS proxy configuration
- Proxy aware scanning tools

2. High-Level Summary

This project demonstrates internal network pivoting using a SOCKS proxy established through Metasploit. After gaining access to an initial Windows system, a SOCKS proxy was configured to tunnel traffic into the internal network. This allowed enumeration and vulnerability assessment of another Windows system from a separate terminal, simulating a realistic lateral movement scenario.

Workflow Overview:

- Initial access to the primary Windows system
- SOCKS proxy configuration within Metasploit
- Routing traffic into the internal network
- Internal host discovery using proxy based tools
- Service enumeration and vulnerability validation
- Successful access to the cloned Windows system

This confirms that SOCKS based pivoting enables effective internal reconnaissance and exploitation without directly interacting from the compromised session.

3. Network Pivoting and Lateral Movement

3.1 Initial Access

The primary Windows system was successfully compromised, resulting in a stable Meterpreter session. This system served as the pivot point into the internal network where the cloned Windows system was located.

3.2 SOCKS Proxy Configuration

A SOCKS proxy was configured within Metasploit and bound to the active session. Routing was added to ensure that traffic destined for the internal network was forwarded through the compromised system. This enabled proxy aware tools to communicate with internal hosts from a separate terminal. This approach allowed testing and enumeration without interacting directly through the Meterpreter console, closely simulating real world pivoting techniques.

3.3 Internal Network Enumeration

Using the configured SOCKS proxy, internal network discovery was performed from another terminal. Host identification and service enumeration confirmed the presence of the cloned Windows system on the internal network.
Further scanning validated that the target system was reachable through the pivot and exposed services suitable for exploitation.

3.4 Screenshots & Evidence

The following figures provide visual evidence of the SOCKS-based pivoting workflow within the lab environment:

01: Initial compromise of the first device, showing successful Meterpreter session establishment and confirmation of active access.
02: Configuration of internal network routing using the Metasploit autoroute module, enabling access to the target subnet through the compromised system.
03: Setup and execution of the SOCKS proxy within Metasploit, running as a background job to support proxy based scanning from an external terminal.
04: Internal network scanning performed from a separate terminal using proxychains and Nmap, identifying active hosts and confirming that port 445 (SMB) was accessible on the second device.

05: Exploitation of the second device via Metasploit using the MS17-010 (EternalBlue) exploit, resulting in successful access and confirmation of lateral movement through the pivot.

All screenshots are stored in the /screenshots directory as supporting documentation for the SOCKS-based pivoting and lateral movement process.