**Enumeration**

**Index:**

|  |  |
| --- | --- |
| 1. **What is Enumeration** | 2 |
| 1. **Services and Ports to Enumerate** | 2 |
| 1. **NetBIOS Enumeration** | 3-5 |
| 1. **Enumerating Shared Resources Using Net View** | 5 |
| 1. **SNMP Enumeration** | 6-8 |
| 1. **LDAP Enumeration** | 8-9 |
| 1. **NDP Enumeration** | 9-10 |
| 1. **NFS Enumeration** | 10 |
| 1. **SMTP Enumeration (theory)** | 10 |
| 1. **DNS Enumeration** | 11-15 |
| 1. **DNS Cache Snoopng** | 15 |
| 1. **SMTP Enumeration (using Nmap)** | 16 |
| 1. **SMB and RPC Enumeration** | 16-18 |
| 1. **Enumerate information using Global Network Inventory** | 18-19 |
| 1. **Enumerate information using Advanced IP scanner** | 19-20 |
| 1. **Enumerate Information from Windows &amp; Samba Hosts using Enum4linux** | 20-21 |
| 1. **Enyx enumeration** | 21 |

**What is Enumeration?**

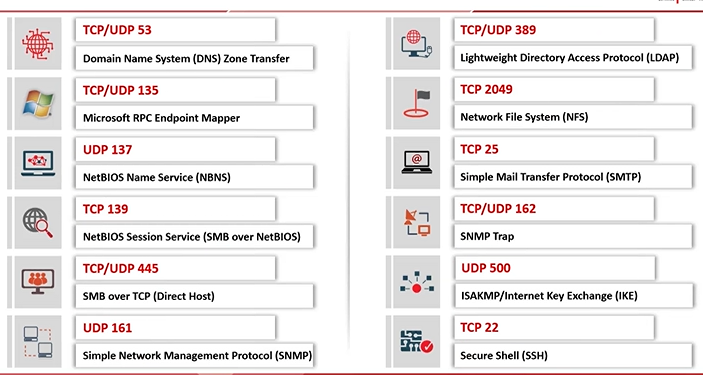
In ethical hacking and cybersecurity, enumeration is the process of actively gathering detailed information about a target’s network, services, or systems. It involves identifying user accounts, open ports, network shares, or vulnerabilities, often using tools like Nmap or NetBIOS. This step helps hackers or security professionals plan further attacks or defenses.

Here are several techniques commonly used for enumeration in ethical hacking and cybersecurity:

1. Network Scanning: Using tools like Nmap to identify active hosts, open ports, and services running on those ports.
2. Service Enumeration: Gathering information about the services running on identified ports, including version numbers and configuration details.
3. DNS Enumeration: Discovering subdomains, hostnames, and IP addresses using tools like DNSmap or DNSenum.
4. User Enumeration: Identifying valid usernames on a system through login attempts, directory listings, or specific error messages.
5. SNMP Enumeration: Using SNMP (Simple Network Management Protocol) queries to gather network device information, including device types, configurations, and running software.
6. NetBIOS Enumeration: Extracting information about Windows systems in a network, such as shares, users, and groups using tools like nbtscan.
7. LDAP Enumeration: Querying an LDAP (Lightweight Directory Access Protocol) directory to gather user, group, and organizational unit details.
8. HTTP Enumeration: Analyzing web servers for exposed directories, files, or services using tools like DirBuster or Burp Suite.
9. Email Enumeration: Collecting valid email addresses from a target domain using techniques like Google dorking or OSINT (Open Source Intelligence).
10. Vulnerability Scanning: Utilizing tools like Nessus or OpenVAS to identify known vulnerabilities in systems and applications.

These techniques help security professionals understand the attack surface and identify potential weaknesses before malicious actors exploit them.

