**Enumeration**

An attacker creates active connections with the system and sends directed queries to gain more information about the target. Collected information can be used to identify vulnerabilities. This technique works in an intranet environment.

Example: During enumeration, attackers may stumble upon a remote inter-process communication (IPC) share, such as IPC$ in Windows, which they can probe further to connect to an administrative share by brute-forcing admin credentials and obtain complete information about the file-system listing that the share represents.

**🡺 What type of information can be collected?**

* Network resources
* Network shares, Routing tables
* Audit and service settings
* SNMP and fully qualified domain name (FQDN) details
* Machine names
* Users and groups
* Applications and banners

**🡺 Techniques, how can we get information’s:**

* Extract usernames using email IDs

Username@domainname

* Using default passwords
* Brute forcing Active Directory (AD)
* DNS Zone Transfer
* Extracting user groups from windows

Note1: attacker should have ID in Active Director.

Note2: This can be achieved after brute forcing Active Directory

* Extracting username using Simple Network Management Protocol (SNMP)

**🡺 TCP/UDP ports that can be enumerated include the following:**

* TCP/UDP 53: DNS Zone Transfer

ADM Worm & Bonk Trojan can be used

* TCP/UDP 135: Microsoft RPC Endpoint Mapper

DoS attack can be used

* UDP 137: NetBIOS Name Service (NBNS)

Attacker attacks on name server first

* TCP 139: NetBIOS Session Service (SMB over NetBIOS)

Improperly managed TCP 139 p0rt can allow unauthorized access to the attacker

* TCP/UDP 445: SMB over TCP (Direct Host)

Directly hosted SMB traffic uses port 445 (TCP and UDP) instead of NetBIOS

* UDP 161: Simple Network Management Protocol (SNMP)

The agent receives requests on port 161 from the managers and responds to the managers on port 162

* TCP/UDP 389: Lightweight Directory Access Protocol (LDAP)

LDAP uses TCP or UDP as its transport protocol over port 389

* TCP 2049: Network File System (NFS)

privilege escalation, inject backdoors or malware on a remote host can be used

* TCP 25: Simple Mail Transfer Protocol (SMTP)mail delivery protocol
* TCP/UDP 162: SNMP Trap

It sends optional variable bindings and the sysUpTime value from an agent to a manage

* UDP 500: Internet Security Association and Key Management Protocol (ISAKMP)/Internet Key Exchange (IKE)
* It can be used to establish, negotiate, modify, and delete SAs and cryptographic keys in a virtual private network (VPN) environment.
* TCP 22: Secure Shell (SSH)

Attackers may exploit the SSH protocol by brute-forcing SSH login credentials

* TCP/UDP 3268: Global Catalog Service(GCS)

Administrators use this port for troubleshooting issues in the Global Catalog by connecting to it using LDAP.

* TCP/UDP 5060, 5061: Session Initiation Protocol (SIP)

5060 (non-encrypted signalling traffic) or 5061 (encrypted traffic with TLS) for SIP to servers and other endpoints.

* TCP 20/21: File Transfer Protocol

sniffing of FTP traffic and FTP brute-force attacks can be used

* TCP 23: Telnet

It transmits login credentials in the cleartext format.

banner grabbing on other protocols such as SSH and SMTP, brute-forcing attacks on login credentials, port-forwarding attacks can be used

* UDP 69: Trivial File Transfer Protocol (TFTP)

Attackers may exploit TFTP to install malicious software or firmware on remote devices

* TCP 179: Border Gateway Protocol (BGP)

dictionary attacks, resource-exhaustion attacks, flooding attacks, and hijacking attacks can be used

**🡺 Services that can be enumerated**

**NetBIOS Enumeration**

Imp Ports: UDP-137, UDP-138, TCP-139

NetBIOS is considered first for enumeration because it extracts a large amount of sensitive information about the target network, such as users and network shares. The first step in enumerating a Windows system is to take advantage of the NetBIOS API.

The NetBIOS name is a unique 16-character ASCII string assigned to Windows systems to identify network devices over TCP/IP; 15 characters are used for the device name, and the 16th is reserved for the service or record type.

NetBIOS uses UDP port 137 (name services), UDP port 138 (datagram services), and TCP port 139 (session services).

An attacker who finds a Windows system with port 139 open can check to see which resources can be accessed or viewed on a remote system.

