**7.Vulnerability Scan Simulation**

1. Attacker machine – running Nmap or Nessus Essentials.
2. Target machine – configured to log events (Sysmon for Windows, syslog).

Step 1: Prepare Your Machines

* Attacker VM: Install Nmap or Nessus Essentials.
* Target VM:
  + Windows: Ensure Sysmon + Winlogbeat are working.
  + Linux: Ensure auditd, syslog, or Filebeat + ELK are running.

Step 2: Run a Scan from the Attacker

Option A: Nmap Scan

From the attacker machine, run:

nmap -sS -sV -O 192.168.157.140

Explanation:

* -sS: Stealth (SYN) scan
* -sV: Version detection
* -O: OS detection

Step 3: Monitor the Target Logs

For Windows (with Sysmon + Winlogbeat)

* Check Event Viewer (Sysmon logs under Event ID 3, 1, 6).
* Review ELK Dashboard (if logs are shipped via Winlogbeat).