Assignment Enumeration

Task to be performed:

1.Network Discovery: Identify a target network or system for your assignment. This can be a virtual lab environment, a specific IP address range, or a predefined network.

Ans. Step 1: In this we have taken windows server 2022 as a target machine with IP address 10.10.1.22 and source IP 10.10.1.21,

NetBIOS helps us connecting and communicating with the devices connected via LAN.

By using nbtstat we can find out information about name, caches, users, domain, status using different options .

Step 2: Lets find basic info like name ,on the target IP using -a. We can see below SERVER2022 name.

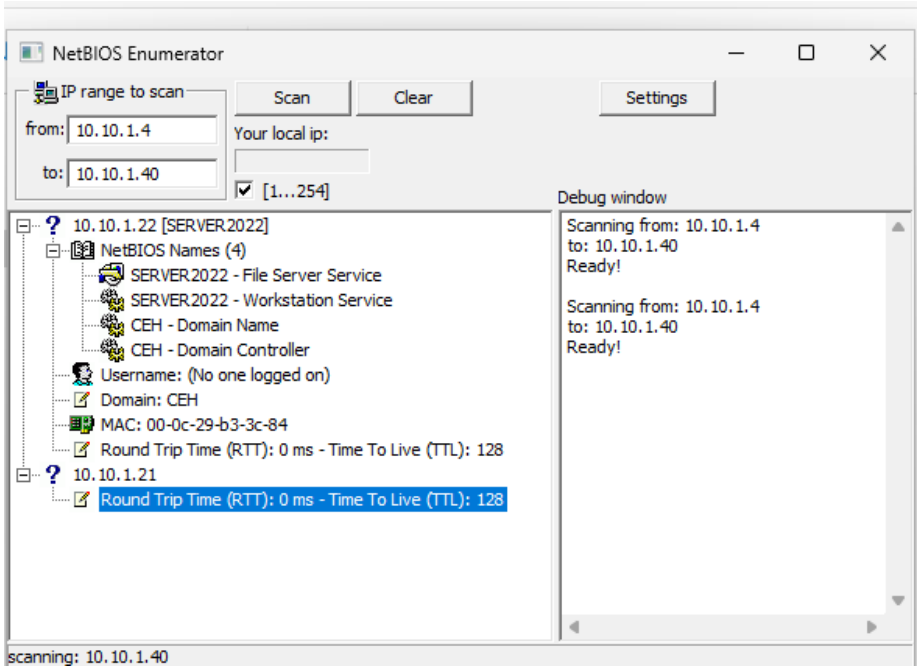
```
C:\Users\User>nbtstat -a 10.10.1.22

Ethernet1:
Node IpAddress: [10.10.1.21] Scope Id: []

           NetBIOS Remote Machine Name Table

       Name               Type         Status
    ---------------------------------------------
    SERVER2022     <20>  UNIQUE      Registered
    SERVER2022     <00>  UNIQUE      Registered
    CEH            <00>  GROUP       Registered
    CEH            <1C>  GROUP       Registered
    CEH            <1B>  UNIQUE      Registered

    MAC Address = 00-0C-29-B3-3C-84


Ethernet0:
Node IpAddress: [192.168.31.128] Scope Id: []

    Host not found.
```

Step 3: Lets find the cache of the remote machine including name and IP address. We can try other options

```
C:\Users\User>nbtstat -c

Ethernet1:
Node IpAddress: [10.10.1.21] Scope Id: []

                  NetBIOS Remote Cache Name Table

        Name             Type       Host Address    Life [sec]
    ------------------------------------------------------------
    SERVER2022     <20>  UNIQUE          10.10.1.22          582

Ethernet0:
Node IpAddress: [192.168.31.128] Scope Id: []

    No names in cache
```

Step 4: Download the NetBIOS enumerator and turn the application on by double clicking on it.

We can enter the range of IP address for which we want to scan. For example, we have entered from 10.10.1.2 to 10.10.1.50. It will scan all the port possible in this range. This method is similar to the above method using nbtstat giving us similar results.



2. Scanning with Nmap:

● Use Nmap to perform an initial network scan. Identify open ports and running services on the target network/system.

● Document the results of your Nmap scan and identify any potential targets for further enumeration.

Ans. We are doing similar to above but we will be using nmap .

Step 1: Open terminal and enter below command, nmap -sV -v –script nbstat.nse <Target IP>, where -sV tells the service versions and -v prints the version.

```
┌─[intellipaat@parrot]─[~]
└──╼ $nmap -sV -v --script nbstat.nse 10.10.1.22
Starting Nmap 7.93 ( https://nmap.org ) at 2024-07-16 05:35 EDT
NSE: Loaded 46 scripts for scanning.
```

Step2: We can observe all the open ports with service and status weather open or closed with versions.

```
Nmap scan report for 10.10.1.22
Host is up (0.00030s latency).
Not shown: 978 closed tcp ports (conn-refused)
PORT     STATE SERVICE         VERSION
53/tcp   open  domain          Simple DNS Plus
80/tcp   open  http            Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
88/tcp   open  kerberos-sec    Microsoft Windows Kerberos (server time: 2024-07-16 22:05:22Z)
135/tcp  open  msrpc           Microsoft Windows RPC
139/tcp  open  netbios-ssn     Microsoft Windows netbios-ssn
389/tcp  open  ldap            Microsoft Windows Active Directory LDAP (Domain: CEH.com0., Site
: Default-First-Site-Name)
445/tcp  open  microsoft-ds?
464/tcp  open  kpasswd5?
593/tcp  open  ncacn_http      Microsoft Windows RPC over HTTP 1.0
636/tcp  open  tcpwrapped
1061/tcp open  kiosk?
1069/tcp open  cognex-insight?
1072/tcp open  cardax?
1801/tcp open  msmq?
2103/tcp open  msrpc           Microsoft Windows RPC
2105/tcp open  msrpc           Microsoft Windows RPC
2107/tcp open  msrpc           Microsoft Windows RPC
2968/tcp open  ftp
```

```
| fingerprint-strings:
|   GenericLines:
|     220 Theef2 FTP Server: Theef210Srv (v2.10)
|     command not understood.
|     command not understood.
|   Help:
|     220 Theef2 FTP Server: Theef210Srv (v2.10)
|     'HELP': command not understood.
|   NULL, SMBProgNeg:
|     220 Theef2 FTP Server: Theef210Srv (v2.10)
|   SSLSessionReq:
|     220 Theef2 FTP Server: Theef210Srv (v2.10)
|_    command not understood.
3268/tcp open  ldap            Microsoft Windows Active Directory LDAP (Domain: CEH.com0.,
: Default-First-Site-Name)
3269/tcp open  tcpwrapped
3389/tcp open  ms-wbt-server   Microsoft Terminal Services
5357/tcp open  http            Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
| http-server-header: Microsoft-HTTPAPI/2.0
```

Below image contains similar data present in previous methodwe performed on question1 i:e name and status.

```
Host script results:
| nbstat: NetBIOS name: SERVER2022, NetBIOS user: <unknown>, NetBIOS MAC: 000c29b33c84 (VMwa
| Names:
|   SERVER2022<00>       Flags: <unique><active>
|   CEH<00>              Flags: <group><active>
|   CEH<1c>              Flags: <group><active>
|   SERVER2022<20>       Flags: <unique><active>
|   CEH<1b>              Flags: <unique><active>
| Statistics:
|   000c29b33c840000000000000000000000
|   000000000000000000000000000000000
|_  00000000000000000000000000
```