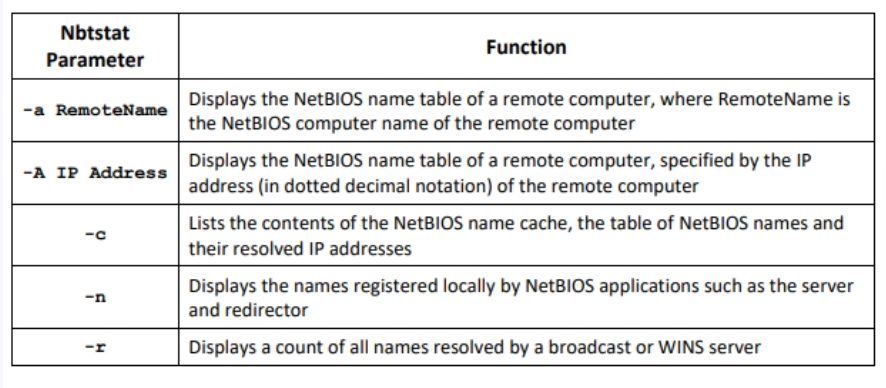
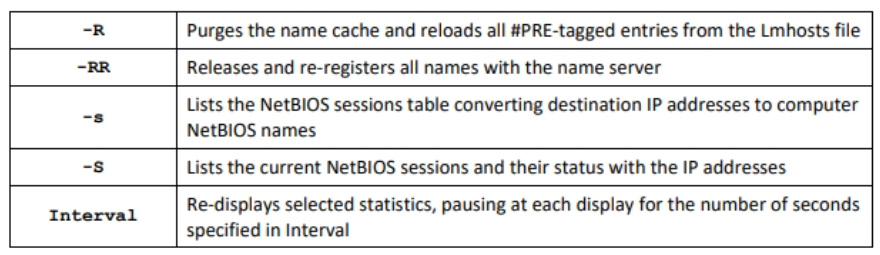
🡺 **What attackers obtain using NetBIOS**

* The list of computers that belong to a domain
* The list of shares on the individual hosts in a network
* Policies and passwords

The nbtstat command removes and corrects preloaded entries using several case-sensitive switches.

syntax:

**nbtstat [-a RemoteName] [-A IP Address] [-c] [-n] [-r] [-R] [-RR] [-s] [-S] [Interval]**



**nmap -sV -v --script nbstat.nse <target IP address>**attacker uses this Nmap command to perform NetBIOS enumeration on a target host

Enumerating Shared Resources Using Net Viewnet view \\<computername> computername is IP

net view \\<computername> /ALL

net view /domain

net view /domain:<domain name>

**SNMP Enumeration**

Imp port: UDP-161, UDP-162

SNMP🡪 Simple Network Management Protocol

SNMP has many security vulnerabilities, such as a lack of auditing.

SNMP enumeration is the process of creating a list of the user’s accounts and devices on a target computer using SNMP.

SNMP management station sends requests to the agent; after receiving the request, the agent replies.

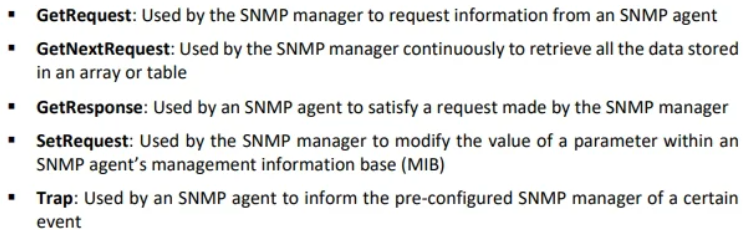
It contains the following two passwords for configuring and accessing the SNMP agent from the management station:

* Read community String (Public) 🡪 configurations can only be viewed using this password
* Read/Write community strings (Private) 🡪 configuration can be changed or edited using this password.

**Example:** When administrators leave the community strings at the default setting, attackers can use these default community strings (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, and shares as well as network information such as ARP tables, routing tables, device-specific information, and traffic statistics.

