Active Recon Lab Manual – Nmap & Masscan

Day 11 – Penetration Testing Series

1. Introduction

In this lab, you will learn how to perform Active Reconnaissance using Nmap and Masscan. Active Recon involves directly interacting with a target system to gather information, such as identifying live hosts, open ports, and services. While this is a powerful step in penetration testing, it must only be conducted on networks you own or have explicit permission to test.

Recap of Day 10

Before starting, remember the passive reconnaissance techniques from Day 10: - WHOIS: To discover domain/IP ownership. - DNS Lookups: To map domain names to IP addresses. - OSINT: To gather information without touching the target system. Now we move to Active Recon, where we actively scan and probe systems.

Risks & Ethics

■ Scanning networks without permission is illegal in many countries. Always perform these activities in a controlled lab environment or with written authorization. Unauthorized scans can result in legal consequences, IP bans, or even damage to systems.

Why Identify Open Ports/Services?

Open ports represent possible entry points into a system. By identifying them, penetration testers can: - Map the attack surface. - Match services to known vulnerabilities. - Tailor their exploitation attempts. Example: Port 21 (FTP) could allow anonymous login if misconfigured.

Nmap vs Masscan

Feature	Nmap	Masscan
Speed	Medium	Very Fast
Detail Level	High	Low (only ports)
Service Detection	Yes	No
OS Detection	Yes	No
Typical Use	Detailed Analysis	Large IP Sweeps

Lab Exercise 1: Nmap Basics

Nmap (Network Mapper) is a versatile scanning tool that can identify live hosts, open ports, running services, and more. Below are some essential commands and their purposes:

Task	Command	Description
Ping Scan for Live Hosts	nmap -sn 192.168.1.0/24	Lists responsive IPs without port sca
TCP SYN + Version Scan	nmap -sS -sV 192.168.1.10	Finds open TCP ports and detects se
Aggressive Scan	nmap -A 192.168.1.10	Performs OS detection, version dete
Save Output (Normal)	nmap -oN scan.txt 192.168.1.10	Saves results in human-readable tex
Save Output (XML)	nmap -oX scan.xml 192.168.1.10	Saves results in XML format for pars
Save Output (Grepable)	nmap -oG scan.gnmap 192.168.1.10	Saves results for grep-based filtering

Lab Exercise 2: Masscan Basics

Masscan is an extremely fast port scanner capable of scanning the entire Internet in under six minutes (at high rates). It is best used for quickly finding open ports over large IP ranges, and then using Nmap for deeper inspection.

Task	Command	Description
Full Port Sweep	masscan 192.168.1.0/24 -p0-65535 --rate 1000	Scans all 65535 TCP ports with a hig
Compare with Nmap Results	Manual	Review differences in detected ports
Tune Scan Speed	masscan 192.168.1.0/24 -p0-65535 --rate 500	Slows scan to reduce detection likeli
Target Specific Ports	masscan 192.168.1.0/24 -p80,443	Scans only ports 80 and 443 for spe

Discussion Prompts

1. Why might Masscan find ports that Nmap misses (and vice versa)? 2. How does network latency affect scanning results? 3. What’s the trade-off between speed and stealth? 4. How would you hide your scan from an IDS/IPS?