**Services and Ports to Enumerate:**

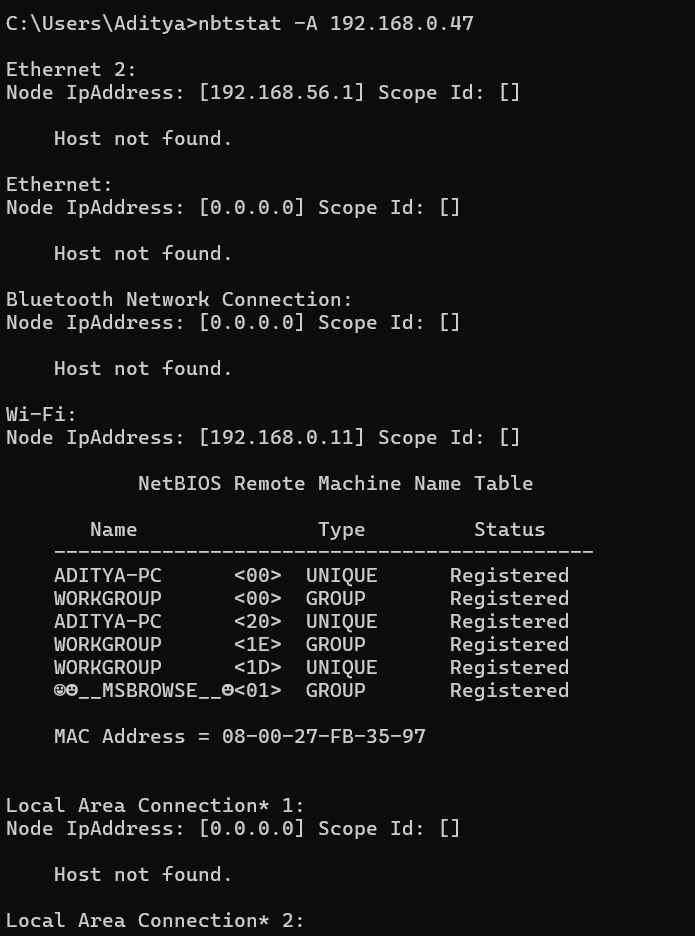


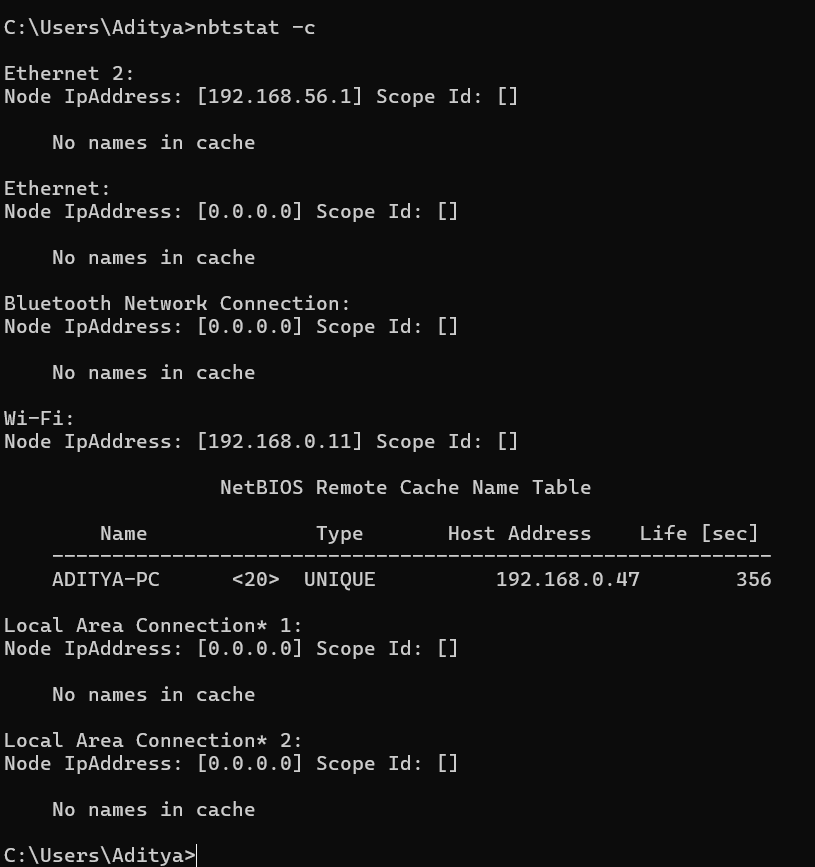
**NetBIOS Enumeration:**

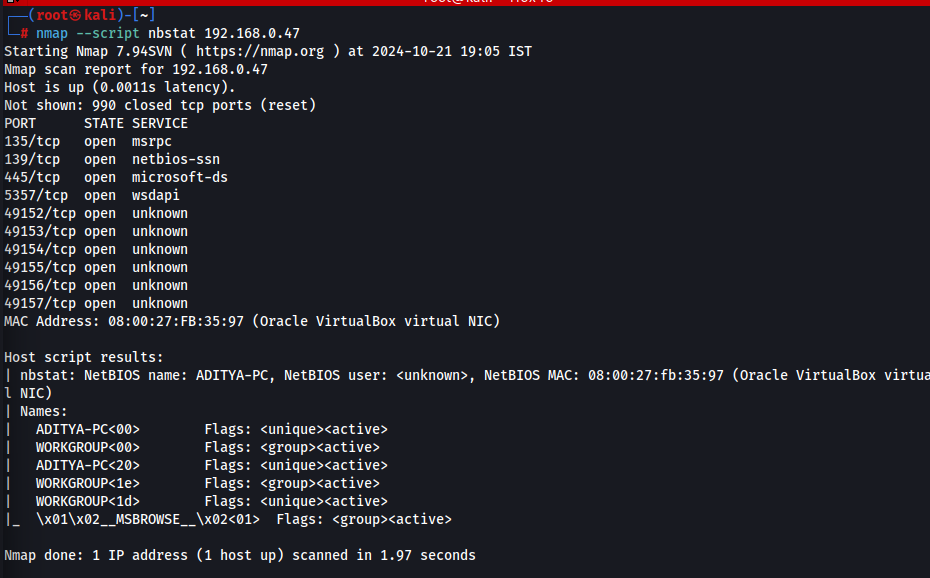
NetBIOS enumeration involves gathering information from Windows systems using the NetBIOS protocol. It helps identify active machines, shared resources, user accounts, and system details on a network. Tools like nbtstat and nbtscan facilitate this process, revealing potential vulnerabilities for further exploitation.

Reasons Hackers Use NetBIOS Enumeration:

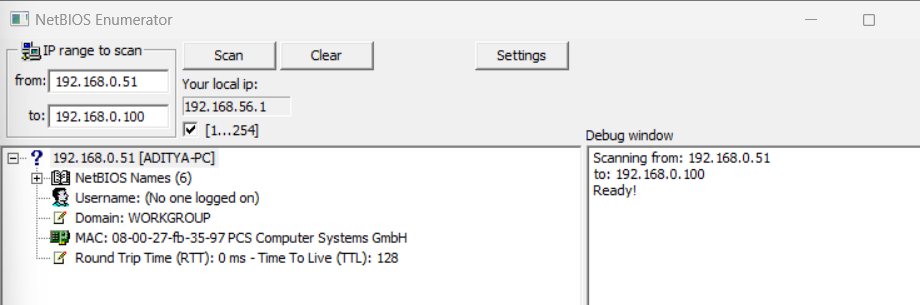
1. User Account Discovery: Hackers can find valid usernames, making it easier to conduct targeted attacks like password guessing or social engineering.
2. Network Resource Mapping: Identifying shared resources such as files and printers can reveal sensitive data or weak points for attacks.
3. Vulnerability Assessment: By understanding the systems and services in use, attackers can pinpoint unpatched vulnerabilities or misconfigurations to exploit.



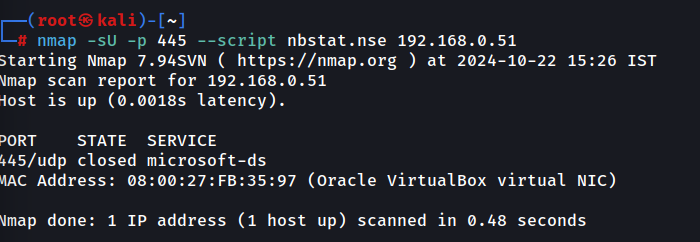
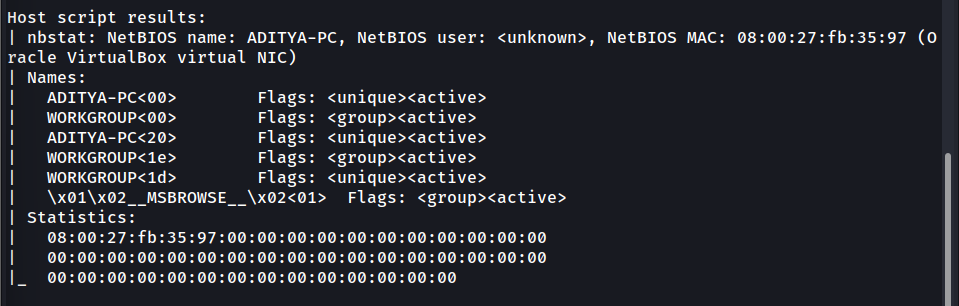
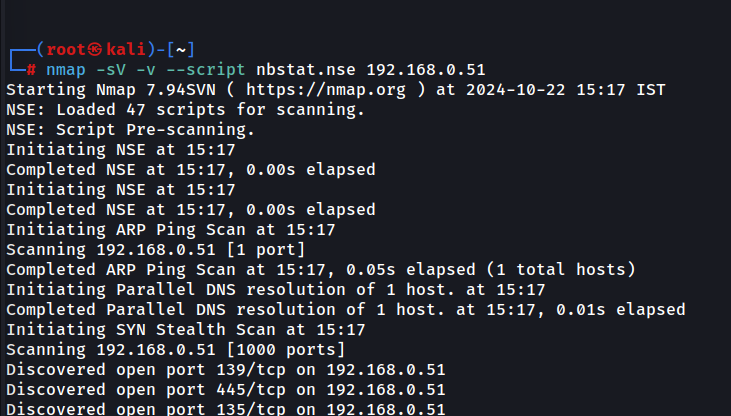




Now, using NETBIOS enumerator:



Using an NSE script:

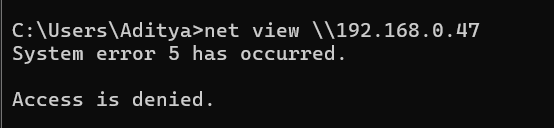


**Enumerating Shared Resources Using Net View:**

The **net view** command in Windows is used to enumerate shared resources on a network, such as files, folders, and printers. By targeting a specific machine or domain, it reveals accessible shares. Hackers leverage this command to identify exposed resources that may contain sensitive data or misconfigurations for exploitation.