**🡪 Commands associated with SNMP:**

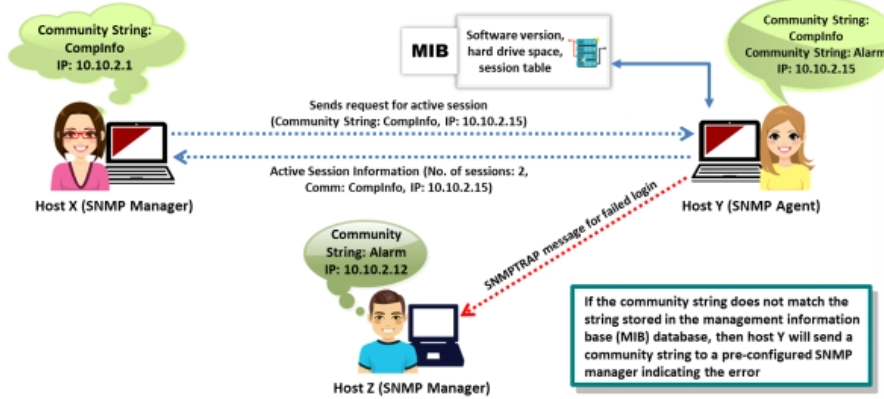
****

**Management Information Base (MIB)**

MIB is a virtual database containing a formal description of all the network objects that SNMP manages. MIB elements are recognized using object identifiers (OIDs).

A user can access the contents of the MIB by using a web browser either by entering the IP address and Lseries.mib or by entering the DNS library name and Lseries.mib.

**🡪 SNMP Process**



Tool:- SNMP check

Syntax: **snmp-check IP Address**

Snmpcheck is an open-source tool distributed under the GNU General Public License (GPL).

Tool:- SoftPerfect Network Scanner, OpUtils, Engineer’s Toolset

**LDAP Enumeration**

Imp ports: UDP/TCP-389

LDAP 🡪 Lightweight Directory Access Protocol

LDAP is one such protocol that accesses the directory listings. LDAP accesses directory listings within Active Directory or from other directory services.

Using this method, we can enumerate user details such as first name, last name, email address, designation, office location, and telephone number.

It uses DNS for quick lookups and the fast resolution of queries.

The Basic Encoding Rules (BER) format is used to transmit information between the client and server.

An attacker can anonymously query the LDAP service for sensitive information such as usernames, addresses, departmental details, and server names, which an attacker can use to launch attacks.

**Tools:-** Softerra LDAP Administrator, LDAP Admin Tool, JXplorer, Active Directory (AD) Explorer

**NTP Enumeration**

Imp port: UDP-123

NTP 🡪 Network Transfer Protocol

NTP is designed to synchronize clocks of networked computers. NTP can maintain time within an error of 10 ms over the public Internet. Furthermore, it can achieve an accuracy of 200 μs or better in LANs under ideal conditions.An attacker can obtain by querying an NTP server:

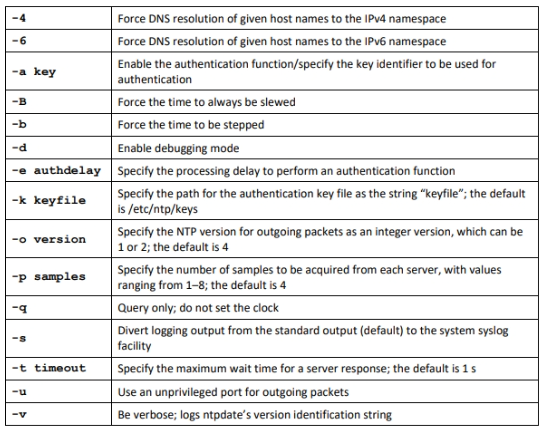
* List of hosts connected to the NTP server
* Clients’ IP addresses in the network, their system names, and OSs
* Internal IPs, if the NTP server is in the demilitarized zone (DMZ)

**🡪 NTP Enumeration Commands**

**ntpdate**

attacker uses this command to collects the number of time samples from several time sources.

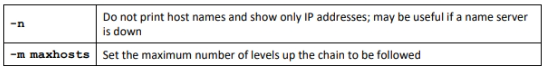
Syntax:

**ntpdate [-46bBdqsuv] [-a key] [-e authdelay] [-k keyfile] [-o version] [-p samples] [-t timeout] [ -U user\_name] server [...]**

**ntptrace**

Attackers use this command to trace the list of NTP servers connected to the network.