Step 3: Scanning UDP ports for possible vulnerability. We can observe 137/udp is open with netbios-ns service available.

```
┌─[root@parrot]─[/home/intellipaat]
└──╼ #nmap -sU -v --script nbstat.nse 10.10.1.22
Starting Nmap 7.93 ( https://nmap.org ) at 2024-07-16 08:53 EDT
NSE: Loaded 1 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 08:53
Completed NSE at 08:53, 0.00s elapsed
Initiating ARP Ping Scan at 08:53
Scanning 10.10.1.22 [1 port]
```

```
Not shown: 974 closed udp ports (port-unreach)
PORT      STATE         SERVICE
53/udp    open          domain
88/udp    open|filtered kerberos-sec
123/udp   open          ntp
137/udp   open          netbios-ns
138/udp   open|filtered netbios-dgm
161/udp   open          snmp
389/udp   open          ldap
464/udp   open|filtered kpasswd5
500/udp   open|filtered isakmp
3389/udp  open|filtered ms-wbt-server
3702/udp  open|filtered ws-discovery
4500/udp  open|filtered nat-t-ike
5353/udp  open|filtered zeroconf
5355/udp  open|filtered llmnr
62575/udp open|filtered unknown
62677/udp open|filtered unknown
62699/udp open|filtered unknown
62958/udp open|filtered unknown
63420/udp open|filtered unknown
63555/udp open|filtered unknown
64080/udp open|filtered unknown
64481/udp open|filtered unknown
64513/udp open|filtered unknown
64590/udp open|filtered unknown
64727/udp open|filtered unknown
65024/udp open|filtered unknown
MAC Address: 00:0C:29:B3:3C:84 (VMware)
```

```
Host script results:
| nbstat: NetBIOS name: SERVER2022, NetBIOS user: <unknown>, NetBIOS MAC: 000c29b33c84 (VMware)
| Names:
|   SERVER2022<20>       Flags: <unique><active>
|   SERVER2022<00>       Flags: <unique><active>
|   CEH<00>              Flags: <group><active>
|   CEH<1c>              Flags: <group><active>
|   CEH<1b>              Flags: <unique><active>
| Statistics:
|   000c29b33c840000000000000000000000
|   000000000000000000000000000000000000
|_  00000000000000000000000000000

NSE: Script Post-scanning.
Initiating NSE at 10:04
Completed NSE at 10:04, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 4265.24 seconds
           Raw packets sent: 1342 (67.978KB) | Rcvd: 1009 (73.912KB)
```

Step 4:Now we ping the 137/udp port to check what we can get out of it.

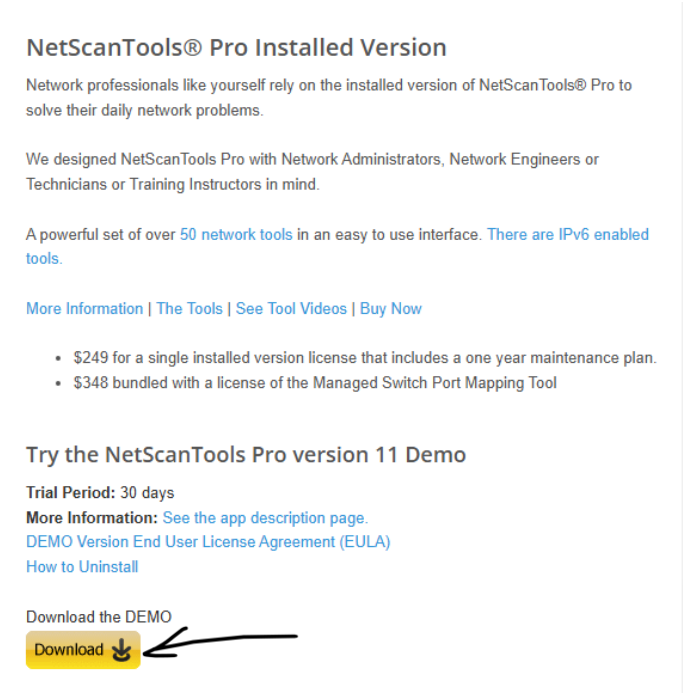
```
┌─[root@parrot]─[/home/intellipaat]
└──╼ #nmap -sU -p 137 --script nbstat.nse 10.10.1.22
Starting Nmap 7.93 ( https://nmap.org ) at 2024-07-17 06:46 EDT
Nmap scan report for 10.10.1.22
Host is up (0.00032s latency).

PORT    STATE SERVICE
137/udp open  netbios-ns
MAC Address: 00:0C:29:B3:3C:84 (VMware)

Host script results:
| nbstat: NetBIOS name: SERVER2022, NetBIOS user: <unknown>, NetBIOS MAC: 000c29b33c84 (VMware)
| Names:
|   SERVER2022<00>       Flags: <unique><active>
|   CEH<00>              Flags: <group><active>
|   SERVER2022<20>       Flags: <unique><active>
|   CEH<1c>              Flags: <group><active>
|_  CEH<1b>              Flags: <unique><active>

Nmap done: 1 IP address (1 host up) scanned in 0.64 seconds
```

3. SMB Enumeration with smbclient and enum4linux:

● Based on the Nmap results, focus on the SMB service. Use smbclient to connect to SMB shares and enum4linux to gather information about the target's Windows environment.

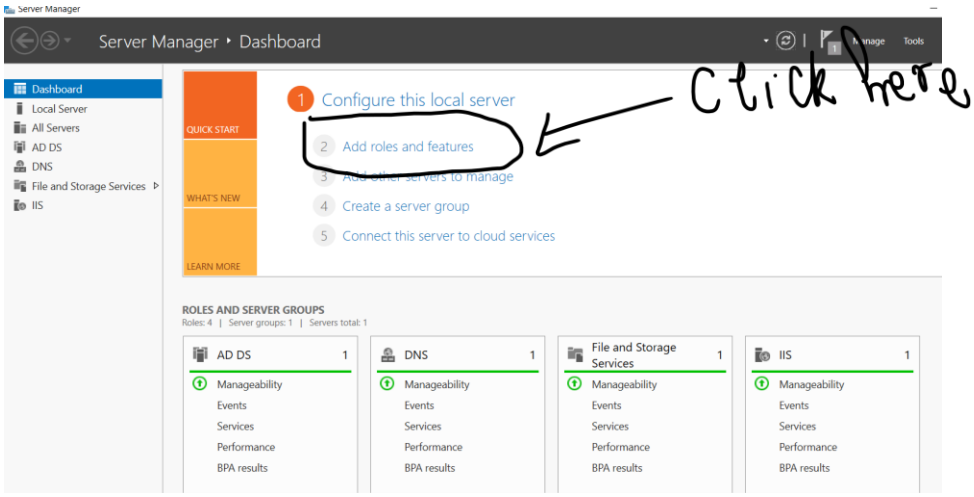
● Enumerate shares, users, groups, and other valuable information related to the SMB service.

Ans. Step 1: First we have to install NetscanTools from net into windows server. We will compare netscan results to results of enum4linux .

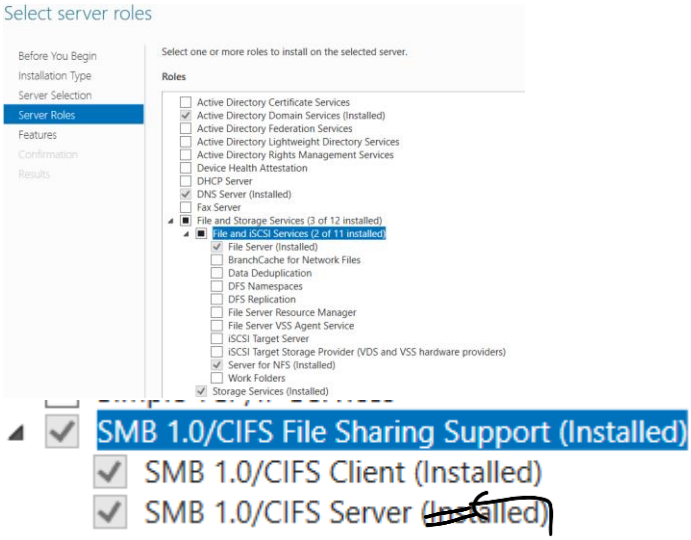


Step 2: Start Server manager in windows server 2022 the target machine, and follow the steps mentioned below.

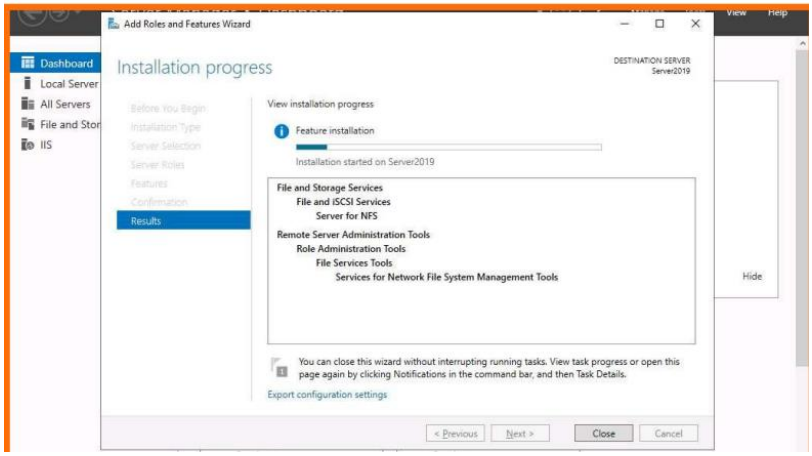
Click on the Add roles and features shown below.



