Dor Amihai – John Bryce – class 7736.37 – lecturer's name Eliran Berkovitch Network Security Script (Project) – Summary

Program code: **ZX305**

Description:

A Bash automation script for controlled network reconnaissance, enumeration and credential-based PT testing on Kali Linux. The script is designed for lab environments and academic PT assignments: collect live hosts and services, enumerate AD-related artifacts (when credentials are provided), perform targeted vulnerability checks and controlled password testing, and produce a structured results package including a PDF report.

1. **User input** –
    - Target network: single IP or CIDR (strict validation).
    - Output directory name (default: SCAN_RESULTS).
    - Domain name and AD credentials (optional) — username/password.
    - Wordlist selection (default: rockyou.txt).
    - Operation level for each mode (Scanning, Enumeration, Exploitation): **Basic / Intermediate / Advanced / None (choose 0)**. Choosing a higher level includes preceding levels.

2. Scanning Mode (per project spec)

- **Basic**
    - Uses nmap -Pn to assume hosts are up.
- **Intermediate**
    - Full TCP port coverage using -p- or masscan -p1-65535 for speed.
- **Advanced**
    - Full UDP port coverage using -p- or masscan -p1-65535 for speed.

3. Enumeration Mode

- **Basic**
    - Identify services with -sV from the last results.
    - Detect Domain Controller IP (LDAP/AD indicators in nmap output). Using nmap -sV on open ports found in the TCP scan.

    - Detect DHCP server via nmap nse script.
- **Intermediate**
    - Enumerate which hosts running: FTP, SSH, SMB, WinRM, LDAP, RDP.
    - Enumerate shared folders (using smbmap, smbclient where permitted).
    - Include three NSE scripts relevant to domain enumeration (examples used):
        - smb-os-discovery.nse
        - smb-vuln-ms17-010.nse
        - nbstat.nse
- **Advanced** *(only if AD credentials provided)*
    - Extract all users.
    - Extract all groups.
    - Extract all shares.
    - Display password policy.
    - Find disabled accounts.
    - Find never-expiring accounts.
    - Display accounts within Domain Admins.

4. Exploitation Mode:

- **Basic**
    - Deploy the NSE vulnerability scanning script.
- **Intermediate**
    - Execute domain-wide password spraying to identify weak credentials by using the user's input pass list.
- **Advanced**
    - Extract and attempt to crack Kerberos tickets using pre-supplied passwords – users extracted from the script - and a python script. Than doing john on the Kerberos ticket and find the hash.

5. End result:

- All results are saved to the specified directory and a report is generated at the end.

6. **Creativity:**
   - Help menu. Used by ./script.sh -h

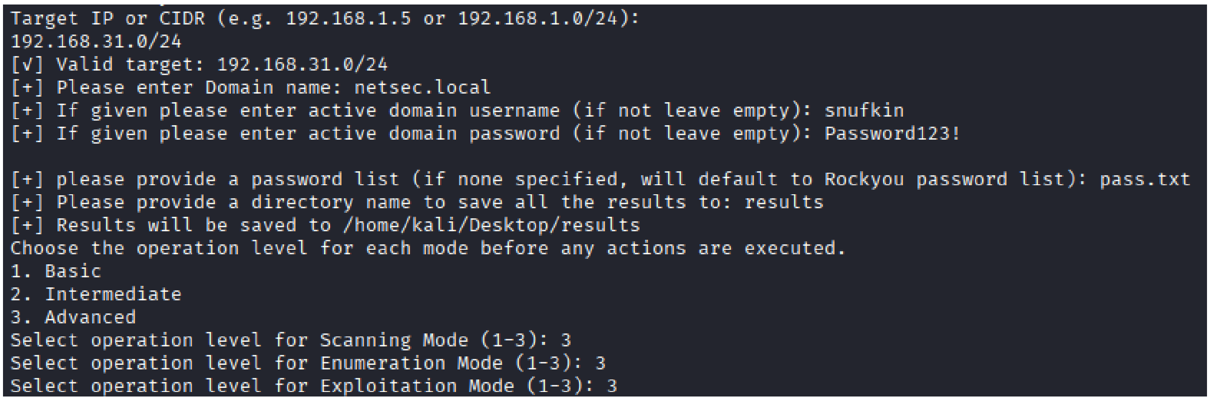
7. **Requirements:**
   - Run as root
   - Make sure the following packages are installed: nmap masscan smbmap crackmapexec john enscript ps2pdf python3

This ZIP file contains:

The script TMagen773637.s23.zx305.sh
This documentation summary

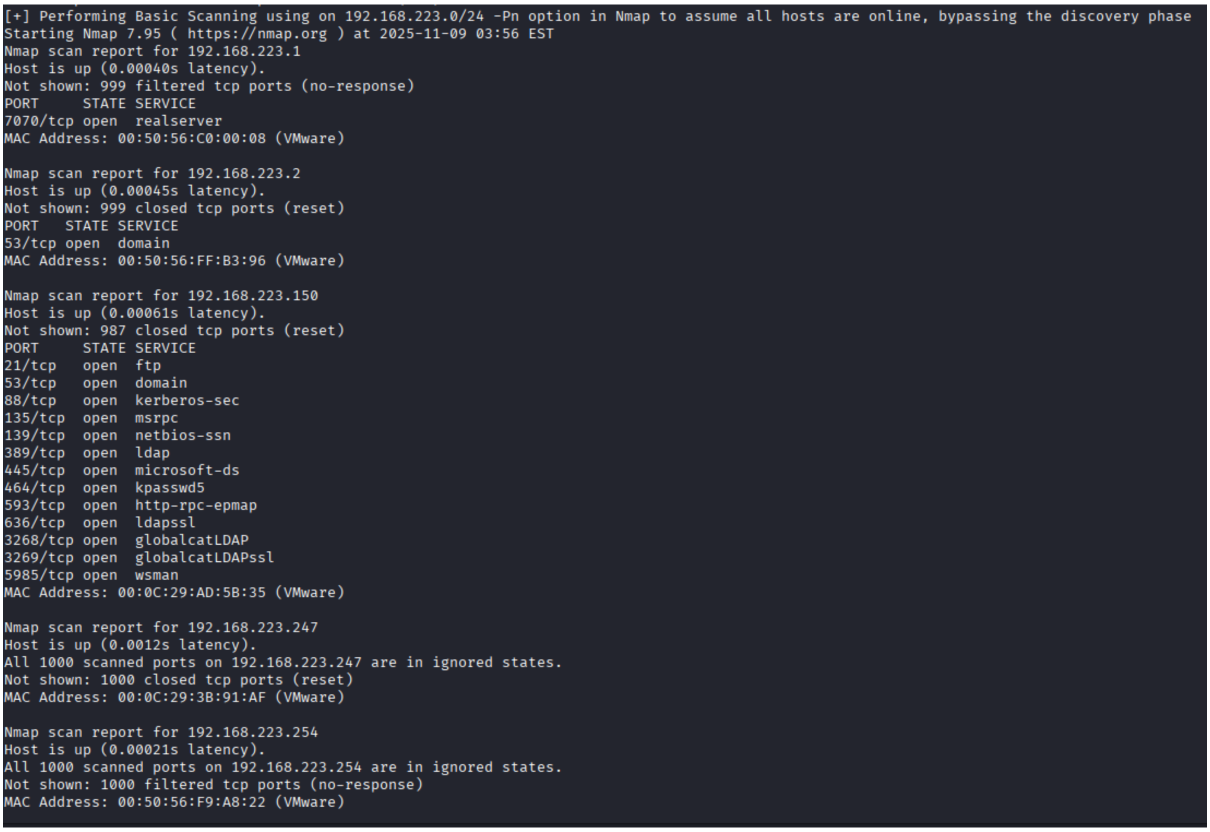
Project assignments proves:

1. Getting the User Input 1.1. Prompt the user to enter the target network range for scanning. 1.2. Ask for the Domain name and Active Directory (AD) credentials. 1.3. Prompt the user to choose a password list, defaulting to Rockyou if none is specified. 1.4. Require the user to select a desired operation level (Basic, Intermediate, Advanced or None) for each mode: Scanning, Enumeration, Exploitation. Note: Selection of a higher level automatically encompasses the capabilities of the preceding levels.

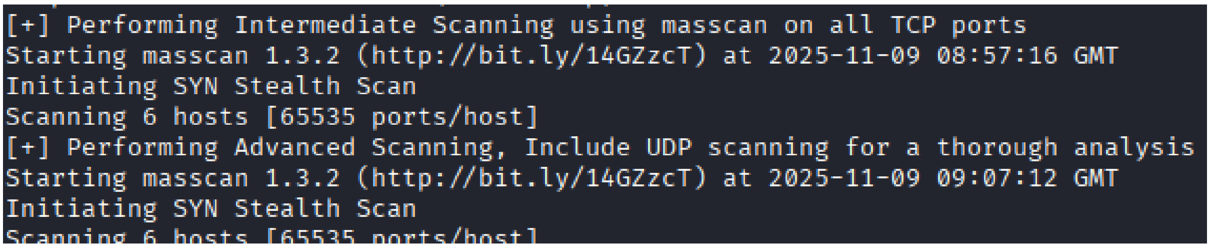


```
Target IP or CIDR (e.g. 192.168.1.5 or 192.168.1.0/24):
192.168.31.0/24
[√] Valid target: 192.168.31.0/24
[+] Please enter Domain name: netsec.local
[+] If given please enter active domain username (if not leave empty): snufkin
[+] If given please enter active domain password (if not leave empty): Password123!

[+] please provide a password list (if none specified, will default to Rockyou password list): pass.txt
[+] Please provide a directory name to save all the results to: results
[+] Results will be saved to /home/kali/Desktop/results
Choose the operation level for each mode before any actions are executed.
1. Basic
2. Intermediate
3. Advanced
Select operation level for Scanning Mode (1-3): 3
Select operation level for Enumeration Mode (1-3): 3
Select operation level for Exploitation Mode (1-3): 3
```