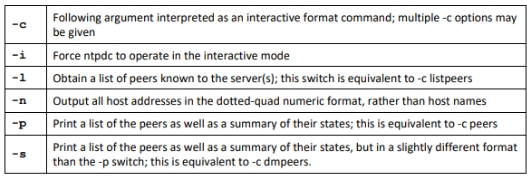
Syntax:

**ntptrace [-n] [-m maxhosts] [servername/IP\_address]**

**Ntpdc**

This command queries the ntpd daemon about its current state and requests changes in that state. Attackers use this command to retrieve the state and statistics of each NTP server connected to the target network.

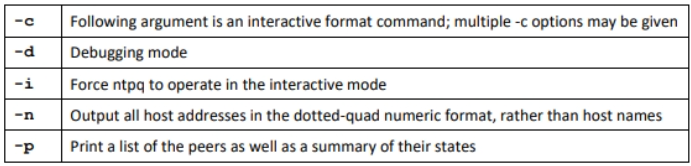
Syntax:

**ntpdc [-ilnps] [-c command] [hostname/IP\_address]**

**ntpq**

This command monitors the operations of the NTP daemon ntpd and determines performance.

Syntax:

**ntpq [-inp] [-c command] [host/IP\_address]**

**Tools for NPS Enumeration:** PRTG Network Monitor

**NFS Enumeration**

Imp Ports: TCP-2049

NFS 🡪 Network File System

NFS is used for the management of remote file access.

An NFS system is generally implemented on a computer network in which the centralization of data is required for critical resources. The remote procedure call (RPC) is used to route and process the request between clients and servers.

The /etc/exports location on the NFS server contains a list of clients allowed to share files on the server.

To access the server, the only credential used is the client’s IP address. NFS versions before version 4 run on the same security specification.

NFS enumeration helps attackers to gather information such as a list of clients connected to the NFS server, along with their IP addresses, and exported directories.

command to scan the target IP address for an open NFS port (port 2049) and the NFS services running on it:

**rcpinfo -p IP address**

command to view the list of shared files and directories:

**showmount -e IP address**

Tools:

* RPCScan

It communicates with RPC services and checks misconfigurations on NFS shares.

**Python3 rpc-scan.py 10.10.10.19 --rpc**

* SuperEnum

An attacker uses the ./superenum script and then enters a text file name “Target.txt” having a target IP address or a list of IP addresses for enumeration.

**SMTP Enumeration**

Imp Ports: TCP-25, TCP-2525, TCP-587

SMTP 🡪 Simple Mail Transfer Protocol

Mail systems commonly use SMTP with POP3 and IMAP, which enable users to save messages in the server mailbox and download them from the server when necessary. SMTP uses mail exchange (MX) servers to direct mail via DNS.

SMTP provides the following three built-in commands:

* VRFY: Validate users
* EXPN: Displays the actual delivery addresses of aliases and mailing list
* RCPT TO: Defines the recipients of the message

Attackers can directly interact with SMTP via the Telnet prompt and collect a list of valid users on the SMTP server.Administrators and pen testers can perform SMTP enumeration using command-line utilities such as Telnet and netcat or by using tools such as Metasploit, Nmap, NetScanTools Pro, and smtp-user-enum to collect a list of valid users, delivery addresses, message recipients, etc.

Tools:

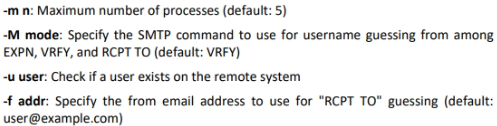
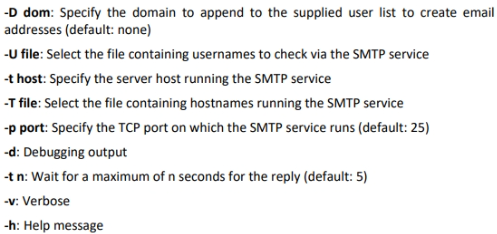
* NetScanTools Pro

Attackers use NetScanTools Pro for SMTP enumeration and extract all the email header parameters, including confirm/urgent flags. Can also record the email session in a log file

* smtp-user-enum

Enumeration is performed by inspecting the responses to VRFY, EXPN, and RCPT TO commands.

Syntax:

**smtp-user-enum.pl [options] (-u username|-U file-of-usernames) (-t host|-T file-of-targets)**

**DNS Enumeration using Zone Transfer**

Imp ports: TCP/UDP-53

DNS 🡪 Domain Name Server

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.

