# Active-Reconnaissance Lab

This lab outlines performing host discovery, port scanning, service version detection, and vulnerability scanning and detection using Nmap. The lab was conducted in a controlled environment to demonstrate various reconnaissance techniques.

## Table of Contents

Introduction

Host Discovery

- Nmap Host Discovery

- ARP Scan

- FPing

- Passive Reconnaissance with Wireshark

- Screenshots

Port Scanning and Host Fingerprinting

- Nmap Port Scanning

- Nmap Service Version Detection

- Screenshots

- Web Server Enumeration on Port 80

- Screenshots

Fingerprinting with Nmap Scripts

- FTP Enumeration

- SSH Enumeration

- SMB Enumeration

- Web Server Enumeration

Acknowledgements

## Introduction

This document contains step-by-step guides for performing active reconnaissance using Nmap and other tools. It covers host discovery, port scanning, service version detection, and web server enumeration. All activity was performed in a virtualized contained environment with three VMs. In this example, arp-scan, nmap, and fping are all utilized to perform network host discovery while the host fingerprinting stage primarily focusing on a Metasploitable2 VM.

## Host Discovery

### ARP-Scan, Nmap Ping Scan, and fping ping sweep

Perform an arp scan, nmap ping scan, and an pfing scan to discover what hosts are connected to the local network.

[Image: arp-scan-nmap-sn.png]

[Image: fping.png]

## Port Scanning and Host Fingerprinting

### SYN scan and service version detection

[Image: Port Scanning and Service Detection.png]

### Full port scan and service version detction

[Image: Full Port Scan.png]

### SYN scan, service version detection, and UDP scan

[Image: SYN-sV-sU.png]

### Port scan for ports 1-10000 and service version detection:

[Image: p1-10000.png]

## Fingerprinting with Nmap Scripts

Use Nmap scripts to fingerprint services and gather detailed information

### FTP Enumeration

[Image: nmapftpanon.png]

[Image: nmapftp-syst.png]

[Image: nmapftpvuln.png]

### SSH Enumeration

[Image: nmapssh-auth-methods.png]

[Image: nmapssh-hostkey.png]

[Image: nmapssh2-enum-algos.png]

### SMB Enumeration

[Image: nmapsmb-os-discovery.png]

[Image: nmapsmb-security-mode.png]

### Web Server Enumeration

[Image: nmaphttp-title.png]

[Image: nmapsChttp-methods.png]

[Image: nmaphttp-headers.png]

## Acknowledgments

### Metasploitable2

Metasploitable2 is a vulnerable virtual machine intended for use as a target for testing security tools and demonstrating common vulnerabilities.  
  
Official download page: https://sourceforge.net/projects/metasploitable/  
  
License: BSD License, GNU General Public License version 2.0 (GLPv2)