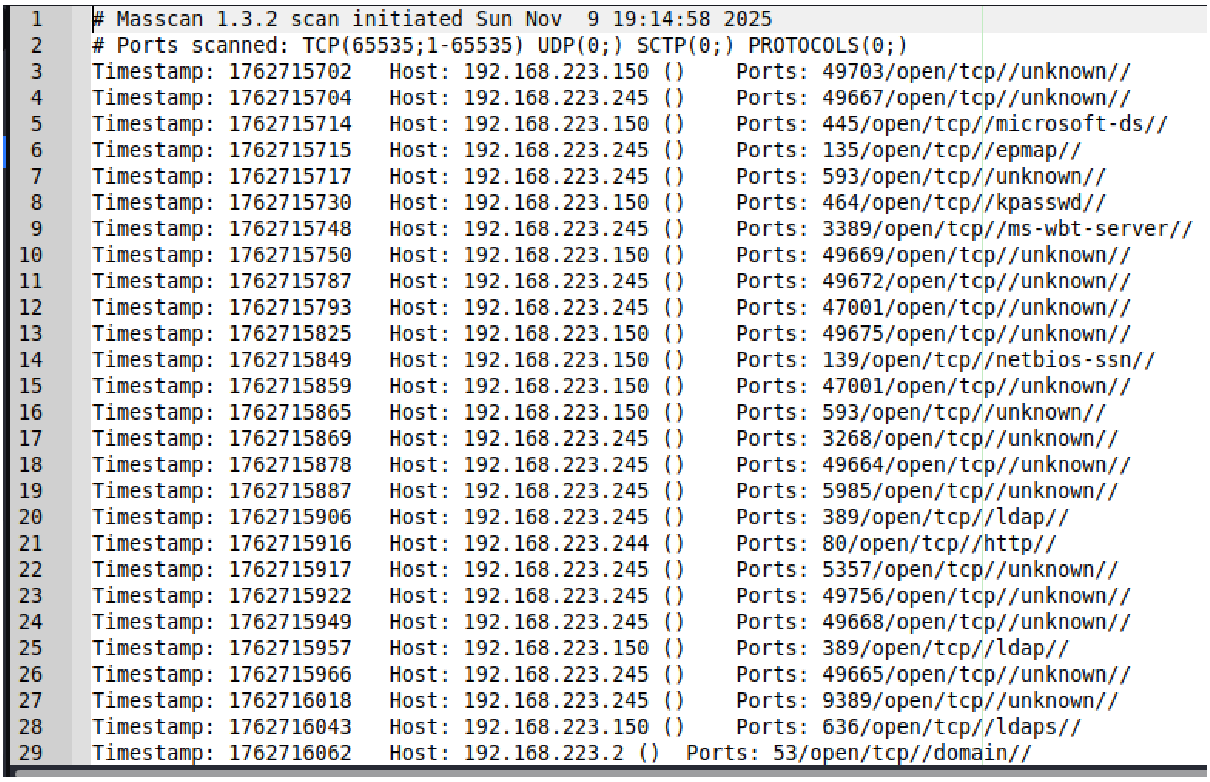
2. Scanning Mode 2.1. Basic: Use the -Pn option in Nmap to assume all hosts are online, bypassing the discovery phase. 2.2. Intermediate: Scan all 65535 ports using the -p- flag. 2.3. Advanced: Include UDP scanning for a thorough analysis.



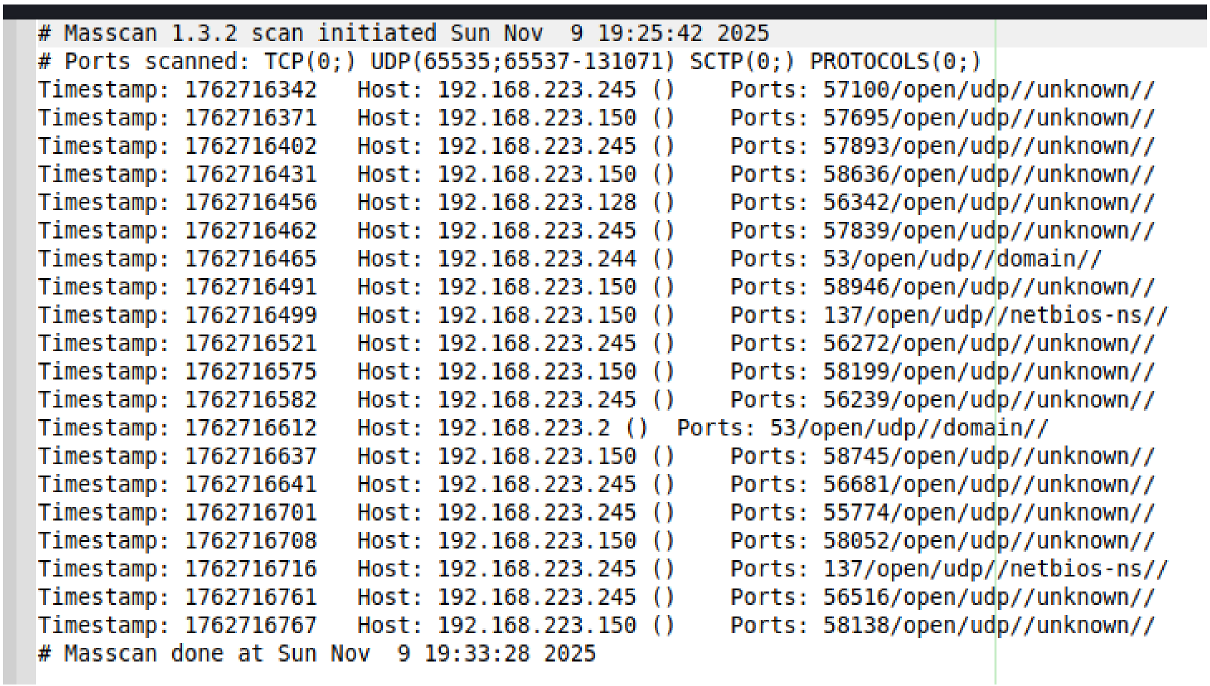
```
[+] Performing Basic Scanning using on 192.168.223.0/24 -Pn option in Nmap to assume all hosts are online, bypassing the discovery phase
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-09 03:56 EST
Nmap scan report for 192.168.223.1
Host is up (0.00040s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT     STATE SERVICE
7070/tcp open  realserver
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for 192.168.223.2
Host is up (0.00045s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
53/tcp open  domain
MAC Address: 00:50:56:FF:B3:96 (VMware)

Nmap scan report for 192.168.223.150
Host is up (0.00061s latency).
Not shown: 987 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
53/tcp   open  domain
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
3268/tcp open  globalcatLDAP
3269/tcp open  globalcatLDAPssl
5985/tcp open  wsman
MAC Address: 00:0C:29:AD:5B:35 (VMware)

Nmap scan report for 192.168.223.247
Host is up (0.0012s latency).
All 1000 scanned ports on 192.168.223.247 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 00:0C:29:3B:91:AF (VMware)

Nmap scan report for 192.168.223.254
Host is up (0.00021s latency).
All 1000 scanned ports on 192.168.223.254 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:F9:A8:22 (VMware)
```



```
[+] Performing Intermediate Scanning using masscan on all TCP ports
Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2025-11-09 08:57:16 GMT
Initiating SYN Stealth Scan
Scanning 6 hosts [65535 ports/host]
[+] Performing Advanced Scanning, Include UDP scanning for a thorough analysis
Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2025-11-09 09:07:12 GMT
Initiating SYN Stealth Scan
Scanning 6 hosts [65535 ports/host]
```



```
# Masscan 1.3.2 scan initiated Sun Nov  9 19:14:58 2025
# Ports scanned: TCP(65535;1-65535) UDP(0;) SCTP(0;) PROTOCOLS(0;)
Timestamp: 1762715702   Host: 192.168.223.150 ()    Ports: 49703/open/tcp//unknown//
Timestamp: 1762715704   Host: 192.168.223.245 ()    Ports: 49667/open/tcp//unknown//
Timestamp: 1762715714   Host: 192.168.223.150 ()    Ports: 445/open/tcp//microsoft-ds//
Timestamp: 1762715715   Host: 192.168.223.245 ()    Ports: 135/open/tcp//epmap//
Timestamp: 1762715717   Host: 192.168.223.245 ()    Ports: 593/open/tcp//unknown//
Timestamp: 1762715730   Host: 192.168.223.150 ()    Ports: 464/open/tcp//kpasswd//
Timestamp: 1762715748   Host: 192.168.223.245 ()    Ports: 3389/open/tcp//ms-wbt-server//
Timestamp: 1762715750   Host: 192.168.223.150 ()    Ports: 49669/open/tcp//unknown//
Timestamp: 1762715787   Host: 192.168.223.245 ()    Ports: 49672/open/tcp//unknown//
Timestamp: 1762715793   Host: 192.168.223.245 ()    Ports: 47001/open/tcp//unknown//
Timestamp: 1762715825   Host: 192.168.223.150 ()    Ports: 49675/open/tcp//unknown//
Timestamp: 1762715849   Host: 192.168.223.150 ()    Ports: 139/open/tcp//netbios-ssn//
Timestamp: 1762715859   Host: 192.168.223.150 ()    Ports: 47001/open/tcp//unknown//
Timestamp: 1762715865   Host: 192.168.223.150 ()    Ports: 593/open/tcp//unknown//
Timestamp: 1762715869   Host: 192.168.223.245 ()    Ports: 3268/open/tcp//unknown//
Timestamp: 1762715878   Host: 192.168.223.245 ()    Ports: 49664/open/tcp//unknown//
Timestamp: 1762715887   Host: 192.168.223.245 ()    Ports: 5985/open/tcp//unknown//
Timestamp: 1762715906   Host: 192.168.223.245 ()    Ports: 389/open/tcp//ldap//
Timestamp: 1762715916   Host: 192.168.223.244 ()    Ports: 80/open/tcp//http//
Timestamp: 1762715917   Host: 192.168.223.245 ()    Ports: 5357/open/tcp//unknown//
Timestamp: 1762715922   Host: 192.168.223.245 ()    Ports: 49756/open/tcp//unknown//
Timestamp: 1762715949   Host: 192.168.223.245 ()    Ports: 49668/open/tcp//unknown//
Timestamp: 1762715957   Host: 192.168.223.150 ()    Ports: 389/open/tcp//ldap//
Timestamp: 1762715966   Host: 192.168.223.245 ()    Ports: 49665/open/tcp//unknown//
Timestamp: 1762716018   Host: 192.168.223.245 ()    Ports: 9389/open/tcp//unknown//
Timestamp: 1762716043   Host: 192.168.223.150 ()    Ports: 636/open/tcp//ldaps//
Timestamp: 1762716062   Host: 192.168.223.2 ()  Ports: 53/open/tcp//domain//
```