An attacker performs DNS zone transfer enumeration to locate the DNS server and access records of the target organization. If the DNS server of the target organization allows zone transfers, then attackers can perform DNS zone transfer to obtain DNS server names, hostnames, machine names, usernames, IP addresses, aliases, etc. assigned within a target domain.

An attacker attempts to retrieve a copy of the entire zone file for a domain from the DNS server. If the DNS transfer setting is enabled on the target name server, it will provide the DNS information; else, it will return an error stating it has failed or refused the zone transfer.

**🡪 Tools for DNS Enumeration using Zone Transfer:**

* dig Commands
* **dig ns <target domain>**

command retrieves all the DNS name servers of the target domain.

* **dig @<domain of name server> <target domain> axfr**

command to test whether the target DNS allows zone transfers.

* nslookup
* **nslookup**

**set querytype=soa**

**<target domain>**

command sets the query type to the Start of Authority (SOA) record to retrieve administrative information about the DNS zone of the target domain

* **/ls -d <domain of name server>** command is used to attempt to transfer the zone of the specified name server
* DNSRecon

**dnsrecon -t axfr -d <target domain>**

Command to check all NS records of the target domain for zone transfers.

-t specifies the type of enumeration to be performed

-d specifies the target domain

axfr specifies the type of enumeration in which all NS servers are tested for a zone transfer

**DNS Cache Snooping**

DNS cache snooping is a type of DNS enumeration technique in which an attacker queries the DNS server for a specific cached DNS record.

By using this cached record, the attacker can determine the sites recently visited by the user. This information can further reveal important information such as the name of the owner of the DNS server, its service provider, the name of its vendor, and bank details.

By using this information, the attacker can perform a social engineering attack on the target user.

🡪 **Tools for DNS Cache Snooping**

Non-Recursive Method

n this method, to snoop on a DNS server, attackers send a non-recursive query by setting the Recursion Desired (RD) bit in the query header to zero. Attackers query the DNS cache for a specific DNS record such as A, CNAME, PTR, CERT, SRV, and MX. If the queried record is present in the DNS cache, the DNS server responds with the information indicating that some user on the system has visited a specific domain.

**dig @<IP of DNS server> <Target domain> A +norecurse**

+norecurse sets query to non-recursive

Recursive Method

In this method, to snoop on the DNS server, attackers send a recursive query by setting the +recurse option instead of the +norecurse option. Similar to the non-recursive method, the attackers query the DNS cache for a specific DNS record such as A, CNAME, PTR, CERT, SRV, and MX.

In this method, the time-to-live (TTL) field is examined to determine the duration for which the DNS record remains in the cache. Here, the TTL value obtained from the result is compared with the TTL that was initially set in the TTL field. If the TTL value in the result is less than the initial TTL value, the record is cached, indicating that someone on the system has visited that site. However, if the queried record were not present in the cache, it will be added to the cache after the first query is sent.

**dig @<IP of DNS server> <Target domain> A +recurse**

**DNSSEC Zone Walking**

DNSSEC 🡪 Domain Name System Security Extensions

DNSSEC zone walking is a type of DNS enumeration technique in which an attacker attempts to obtain internal records if the DNS zone is not properly configured. The enumerated zone information can assist the attacker in building a host network map.

This security feature uses digital signatures based on public-key cryptography to strengthen authentication in DNS. While DNSSEC provides Internet security, it is also susceptible to a vulnerability called zone enumeration or zone walking.

To overcome the zone enumeration vulnerability, a new version of DNSSEC that uses Next Secure version 3 (NSEC3) is used.

**🡪 Tools for DNSSEC Zone Walking:**

* LDNS

**ldns-walk @<IP of DNS Server> <Target domain>**

LDNS-walk enumerates the DNSSEC zone and obtains results on the DNS record files.

* DNSRecon

**dnsrecon -d <target domain> -z**

It performs NSEC zone enumeration to obtain DNS record files of a target domain.

**IPsec Enumeration**

Imp ports: UDP-500

IPsec is the most commonly implemented technology for both gateway-to-gateway (LAN-to-LAN) and host-to-gateway (remote access) enterprise VPN solutions.

Most IPsec-based VPNs use the Internet Security Association Key Management Protocol (ISAKMP), a part of IKE, to establish, negotiate, modify, and delete Security Associations (SA) and cryptographic keys in a VPN environment.