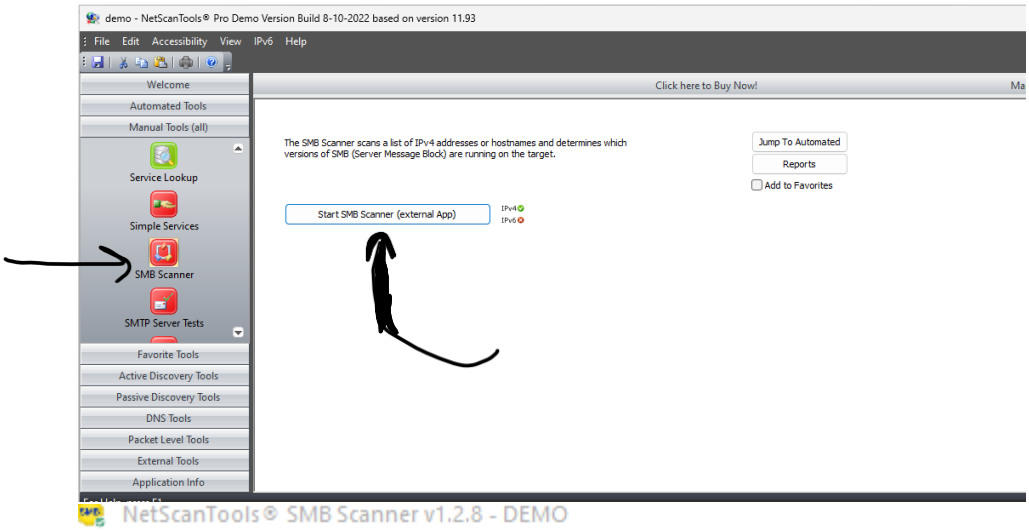
Go to Server Roles, under the options below click on File and storage drop box and click on File and ISCSI service drop box and select the checkbox on Server to NFS

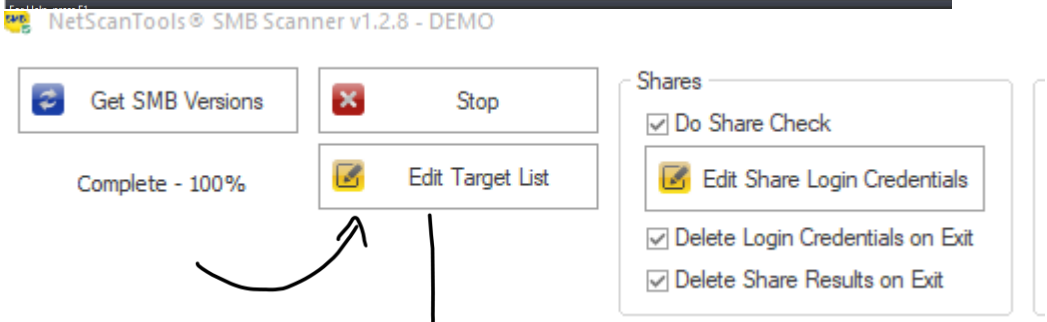


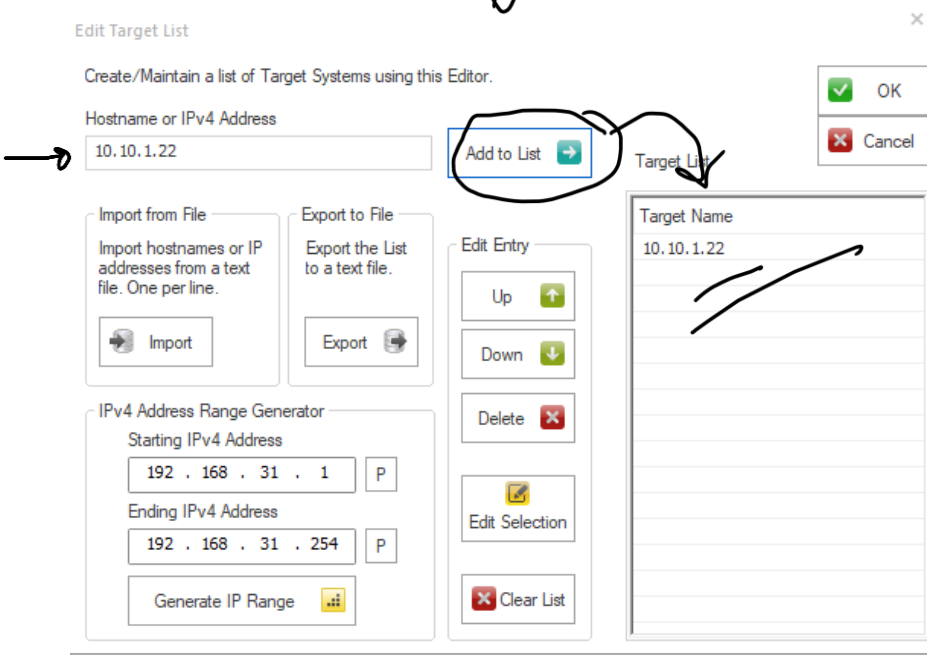
Click on Install to install the features into our server manager which we selected above. Meanwhile we open Netscan tool to proceed further.

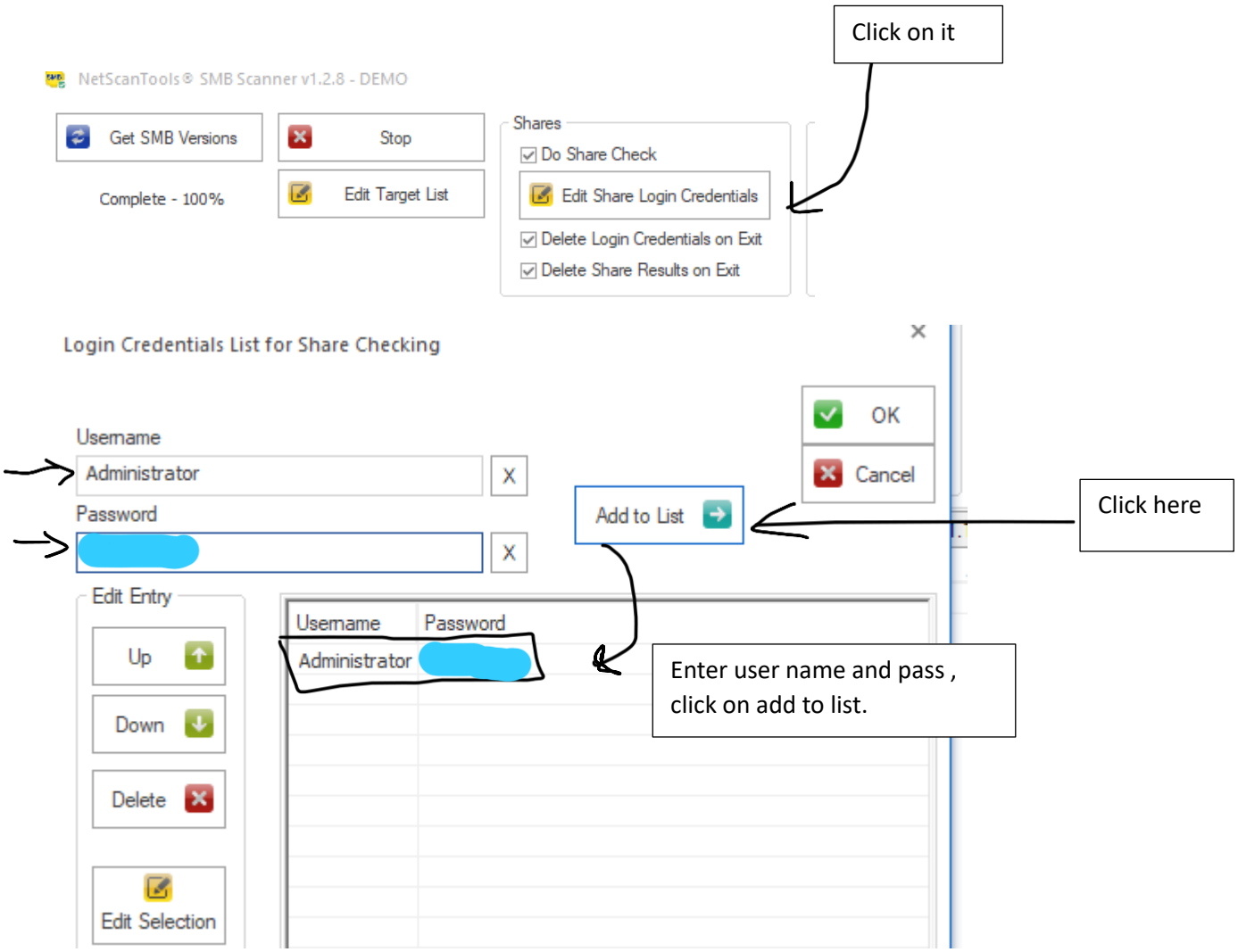


Step 3. Go to Windows 11 and install the Netscan tool and we will be using for SMB scanning. Search SMB scan under Manual Tool(all) drop box left side of the screen and click on it. Then there will be a button visible click on it.

