# Enumeration

## Chapter 6



SYBEX

# What Is Enumeration?

- Gathers detailed information beyond scanning
- Uses different protocols such as ICMP and SNMP
- Can create effective picture of network
- Relies on both manual and automated methods

SYBEX

# Enumeration

You can expect to gain even more information during this step as you are digging deeper and gathering information such as usernames, host names, share names, services, application data, group information, and much more.

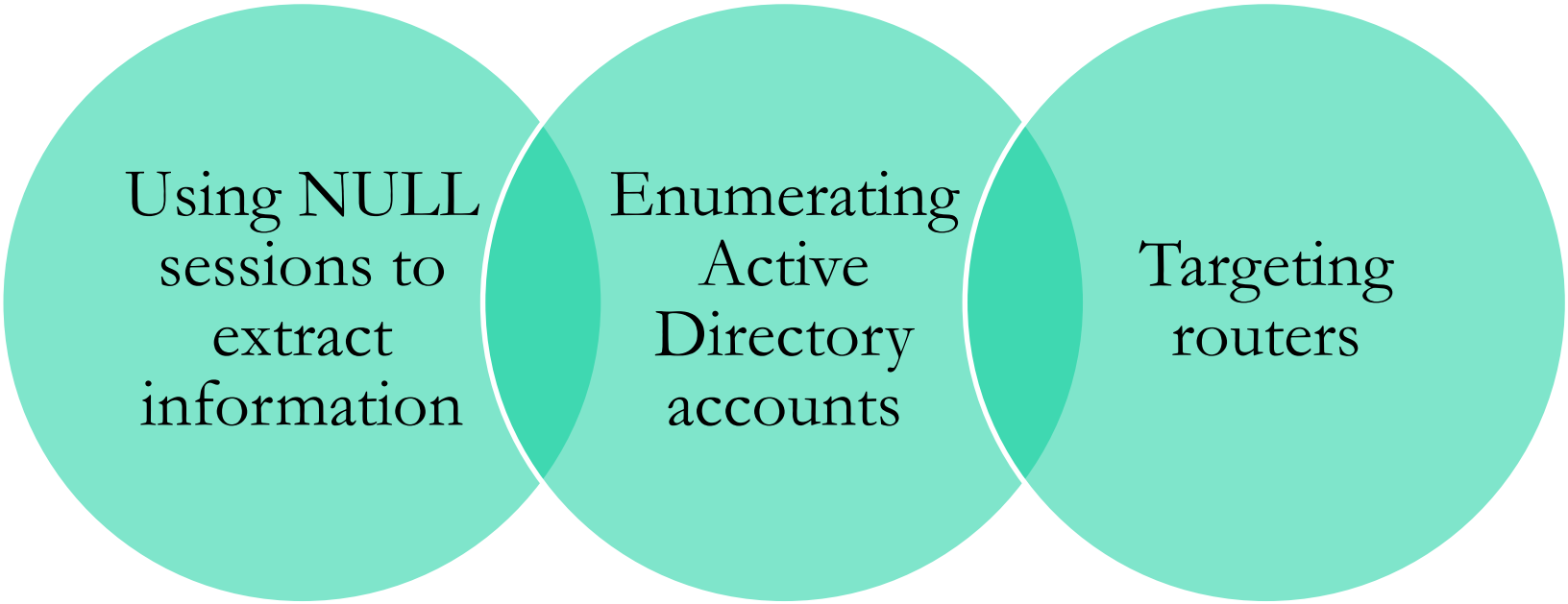
- Network resources and shares
- Users and groups
- Routing tables
- Auditing and service settings
- Applications and banners
- SNMP and DNS details



SYBEX

# What to Uncover and How

The process of enumeration is finding out about what services are running, including versions, open shares, account details, or possible points of entry. One such target is SMB.




SYBEX

# Ports of Interest

- TCP 53: This is used for DNS zone transfers.
- TCP 135: This is used by email clients to connect to email servers.
- TCP 137: NBNS provides name resolution services for the NetBIOS protocol.
- TCP 139: This is for NetBIOS Session Service or SMB over NetBIOS.
- TCP 445: SMB over TCP or Direct Host improves network access.
- UDP 161: SNMP is a protocol used for network management.
- TCP/UDP 389: LDAP is used by many directory applications.
- TCP / UDP 3368: This is the Global Catalog Service associated with Active Directory.
- TCP 25: SMTP is used for the transmission of messages.

SYBEX

# NetBIOS

This service was originally intended to assist in the access to resources on a LAN only.

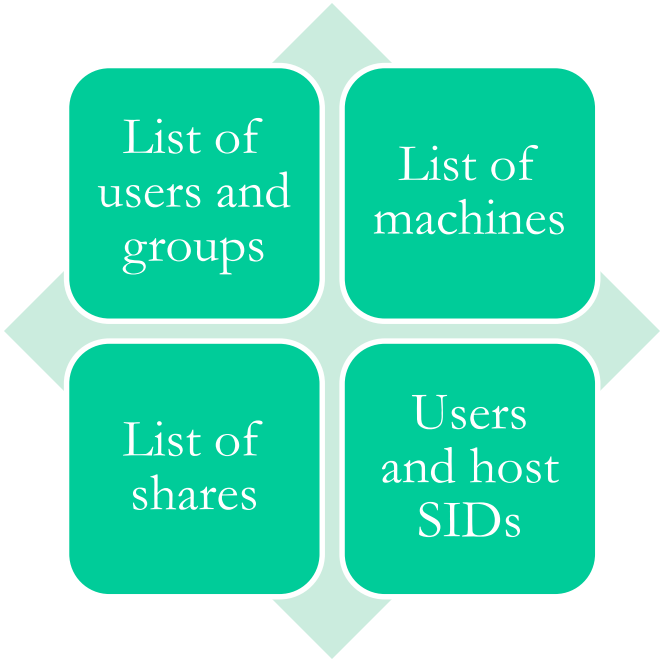
- Commonly exploited service
- Designed for small networks
- Is extremely vulnerable
- Can be used to extract all sorts of information from a target
- Considered a legacy protocol
- Still available and running on Windows systems by default



