Enumeration is a process which creates an active connection with the target hosts for discovering potential attack vectors, or for further exploiting the system.

It is used to gather the following:

* Hostnames
* Usernames, group names
* IP tables and routing tables
* Application and banners
* Network shares and services
* Audit configurations and service settings
* DNS and SNMP details

**Importance of Enumeration**

Enumeration is often considered to be an important phase during penetration testing, since its outcome can directly be used to exploit the system

**Classifying Enumeration**

**Network Basic Input Output System (NetBIOS)**

NetBIOS runs on port 139 on Windows OS. On a remote machine, an attacker is able to perform the following:

* read or write to a remote machine, depending on sharing availability
* launch a Denial of Service (DoS) attack on remote machine
* enumerate password policy on remote machine.

To prevent NetBIOS enumeration attacks, we can perform the following security controls:

* remove printer and file sharing in Windows operating systems
* minimize attack surface by limiting unnecessary services

**Simple Network Management Protocol (SNMP)**

SNMP is used to manage network devices. Default SNMP password allows an attacker to modify or view the configuration settings. An attacker can enumerate SNMP on a remote network device for:

* ARP and routing
* Device-specific information
* Network resources information
* Traffic statistics

To prevent SNMP enumeration attacks, we can perform the following security controls:

* Change public default community strings
* Minimise attack surface by removing SNMP agents where they aren’t required
* Implement a group policy to restrict anonymous connections
* Implement firewalls
* Encrypt and authenticate with IPSEC

**Light-Weight Directory Access Protocol (LDAP)**

LDAP is an internet protocol to access distributed directories like Open LDAP or Active Directory. It supports remote anonymous server queries, which disclose critical information such as username, contact details, address, etc.

To prevent LDAP enumeration attacks, we can perform the following security controls:

* Use SSL for encrypting LDAP communication
* Restrict brute-force attacks by enabling account lockout
* Restricting access to known users by using Kerberos

**Network Time Protocol (NTP)**

NTP was designed to synchronize clocks of computers in a network. An attacker is able to enumerate the following information by communicating with an NTP server

* IP addresses, operating systems and hostnames of internal client
* List of hosts connected to the server

To prevent NTP enumeration attacks, we can perform the following security controls:

* Filter traffic with IPTables
* Enable logging for events and messages
* Restrict NTP usage and enable NTPSec when possible

**Simple Mail Transfer Protocol (SMTP)**

SMTP is designed for email transmissions. It provides three commands that are built-in. the SMTP servers respond variably to each of the commands and enumeration is possible due to these varied responses. An attacker can determine a valid user with the same method.

Aardwolf Security provides many different penetration testing options, get it touch with us for a [web Application pen test quote](https://aardwolfsecurity.com/).