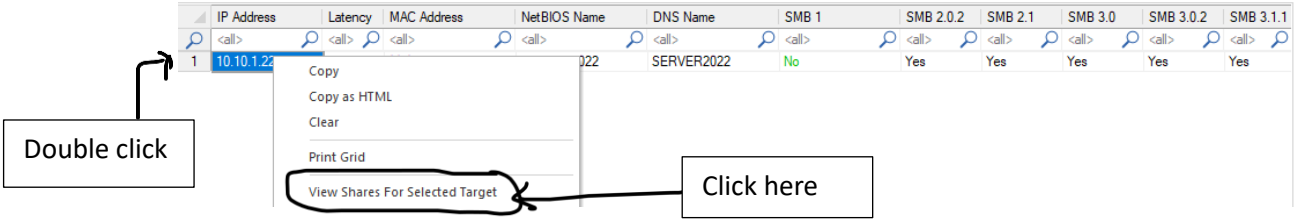

demo - NetScanTools® Pro Demo Version Build 8-10-2022 based on version 11.93
File Edit Accessibility View IPv6 Help
Welcome
Automated Tools
Manual Tools (all)
Service Lookup
Simple Services
SMB Scanner
SMTP Server Tests
Favorite Tools
Active Discovery Tools
Passive Discovery Tools
DNS Tools
Packet Level Tools
External Tools
Application Info
Click here to Buy Now!
The SMB Scanner scans a list of IPv4 addresses or hostnames and determines which versions of SMB (Server Message Block) are running on the target.
Jump To Automated
Reports
Add to Favorites
Start SMB Scanner (external App)


NetScanTools® SMB Scanner v1.2.8 - DEMO
Get SMB Versions
Stop
Complete - 100%
Edit Target List
Shares
Do Share Check
Edit Share Login Credentials
Delete Login Credentials on Exit
Delete Share Results on Exit


Edit Target List
Create/Maintain a list of Target Systems using this Editor.
OK
Cancel
Hostname or IPv4 Address
10.10.1.22
Add to List
Target List
Import from File
Import hostnames or IP addresses from a text file. One per line.
Import
Export to File
Export the List to a text file.
Export
Edit Entry
Up
Down
Delete
Edit Selection
Clear List
Target Name
10.10.1.22
IPv4 Address Range Generator
Starting IPv4 Address
192 . 168 . 31 . 1
P
Ending IPv4 Address
192 . 168 . 31 . 254
P
Generate IP Range



After the procedure , we click on SMB version on top left, to generate the report.



Shares for 10.10.1.22

Share Name	Type	Remark	Path	Permissions	Credentials Used
NETLOGON	Disk Drive Share	Logon server share	C:\Windows\SYSVOL\sysvol\CEH.com\SCRIPTS	N/A	Administrator
SYSVOL	Disk Drive Share	Logon server share	C:\Windows\SYSVOL\sysvol	N/A	Administrator
ADMIN$	Disk Drive Share, Special Share	Remote Admin	C:\Windows	N/A	Administrator
C$	Disk Drive Share, Special Share	Default share	C:\	N/A	Administrator
IPC$	Disk Drive Share, Special Share	Remote IPC		N/A	Administrator

These information we were looking for, share name, type, remark, path, Permissions, Credentials Used.

Method 2:-Now we will be using nmap extracting info on open ports and attacking specific ports to get our data. To scan the port we will use nmap and enum4linux tool for extracting server related info like groups, shares, etc.

Step1. Scanning TCP ports , open terminal and enter the below command. Sudo nmap -sT 10.10.1.22. It is said that port 445 is related to smb.

```
┌──[intellipaat@parrot]─[~]
└─$sudo nmap -sT 10.10.1.22
Starting Nmap 7.93 ( https://nmap.org ) at 2024-07-17 08:42 EDT
Nmap scan report for 10.10.1.22
Host is up (0.0025s latency).
Not shown: 978 closed tcp ports (conn-refused)
PORT     STATE SERVICE
53/tcp   open  domain
80/tcp   open  http
88/tcp   open  kerberos-sec
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
389/tcp  open  ldap
445/tcp  open  microsoft-ds
464/tcp  open  kpasswd5
593/tcp  open  http-rpc-epmap
636/tcp  open  ldapssl
1061/tcp open  kiosk
1069/tcp open  cognex-insight
1072/tcp open  cardax
1801/tcp open  msmq
2103/tcp open  zephyr-clt
2105/tcp open  eklogin
2107/tcp open  msmq-mgmt
2968/tcp open  enpp
3268/tcp open  globalcatLDAP
3269/tcp open  globalcatLDAPssl
3389/tcp open  ms-wbt-server
5357/tcp open  wsdapi
MAC Address: 00:0C:29:B3:3C:84 (VMware)
```

There is a another way , where we can scan TCP UDP ports and store under a file, which we can use for comparing between the content by comm or diff commands. This makes easy if we want to compare both the port numbers.

Step 2: We particularly scan 445 port aggressively using the command nmap -p 445 -A 10.10.1.22.

```
┌──[intellipaat@parrot]─[~]
└─$sudo nmap -p 445 -A 10.10.1.22
Starting Nmap 7.93 ( https://nmap.org ) at 2024-07-17 08:44 EDT
Nmap scan report for 10.10.1.22
Host is up (0.00048s latency).

PORT    STATE SERVICE       VERSION
445/tcp open  microsoft-ds?
MAC Address: 00:0C:29:B3:3C:84 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Microsoft Windows 10 1703 (97%), Microsoft Windows Server 2016 build 10586 - 14393 (97%), Microsoft Windows Server 201
 (95%), Microsoft Windows 10 1507 - 1607 (94%), Microsoft Windows Server 2012 R2 Update 1 (94%), Microsoft Windows 7, Windows Server 2012, or
Windows 8.1 Update 1 (94%), Microsoft Windows 10 1511 (93%), Microsoft Windows Server 2012 (93%), Microsoft Windows Server 2012 or Server 201
 R2 (93%), Microsoft Windows Longhorn (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

Host script results:
|_nbstat: NetBIOS name: SERVER2022, NetBIOS user: <unknown>, NetBIOS MAC: 000c29b33c84 (VMware)
|_clock-skew: 11h50m00s
| smb2-security-mode:
|   311:
|     Message signing enabled and required
| smb2-time:
|   date: 2024-07-18T00:34:36
|_  start_date: N/A

TRACEROUTE
HOP RTT     ADDRESS
1   0.48 ms 10.10.1.22

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 29.19 seconds
```

Step 3: Now we will use enum4linux to enumerate users.

```
┌─[root@parrot]─[/home/intellipaat]
└──╼ #enum4linux -U -u Administrator -p [redacted] 10.10.1.[redacted]
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Sun Jul 21 03:08:26 20

 ==========================
|    Target Information    |
 ==========================
Target ........... 10.10.1.22
RID Range ........ 500-550,1000-1050
Username ......... 'Administrator'
Password ......... '[redacted]'
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 ===================================================
|    Enumerating Workgroup/Domain on 10.10.1.22    |
 ===================================================
[+] Got domain/workgroup name: CEH
```

```
 ================================
|    Session Check on 10.10.1.22    |
 ================================
[+] Server 10.10.1.22 allows sessions using username 'Administrator', password '[redacted]'

 ========================================
|    Getting domain SID for 10.10.1.22    |
 ========================================
Domain Name: CEH
Domain Sid: S-1-5-21-3011248926-652701544-240057437
[+] Host is part of a domain (not a workgroup)

 =========================
|    Users on 10.10.1.22    |
 =========================
index: 0xeda RID: 0x1f4 acb: 0x00000210 Account: Administrator  Name: (null)    Desc: Built-in account for administering the computer/domain
index: 0xedb RID: 0x1f5 acb: 0x00000215 Account: Guest  Name: (null)    Desc: Built-in account for guest access to the computer/domain
index: 0xfad RID: 0x44f acb: 0x00000210 Account: jason  Name: Jason M.  Desc: (null)
index: 0xf0f RID: 0x1f6 acb: 0x00000011 Account: krbtgt Name: (null)    Desc: Key Distribution Center Service Account
index: 0xfae RID: 0x450 acb: 0x00000210 Account: martin Name: Martin C. Desc: (null)
index: 0xfaf RID: 0x451 acb: 0x00000210 Account: shiela Name: Shiela D. Desc: (null)

user:[Administrator] rid:[0x1f4]
user:[Guest] rid:[0x1f5]
user:[krbtgt] rid:[0x1f6]
user:[jason] rid:[0x44f]
user:[martin] rid:[0x450]
user:[shiela] rid:[0x451]
enum4linux complete on Sun Jul 21 03:08:26 2024
```

