Enumeration

Edited by:
Dr. Ahmed Redha
PSU

Key Concepts

- Process of enumeration,
- Tools used to perform enumeration

* اين يسوي
* اين المعلومات اللي يحصل عليها الاتاكر لكل واحد منهم

Enumeration in Ethical Hacking

- Enumeration is extracting a system's valid usernames, machine names, share names, directory names, and other information.
- It is a key component of ethical hacking and penetration testing, as it can provide attackers with a wealth of information that can be used to exploit vulnerabilities.
- Enumeration can be used in both an offensive and defensive manner.
- Enumeration is one of the most important steps in ethical hacking because it gives hackers the necessary information to launch an attack. For example, hackers who want to crack passwords need to know the usernames of valid users on that system. Enumerating the target system can extract this information

Enumeration can be used to gather any of the following information:

- Operating system details
- Network infrastructure details
- Usernames of valid users
- Machine names
- Share names
- Directory names
- Printer names
- Web server details

Why Is Enumeration Important?

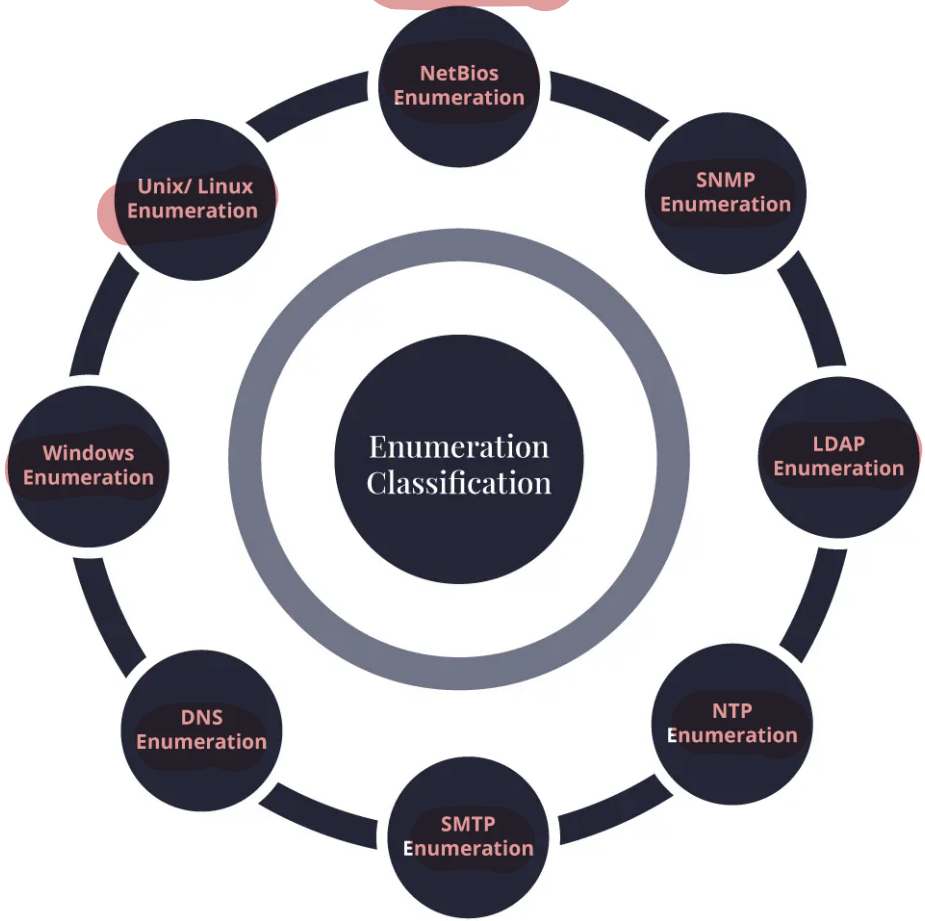
- Enumeration lets you understand what devices are on your network, where they are located, and what services they offer. To put it simply, enumeration can be used to find security vulnerabilities within systems and networks.
- By conducting an enumeration scan, you can see what ports are open on devices, which ones have access to specific services, and what type of information is being transmitted. This information can then be used to exploit weaknesses and gain unauthorized access.
- Carrying out an enumeration scan requires both time and patience. However, it's a crucial step in the hacking process as it allows you to gather intelligence about your target.
- Enumeration can be performed manually or with automated tools. Whichever method you choose, it's important to be thorough in your scan to maximize the amount of information you can collect.