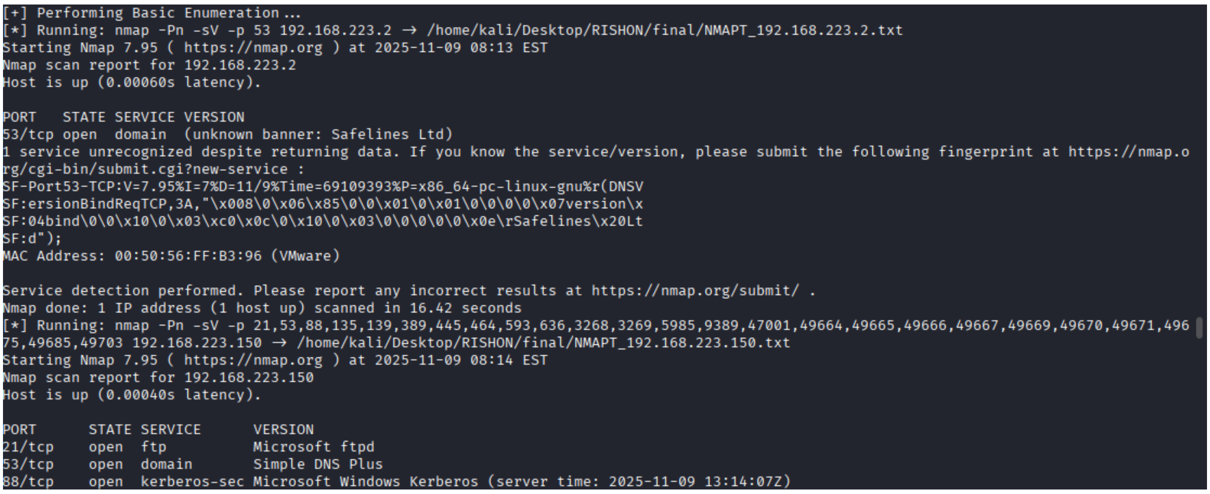


```
# Masscan 1.3.2 scan initiated Sun Nov  9 19:25:42 2025
# Ports scanned: TCP(0;) UDP(65535;65537-131071) SCTP(0;) PROTOCOLS(0;)
Timestamp: 1762716342   Host: 192.168.223.245 ()    Ports: 57100/open/udp//unknown//
Timestamp: 1762716371   Host: 192.168.223.150 ()    Ports: 57695/open/udp//unknown//
Timestamp: 1762716402   Host: 192.168.223.245 ()    Ports: 57893/open/udp//unknown//
Timestamp: 1762716431   Host: 192.168.223.150 ()    Ports: 58636/open/udp//unknown//
Timestamp: 1762716456   Host: 192.168.223.128 ()    Ports: 56342/open/udp//unknown//
Timestamp: 1762716462   Host: 192.168.223.245 ()    Ports: 57839/open/udp//unknown//
Timestamp: 1762716465   Host: 192.168.223.244 ()    Ports: 53/open/udp//domain//
Timestamp: 1762716491   Host: 192.168.223.150 ()    Ports: 58946/open/udp//unknown//
Timestamp: 1762716499   Host: 192.168.223.150 ()    Ports: 137/open/udp//netbios-ns//
Timestamp: 1762716521   Host: 192.168.223.245 ()    Ports: 56272/open/udp//unknown//
Timestamp: 1762716575   Host: 192.168.223.150 ()    Ports: 58199/open/udp//unknown//
Timestamp: 1762716582   Host: 192.168.223.245 ()    Ports: 56239/open/udp//unknown//
Timestamp: 1762716612   Host: 192.168.223.2 ()  Ports: 53/open/udp//domain//
Timestamp: 1762716637   Host: 192.168.223.150 ()    Ports: 58745/open/udp//unknown//
Timestamp: 1762716641   Host: 192.168.223.245 ()    Ports: 56681/open/udp//unknown//
Timestamp: 1762716701   Host: 192.168.223.245 ()    Ports: 55774/open/udp//unknown//
Timestamp: 1762716708   Host: 192.168.223.150 ()    Ports: 58052/open/udp//unknown//
Timestamp: 1762716716   Host: 192.168.223.245 ()    Ports: 137/open/udp//netbios-ns//
Timestamp: 1762716761   Host: 192.168.223.245 ()    Ports: 56516/open/udp//unknown//
Timestamp: 1762716767   Host: 192.168.223.150 ()    Ports: 58138/open/udp//unknown//
# Masscan done at Sun Nov  9 19:33:28 2025
```

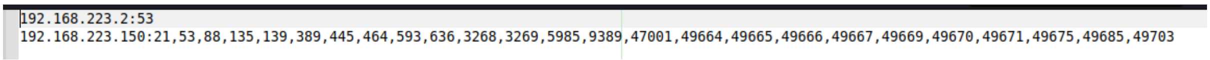
3. Enumeration Mode

3.1. Basic: 3.1.1. Identify services (-sV) running on open ports. 3.1.2. Identify the IP Address of the Domain Controller. 3.1.3. Identify the IP Address of the DHCP server.

Using nmap -sV for every live host from the tcp scan. The script create an isolated file called: open_ports_to_scan.txt, in order to do this.



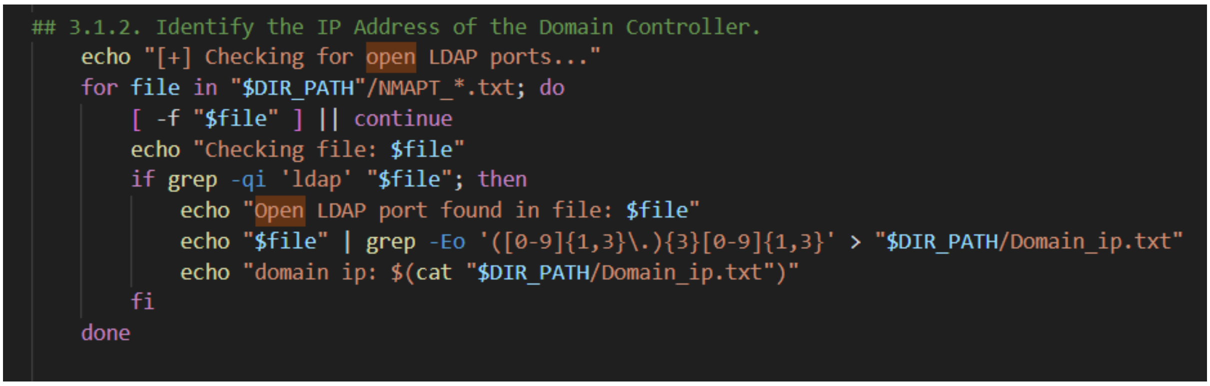
```
[+] Performing Basic Enumeration ...
[*] Running: nmap -Pn -sV -p 53 192.168.223.2 → /home/kali/Desktop/RISHON/final/NMAPT_192.168.223.2.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-09 08:13 EST
Nmap scan report for 192.168.223.2
Host is up (0.00060s latency).

PORT   STATE SERVICE VERSION
53/tcp open  domain  (unknown banner: Safelines Ltd)
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.o
rg/cgi-bin/submit.cgi?new-service :
SF-Port53-TCP:V=7.95%I=7%D=11/9%Time=69109393%P=x86_64-pc-linux-gnu%r(DNSV
SF:ersionBindReqTCP,3A,"\x008\0\x06\x85\0\0\x01\0\x01\0\0\0\0\x07version\x
SF:04bind\0\0\x10\0\x03\xc0\x0c\0\x10\0\x03\0\0\0\0\0\x0e\rSafelines\x20Lt
SF:d");
MAC Address: 00:50:56:FF:B3:96 (VMware)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.42 seconds
[*] Running: nmap -Pn -sV -p 21,53,88,135,139,389,445,464,593,636,3268,3269,5985,9389,47001,49664,49665,49666,49667,49669,49670,49671,496
75,49685,49703 192.168.223.150 → /home/kali/Desktop/RISHON/final/NMAPT_192.168.223.150.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-09 08:14 EST
Nmap scan report for 192.168.223.150
Host is up (0.00040s latency).

PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          Microsoft ftpd
53/tcp    open  domain       Simple DNS Plus
88/tcp    open  kerberos-sec Microsoft Windows Kerberos (server time: 2025-11-09 13:14:07Z)
```



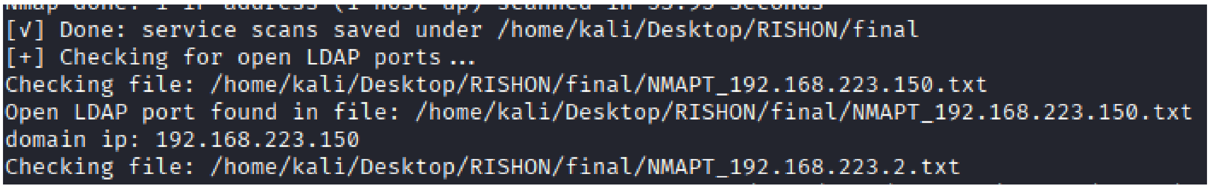
```
192.168.223.2:53
192.168.223.150:21,53,88,135,139,389,445,464,593,636,3268,3269,5985,9389,47001,49664,49665,49666,49667,49669,49670,49671,49675,49685,49703
```

All results saved under NMAPT_*.txt

Domain controller is being found by text manipulation (grep) on the results text files.

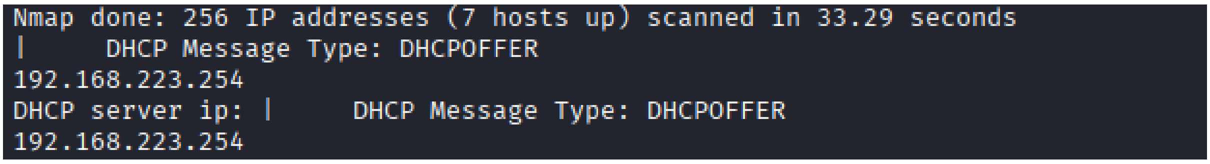


```
## 3.1.2. Identify the IP Address of the Domain Controller.
    echo "[+] Checking for open LDAP ports..."
    for file in "$DIR_PATH"/NMAPT_*.txt; do
        [ -f "$file" ] || continue
        echo "Checking file: $file"
        if grep -qi 'ldap' "$file"; then
            echo "Open LDAP port found in file: $file"
            echo "$file" | grep -Eo '([0-9]{1,3}\.){3}[0-9]{1,3}' > "$DIR_PATH/Domain_ip.txt"
            echo "domain ip: $(cat "$DIR_PATH/Domain_ip.txt")"
        fi
    done
```



```
Nmap done: 1 IP address (1 host up) scanned in 33.93 seconds
[√] Done: service scans saved under /home/kali/Desktop/RISHON/final
[+] Checking for open LDAP ports ...
Checking file: /home/kali/Desktop/RISHON/final/NMAPT_192.168.223.150.txt
Open LDAP port found in file: /home/kali/Desktop/RISHON/final/NMAPT_192.168.223.150.txt
domain ip: 192.168.223.150
Checking file: /home/kali/Desktop/RISHON/final/NMAPT_192.168.223.2.txt
```

For DHCP server, nmap --script broadcast-dhcp-discover on the $net, then with text manipulation finding DHCP server:

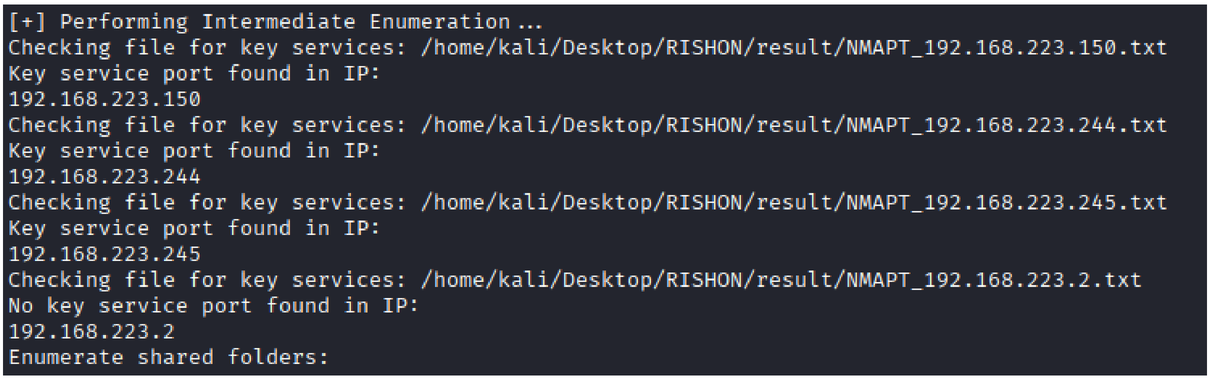


```
Nmap done: 256 IP addresses (7 hosts up) scanned in 33.29 seconds
|     DHCP Message Type: DHCPOFFER
192.168.223.254
DHCP server ip: |     DHCP Message Type: DHCPOFFER
192.168.223.254
```

Result saved under dhcp_discover.txt.