User

Step 4: Next we will enumerate for share list.

```
┌─[root@parrot]─[/home/intellipaat]
└──╼ #enum4linux -S -u Administrator -p [redacted] 10.10.1.[redacted]
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux

 ==========================
|    Target Information    |
 ==========================
Target ........... 10.10.1.[redacted]
RID Range ........ 500-550,1000-1050
Username ......... 'Administrator'
Password ......... '[redacted]'
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none
```

```
 ==========================================
|    Share Enumeration on 10.10.1.[redacted]    |
 ==========================================

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
        NETLOGON        Disk      Logon server share
        SYSVOL          Disk      Logon server share
SMB1 disabled -- no workgroup available
```

Step 5: Now we will list out the groups.

```
┌──[root@parrot]─[/home/intellipaat]
└─── #enum4linux -G -u Administrator -p [redacted] 10.10.1.[redacted]
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/en
```

```
|    Groups on 10.10.1.22    |
 ============================

[+] Getting builtin groups:
group:[Server Operators] rid:[0x225]
group:[Account Operators] rid:[0x224]
group:[Pre-Windows 2000 Compatible Access] rid:[0x22a]
group:[Incoming Forest Trust Builders] rid:[0x22d]
group:[Windows Authorization Access Group] rid:[0x230]
group:[Terminal Server License Servers] rid:[0x231]
group:[Administrators] rid:[0x220]
group:[Users] rid:[0x221]
group:[Guests] rid:[0x222]
group:[Print Operators] rid:[0x226]
group:[Backup Operators] rid:[0x227]
group:[Replicator] rid:[0x228]
group:[Remote Desktop Users] rid:[0x22b]
group:[Network Configuration Operators] rid:[0x22c]
group:[Performance Monitor Users] rid:[0x22e]
group:[Performance Log Users] rid:[0x22f]
group:[Distributed COM Users] rid:[0x232]
group:[IIS_IUSRS] rid:[0x238]
group:[Cryptographic Operators] rid:[0x239]
group:[Event Log Readers] rid:[0x23d]
group:[Certificate Service DCOM Access] rid:[0x23e]
group:[RDS Remote Access Servers] rid:[0x23f]
group:[RDS Endpoint Servers] rid:[0x240]
group:[RDS Management Servers] rid:[0x241]
group:[Hyper-V Administrators] rid:[0x242]
group:[Access Control Assistance Operators] rid:[0x243]
group:[Remote Management Users] rid:[0x244]
group:[Storage Replica Administrators] rid:[0x246]
```

```
[+] Getting builtin group memberships:
Group 'Guests' (RID: 546) has member: CEH\Guest
Group 'Guests' (RID: 546) has member: CEH\Domain Guests
Group 'Pre-Windows 2000 Compatible Access' (RID: 554) has member: NT AUTHORITY\Authenticated Users
Group 'IIS_IUSRS' (RID: 568) has member: NT AUTHORITY\IUSR
Group 'Users' (RID: 545) has member: NT AUTHORITY\INTERACTIVE
Group 'Users' (RID: 545) has member: NT AUTHORITY\Authenticated Users
Group 'Users' (RID: 545) has member: CEH\Domain Users
Group 'Windows Authorization Access Group' (RID: 560) has member: NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS
Group 'Administrators' (RID: 544) has member: CEH\Administrator
Group 'Administrators' (RID: 544) has member: CEH\Enterprise Admins
Group 'Administrators' (RID: 544) has member: CEH\Domain Admins
Group 'Administrators' (RID: 544) has member: CEH\jason
Group 'Administrators' (RID: 544) has member: CEH\martin
Group 'Administrators' (RID: 544) has member: CEH\shiela
```

```
[+] Getting local groups:
group:[Cert Publishers] rid:[0x205]
group:[RAS and IAS Servers] rid:[0x229]
group:[Allowed RODC Password Replication Group] rid:[0x23b]
group:[Denied RODC Password Replication Group] rid:[0x23c]
group:[DnsAdmins] rid:[0x44d]

[+] Getting local group memberships:
Group 'Denied RODC Password Replication Group' (RID: 572) has member: CEH\krbtgt
Group 'Denied RODC Password Replication Group' (RID: 572) has member: CEH\Domain Controllers
Group 'Denied RODC Password Replication Group' (RID: 572) has member: CEH\Schema Admins
Group 'Denied RODC Password Replication Group' (RID: 572) has member: CEH\Enterprise Admins
Group 'Denied RODC Password Replication Group' (RID: 572) has member: CEH\Cert Publishers
Group 'Denied RODC Password Replication Group' (RID: 572) has member: CEH\Domain Admins
Group 'Denied RODC Password Replication Group' (RID: 572) has member: CEH\Group Policy Creator Owners
Group 'Denied RODC Password Replication Group' (RID: 572) has member: CEH\Read-only Domain Controllers

[+] Getting domain groups:
group:[Enterprise Read-only Domain Controllers] rid:[0x1f2]
group:[Domain Admins] rid:[0x200]
group:[Domain Users] rid:[0x201]
group:[Domain Guests] rid:[0x202]
group:[Domain Computers] rid:[0x203]
group:[Domain Controllers] rid:[0x204]
group:[Schema Admins] rid:[0x206]
group:[Enterprise Admins] rid:[0x207]
group:[Group Policy Creator Owners] rid:[0x208]
group:[Read-only Domain Controllers] rid:[0x209]
group:[Cloneable Domain Controllers] rid:[0x20a]
group:[Protected Users] rid:[0x20d]
group:[Key Admins] rid:[0x20e]
group:[Enterprise Key Admins] rid:[0x20f]
group:[DnsUpdateProxy] rid:[0x44e]
```

```
[+] Getting domain group memberships:
Group 'Domain Users' (RID: 513) has member: CEH\Administrator
Group 'Domain Users' (RID: 513) has member: CEH\krbtgt
Group 'Domain Users' (RID: 513) has member: CEH\jason
Group 'Domain Users' (RID: 513) has member: CEH\martin
Group 'Domain Users' (RID: 513) has member: CEH\shiela
Group 'Domain Admins' (RID: 512) has member: CEH\Administrator
Group 'Enterprise Admins' (RID: 519) has member: CEH\Administrator
Group 'Group Policy Creator Owners' (RID: 520) has member: CEH\Administrator
Group 'Domain Controllers' (RID: 516) has member: CEH\SERVER2022$
Group 'Schema Admins' (RID: 518) has member: CEH\Administrator
Group 'Domain Guests' (RID: 514) has member: CEH\Guest
enum4linux complete on Sun Jul 21 15:50:51 2024
```

Step 6:Password Policy list. We can observe that there is 0 to no

```
┌──[root@parrot]─[/home/intellipaat]
└─── #enum4linux -P -u Administrator -p [redacted] 10.10.1.[redacted]
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/applic
```

```
 =========================================================
|    Password Policy Information for 10.10.1.22    |
 =========================================================

[+] Attaching to 10.10.1.22 using Administrator:Intellip@@t

[+] Trying protocol 139/SMB...

        [!] Protocol failed: Cannot request session (Called Name:10.10.1.22)
```

```
[+] Trying protocol 445/SMB...

[+] Found domain(s):

        [+] CEH
        [+] Builtin

[+] Password Info for Domain: CEH

        [+] Minimum password length: None
        [+] Password history length: None
        [+] Maximum password age: Not Set
        [+] Password Complexity Flags: 000000

                [+] Domain Refuse Password Change: 0
                [+] Domain Password Store Cleartext: 0
                [+] Domain Password Lockout Admins: 0
                [+] Domain Password No Clear Change: 0
                [+] Domain Password No Anon Change: 0
                [+] Domain Password Complex: 0
```

```
        [+] Minimum password age: None
        [+] Reset Account Lockout Counter: 30 minutes
        [+] Locked Account Duration: 30 minutes
        [+] Account Lockout Threshold: None
        [+] Forced Log off Time: Not Set

[+] Retieved partial password policy with rpcclient:

Password Complexity: Disabled
Minimum Password Length: 0

enum4linux complete on Sun Jul 21 15:56:27 2024
```

4. Email Enumeration with theHarvester:

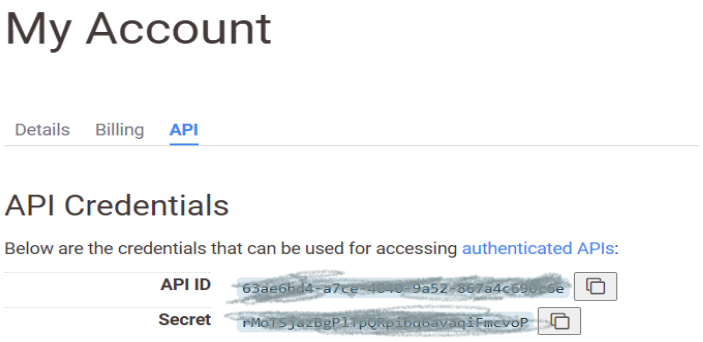
● Utilize theHarvester to search for email addresses and associated information related to the target network or organization.