Enumeration (Purpose)

- Dig deeper into the target system
- Uncover specific information about the system
- Determine what services and settings that are present
- Modify attack to make activity more productive

Enumeration Classification

We can perform enumeration on the following:



Different Enumeration classification

① NetBios: (Shared files)

- Used in windows
- Help computers communicate & share files, Printers
- Use Port 139
- NetBios names: 16 characters
- First 15 → device name
  Last one → service type
- File & Printer sharing must be enabled
- Use suffix to identify services

What an attacker can get:

- list of computers in a domain
- Shared folders
- Security Policies
- Sometimes Passwords

---

② SNMP

- a Protocol to manage network devices
- Used on Routers, Servers, Switches
- it use UDP

Components:

- SNMP Agent: Runs on the device
- SNMP Manager: Controls/queries devices

1- NetBIOS Enumeration

- The first step in enumerating a Windows machine is to take advantage of the NetBIOS API. NetBIOS stands for Network Basic Input Output System. IBM, in association with Sytek, developed NetBIOS. It was developed as an Application Programming Interface (API), originally to facilitate the access of LAN resources by the client's software. The NetBIOS name is a unique 16 ASCII character string used to identify the network devices over TCP/IP; 15 characters are used for the device name and the 16th character is reserved for the service or name record type.

Attackers use the NetBIOS enumeration to obtain:

- List of computers that belong to a domain and shares of the individual hosts on the network
- Policies and passwords

- If an attacker finds a Windows OS with port 139 open, he or she would be interested in checking what resources he or she can access, or view, on the remote system.
- However, to enumerate the NetBIOS names, the remote system must have enabled file and printer sharing.
- Using these techniques, the attacker can launch two types of attacks on a remote computer that has NetBIOS:

The attacker can choose to read/write to a remote computer system, depending on the availability of shares, or launch a denial-of-service.

NetBIOS names and suffixes

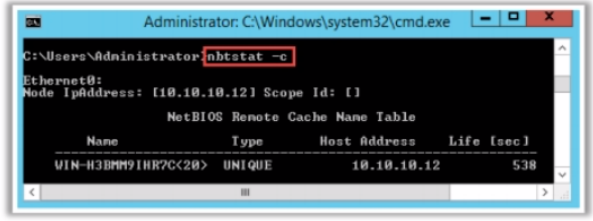
NetBIOS name	Suffix	Description
<computer name>	4C	Indicates that DEC Pathworks TCP/IP is configured on the computer.
<computer name>	52	Also indicates that DEC Pathworks is configured on the computer.
<computer name>	87	Signifies that Microsoft Exchange Message Transfer Agent (MTA) is running on this computer.
<computer name>	6A	Indicates that Microsoft Exchange Internet Mail Connector (IMC) is running.
<computer name>	BE	Signifies that Netmon Agent (a Microsoft network-monitoring tool) is running.
<computer name>	BF	Indicates that the Netmon application is running.
<username>	03	Indicates that the Messenger service is running.
<domain name>	00	Indicates that Domain Name System (DNS) is running.
<domain name>	1B	Identifies the computer as a domain master browser.
<domain name>	1C	Identifies the computer as a domain controller.
<domain name>	1D	Identifies the computer as a domain master browser.
<domain name>	1E	Signifies that Browser Services Election is running.
<iNet~Services>	1C	Indicates that Internet Information Services (IIS) is running.
<IS~computer name>	00	Also indicates that IIS is running.