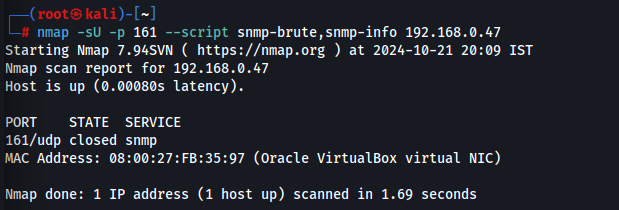
net view \\192.168.0.47

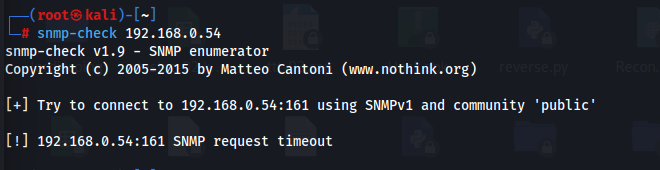
This lists all shared resources on the target machine.



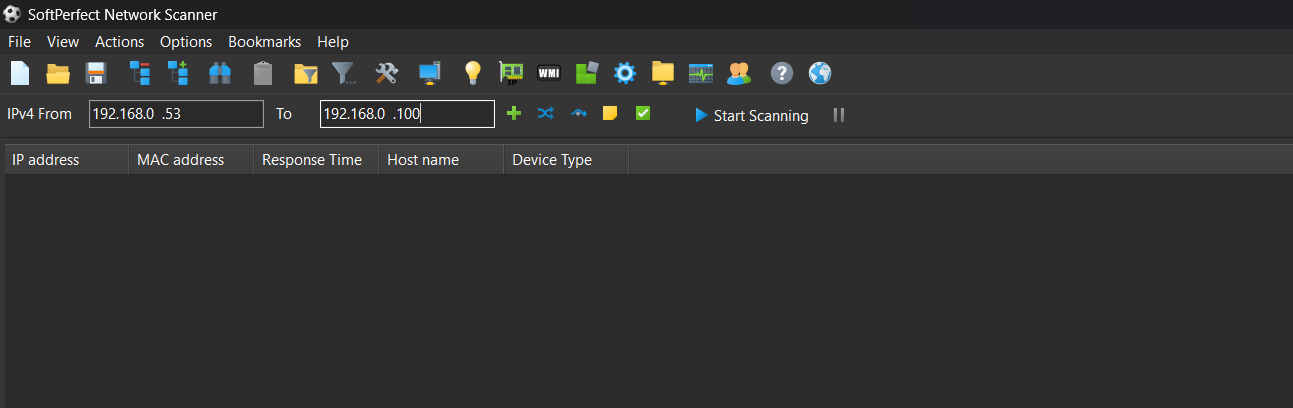
**SNMP Enumeration:**

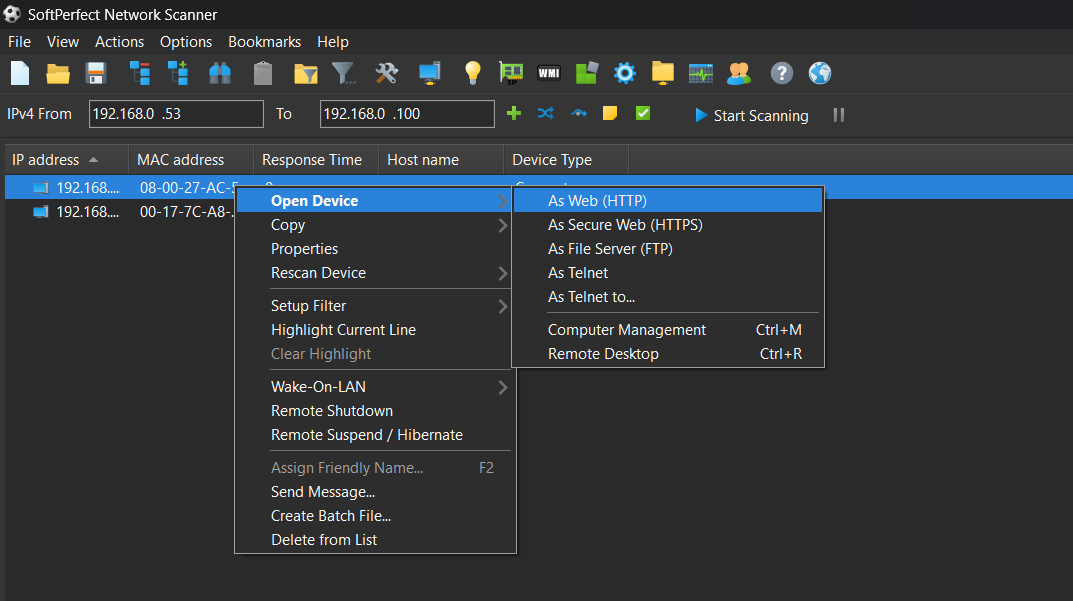
SNMP enumeration involves extracting detailed information about network devices (like routers, switches, or printers) using the Simple Network Management Protocol (SNMP). Attackers query public or misconfigured SNMP agents to gather system details, configurations, running services, and network topology, which can be exploited for further attacks. Tools include SNMPwalk and Onesixtyone.



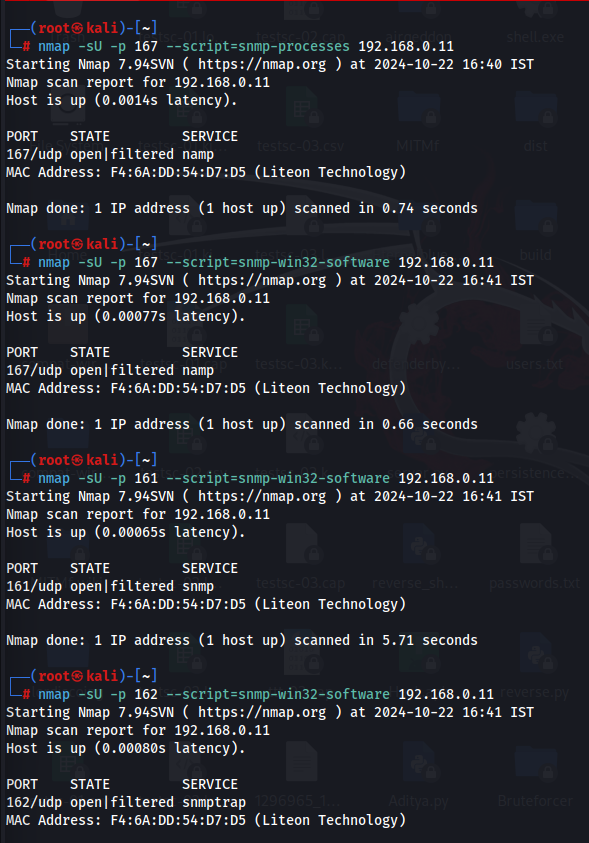
Using snmp-check: 

Using SoftPerfect Network scanner:





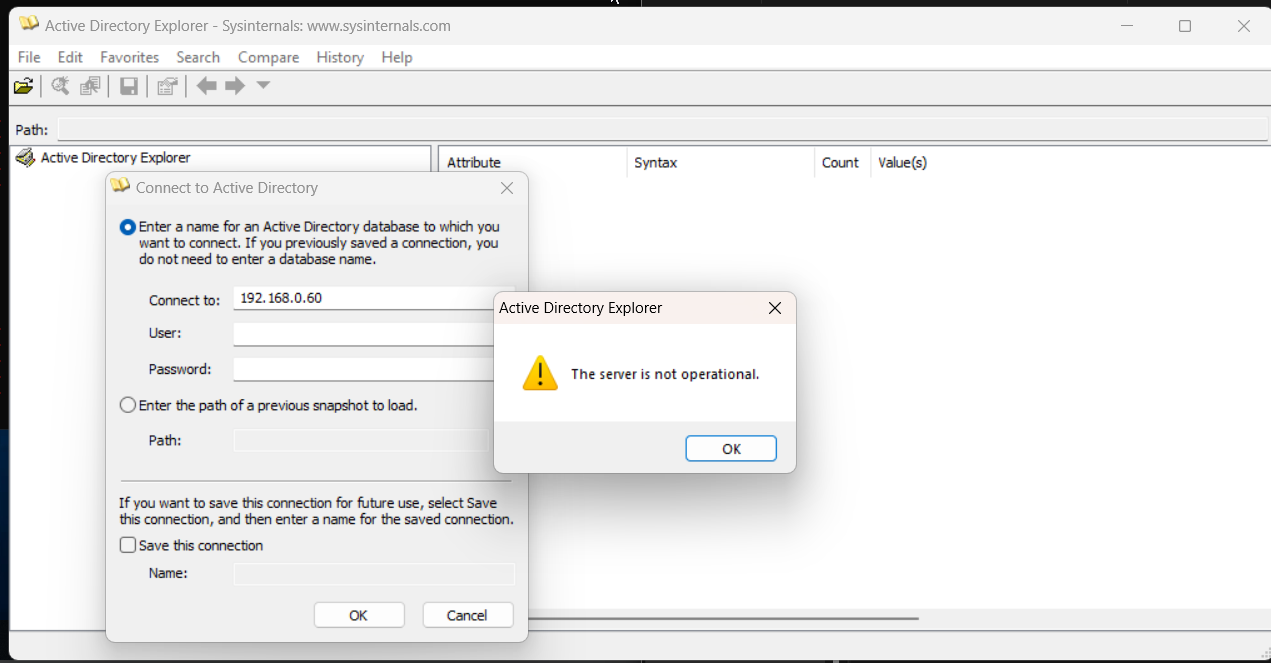
Using NMAP:



**LDAP Enumeration:**

LDAP enumeration involves querying the Lightweight Directory Access Protocol (LDAP) service to extract sensitive information such as usernames, groups, organizational units, and policies from directory services (e.g., Microsoft Active Directory). Attackers exploit misconfigurations to gather intelligence for privilege escalation, lateral movement, or password attacks. Tools include ldapsearch and ADExplorer.

Using AD explorer:



**NTP Enumeration:**

NTP enumeration involves querying the Network Time Protocol (NTP) service, typically on UDP port 123, to gather information such as system time, network devices, and connected clients. Attackers use tools like ntpq and Nmap to identify misconfigured NTP servers, which can aid in reconnaissance or be exploited for amplification attacks (DDoS).

Here are common NTP enumeration commands used for gathering information from NTP servers:

Nmap NTP Enumeration:

bash

nmap sU p 123 script ntpinfo <target\_ip>

Queries NTP servers to retrieve version and configuration details.

ntpq Command:

bash

ntpq p <target\_ip>

Displays the list of peers and their synchronization status with the target NTP server.

ntpdate Command:

bash

ntpdate q <target\_ip>

Queries the time from the NTP server without setting the local clock.

NTPv3 Mode 6 Query (ntpdc):

bash

ntpdc c monlist <target\_ip>

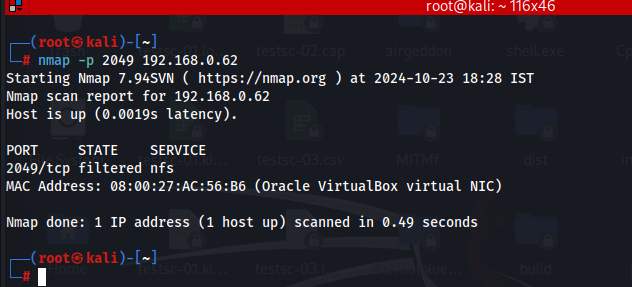
Retrieves the list of clients connected to the NTP server (if vulnerable).

**NFS Enumeration:**

NFS enumeration involves discovering and analyzing shared directories exported by a Network File System (NFS) server. Attackers use tools like showmount to list accessible shares and check permissions. Misconfigured NFS shares can expose sensitive files or allow unauthorized access, leading to privilege escalation or lateral movement within a network.

Works on port 2049.

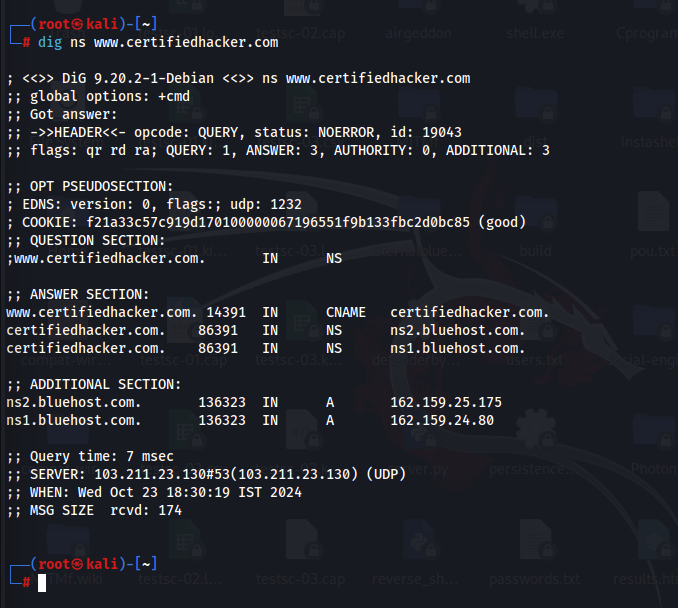
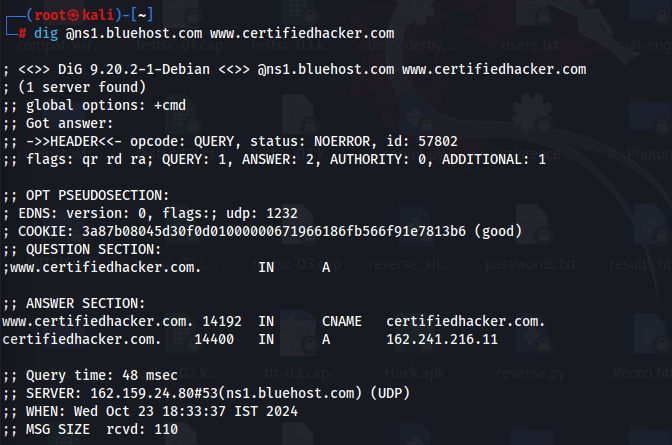
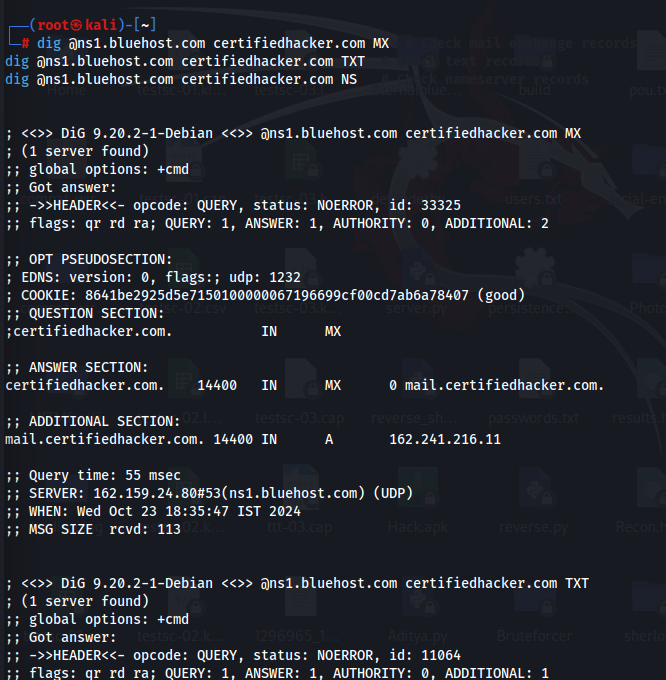
Using nmap:



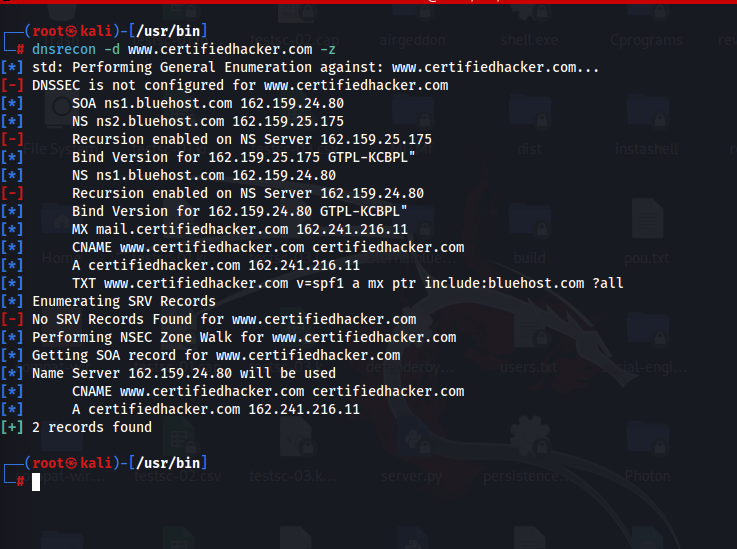
**SMTP Enumeration:**

SMTP enumeration is the process of gathering information from an SMTP (Simple Mail Transfer Protocol) server to identify valid email addresses, users, or server configurations. Attackers use commands like `VRFY`, `EXPN`, or `RCPT TO` to probe the server, often as part of reconnaissance for phishing or spam campaigns.

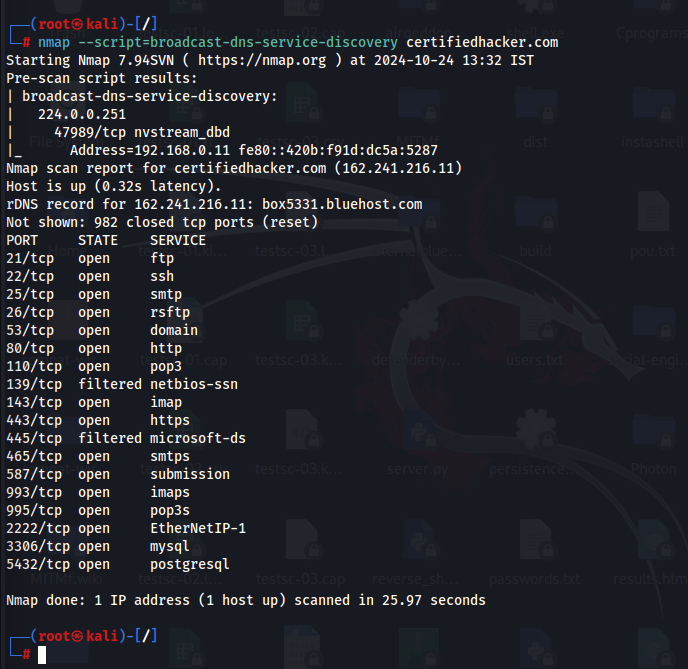
**DNS Enumeration:**

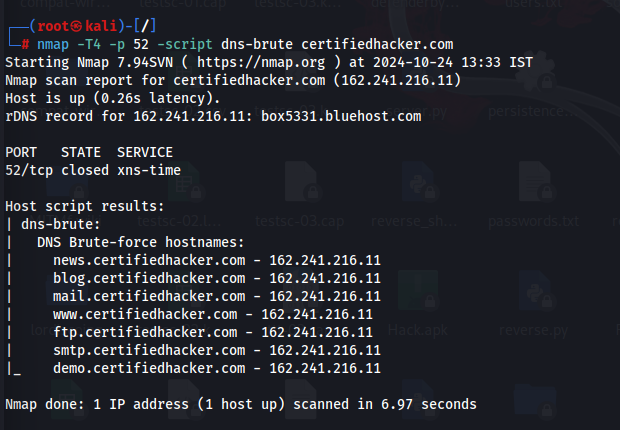
Using ZoneTransfer: **  
  
**

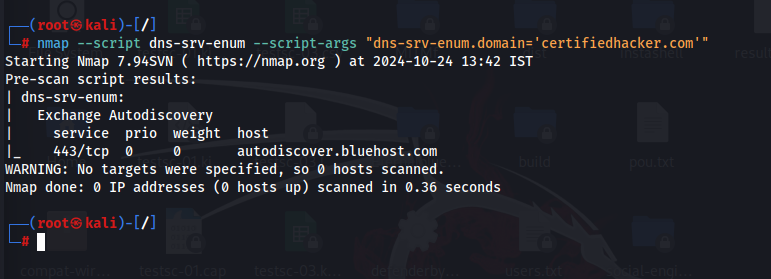
Using DNSSEC zone walking:

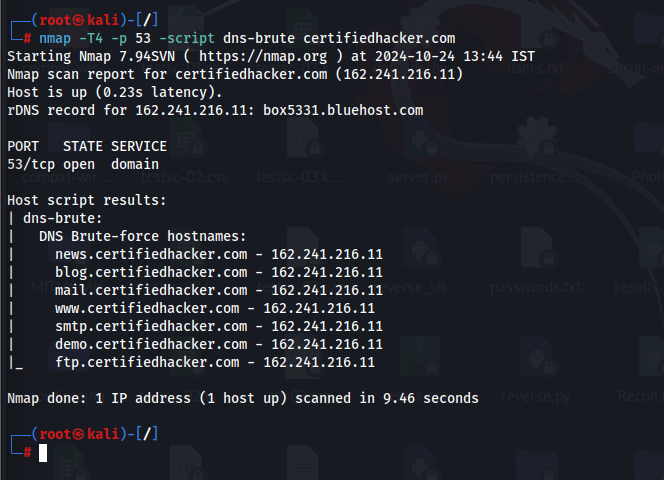


Using NMAP:









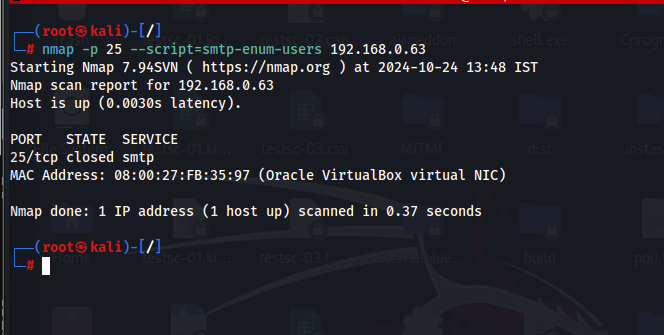
**DNS Cache Snooping:**

DNS cache snooping is a DNS enumeration technique whereby an attacker queries the DNS server for a specific cached DNS record.

