**Module 4: Enumeration**

(Enumeration is depth form of Scanning) Mainly, it is done for collection information from LDAP, NetBIOS and SNMP.

* **Netbios Enumeration in Windows:**

Command prompt> Run as Administrator> nbtstat ?

Command Usage: NBTSTAT [ [-a RemoteName] [-A IP address] [-c] [-n]

[-r] [-R] [-RR] [-s] [-S] [interval] ]

* -a (adapter status) Lists the remote machine's name table given its name
* -A (Adapter status) Lists the remote machine's name table given its
  + - IP address.
* -c (cache) Lists NBT's cache of remote [machine] names and their IP addresses
* -n (names) Lists local NetBIOS names.
* -r (resolved) Lists names resolved by broadcast and via WINS
* -R (Reload) Purges and reloads the remote cache name table
* -S (Sessions) Lists sessions table with the destination IP addresses
* -s (sessions) Lists sessions table converting destination IP
  + - addresses to computer NETBIOS names.
* -RR (ReleaseRefresh) Sends Name Release packets to WINS.
* **Netbios Enumeration in Linux**:

Terminal > sudo apt install nbtscan > nbtscan –h > nbtscan (define parameter) “target ip/Network)

<https://www.computerhope.com/nbtstat.htm> : info

* **Snmp-check tool (in linux) [important ]**

Snmp uses udp port i:e; 161

* Command usage: Sudo snmp-check “Target ip”

Eg: Sudo snmp-check 10.10.10.22

* **Snmpwalk Tool (in linux)**

Usage command: Sudo snmpwalk – V(version) – C(Community) “Target Ip”

Eg: Sudo snmpwalk –V

* **LDAP Enumeration Tool:**

**LDAP in windows: Light weight Directory Access protocol**

* **Active Directory Explorer tool (in windows)**
* LDAP port no: 389

**LDAP in Linux:**

* **LDAP Search tool (ldapsearch)**

Command Usage: Sudo ldapsearch (options) Filter[attributes]

<https://www.ibm.com/docs/en/power8/9119-MME?topic=commands-ldapsearch-command> : info

* **Domain Enumeration in linux:**
* **dig tool**
* terminal> dig –h > dig “website/ip”
* terminal > dig –ns / -mx “website /ip”

-ns: name server , -mx: mail server

* **DNS Recon tool in linux:**
* **dnsrecon**
* Check DNS server cache records for A, AAAA and CNAME records given a list of host records in a text file
* Enumerate general DNS records for a given domain (MX, SOA, NS, A, AAAA, SPF and TXT)
* Check all NS records for zone transfers
* Check for wildcard resolution
* Perform common SRV record enumeration and top-level domain (TLD) expansion

Steps : Terminal > dnsrecon –d (domain) –n (name server)