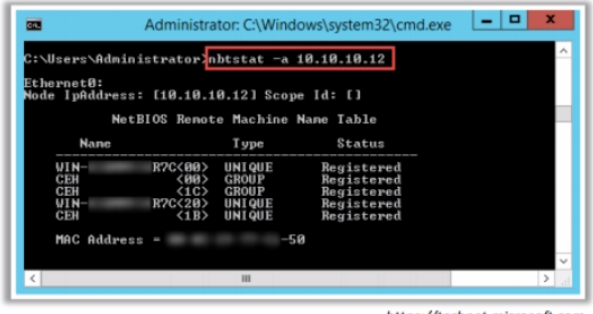
NetBIOS Enumeration

- Nbtstat utility in Windows displays NetBIOS over **TCP/IP** (NetBT) **protocol statistics**, **NetBIOS name tables** for both the local and remote computers, and the **NetBIOS name cache**

Run **nbtstat** command "**nbtstat.exe -c**" to get the contents of the NetBIOS name cache, the table of NetBIOS names, and their resolved IP addresses

Run **nbtstat** command "**nbtstat.exe -a <IP address of the remote machine>**" to get the NetBIOS name table of a remote computer





https://technet.microsoft.com

2- SNMP (Simple Network Management Protocol)

Enumeration

- SNMP (Simple Network Management Protocol) is an application layer protocol that runs on UDP, and is used to maintain and manage routers, hubs, and switches on an IP network. SNMP agents run on Windows and UNIX networks on networking devices.
- SNMP enumeration is the process of enumerating the user's accounts and devices on a target computer using SNMP. Two types of software components are employed by SNMP for communicating. They are the SNMP agent and SNMP management station. The SNMP agent is located on the networking device whereas the SNMP management station is communicated with the agent.

SNMP contains two passwords that you can use for configuring as well as for accessing the SNMP agent from the management station.

- The two SNMP passwords are:

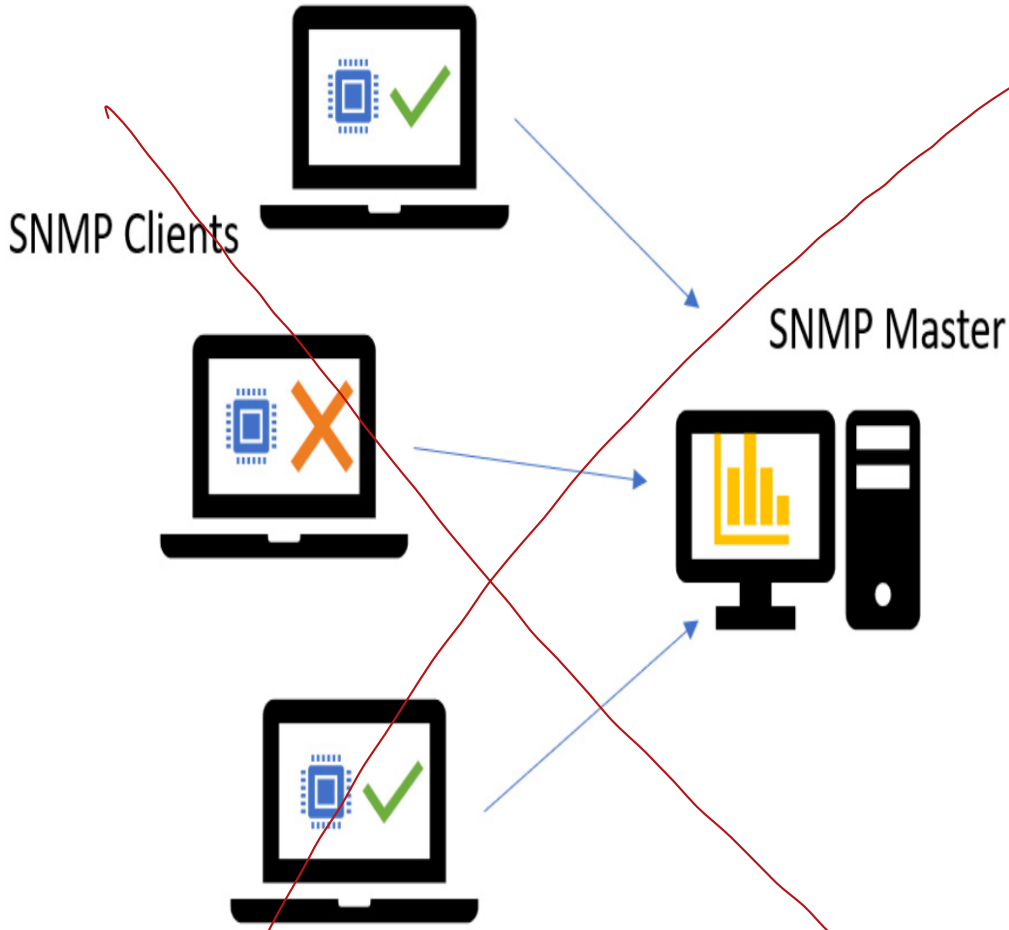
• Read community string:

  - Configuration of the device or system can be viewed with the help of this password
  - These strings are public

• Read/write community string:

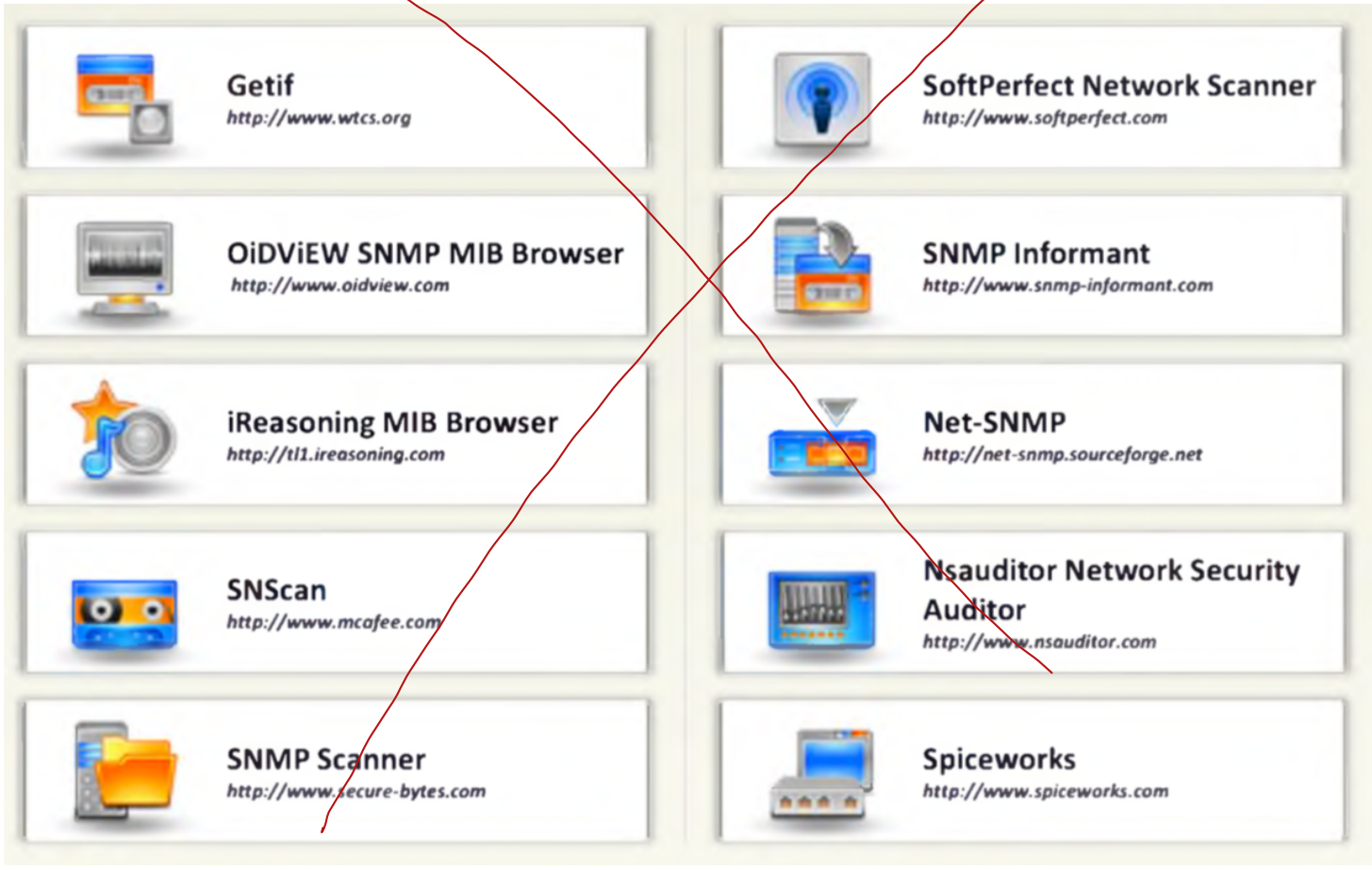
  - Configuration on the device can be changed or edited using this password
  - These strings are private

- When the community strings are left at the default setting, attackers take the opportunity and find the loopholes in it. Then, the attacker can use these default passwords for changing or viewing the configuration of the device or system. Attackers enumerate SNMP to extract information about network resources such as hosts, routers, devices, shares, etc. and network information such as ARP tables, routing tables, device specific information, and traffic statistics.