Attackers can perform simple direct scanning for ISAKMP at UDP-500 using following command

**nmap –sU –p 500 <target IP address>**

In this type of scan, specially crafted IKE packets with an ISAKMP header are sent to the target gateway, and the responses are recorded.

command for initial IPsec VPN discovery with ike-scan tool

**ike-scan –M <target gateway IP address>**

ke-scan discovers IKE hosts and can fingerprint them using the retransmission backoff pattern. ike-scan can perform the following functions:

* Discovery
* Fingerprinting
* Transform Enumeration
* User Enumeration
* Pre-shared key craking

**VoIP Enumeration**

Imp Ports: UDP/TCP-2000, 2001, 5050, 5061 under SIP Service

VoIP is an advanced technology that has replaced the conventional public switched telephone network (PSTN) in both corporate and home environments. VoIP uses internet infrastructure to establish connections for voice calls; data are also transmitted on the same network.

Attackers use Svmap and Metasploit tools to perform VoIP enumeration. Through VoIP enumeration, attackers can gather sensitive information such as VoIP gateway/servers, IP-private branch exchange (PBX) systems, and User-Agent IP addresses and user extensions of client software (softphones) or VoIP phones. This information can be used to launch VoIP attacks: DoS attacks, session hijacking, caller ID spoofing, eavesdropping, spam over Internet telephony (SPIT), and VoIP phishing (Vishing).

Command to enumerate SIP device details using svmap tool

**svmap <target network range>**

Attackers use Metasploit’s SIP Username Enumerator to scan numeric usernames/extensions of VoIP phones.

**RPC Enumeration**

Imp ports: TCP/UDP-111

RPC 🡪 Remote Procedure Call

(RPC) is a technology used for creating distributed client/server programs. RPC allows clients and servers to communicate in distributed client/server programs.

The portmapper service listens on TCP and UDP port 111 to detect the endpoints and present clients, along with details of listening RPC services.

Enumerating RPC endpoints enables attackers to identify any vulnerable services on these service ports. In networks protected by firewalls and other security establishments, this portmapper is often filtered. Therefore, attackers scan wide port ranges to identify RPC services, open to direct attack.

Tool:

* Zenmap

Commands to identify the RPC service running on the network

**nmap -sR <target IP/network>**

**nmap -T4 –A <target IP/network>**

* NetScanTools Pro

Capture the RPC information of the target network.

Detect and access the portmapper daemon/service that typically runs on port 111 of Unix or Linux machines.

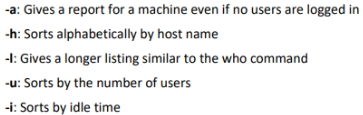
**Unix/Linux Enumeration**

Unix/Linux user enumeration provides a list of users along with details such as the username, host name, and start date and time of each session

Commands:

* rusers

displays a list of users who are logged in to remote machines or machines on the local network. Similar output as whoc command does but for the hosts/systems on local network.

**/usr/bin/rusers [-a] [-l] [-u| -h| -i] [Host ...]**

* rwho

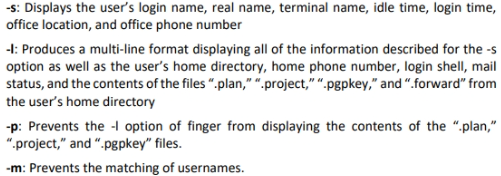
displays a list of users who are logged in to hosts on the local network. Similar output as whoc command does and contains information about the username, host name, and start date and time of each session for all machines on the local network

**rwho [ -a]**

a: Includes all users; without this flag, users whose sessions are idle for an hour or more are not included in the report

* finger

displays information about system users such as the user’s login name, real name, terminal name, idle time, login time, office location, and office phone numbers.

**finger [-l] [-m] [-p] [-s] [user ...] [user@host ...**

**Telnet Enumeration**

Imp port: TCP-23

Telnet is a network terminal protocol that allows users to access remote computers or servers over the Internet. This protocol provides two-way interactive communication for computers on LANs and the Internet.

Attackers perform port scanning to gather information regarding open ports and services on the target server. If the Telnet port is found to be open, attackers can learn about the information being shared, including hardware and software information of the target.

By using this information, attackers can exploit their specific vulnerabilities and perform a brute-force attack to gain unauthorized access to the target system. Attackers can use the Nmap tool to perform simple direct scanning for Telnet port 23.

