Title: System Enumeration & Service Discovery — Assessment Report
Author: Salmata Lamin
Date: *2025-11-04*
Environment: Kali Linux (VM), target hosts discovered in reconnaissance phase

Objective

Perform deep enumeration on identified hosts to discover exposed services, user accounts, network shares, directory information, and SNMP/LDAP details to prioritize targets for vulnerability analysis

Tools & Commands Used

- `enum4linux -a <target>` — SMB/NetBIOS enumeration (users, shares, OS info)
- `snmpwalk -v2c -c public <target>` — SNMP interrogation for system OIDs and interfaces
- `ldapsearch -x -h <target> -b "dc=example,dc=com"` — LDAP directory enumeration
- `rpcclient, smbclient` — additional SMB queries

Process Summary

- Ran enum4linux against Windows hosts to capture SMB shares and user enumeration.
- Queried SNMP on network appliances to reveal device metadata and interface counts.
- Executed LDAP queries against the directory server to extract base DN and sample user objects.
- Correlated findings with prior reconnaissance to confirm host ownership and role.

Findings (summary)

Process Summary

- **SMB/NetBIOS:** Host 10.10.10.12 reveals shares \\FILES\Public and \\ADMIN$ and user accounts including jdoe and svc_backup.
- **SNMP:** Host 10.10.10.30 exposed system OID sysDescr showing “Cisco IOS 15.x” and multiple interface entries. Default community string public responded.
- **LDAP:** LDAP server at 10.10.10.40 allowed anonymous bind; base DN dc=example,dc=com returned user objects cn=admin and cn=svc_app.

Recommendations

- **Risk:** Exposed SMB shares and identifiable service accounts provide easy pivot points for lateral movement. Unprotected SNMP and anonymous LDAP increases reconnaissance surface for attackers.
- **Recommendations:**
  - Restrict SMB share permissions and remove unnecessary shares.
  - Change SNMP community strings from defaults and limit SNMP access to management subnets.
  - Disable anonymous LDAP bind and enforce least-privilege on directory queries.
  - Follow up with authenticated vulnerability scans and password audits for discovered accounts.

Evidence

- Results/enum4linux_output.txt
- Results/snmpwalk_output.txt
- Results/ldapsearch_output.txt
- Screenshots/01_enum4linux_output.png, 02_snmpwalk_output.png, 03_rpc_smb_output.png