6.1.5 Enumeration Facts

The word enumerate means to list items one by one. During the enumeration phase of ethical hacking, you will extract and record as much information as you can about a network or system.

This lesson covers the following topics:

- Enumeration processes
- Windows enumeration
- Linux enumeration
- Enumeration tools

Enumeration Processes

Now that you have been able to establish active connections, you can gather information about usernames, group names, machine names, routing tables, network shares, applications, and more. Unlike the more passive phases of reconnaissance and scanning, we are moving into a more active approach to information gathering. The odds of getting caught are even higher now. You'll want every action to be strategic and precise.

It's also important to note that although you're still only gathering information, you're at the point where your actions could be considered illegal. Make sure your permission documentation is in order.

Process	Description
Extract email IDs	An email address contains two parts, the username and the domain name.
Use default passwords	All devices have default passwords. These passwords are often left in place, providing an easy access point for an attacker.
Attack directory services	A directory service is a database of information that is used for network administration. Some directories are vulnerable to input verification deficiencies. Because of this, they are susceptible to brute force attacks. These attacks are usually automated. The program tries different combinations of usernames and passwords until it finds something that works.
Exploit SNMP	The Simple Network Management Protocol (SNMP) is used to manage devices such as routers, hubs, and switches. SNMP works with an SNMP agent and an SNMP management station. The agent is found on the device that is being managed, and the SNMP management station serves as the communication point for the agent. SNMP has two configuration passwords by default, one for public access, and one for private access. The public community string includes the configuration of the device or system. The private read/write community string provides read and write access to the device configuration. If the passwords were not changed from the default, a hacker will have access to these strings and therefore have access to usernames, information about network devices, routing tables, network traffic, and file shares.
Exploit SMTP	Simple Mail Transfer Protocol (SMTP) is the protocol used by most email servers and clients to send email messages. Scanning tools and commands can be used to verify the existence of specific email addresses. They can even provide a list of all users on a distribution list.
Perform DNS zone transfers	DNS zone transfer is the process of transferring a copy of the DNS zone file from the primary DNS server to a secondary DNS server. Zone transfers are designed to provide updated network and access information to DNS servers. This type of structural data could be valuable to a hacker. It could be used to provide a mapping of the network. To perform a DNS zone transfer, the hacker, pretending to be a client, sends a zone transfer request to the DNS server. The DNS server then sends a portion of its database as a zone to the hacker. This zone may contain a lot of information about the DNS zone network.
Retrieve system policies	Large networks, especially enterprise environments, frequently have policy settings in place to determine how security matters are handled. If you're able to gain access to these settings, you will know more about your target. The technique will vary depending on the operating system that you are targeting.
Enumerate IPsec	IPsec uses ESP (Encapsulation Security Payload), AH (Authentication Header), and IKE (Internet Key Exchange) to secure communication between virtual private network (VPN) endpoints. Using enumeration tools, hackers can pull sensitive information such as the encryption and hashing algorithm, authentication type, and key distribution algorithm.
Enumerate VoIP	VoIP uses SIP (Session Initiation Protocol) to enable voice and video calls over an IP network. SIP service generally uses UDP/TCP ports 2000, 2001, 5050, 5061.
Enumerate RPC	Remote Procedure Call (RPC) allows client and server to communicate in distributed client/server programs. Enumerating RPC endpoints enable hackers to identify any vulnerable services on these service ports. You can use the following nmap scan commands

	to identify RPC services running on the network: - **nmap -sR IP/network** - **map -T4 –A IP/network**

Windows Enumeration

In Windows, a user account is an object that contains information about a user, the user access level, groups the user is a member of, and user access privileges. The default Windows installation includes two primary user accounts, the administrator and the guest. There are also a few other built-in accounts that are designed to run background processes as needed. These include local service, network service, and system.