SNMP clients gather performance intel and report back to a centralized reporting point

SNMP Enumeration Tools



3- LDAP Enumeration

- The Lightweight Directory Access Protocol (LDAP) enables applications to access directory listings from directory services such as an Active Directory.
- An LDAP is usually integrated into the **Domain Name System (DNS)** for quicker resolution of queries and an expedited lookup process. An attacker can exploit a **directory scanner to query the LDAP service through port 389 anonymously**. This gives the attacker access to a host of information that can be misused to orchestrate social engineering or brute force attacks. Though the impact of such attacks varies, information uncovered by LDAP enumeration attacks generally includes active directory objects, access lists, usernames, groups, trusts, sessions, etc.

4- NTP Enumeration

it focus on time

- The Network Time Protocol (NTP) is used to synchronize the system clocks of networked computers. NTP agents are connected to time servers globally that sync systems across different time zones. Agents usually request synchronization by sending mode four packets to the remote machine servers, which respond with mode three packets. Orchestrating such attacks require attackers to query the NTP agent via UDP port 123, which returns information related to the machines communicating with the NTP server, system names, client OSs, detailed interface info, IP addresses, etc

5- DNS Enumeration

- The DNS service enables **consistency using zone transfers** to copy the information across servers. The zone transfer service requires **no authentication**, enabling malicious actors to **obtain a copy** of the **entire DNS zone** from any DNS server. This facilitates **exposing information** about the configuration of all hosts within the domain, which **opens up security gaps** within the network's topology.

Techniques for Enumeration

Services	Ports
DNS Zone Transfer	TCP 53
DNS Queries	UDP 53
SNMP	UDP 161
SNMP Trap	TCP/UDP 162
Microsoft RPC Endpoint Mapper	TCP/UDP 135
LDAP	TCP/UDP 389
NBNS	UDP 137
Global Catalog Service	TCP/UDP 3268
NetBIOS	TCP 139
SMTP	TCP 25

Table 4.01 Services and Port to Enumerate

Ports and services to know about

* Should Know each service and it's Port # * MCQs

- Most of the DNS information that goes across the network is going to be using port **53**.
- Simple Mail Transfer Protocol (SMTP) typically uses port **25**. Microsoft RPC endpoints use TCP **135.**
- The global catalog service, which is a stripped-down version of Active Directory that users and applications take advantage of all the time, queries port **3286.**
- The NetBIOS naming service, which is typically the computer name to an IP address, uses port **137,** both TCP and UDP.
- LDAP or LDP is the protocol used by Active Directory, Open Directory, and all the different directory services out there. It uses TCP and UDP port **389.**
- SMB, which is our server message block over NetBIOS, is what creates shared resources or shared folders, and it uses TCP **139** to make connections.
- We also have SNMP, which uses UDP **161.** The other SMB technology that it can use is TCP, which is going to be associated with port **445** on TCP.