**SMTP Enumeration:**

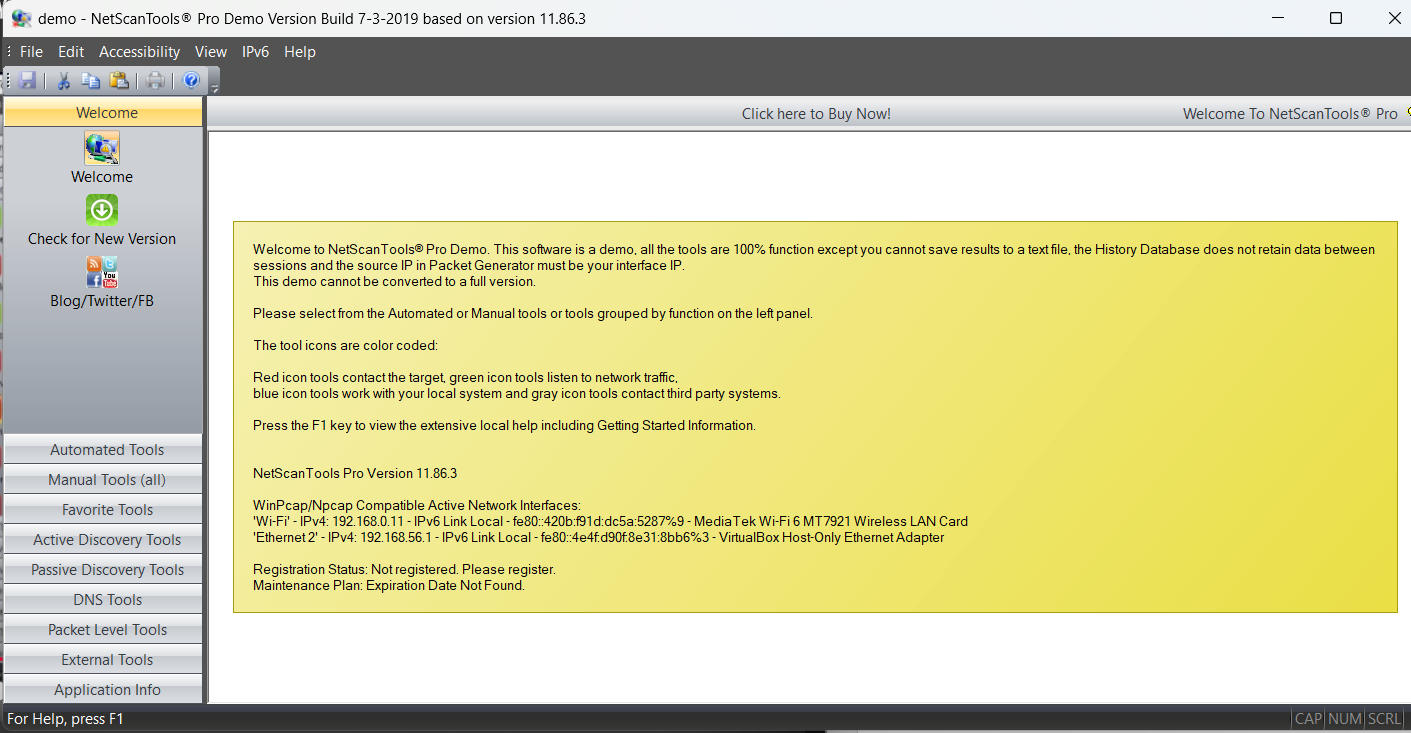
SMTP enumeration is a technique used to gather valid email addresses and user information from an email server. By interacting with the server using commands like VRFY, EXPN, or RCPT TO, attackers identify valid users and potential entry points. It helps in reconnaissance for phishing, spam campaigns, or social engineering.

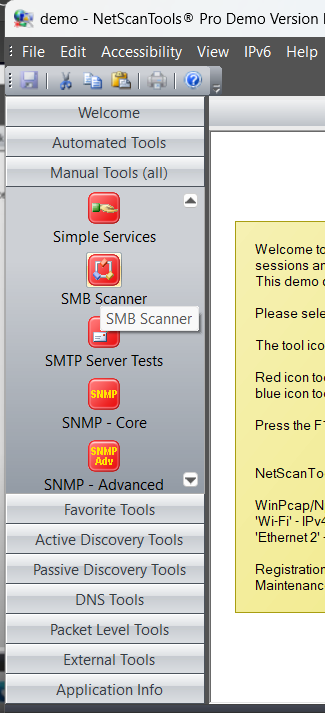
Using nmap:

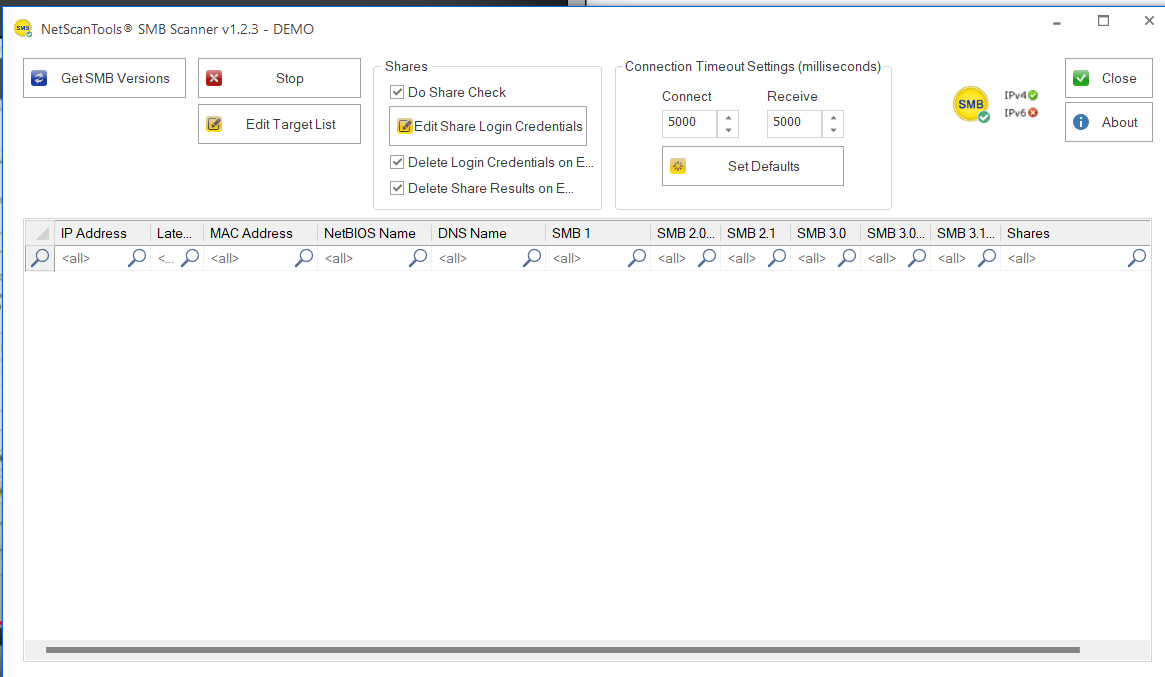


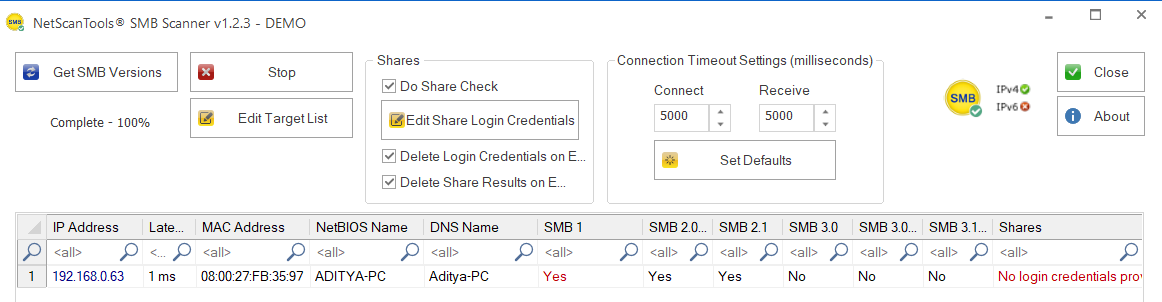
**SMB and RPC Enumeration:**

Using NetScanTools:



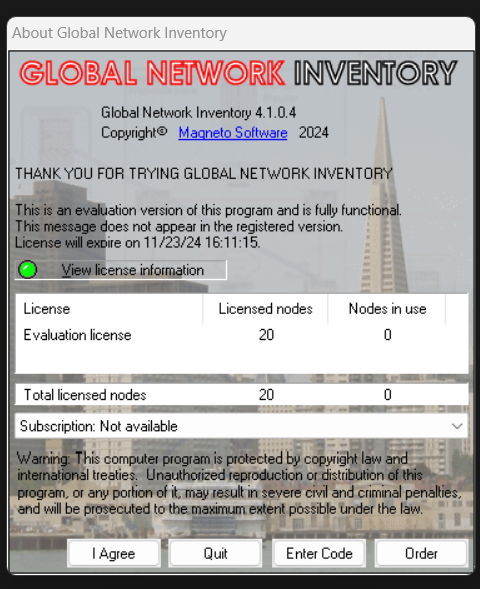


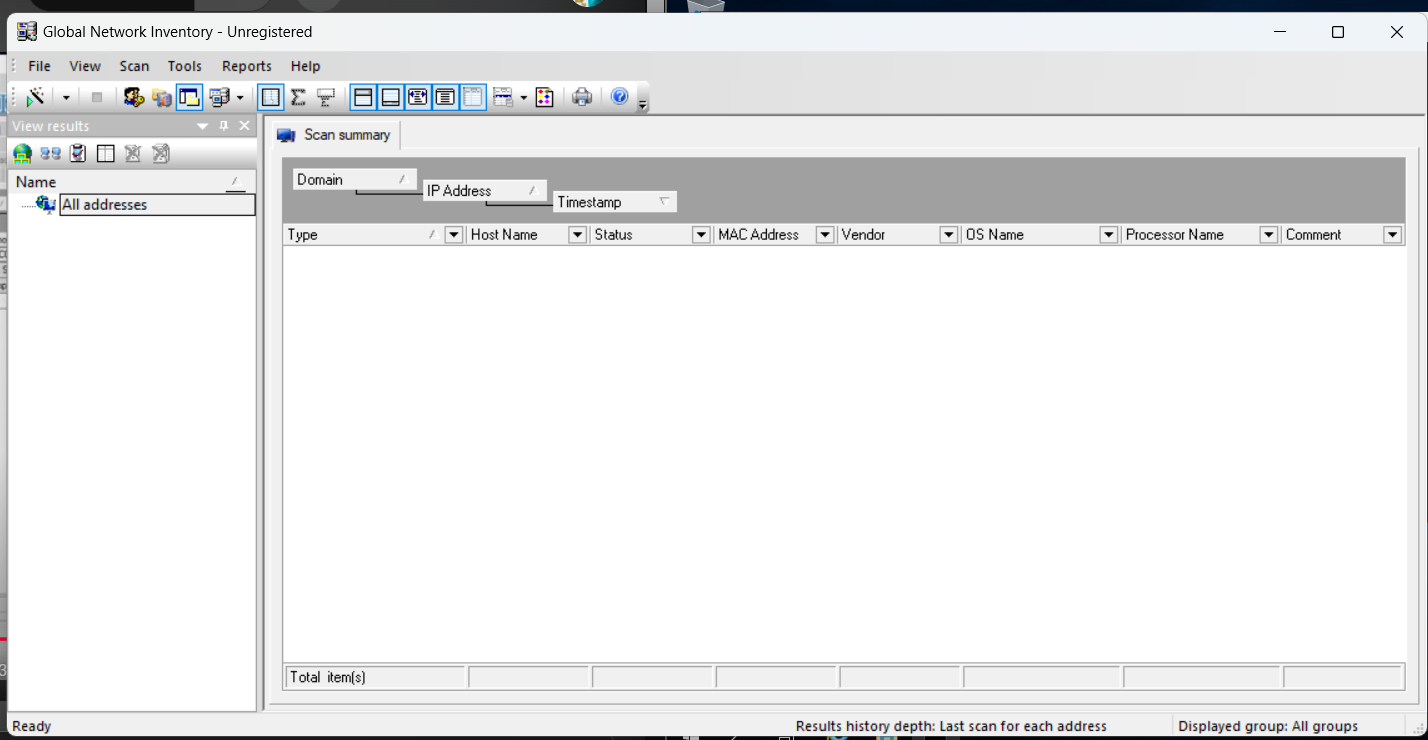


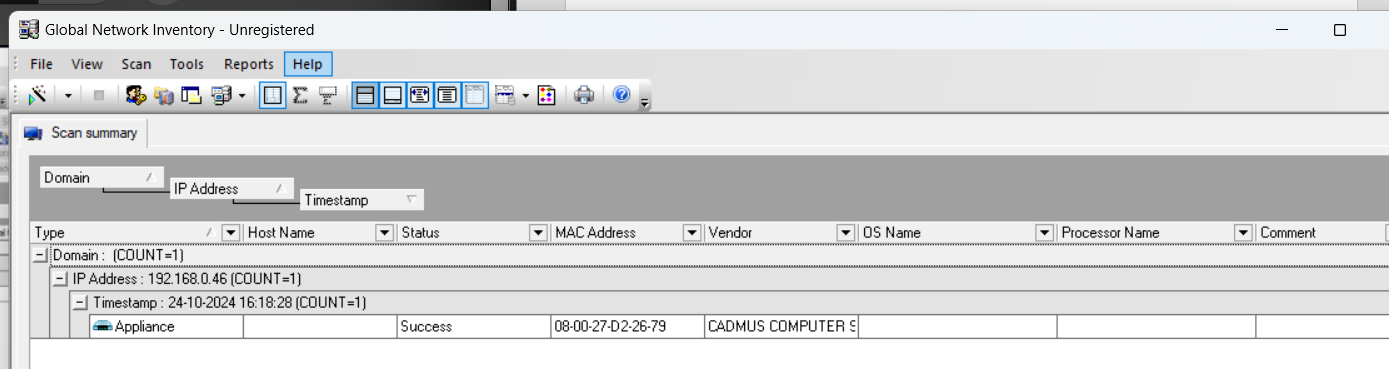




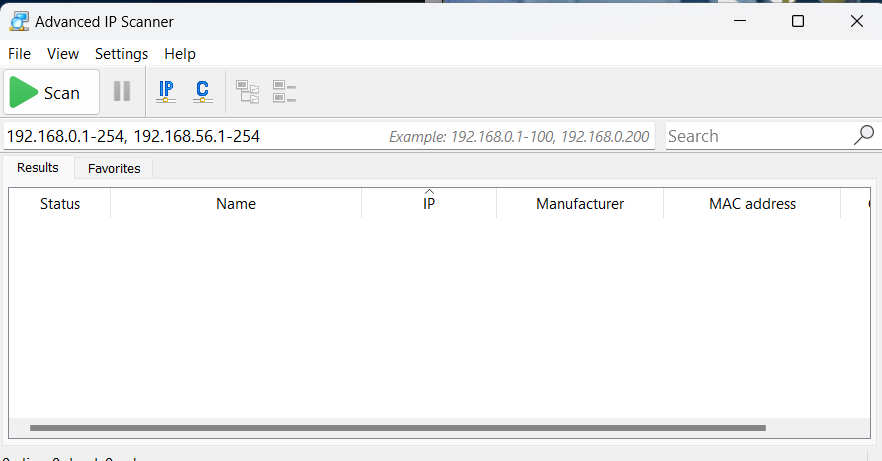
**Enumerate information using Global Network Inventory:**

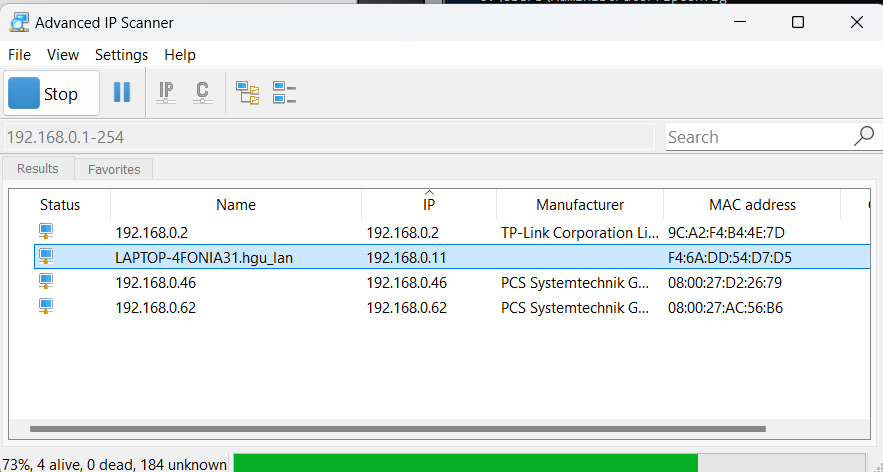
****

****

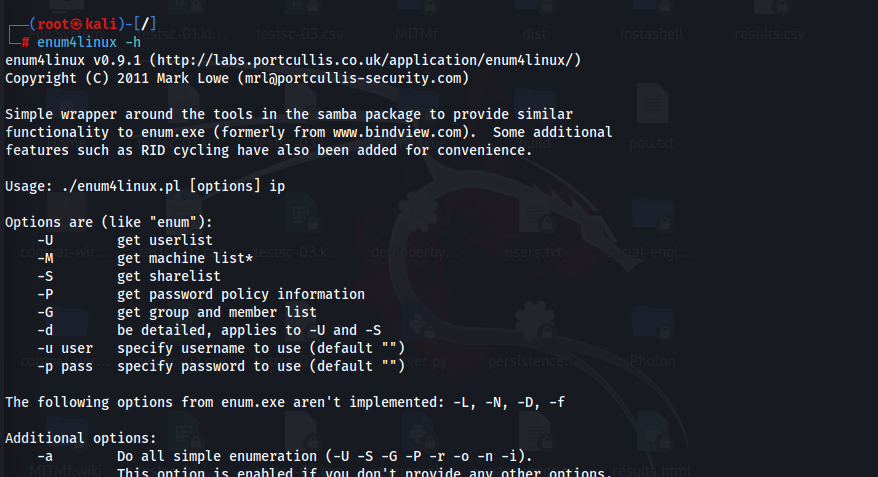
****

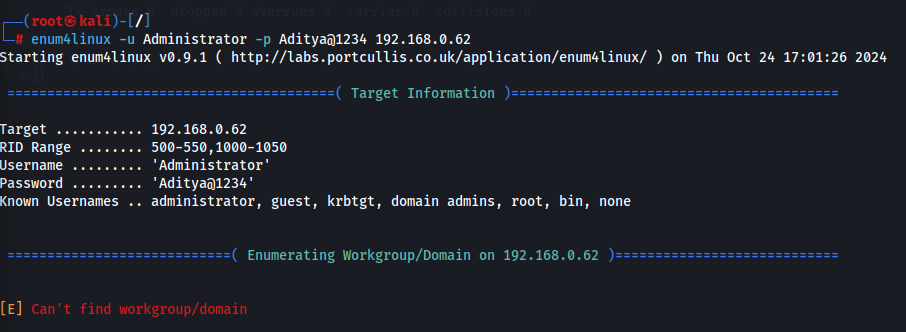
**Enumerate information using Advanced IP scanner:**

****

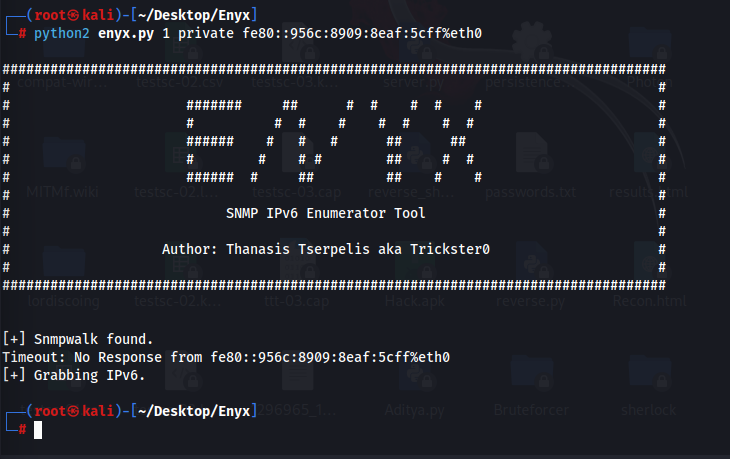
****

**Enumerate Information from Windows & Samba Hosts using Enum4linux:**

****

****

**Enyx enumeration:**

****