Command:

To enumerate the Telnet service running on the target system

**nmap -p 23 <target domain>**

Attackers can enumerate information from remote Microsoft Telnet services with New Technology LAN Manager (NTLM) authentication enabled

**nmap -p 23 --script telnet-ntlm-info <target IP>**

Now attackers have information about target script they can perform a brute-force attack against the Telnet server

**nmap -p 23 –script telnet-brute.nse –script-argsuserdb=/root/Desktop/user.txt,passdb=/root/Desktop/pass.txt <target IP>**

**SMB Enumeration**

Imp ports: TCP-445

SMP 🡪 Server Message Block

SMB is a transport protocol that is generally used by Windows systems for providing shared access to files, printers, and serial ports as well as remote access to Windows services. It can also be run via NetBIOS API on UDP ports 137 and 138 and TCP ports 137 and 139.

SMB service also allows application users to read, write, and modify the files on the remote server. A network running this service is highly vulnerable to SMB enumeration, which provides a good amount of information about the target.

attackers generally perform banner grabbing to obtain information such as OS details and versions of services running. By using this information, attackers can perform various attacks such as SMB relay attacks and brute-force attacks.

Tools: Nmap, SMBMap, enum4linux, nullinux, and NetScanTool Pro

Nmap command to enumerate the SMB service running on the target IP address

**nmap -p 445 -A <target IP>**

-p specifies a port to scan

-A is used for OS detection, version detection, script scanning, and traceroute information

Using this command, attackers can also obtain details on the OS and traceroute of the specified target.

**FTP Enumeration**

Imp port: TCP-20, TCP-21

FTP 🡪 File Transfer Protocol

(FTP) is used to transfer files over TCP, and its default port is 21. In FTP, data are transferred between a sender and receiver in plaintext, exposing critical information such as usernames and passwords to attackers. FTP offers neither a secure network environment nor secure user authentication.

Attackers can scan and enumerate open port 21 running FTP services and further use this information to launch various attacks such as FTP bounce, FTP brute force, and packet sniffing.

Nmap command is used by the attackers to enumerate the FTP service running on the target domain

**nmap -p 21 <target domain>**Attackers also use Metasploit to enumerate FTP services running on remote hosts. The following commands can be used to detect the FTP version of the target server

**use auxiliary/scanner/ftp/ftp\_version**

**msf auxiliary(scanner/ftp/ftp\_version) > set RHOSTS <target IP>**

**msf auxiliary(scanner/ftp/ftp\_version) > exploit**

**TFTP Enumeration**

Imp port: UDP-69

TFTP 🡪 Trivial File Transfer Protocol

This protocol is used when directory visibility and user authentication are not required; therefore, it provides no security features.

Attackers use tools such as PortQry and Nmap to extract information such as running TFTP services and files stored on a remote server. By using the enumerated information, attackers can further gain unauthorized access to the target system, steal important files, and upload malicious scripts to launch further attacks. Furthermore, this information enables attackers to perform various attacks such as DNS amplification attacks, TFTP reflection attacks, and DDoS attacks.

Attackers use the PortQry command-line utility to perform TFTP enumeration using the following command

**portqry -n <target domain> -e 69 -p udp**

Attackers can use the Nmap tool to perform simple direct scanning for TFTP port 69 and to enumerate the TFTP service running on the target domain

**nmap -p 69 <target domain>**

**IPv6 Enumeration**

(IPv6) is an addressing protocol that identifies computer systems, including location information, and assists in routing traffic from one system to another system across a network.

Attackers perform IPv6 enumeration on target hosts to obtain their IPv6 addresses and further scan the enumerated IP addresses to detect various security problems such as access to routing structure, exposure of sensitive content, and users’ access control lists. By using this information, attackers can launch various attacks such as SYN flood attacks, DNS amplification attacks, and DDoS attacks.

Tool:

* ENYX

Enyx is an enumeration tool that fetches the IPv6 address of a machine through SNMP.

command to enumerate the IPv6 address of a target machine by setting the SNMP version to 2c and community string to public

**Python enyx.py 2c public <target IP>**

* IPv6 Hackit

Hackit is a scanning tool that provides a list of active IPv6 hosts. It can perform TCP port scanning and identify AAAA IPv6 host records

Attackers can specify the target machine and run a scan to enumerate the IPv6 information.