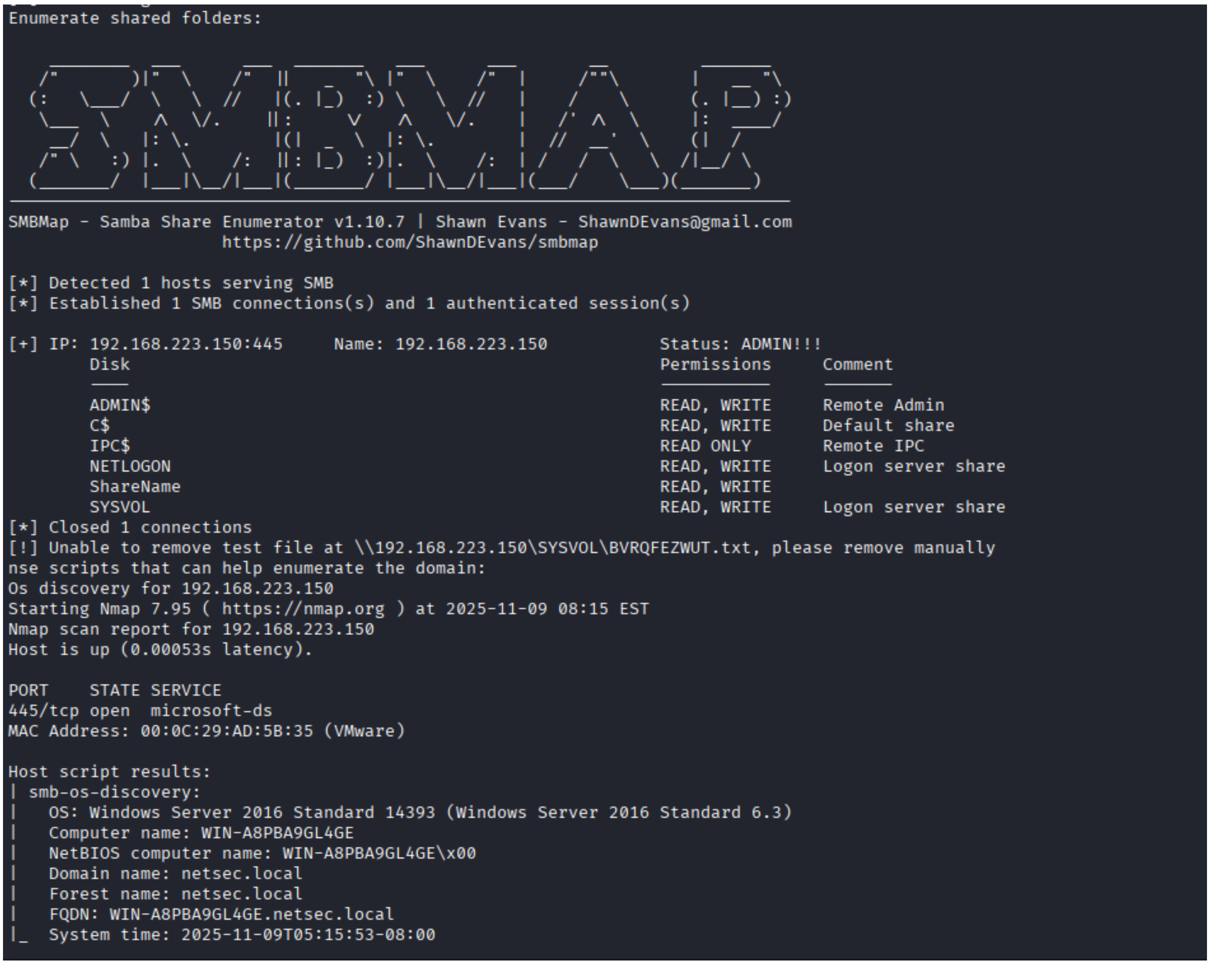
3.2. Intermediate: 3.2.1. Enumerate IPs for key services: FTP, SSH, SMB, WinRM, LDAP, RDP. 3.2.2. Enumerate shared folders. 3.2.3. Add three (3) NSE scripts you think can be relevant for enumerating domain networks.

Text manipulation on the open services results to see which IP'S contains the key services:



```
[+] Performing Intermediate Enumeration ...
Checking file for key services: /home/kali/Desktop/RISHON/result/NMAPT_192.168.223.150.txt
Key service port found in IP:
192.168.223.150
Checking file for key services: /home/kali/Desktop/RISHON/result/NMAPT_192.168.223.244.txt
Key service port found in IP:
192.168.223.244
Checking file for key services: /home/kali/Desktop/RISHON/result/NMAPT_192.168.223.245.txt
Key service port found in IP:
192.168.223.245
Checking file for key services: /home/kali/Desktop/RISHON/result/NMAPT_192.168.223.2.txt
No key service port found in IP:
192.168.223.2
Enumerate shared folders:
```

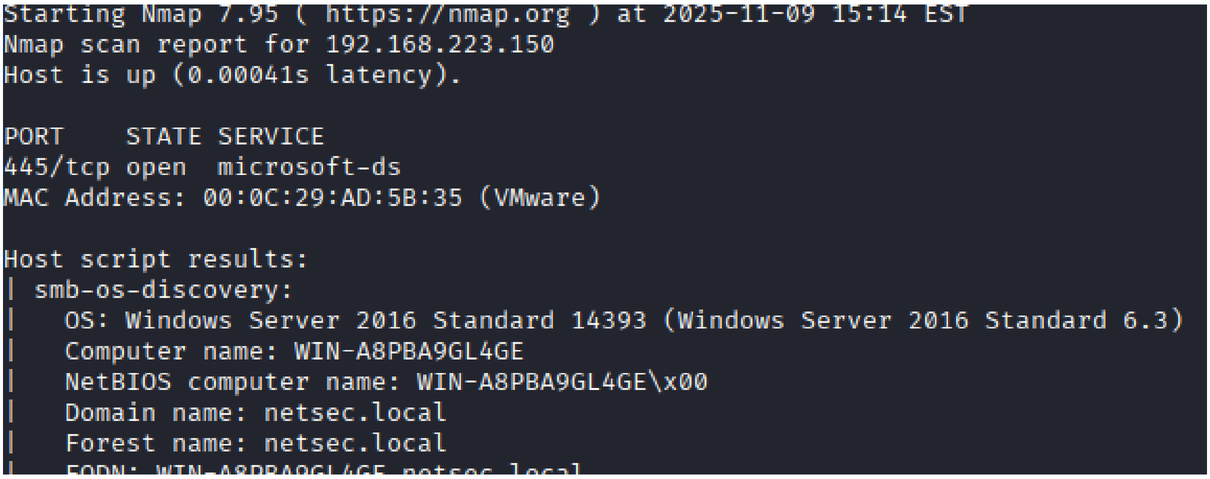
Enumerate shared folder by using smbmap with the user cardentials.



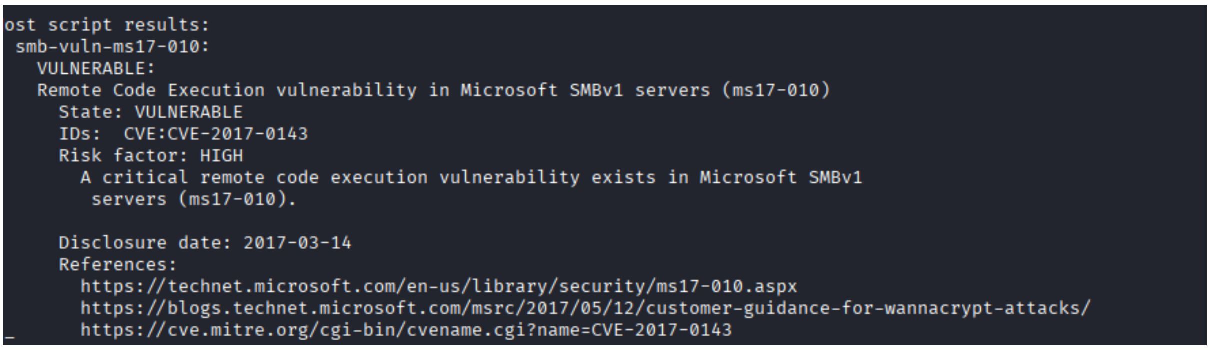
```
Enumerate shared folders:

    ________  ___      ___  _______   ___      ___       __         _______
   /"       )|"  \    /"  ||   _  "\ |"  \    /"  |     /""\       |   __ "\
  (:   \___/  \   \  //   |(. |_)  :) \   \  //   |    /    \      (. |__) :)
   \___  \    /\  \/.    ||:     \/   /\  \/.    |   /' /\  \     |:  ____/
    __/  \  |: \.        |(|  _  \  |: \.        |  //  __'  \    (|  /
   /" \   :) |.  \    /:  ||: |_)  :) |.  \    /:  | /   /  \  \  /|__/ \
  (_______/  |___|\__/|___|(_______/  |___|\__/|___|(___/    \___)(_______)
 -----------------------------------------------------------------------------
SMBMap - Samba Share Enumerator v1.10.7 | Shawn Evans - ShawnDEvans@gmail.com
                     https://github.com/ShawnDEvans/smbmap

[*] Detected 1 hosts serving SMB
[*] Established 1 SMB connections(s) and 1 authenticated session(s)

[+] IP: 192.168.223.150:445     Name: 192.168.223.150           Status: ADMIN!!!
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        ADMIN$                                                  READ, WRITE     Remote Admin
        C$                                                      READ, WRITE     Default share
        IPC$                                                    READ ONLY       Remote IPC
        NETLOGON                                                READ, WRITE     Logon server share
        ShareName                                               READ, WRITE
        SYSVOL                                                  READ, WRITE     Logon server share
[*] Closed 1 connections
[!] Unable to remove test file at \\192.168.223.150\SYSVOL\BVRQFEZWUT.txt, please remove manually
nse scripts that can help enumerate the domain:
Os discovery for 192.168.223.150
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-09 08:15 EST
Nmap scan report for 192.168.223.150
Host is up (0.00053s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:AD:5B:35 (VMware)

Host script results:
| smb-os-discovery:
|   OS: Windows Server 2016 Standard 14393 (Windows Server 2016 Standard 6.3)
|   Computer name: WIN-A8PBA9GL4GE
|   NetBIOS computer name: WIN-A8PBA9GL4GE\x00
|   Domain name: netsec.local
|   Forest name: netsec.local
|   FQDN: WIN-A8PBA9GL4GE.netsec.local
|_  System time: 2025-11-09T05:15:53-08:00
```

