# Step-by-Step Guide: Nmap Scanning and Nessus Vulnerability Assessment

This document provides a structured step-by-step guide for performing reconnaissance and vulnerability assessment activities on a target host (192.168.1.157). The guide covers two main phases:   
1. Nmap scanning and service enumeration   
2. Nessus Essentials vulnerability scanning.   
This excludes exploitation steps (Metasploit), focusing only on discovery, documentation, and analysis.

## 🔍 Part 1: Nmap Scanning & Service Enumeration

Target IP: 192.168.1.157

1. Step 1: TCP Full Port Scan

Command:  
sudo nmap -sS -p- -T4 -oN tcp\_full\_scan.txt 192.168.1.157  
  
Purpose:  
Performs a full TCP SYN scan of all 65,535 ports. The results are saved in tcp\_full\_scan.txt for documentation.

1. Step 2: UDP Scan (Common Ports)

Command:  
sudo nmap -sU --top-ports 100 -T4 -oN udp\_scan.txt 192.168.1.157  
  
Purpose:  
Scans the top 100 UDP ports, which are commonly used by network services. UDP scanning is slower, so limiting ports is recommended. Results saved in udp\_scan.txt.

1. Step 3: Service & Version Detection

Command:  
sudo nmap -sV -sC -oN service\_scan.txt 192.168.1.157  
  
Purpose:  
Detects the version of running services and executes default NSE (Nmap Scripting Engine) scripts for additional enumeration. Results saved in service\_scan.txt.

1. Step 4: Documentation

Ensure that raw outputs are saved:  
- tcp\_full\_scan.txt  
- udp\_scan.txt  
- service\_scan.txt  
  
Screenshots of terminal results should be included in the report. Highlight open ports, identified services, and potential targets for deeper analysis.

## 🛠️ Part 2: Vulnerability Scanning with Nessus Essentials

1. Step 1: Start Nessus

Run the Nessus service and open it in a browser:  
https://localhost:8834  
  
If service is not active, start it with:  
sudo systemctl start nessusd

1. Step 2: Configure a Basic Scan

1. Log in to Nessus Essentials  
2. Go to 'My Scans' → '+ New Scan' → 'Basic Network Scan'  
3. Name: Scan-192.168.1.157  
4. Target: 192.168.1.157  
5. In settings, enable:  
 - OS detection  
 - Service detection  
 - Safe checks

1. Step 3: Run the Scan

Click Save → Launch. Allow several minutes for results to populate.

1. Step 4: Export and Analyze Results

1. Open the scan after completion.  
2. Export results as PDF for evidence.  
3. Document at least 3 vulnerabilities with details:  
 - Name and severity  
 - CVSS score  
 - Potential impact  
 - Recommended mitigations

1. Step 5: Verification & Documentation

Include in your report:  
- Scan configurations (screenshots or notes)  
- Exported raw results (PDF + text files)  
- Analysis of 3 or more vulnerabilities  
- False positive checks and verification steps

## 📄 Outcome

By following these steps, the student will produce a professional-grade security assessment consisting of Nmap scan data, service enumeration results, and a Nessus vulnerability report. This provides a complete evidence package suitable for cybersecurity labs, reports, or academic submissions.