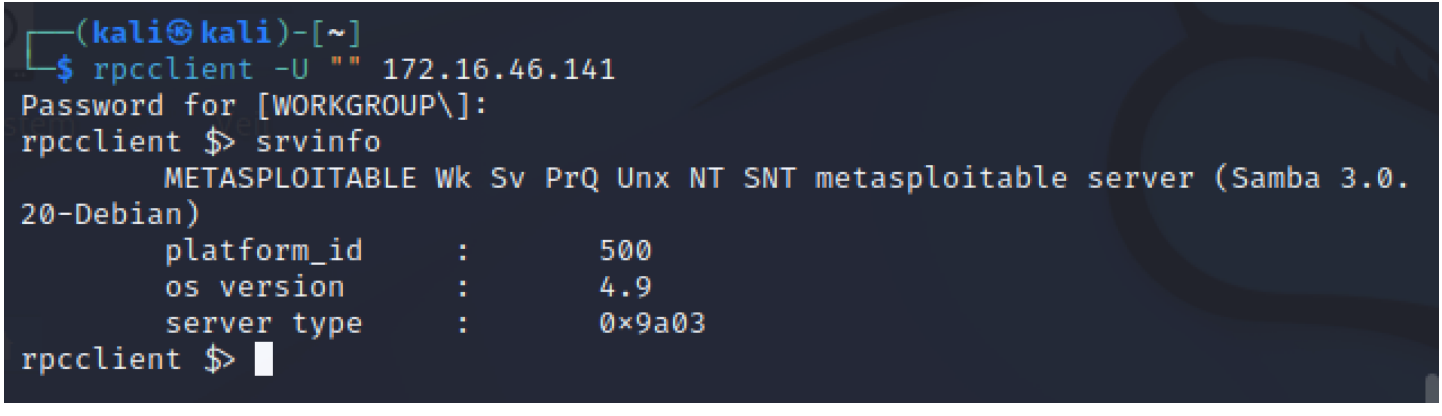
NULL Session

- List of users and groups
- List of computers and devices
- List of shares
- Users and host SIDs

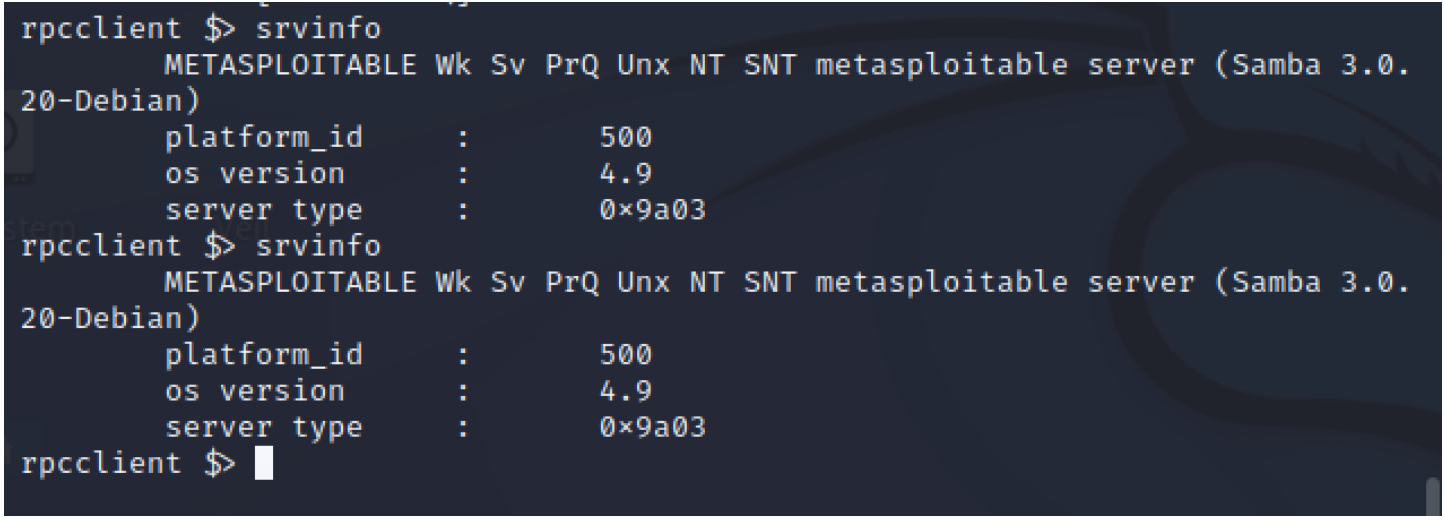
NULL Session (Cont.)

In a null session, an attacker is able to log in to a target using a null account. A null account is an account that does not actually exist. How is this possible? Some systems are vulnerable to allowing anonymous login. Once a user is able to log in anonymously, the null user is able to retrieve sensitive information stored on the target.

We can attempt a null session enumeration from our Kali Linux machine (attacker) on to the target, Metasploitable, by using the rpcclient -U "" 10.10.10.100 command, as shown in the following screenshot:



Using the srvinfo command, the target will return its operating system type to us. For a full listing of query commands, you can use the rpcclient --help command.



6- UNIX/Linux Enumeration Commands