I added three nse scripts which I think are important for enumeration

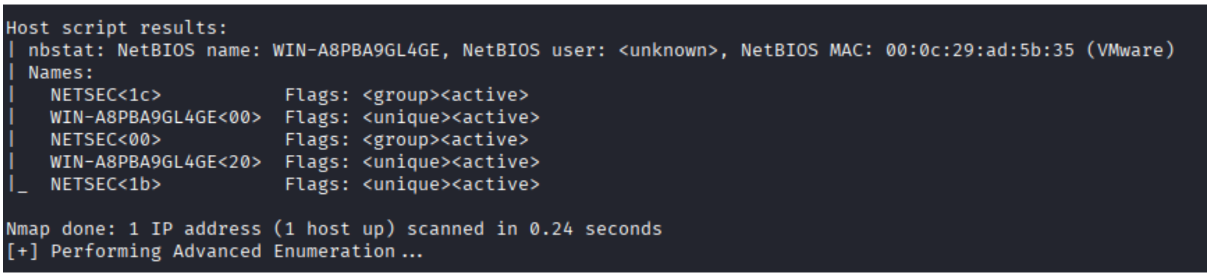
Os discovery , NetBIOS / NetBT name enumeration (nbstat), Vuln MS17-010



```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-09 15:14 EST
Nmap scan report for 192.168.223.150
Host is up (0.00041s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:AD:5B:35 (VMware)

Host script results:
| smb-os-discovery:
|   OS: Windows Server 2016 Standard 14393 (Windows Server 2016 Standard 6.3)
|   Computer name: WIN-A8PBA9GL4GE
|   NetBIOS computer name: WIN-A8PBA9GL4GE\x00
|   Domain name: netsec.local
|   Forest name: netsec.local
|   FQDN: WIN-A8PBA9GL4GE.netsec.local
```



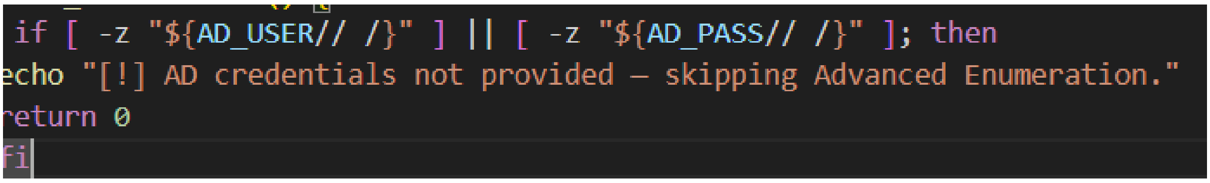
```
ost script results:
 smb-vuln-ms17-010:
   VULNERABLE:
   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
     State: VULNERABLE
     IDs:  CVE:CVE-2017-0143
     Risk factor: HIGH
       A critical remote code execution vulnerability exists in Microsoft SMBv1
        servers (ms17-010).

     Disclosure date: 2017-03-14
     References:
       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
```



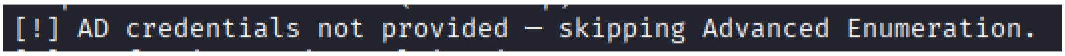
```
Host script results:
| nbstat: NetBIOS name: WIN-A8PBA9GL4GE, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:ad:5b:35 (VMware)
| Names:
|   NETSEC<1c>           Flags: <group><active>
|   WIN-A8PBA9GL4GE<00>  Flags: <unique><active>
|   NETSEC<00>           Flags: <group><active>
|   WIN-A8PBA9GL4GE<20>  Flags: <unique><active>
|_  NETSEC<1b>           Flags: <unique><active>

Nmap done: 1 IP address (1 host up) scanned in 0.24 seconds
[+] Performing Advanced Enumeration...
```

3.3. Advanced (Only if AD credentials were entered): 3.3.1. Extract all users. 3.3.2. Extract all groups. 3.3.3. Extract all shares. 3.3.4. Display password policy. 3.3.5. Find disabled accounts. 3.3.6. Find never-expired accounts. 3.3.7. Display accounts that are members of the Domain Admins group.

1st rule:



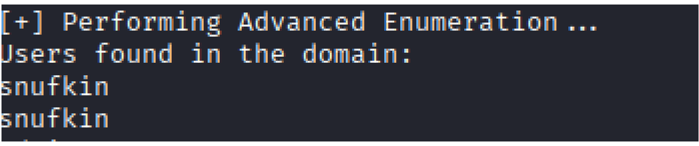
```
 if [ -z "${AD_USER// /}" ] || [ -z "${AD_PASS// /}" ]; then
echo "[!] AD credentials not provided — skipping Advanced Enumeration."
return 0
fi
```



```
 [!] AD credentials not provided — skipping Advanced Enumeration.
```

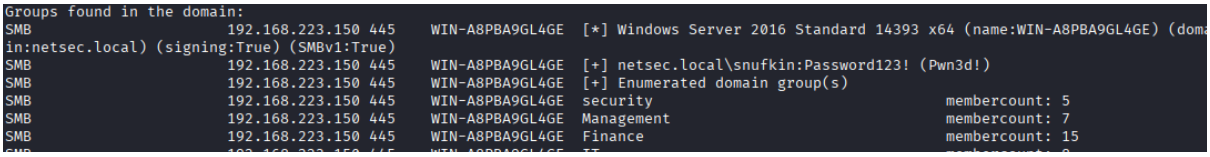
Than doing all asked by using crackmapexec smb command

1.



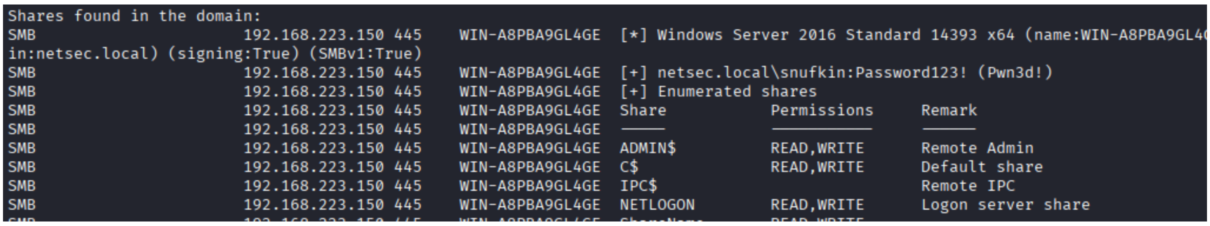
```
[+] Performing Advanced Enumeration...
Users found in the domain:
snufkin
snufkin
```

2.



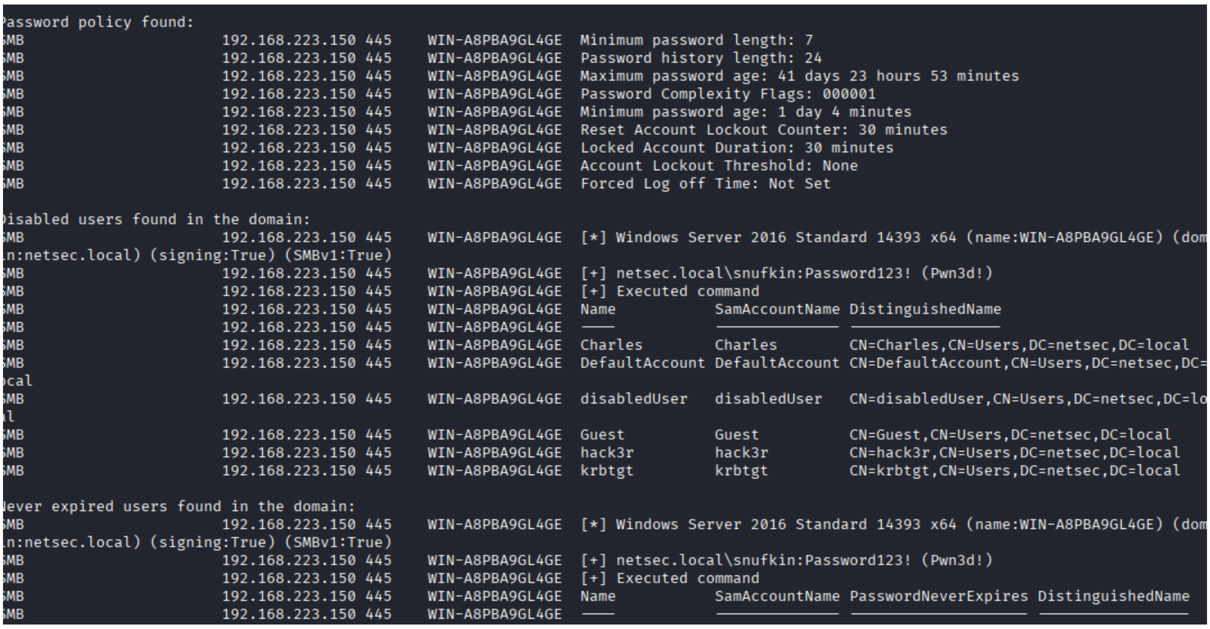
```
Groups found in the domain:
SMB                      192.168.223.150 445    WIN-A8PBA9GL4GE  [*] Windows Server 2016 Standard 14393 x64 (name:WIN-A8PBA9GL4GE) (doma
in:netsec.local) (signing:True) (SMBv1:True)
SMB                      192.168.223.150 445    WIN-A8PBA9GL4GE  [+] netsec.local\snufkin:Password123! (Pwn3d!)
SMB                      192.168.223.150 445    WIN-A8PBA9GL4GE  [+] Enumerated domain group(s)
SMB                      192.168.223.150 445    WIN-A8PBA9GL4GE  security                                 membercount: 5
SMB                      192.168.223.150 445    WIN-A8PBA9GL4GE  Management                               membercount: 7
SMB                      192.168.223.150 445    WIN-A8PBA9GL4GE  Finance                                  membercount: 15
```

3.



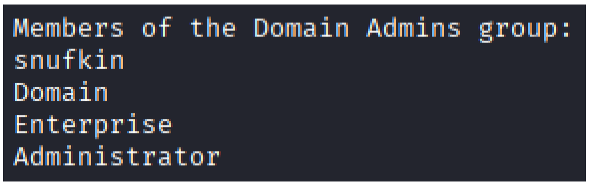
```
Shares found in the domain:
SMB                      192.168.223.150 445    WIN-A8PBA9GL4GE  [*] Windows Server 2016 Standard 14393 x64 (name:WIN-A8PBA9GL4G
in:netsec.local) (signing:True) (SMBv1:True)
SMB                      192.168.223.150 445    WIN-A8PBA9GL4GE  [+] netsec.local\snufkin:Password123! (Pwn3d!)
SMB                      192.168.223.150 445    WIN-A8PBA9GL4GE  [+] Enumerated shares
SMB                      192.168.223.150 445    WIN-A8PBA9GL4GE  Share           Permissions     Remark
SMB                      192.168.223.150 445    WIN-A8PBA9GL4GE  -----           -----------     ------
SMB                      192.168.223.150 445    WIN-A8PBA9GL4GE  ADMIN$          READ,WRITE      Remote Admin
SMB                      192.168.223.150 445    WIN-A8PBA9GL4GE  C$              READ,WRITE      Default share
SMB                      192.168.223.150 445    WIN-A8PBA9GL4GE  IPC$                            Remote IPC
SMB                      192.168.223.150 445    WIN-A8PBA9GL4GE  NETLOGON        READ,WRITE      Logon server share
```

4.5.6.