**BGP Enumeration**

Imp ports: 179

BGP 🡪 Border Gateway Protocol

BGP is a routing protocol used to exchange routing and reachability information between different autonomous systems (AS) on the Internet. Because this protocol is used to connect one AS to another ASs, it is also called external BGP (eBGP). BGP finds the shortest path to route traffic from one IP address to another efficiently. BGP creates its TCP session on port 179.

Attackers perform BGP enumeration on the target using tools such as Nmap and BGP Toolkit to discover the IPv4 prefixes indicated by the AS number and the routing path followed by the target. Attackers use this information to launch various attacks against the target, such as man-in-the-middle attacks, BGP hijacking attacks, and DoS attacks.

Tool: BGP Toolkit

It can be used to search for the target domain and obtain details such as DNS information, website information, IP information, AS information, and whois information.

command to enumerate BGP running on the target system

**nmap -p 179 <target IP>**

**Countermeasures**

**SNMP Enumeration Countermeasures**

* Remove the SNMP agent or turn off the SNMP service.
* If turning off SNMP is not an option, then change the default community string names.
* Upgrade to SNMP3, which encrypts passwords and messages.
* Implement the Group Policy security option called “Additional restrictions for anonymous connections.”Ensure that the access to null session pipes, null session shares, and IPsec filtering is restricted.Block access to TCP/UDP port 161.
* Do not install the management and monitoring Windows component unless required.
* Encrypt or authenticate using IPsec.  Do not misconfigure the SNMP service with read-write authorization.

**DNS Enumeration Countermeasures**

* Disable DNS zone transfers to untrusted hosts.
* Ensure that the private hosts and their IP addresses are not published in the DNS zone files of the public DNS server.
* Use premium DNS registration services that hide sensitive information such as host information (HINFO) from the public.
* Use standard network admin contacts for DNS registrations to avoid social engineering attacks.
* Prune DNS zone files to prevent revealing unnecessary information.

**SMTP Enumeration Countermeasures**

* Ignore email messages to unknown recipients.
* Exclude sensitive information on mail servers and local hosts in mail responses.
* Disable the open relay feature.
* Limit the number of accepted connections from a source to prevent brute-force attacks.
* Disable EXPN, VRFY, and RCPT TO commands or restrict them to authentic users.
* Ignore emails to unknown recipients by configuring SMTP ser

**LDAP Enumeration Countermeasures**

* By default, LDAP traffic is transmitted unsecured; therefore, use Secure Sockets Layer (SSL) or STARTTLS technology to encrypt the traffic.
* Select a username different from the email address and enable account lockout.
* Restrict access to Active Directory by using software such as Citrix.
* Use NTLM or any basic authentication mechanism to limit access to legitimate users.

**SMB Enumeration Countermeasures**

* Ensure that Windows Firewall or similar endpoint protection systems are enabled on the system.
* Install the latest security patches for Windows and third-party software.
* Implement a proper authentication mechanism with a strong password policy.
* Implement strong permissions to keep the stored information safe.
* Perform a regular audit of system logs.
* Perform active system monitoring to monitor the systems for any malicious incident.

**NFS Enumeration Countermeasures**

* Implement proper permissions (read/write must be restricted to specific users) in exported file systems.Implement firewall rules to block NFS port 2049.
* Ensure the proper configuration of files such as /etc/smb.conf, /etc/exports, and etc/hosts.allow to protect the data stored in the server.
* Log the requests to access the system files on the NFS server.
* Keep the root\_squash option in /etc/exports file turned ON so that no requests made as root on the client are trusted.
* Implement NFS tunneling through SSH to encrypt the NFS traffic over the network.

**FTP Enumeration Countermeasures**

* Implement secure FTP (SFTP, which uses SSH) or FTP secure (FTPS, which uses SSL) to encrypt the FTP traffic over the network.Implement strong passwords or a certification-based authentication policy.
* Ensure that the unrestricted uploading of files on the FTP server is not allowed.
* Disable anonymous FTP accounts. If this is not possible, monitor anonymous FTP accounts regularly.
* Restrict access by IP or domain name to the FTP server.
* Configure access controls on authenticated FTP accounts with the help of access control lists (ACLs).
* Restrict login attempts and time.
* Configure filtering rules for the FTP services.
* Use SSL/FTPS for authenticated FTP accounts.