SYBEX

# NULL Sessions and NetBIOS

This feature is used to allow clients or endpoints of a connection to access certain types of information across the network.




The NULL session allows access to a system using a special account known as a NULL user. The account can be used to reveal information about system shares or user accounts while not requiring a username or password to do so.

SYBEX

# Working with NIULL Sessions

NULL sessions can be used to retrieve extreme amounts of information.

Information includes user IDs, share names, security policy settings, users currently logged in, and more.

Windows XP and Windows Server 2003 are not vulnerable to null session attacks.

Patches won't fix the issue, and most hardening techniques won't keep it from being exploited.

SYBEX

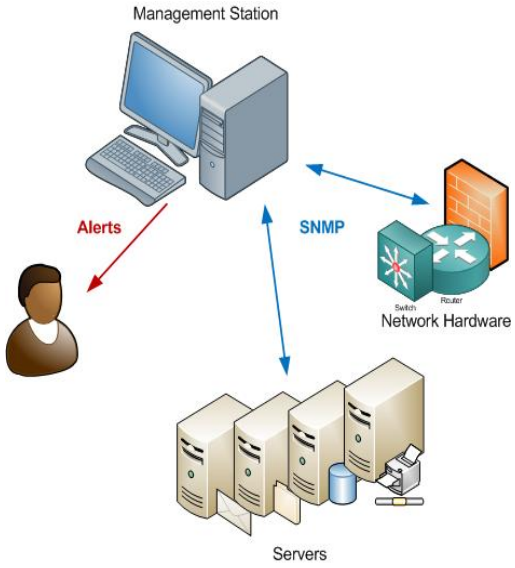
# Using a NULL Session

- **Requires a short list of commands**
- **Main command is the "net" command**
- **To connect to a remote session, use:**
  - net use \\<machine name> "/user:"
- **To view shares on a remote system, use:**
  - net view \\<machine name>
- **To connect to a remote share, use:**
  - net use <drive letter> \\<machine name>\<shared folder name>

SYBEX

# Extracting from SNMP

SNMPWalk is an open source tool that was part of the Net-SNMP project at Carnegie Mellon University in the early 1990s when SNMP was first deployed.




- Retrieves information from SNMP
- Preys upon plaintext information
- Queries devices to determine if information is kept secret
- SNMP is open source and can inform administrators

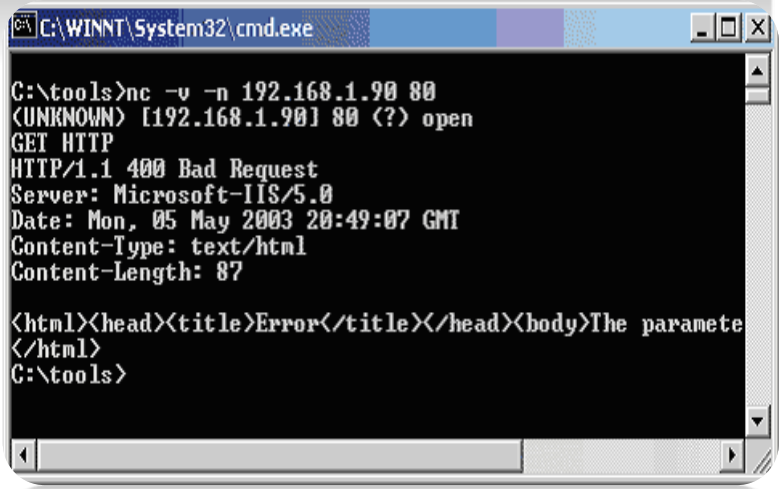
# PsTools Suite for Enumeration

- PsTools made by Systernals (now Microsoft)
- Patterned after UNIX commands
- Tools allow for detailed exploration of a remote system
- Can perform many actions and tasks

PsTools is a useful suite for both remote and local system assessment and exploitation.

SYBEX

# NetCat for Enumeration


- Freeware utility
- Commonly used for backdoor utility
- Can be used to push files from one system to another
- Can grab banners, do port scanning and port enumeration, and perform remote actions

# What About Metasploit?

The Metasploit framework was introduced as a research project by the well-known security researchers H.D. Moore and spoonm.


Metasploit was designed for security research and assessments

Contains numerous exploits to be used

Can target applications and many operating systems

Is command line but also has web interface

SYBEX

# Summary

- Enumeration follows scanning.
- Enumeration seeks to reveal information from a system.
- Enumeration is an active measure.
- Information can include usernames, group information, printer data, and other data.

SYBEX