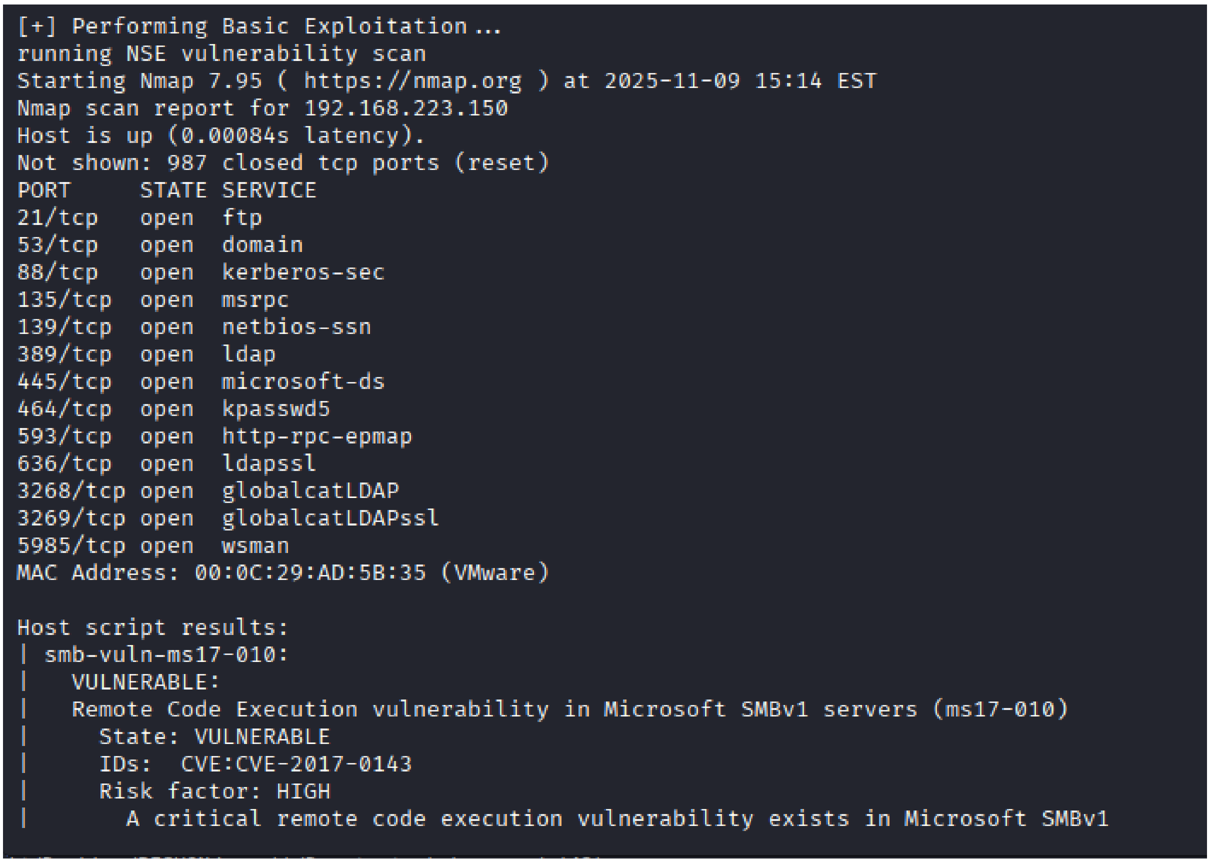
```
assword policy found:
MB                      192.168.223.150 445    WIN-A8PBA9GL4GE  Minimum password length: 7
MB                      192.168.223.150 445    WIN-A8PBA9GL4GE  Password history length: 24
MB                      192.168.223.150 445    WIN-A8PBA9GL4GE  Maximum password age: 41 days 23 hours 53 minutes
MB                      192.168.223.150 445    WIN-A8PBA9GL4GE  Password Complexity Flags: 000001
MB                      192.168.223.150 445    WIN-A8PBA9GL4GE  Minimum password age: 1 day 4 minutes
MB                      192.168.223.150 445    WIN-A8PBA9GL4GE  Reset Account Lockout Counter: 30 minutes
MB                      192.168.223.150 445    WIN-A8PBA9GL4GE  Locked Account Duration: 30 minutes
MB                      192.168.223.150 445    WIN-A8PBA9GL4GE  Account Lockout Threshold: None
MB                      192.168.223.150 445    WIN-A8PBA9GL4GE  Forced Log off Time: Not Set

isabled users found in the domain:
MB                      192.168.223.150 445    WIN-A8PBA9GL4GE  [*] Windows Server 2016 Standard 14393 x64 (name:WIN-A8PBA9GL4GE) (dom
n:netsec.local) (signing:True) (SMBv1:True)
MB                      192.168.223.150 445    WIN-A8PBA9GL4GE  [+] netsec.local\snufkin:Password123! (Pwn3d!)
MB                      192.168.223.150 445    WIN-A8PBA9GL4GE  [+] Executed command
MB                      192.168.223.150 445    WIN-A8PBA9GL4GE  Name           SamAccountName DistinguishedName
MB                      192.168.223.150 445    WIN-A8PBA9GL4GE  ----           -------------- -----------------
MB                      192.168.223.150 445    WIN-A8PBA9GL4GE  Charles        Charles        CN=Charles,CN=Users,DC=netsec,DC=local
MB                      192.168.223.150 445    WIN-A8PBA9GL4GE  DefaultAccount DefaultAccount CN=DefaultAccount,CN=Users,DC=netsec,DC=
cal
MB                      192.168.223.150 445    WIN-A8PBA9GL4GE  disabledUser   disabledUser   CN=disabledUser,CN=Users,DC=netsec,DC=lo
l
MB                      192.168.223.150 445    WIN-A8PBA9GL4GE  Guest          Guest          CN=Guest,CN=Users,DC=netsec,DC=local
MB                      192.168.223.150 445    WIN-A8PBA9GL4GE  hack3r         hack3r         CN=hack3r,CN=Users,DC=netsec,DC=local
MB                      192.168.223.150 445    WIN-A8PBA9GL4GE  krbtgt         krbtgt         CN=krbtgt,CN=Users,DC=netsec,DC=local

ever expired users found in the domain:
MB                      192.168.223.150 445    WIN-A8PBA9GL4GE  [*] Windows Server 2016 Standard 14393 x64 (name:WIN-A8PBA9GL4GE) (dom
n:netsec.local) (signing:True) (SMBv1:True)
MB                      192.168.223.150 445    WIN-A8PBA9GL4GE  [+] netsec.local\snufkin:Password123! (Pwn3d!)
MB                      192.168.223.150 445    WIN-A8PBA9GL4GE  [+] Executed command
MB                      192.168.223.150 445    WIN-A8PBA9GL4GE  Name           SamAccountName PasswordNeverExpires DistinguishedName
MB                      192.168.223.150 445    WIN-A8PBA9GL4GE  ----           -------------- -------------------- -----------------
```

7.



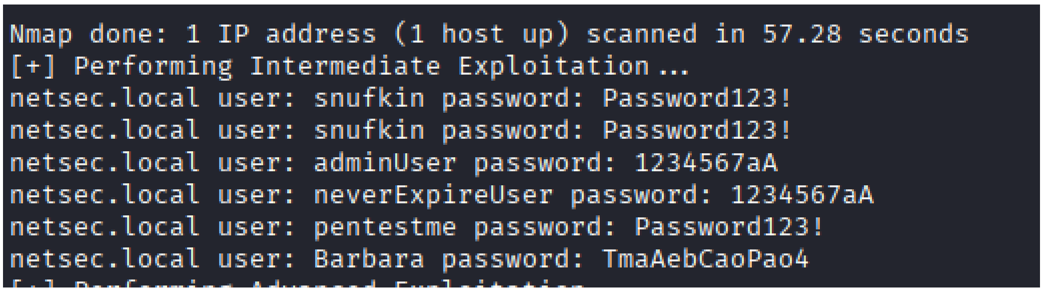
```
Members of the Domain Admins group:
snufkin
Domain
Enterprise
Administrator
```

4. Exploitation Mode 4.1. Basic: Deploy the NSE vulnerability scanning script. 4.2. Intermediate: Execute domain-wide password spraying to identify weak credentials. 4.3. Advanced: Extract and attempt to crack Kerberos tickets using pre-supplied passwords.



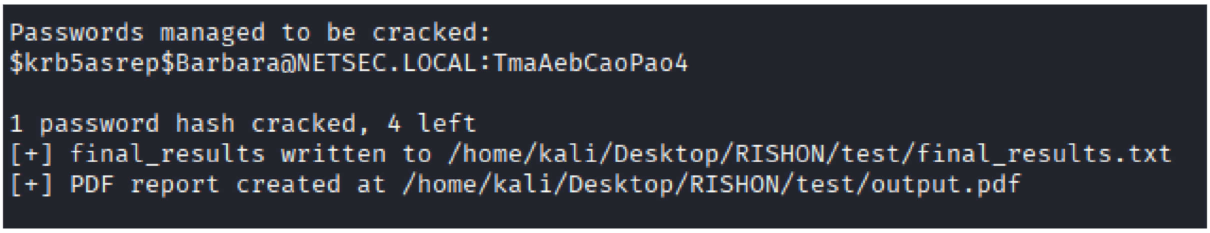
```
[+] Performing Basic Exploitation ...
running NSE vulnerability scan
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-09 15:14 EST
Nmap scan report for 192.168.223.150
Host is up (0.00084s latency).
Not shown: 987 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
53/tcp   open  domain
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
3268/tcp open  globalcatLDAP
3269/tcp open  globalcatLDAPssl
5985/tcp open  wsman
MAC Address: 00:0C:29:AD:5B:35 (VMware)

Host script results:
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
```

Password spraying used by crackmapexec smb continue on success.