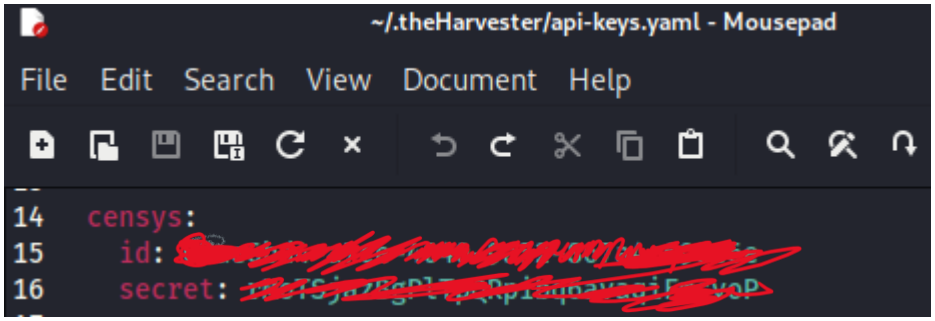
● Document the email addresses and any other relevant information you discover.

Ans. Before using theHarvester we have to add some Api keys for censys and shodan in api-keys.yaml file.

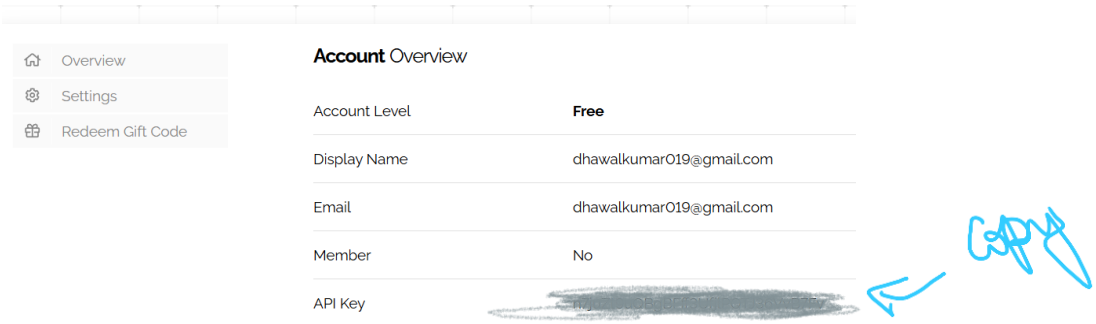
Step 1: change directory or enter the command in terminal sudo mousepad /root/.theHarvester/api-keys.yaml.

Step 2. Go to censys and create an account open where you will find Api credentials for your account. Copy the Api id and secret in api-key.yaml.



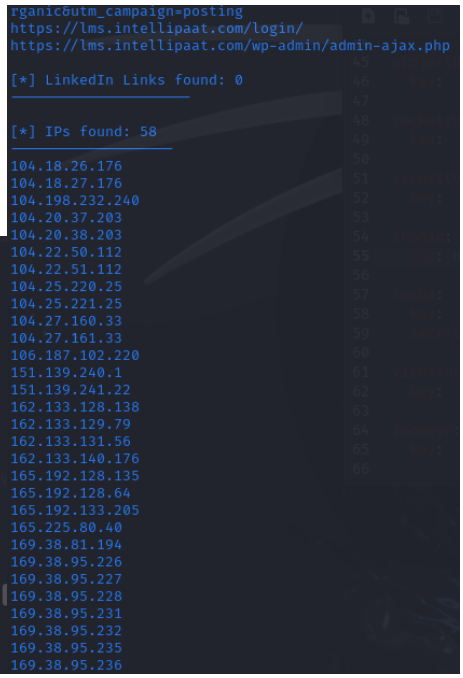


Step 3: Go to Shodan , and click on account. Then u will click on overview where you will find Api key. Paste it in the api-keys file.



Save and exit.

Step 4: Go to terminal, and enter the following command pasted below. My Target domain is intellipaat. We can observe that it has discovered many IP associated with intellipaat.com, Asns found 5, found 0 linkedin, it also found 1 email(sales@intellipaat.com) and 184 host. Some data out of all the findings are been presented as images.



```
45.33.79.77
52.6.34.242
67.225.221.78
69.175.25.154
74.115.51.8
74.115.51.9

[*] Emails found: 1
____________________

sales@intellipaat.com

[*] Hosts found: 184
____________________

*.intellipaat.com
affiliates.intellipaat.com
alpha.intellipaat.com
alpha.intellipaat.com:104.18.26.176
alpha.intellipaat.com:104.18.27.176
alpha.intellipaat.com:2606:4700::6812:1ab0
alpha.intellipaat.com:2606:4700::6812:1bb0
alpha.intellipaat.com:2a06:98c1:3122:e000::5
alpha.intellipaat.com:2a06:98c1:3123:e000::5
alpha.intellipaat.com:3.216.13.54
alpha.intellipaat.com:52.70.255.57
app.intellipaat.com
app.intellipaat.com:104.18.26.176
app.intellipaat.com:104.18.27.176
app.intellipaat.com:104.22.50.112
app.intellipaat.com:172.67.31.242
app.intellipaat.com:2606:4700:10::6816:3270
app.intellipaat.com:2606:4700:10::6816:3370
app.intellipaat.com:2606:4700:10::ac43:1ff2
app.intellipaat.com:2606:4700::6812:1ab0
app.intellipaat.com:2606:4700::6812:1bb0
```

```
spam.intellipaat.com:2606:4700::6812:1bb0
spam.intellipaat.com:2a06:98c1:3122:e000::
spam.intellipaat.com:2a06:98c1:3123:e000::
stage.intellipaat.com
stage.intellipaat.com:104.18.26.176
stage.intellipaat.com:104.18.27.176
stage.intellipaat.com:104.22.50.112
stage.intellipaat.com:2606:4700:10::6816:3270
stage.intellipaat.com:2606:4700:10::6816:3370
stage.intellipaat.com:2606:4700:10::ac43:1ff2
stage.intellipaat.com:2606:4700::6812:1ab0
stage.intellipaat.com:2606:4700::6812:1bb0
studio.learn.intellipaat.com
studio.learn.intellipaat.com:intellipaat.skillsnetwork.site
studio.learn.intellipaat.com:learn.intellipaat.com
studio.learn.intellipaat.com:learn.intellipaat.com.
support.learn.intellipaat.com
support.learn.intellipaat.com:intellipaat.skillsnetwork.site
support.learn.intellipaat.com:learn.intellipaat.com
support.learn.intellipaat.com:learn.intellipaat.com.
test.intellipaat.com
test.intellipaat.com:104.18.26.176
test.intellipaat.com:104.18.27.176
test.intellipaat.com:104.22.50.112
test.intellipaat.com:104.22.51.112
test.intellipaat.com:188.114.98.224
test.intellipaat.com:188.114.99.224
test.intellipaat.com:2606:4700:10::6816:3270
test.intellipaat.com:2606:4700:10::6816:3370
test.intellipaat.com:2606:4700:10::ac43:1ff2
test.intellipaat.com:2606:4700::6812:1ab0
test.intellipaat.com:2606:4700::6812:1bb0
test.intellipaat.com:2a06:98c1:3122:e000::a
test.intellipaat.com:2a06:98c1:3123:e000::a
unsubscribe.intellipaat.com
upgrade.intellipaat.com
upgrade.intellipaat.com:3.239.161.55
webdisk.intellipaat.com
webdisk.intellipaat.com:69.175.25.154
webmail.intellipaat.com
webmail.intellipaat.com:69.175.7.170
```

