Day 43

Topic: Enumeration Techniques

Objective: To extract detailed information such as usernames, machine names, and shares from the system.

Theoretical Concepts:
Enumeration involves active connections to the system to query for more details. We focused on NetBIOS enumeration, SNMP enumeration, and SMB (Server Message Block) enumeration. This phase bridges the gap between scanning and exploitation.

Practical Work:
We used **Enum4linux**, a tool specifically designed to extract info from Windows and Samba systems. We ran *enum4linux -a [target_ip]* to retrieve the user list, share list, and password policy information. We also tried basic SNMP enumeration to find community strings using *snmp-check*. We identified a "guest" account and a writable share directory.

Tools Used: Nmap (Scripts), Enum4linux.

Outcome: Successfully extracted a list of valid users and network shares from a target machine.