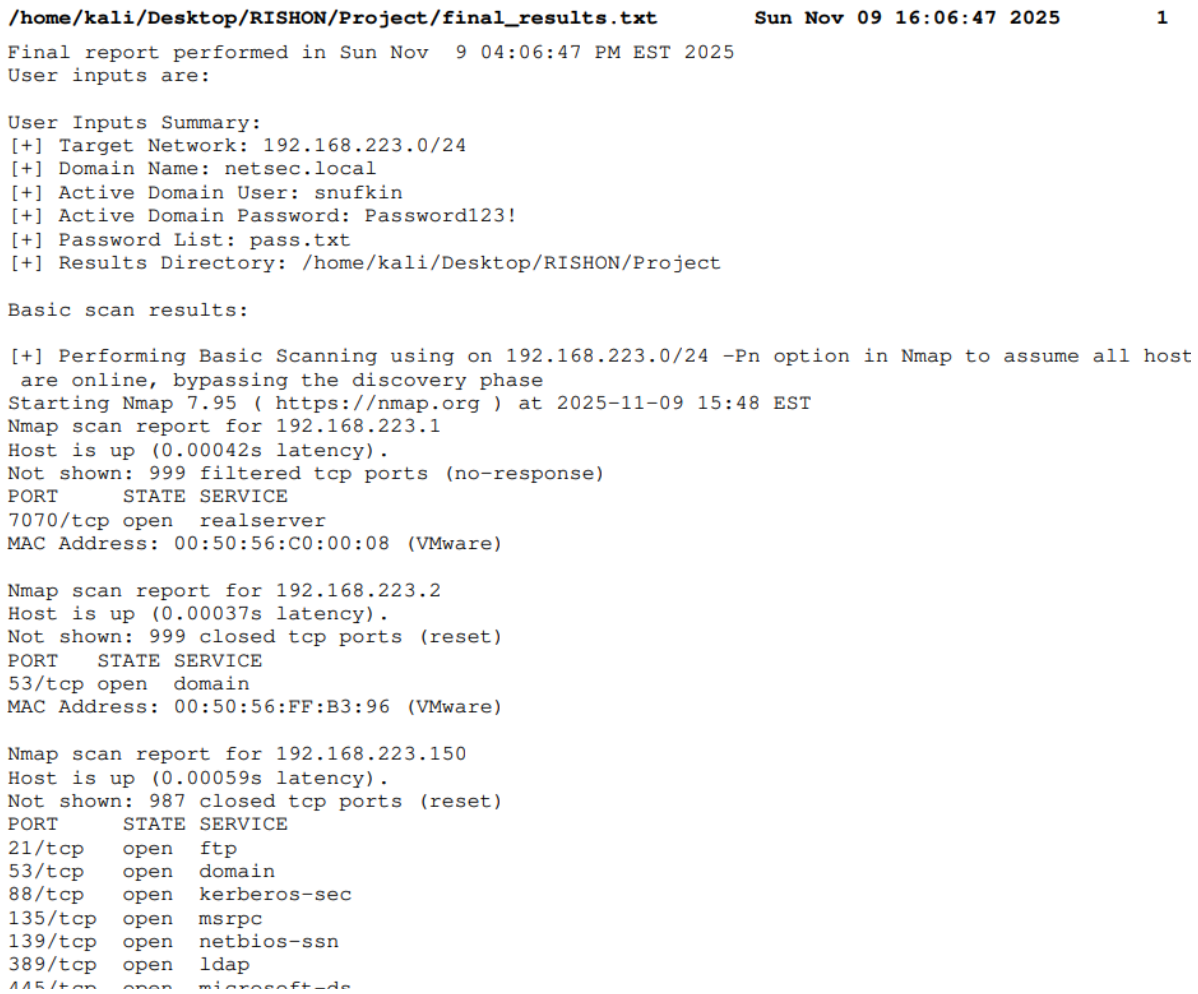
```
Nmap done: 1 IP address (1 host up) scanned in 57.28 seconds
[+] Performing Intermediate Exploitation ...
netsec.local user: snufkin password: Password123!
netsec.local user: snufkin password: Password123!
netsec.local user: adminUser password: 1234567aA
netsec.local user: neverExpireUser password: 1234567aA
netsec.local user: pentestme password: Password123!
netsec.local user: Barbara password: TmaAebCaoPao4
```

Producing Kerberos ticket using GetNPUsers python and john.



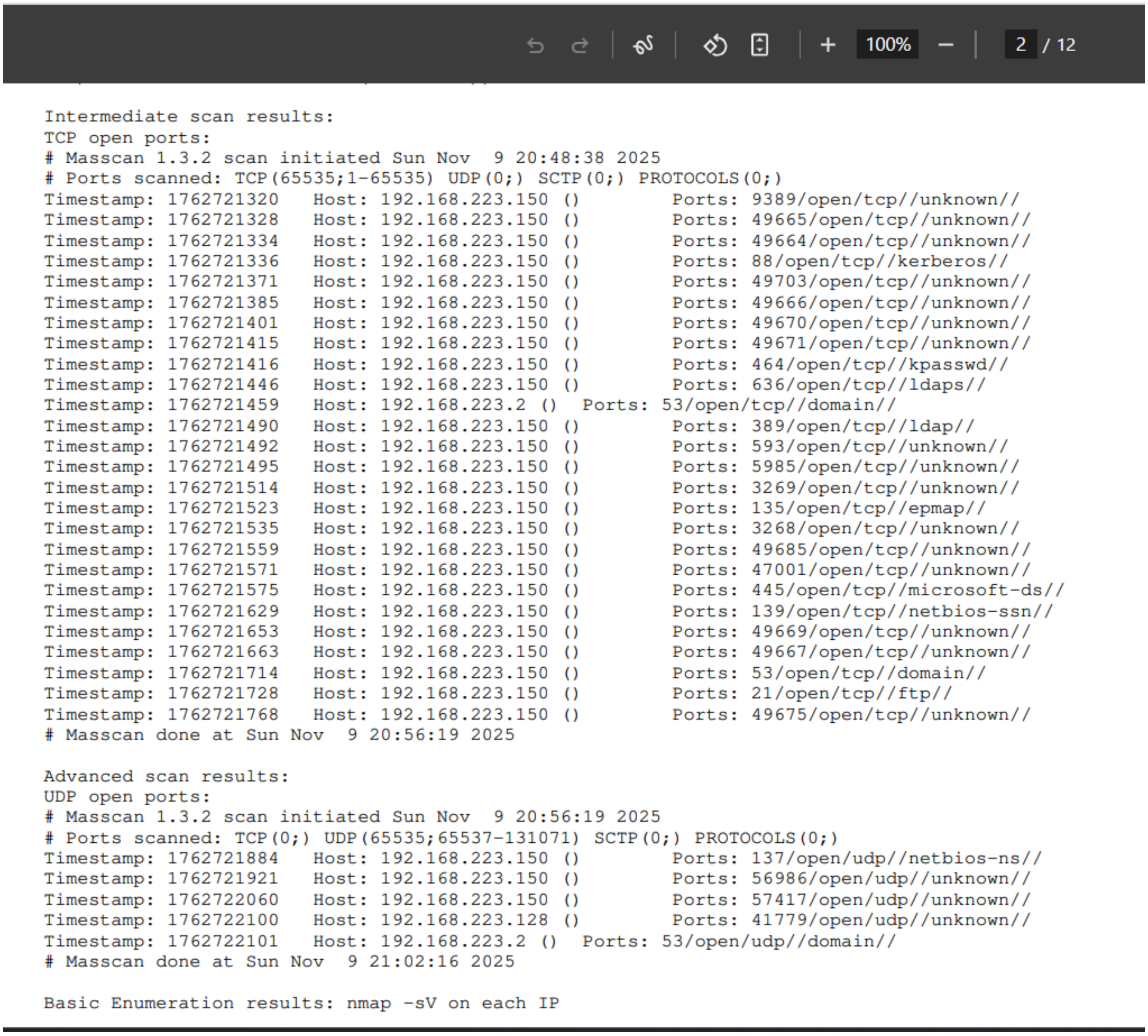
```
Passwords managed to be cracked:
$krb5asrep$Barbara@NETSEC.LOCAL:TmaAebCaoPao4

1 password hash cracked, 4 left
[+] final_results written to /home/kali/Desktop/RISHON/test/final_results.txt
[+] PDF report created at /home/kali/Desktop/RISHON/test/output.pdf
```

All results saved to pdf. For example

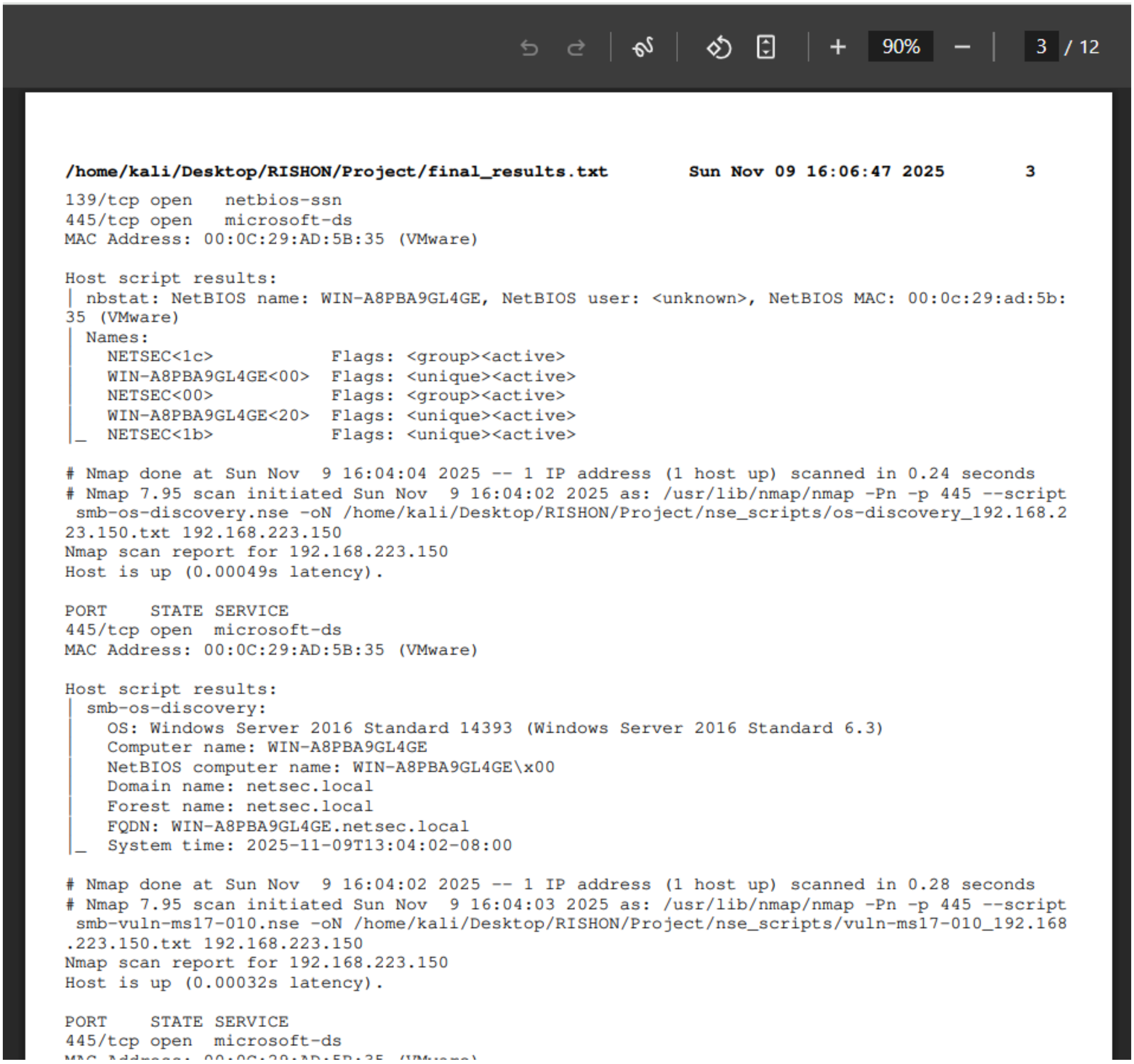


/home/kali/Desktop/RISHON/Project/final_results.txt   Sun Nov 09 16:06:47 2025   1