User	Description
Guest	The guest account has been part of Windows for quite some time. By design, this account has remained pretty much the same and is meant to be used only in very limited circumstances. Although included in the Windows installation, it is not enabled by default.
Administrator	The administrator account has gone through quite a few changes as the operating system has evolved. In earlier versions of Windows, the administrator account was enabled by default. However, in more recent releases, Windows Vista and beyond, the administrator account has been disabled by default. This change was made primarily for security purposes. The administrator account was often used as a normal user account and, as a result, the everyday user had unlimited access to permissions that the user didn't necessarily know what to do with. If malware or other applications were running in the background, those programs also had access to those unlimited permissions. As you can imagine, that doesn't end well. Current versions of Windows require user accounts to be created. Although you can enable administrator privileges to the account, additional permission needs to be granted when elevated administrator privileges are needed. This way, the user cannot unintentionally allow an unwanted application or process to run in the background.
Local service	This account provides high-level access to the local machine, but only limited access to the network.
Network service	This account provides normal access to the network, but provides only limited access to the local machine.
System	This account provides almost unlimited access to the local machine.

Windows provides an efficient way of managing user control access. Users can be assigned to groups and permissions can be assigned to these groups. You can create your own groups based on departments, locations, or other methods. Microsoft also includes a few preconfigured user groups. These groups can be used as-is or modified to suit your needs.

Group	Description
Anonymous logon	This group provides anonymous access to resources, typically on a web server or web application.
Batch	This group is used to run scheduled batch tasks.
Creator group	A Windows 2000-specific group, the Creator group is used to grant permissions to users who are members of the same group as the creator of a directory or file.
Creator owner	The file or directory creator is a member of this group. By default, all releases after Windows 2000 use this group to grant permissions to the creator of the file or directory.
Everyone	All users are members of this group. It is used to provide wide-range access to resources.
Network	All users that access a system through a network are members of this group. It provides all remote users access to a specific resource.

Although we typically think of the username as being the unique identifier, behind the scenes, Windows actually relies on a security identifier (SID). When a user object is created, Windows assigns it an SID. And, unlike a username, that ID cannot be used again. Why is this necessary? Consider how many times a username could undergo a change. If permissions were tied to a specific name, a new account would have to be created every time. However, since Windows is looking at the SID, you simply adjust the username and maintain the same SID.

SID identifiers can help you know more about the account. For example, if you find an account ending in 500, then you've found the built-in administrator account. If you find an account ending in 501, you've found the built-in guest account. The Windows Security Accounts Manager (SAM) is a part of the system registry and stores all usernames and passwords. The passwords are not saved in plain text, of course, but are encrypted in LM and NTLM hash formats. For larger networks, Microsoft's Active Directory manages this data.

Linux Enumeration

A user account is needed to access a Linux system. When a user account is created, the values are stored in the etc/passwd file. This file is accessible with a text editor.

Value	Description
Username	A username and user ID (UID) are used to identify users. When a username is created, it is given a UID. This number is selected from a range of numbers, typically above 500.
Password	Each account has a password that is encrypted and saved on the computer or on the network.
Groups	Groups are used to manage permissions and rights. Group identification numbers (GIDs) are stored in the /etc/passwd file. All users are assigned to the default primary group and can be assigned to additional groups that are called secondary groups. Secondary groups are listed in the /etc/group file.

Enumeration Tools

The following table lists enumeration tools.

Tool	Description
finger	The Linux finger command provides information about a user. Use **finger –s *username*** to obtain the specified user's login name, real name, terminal name and write status, idle time, login time, office location, and office phone number. You can use **finger –s** to obtain the same information about all users on a system. Use **finger –l user@host** to obtain information about all users on a remote system.
NULL session	Null sessions are created when no credentials are used to connect to a Windows system. They are designed to allow clients access to limited types of information across a network. These sessions can be exploited to find information about users, groups, machines, shares, and host SIDs. A hacker can enter **net use //hostname/ipc$** ***hostname*****ipc$ “” /user:”“** to connect to a system. A hacker can use the command **net view** \\***hostname*** to display shares available on a system. The command **net use s:** \\hostname\shared folder name allows a hacker to connect to and view one of these shares.
PsTools	*PsTools* is a suite of very powerful tools that allow you to manage local and remote Windows systems. The package includes tools that can change account passwords, suspend processes, measure network performance, dump event log records, kill processes, or view and control services.
SuperScan	SuperScan can be used to enumerate information from a Windows host. Information can be gathered on the following: NetBIOS name table, services, NULL session, trusted domains, MAC addresses, logon sessions, workstation type, account policies, users, and groups.

TestOut Corporation All rights reserved.