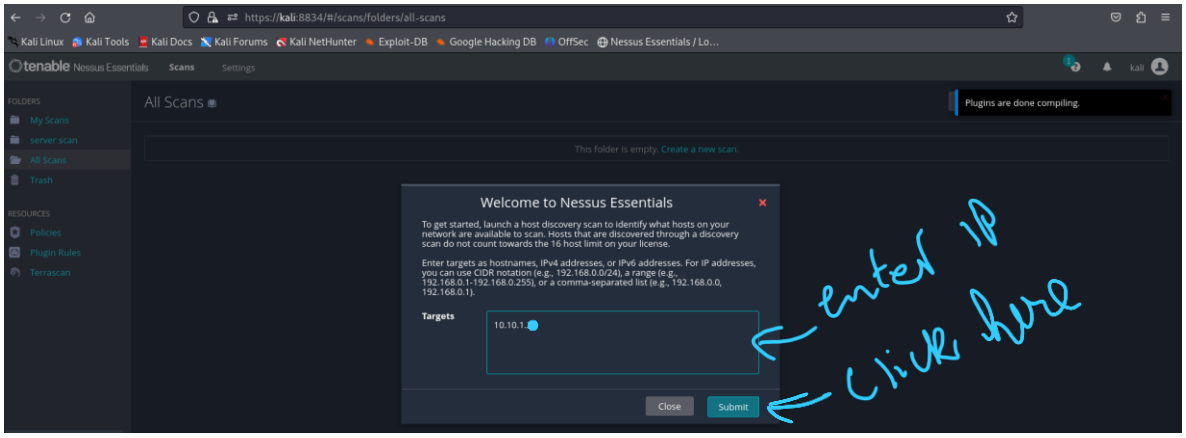
5. Vulnerability Scanning with Nessus:

● Perform a vulnerability scan on the target network/system to identify potential security vulnerabilities.

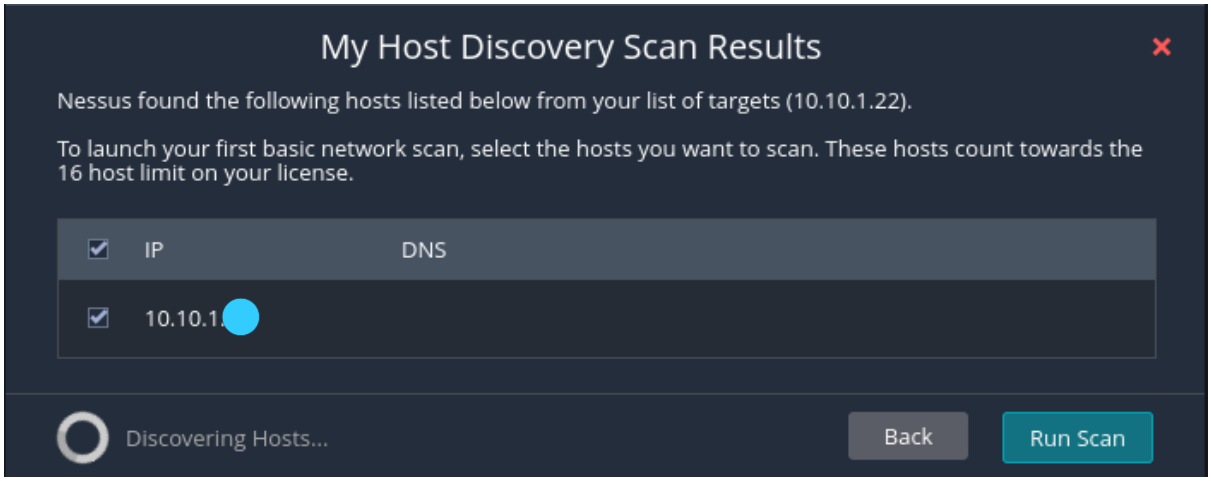
● Document the vulnerabilities, their severity, and any recommendations provided by Nessus

Ans. Lets turn on Nessus and start scanning.

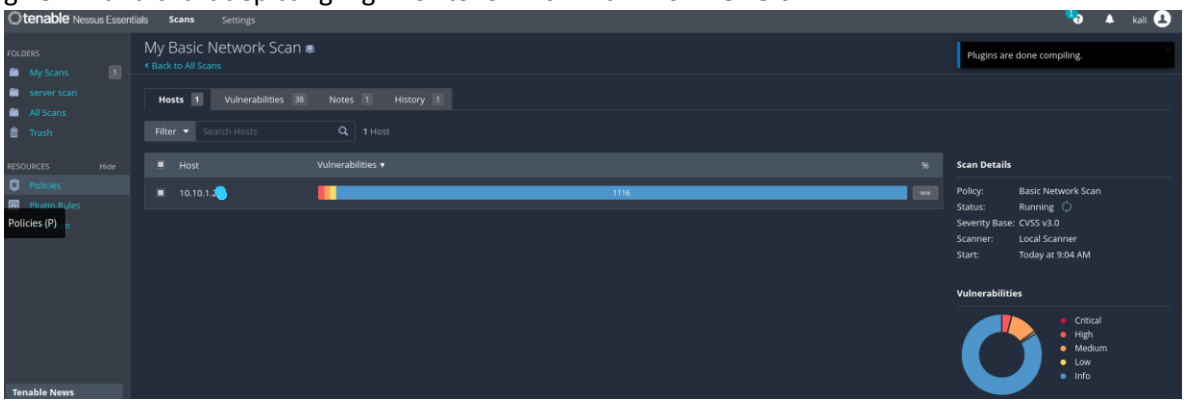
Step1: entering IP in the target box and click on submit.



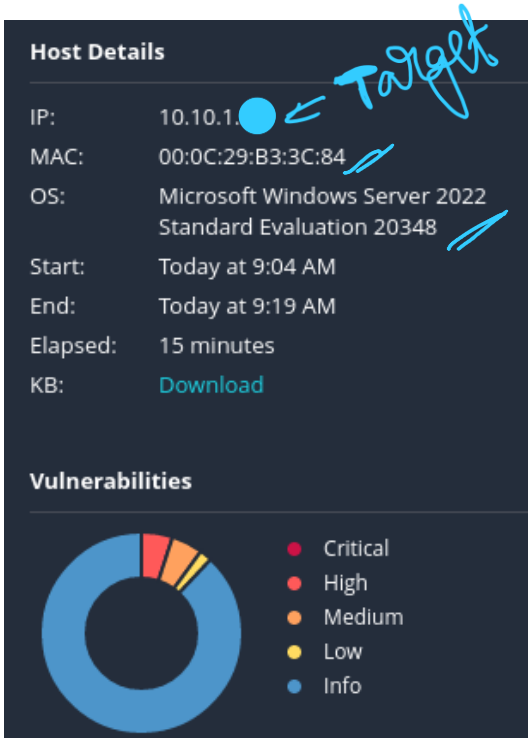
After adding IP, you will check box below. Select it and hit run scan button and wait for the response.



Step 2: After scan completes, Results are available to be accessed. Right side details on scan is been given with a chart depicting high risk to low risk with info.Twewers



Information tells even about the target OS,MAC. Red depicts critical, orange- high, lighter orange-medium,yellow-low.



Step 3: Right click on the result, where you can see all the listed vulnerabilities.

Sev	CVSS	VPR	Name	Family	Count
MIXED	...	...	SNMP (Multiple Issues)	SNMP	12
MIXED	...	...	SSL (Multiple Issues)	General	9
MIXED	...	...	TLS (Multiple Issues)	Service detection	4
MIXED	...	...	Microsoft Windows (Multiple Issues)	Misc.	2
LOW	2.1 *		ICMP Timestamp Request Remote Date Disclosure	General	1
INFO	...	...	SMB (Multiple Issues)	Windows	7
INFO	...	...	HTTP (Multiple Issues)	Web Servers	6
INFO	...	...	LDAP (Multiple Issues)	Misc.	4
INFO	...	...	RPC (Multiple Issues)	RPC	2
INFO	...	...	TLS (Multiple Issues)	General	2
INFO			DCE Services Enumeration	Windows	17
INFO			Service Detection	Service detection	7

Double tap on first vulnerability (SNP). You will see below list of issues. And when u deep dive in to it,we can see what the actual problem is ,info on vulnerability what to do to prevent it.

Sev	CVSS	VPR	Name	Family	Count
HIGH	7.5 *		SNMP Agent Default Community Name (public)	SNMP	1
HIGH	7.3		Microsoft Windows LAN Manager SNMP LanMan Services Disclosure	SNMP	1
MEDIUM	5.3		Microsoft Windows LAN Manager SNMP LanMan Shares Disclosure	SNMP	1
MEDIUM	5.3		Microsoft Windows LAN Manager SNMP LanMan Users Disclosure	SNMP	1

1.

HIGH SNMP Agent Default Community Name (public)

Description

It is possible to obtain the default community name of the remote SNMP server.

An attacker may use this information to gain more knowledge about the remote host, or to change the configuration of the remote system (if the default community allows such modifications).

Solution

Disable the SNMP service on the remote host if you do not use it.
Either filter incoming UDP packets going to this port, or change the default community string.

Output

```
The remote SNMP server replies to the following default community
string :

public
```

To see debug logs, please visit individual host

Port	Hosts
161 / udp / snmp	10.10.1.

Plugin Details

Severity: High
ID: 41028
Version: 1.14
Type: remote
Family: SNMP
Published: November 25, 2002
Modified: June 1, 2022

Risk Information

Risk Factor: High
CVSS v2.0 Base Score: 7.5
CVSS v2.0 Temporal Score: 5.5
CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P
CVSS v2.0 Temporal Vector: CVSS2#E:U/RL:OF/RC:C

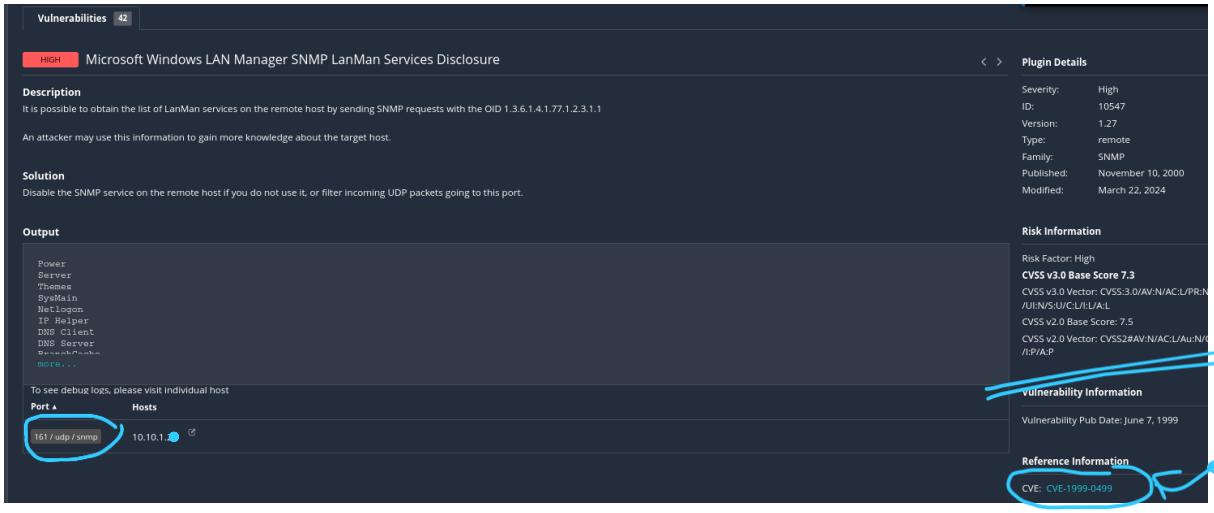
Vulnerability Information

Exploit Available: false
Exploit Ease: No exploit is required
Vulnerability Pub Date: November 17, 1998

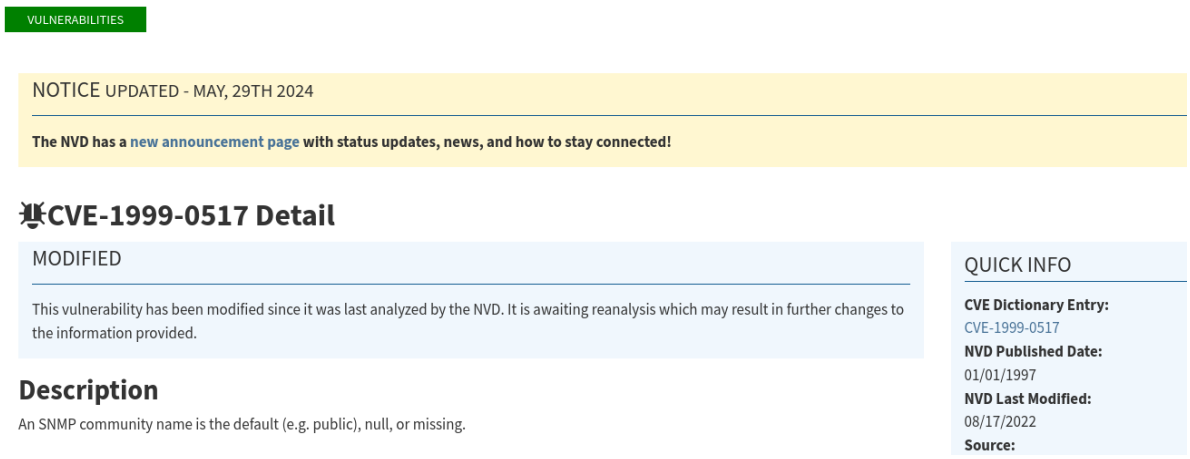
Reference Information

BID: 2112
CVE: CVE-1999-0517

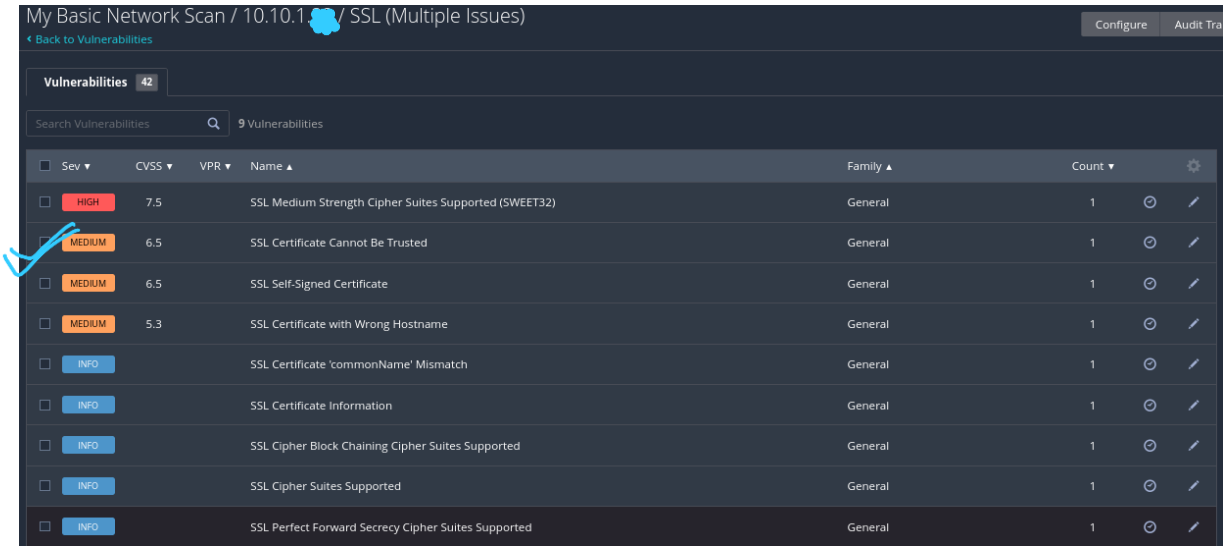
2.



Bottom right we can see reference infor, click on it which will redirect to a page which has detail on the information. This issue arises, when snmp community name is default ,null or missing.



Click on the second ,SSL(issues).You will find list of issues related to SSL.



Double click on the first critical option. Issues and solution are both given below.

HIGH SSL Medium Strength Cipher Suites Supported (SWEET32)

Description

The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.

Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.

Solution

Reconfigure the affected application if possible to avoid use of medium strength ciphers.

See Also

https://www.openssl.org/blog/blog/2016/08/24/sweet32/
https://sweet32.info

Output

```
  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    Name                        Code            KEX           Auth     Encryption            MAC
    ----------------------      ----------      ---           ----     --------------------  ---
    DES-CBC3-SHA                0x00, 0x0A      RSA           RSA      3DES-CBC(168)         SHA1

 The fields above are :

   {Tenable ciphername}
   {Cipher ID code}
   Kex={key exchange}
   Auth={authentication}
   Encrypt={symmetric encryption method}
   MAC={message authentication code}
   {export flag}
```

To see debug logs, please visit individual host

Port ▲	Hosts
3389 / tcp / msrdp	10.10.1.5

Conclusion: -

Recommendation: -

1. Close all un wanted port and services.
2. Use firewalls and ids to monitor incoming traffic to filter malicious packets.
3. Use of filters on open ports.
4. Only accept requests or packets from known systems.
5. Using of good password policy.
6. Follow the solution advised by Nessus above for each vulnerability.

----------END----------