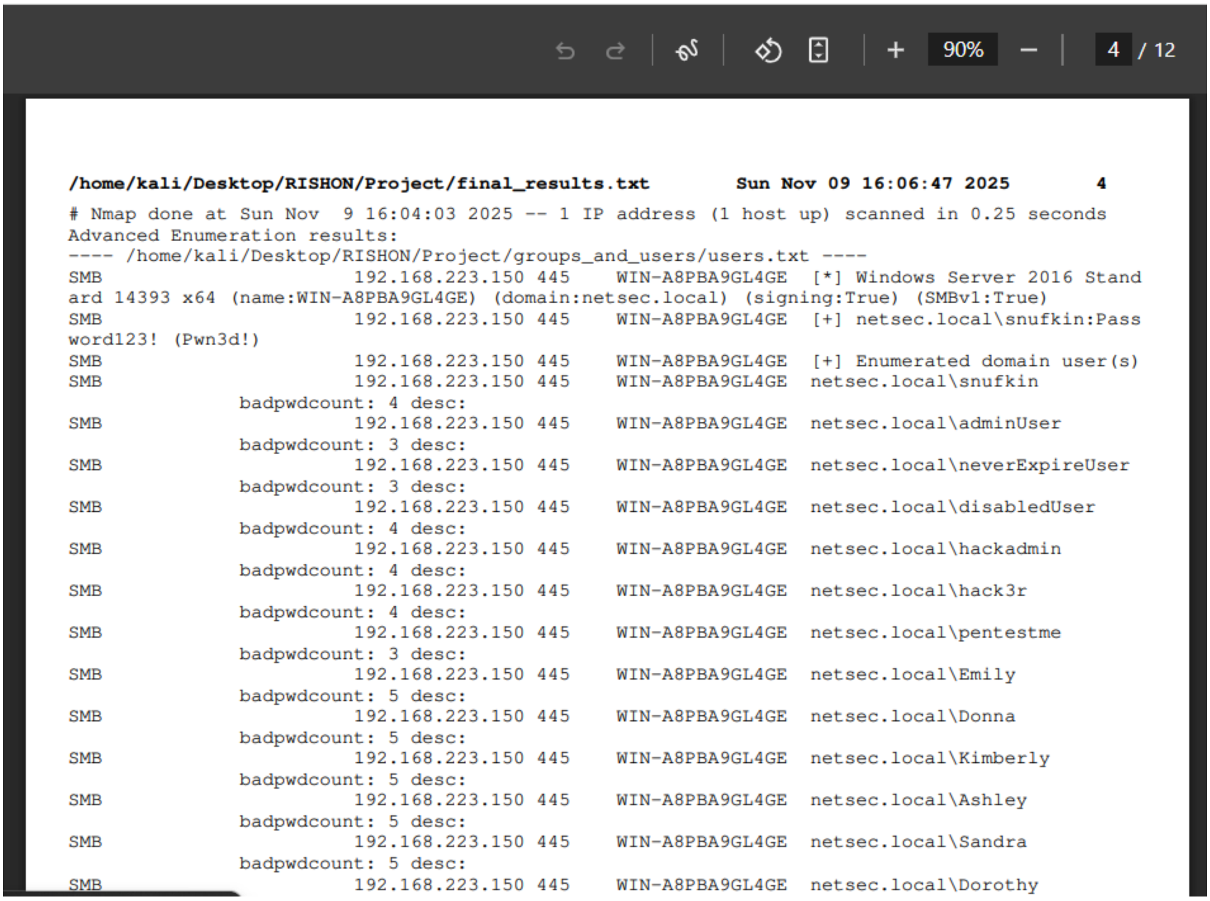
```
Final report performed in Sun Nov  9 04:06:47 PM EST 2025
User inputs are:

User Inputs Summary:
[+] Target Network: 192.168.223.0/24
[+] Domain Name: netsec.local
[+] Active Domain User: snufkin
[+] Active Domain Password: Password123!
[+] Password List: pass.txt
[+] Results Directory: /home/kali/Desktop/RISHON/Project

Basic scan results:

[+] Performing Basic Scanning using on 192.168.223.0/24 -Pn option in Nmap to assume all host
 are online, bypassing the discovery phase
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-09 15:48 EST
Nmap scan report for 192.168.223.1
Host is up (0.00042s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT     STATE SERVICE
7070/tcp open  realserver
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for 192.168.223.2
Host is up (0.00037s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
53/tcp open  domain
MAC Address: 00:50:56:FF:B3:96 (VMware)

Nmap scan report for 192.168.223.150
Host is up (0.00059s latency).
Not shown: 987 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
53/tcp   open  domain
88/tcp   open  kerberos-sec
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
389/tcp  open  ldap
445/tcp  open  microsoft-ds
```



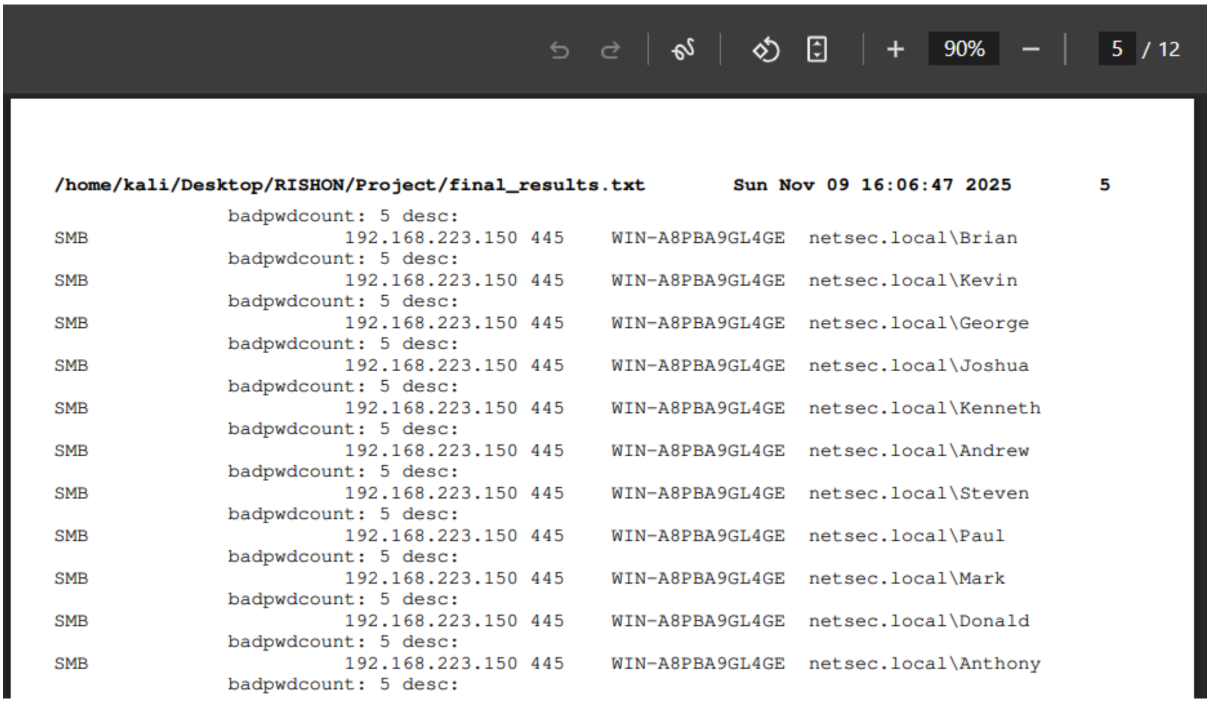
```
Intermediate scan results:
TCP open ports:
# Masscan 1.3.2 scan initiated Sun Nov  9 20:48:38 2025
# Ports scanned: TCP(65535;1-65535) UDP(0;) SCTP(0;) PROTOCOLS(0;)
Timestamp: 1762721320   Host: 192.168.223.150 ()        Ports: 9389/open/tcp//unknown//
Timestamp: 1762721328   Host: 192.168.223.150 ()        Ports: 49665/open/tcp//unknown//
Timestamp: 1762721334   Host: 192.168.223.150 ()        Ports: 49664/open/tcp//unknown//
Timestamp: 1762721336   Host: 192.168.223.150 ()        Ports: 88/open/tcp//kerberos//
Timestamp: 1762721371   Host: 192.168.223.150 ()        Ports: 49703/open/tcp//unknown//
Timestamp: 1762721385   Host: 192.168.223.150 ()        Ports: 49666/open/tcp//unknown//
Timestamp: 1762721401   Host: 192.168.223.150 ()        Ports: 49670/open/tcp//unknown//
Timestamp: 1762721415   Host: 192.168.223.150 ()        Ports: 49671/open/tcp//unknown//
Timestamp: 1762721416   Host: 192.168.223.150 ()        Ports: 464/open/tcp//kpasswd//
Timestamp: 1762721446   Host: 192.168.223.150 ()        Ports: 636/open/tcp//ldaps//
Timestamp: 1762721459   Host: 192.168.223.2 ()  Ports: 53/open/tcp//domain//
Timestamp: 1762721490   Host: 192.168.223.150 ()        Ports: 389/open/tcp//ldap//
Timestamp: 1762721492   Host: 192.168.223.150 ()        Ports: 593/open/tcp//unknown//
Timestamp: 1762721495   Host: 192.168.223.150 ()        Ports: 5985/open/tcp//unknown//
Timestamp: 1762721514   Host: 192.168.223.150 ()        Ports: 3269/open/tcp//unknown//
Timestamp: 1762721523   Host: 192.168.223.150 ()        Ports: 135/open/tcp//epmap//
Timestamp: 1762721535   Host: 192.168.223.150 ()        Ports: 3268/open/tcp//unknown//
Timestamp: 1762721559   Host: 192.168.223.150 ()        Ports: 49685/open/tcp//unknown//
Timestamp: 1762721571   Host: 192.168.223.150 ()        Ports: 47001/open/tcp//unknown//
Timestamp: 1762721575   Host: 192.168.223.150 ()        Ports: 445/open/tcp//microsoft-ds//
Timestamp: 1762721629   Host: 192.168.223.150 ()        Ports: 139/open/tcp//netbios-ssn//
Timestamp: 1762721653   Host: 192.168.223.150 ()        Ports: 49669/open/tcp//unknown//
Timestamp: 1762721663   Host: 192.168.223.150 ()        Ports: 49667/open/tcp//unknown//
Timestamp: 1762721714   Host: 192.168.223.150 ()        Ports: 53/open/tcp//domain//
Timestamp: 1762721728   Host: 192.168.223.150 ()        Ports: 21/open/tcp//ftp//
Timestamp: 1762721768   Host: 192.168.223.150 ()        Ports: 49675/open/tcp//unknown//
# Masscan done at Sun Nov  9 20:56:19 2025

Advanced scan results:
UDP open ports:
# Masscan 1.3.2 scan initiated Sun Nov  9 20:56:19 2025
# Ports scanned: TCP(0;) UDP(65535;65537-131071) SCTP(0;) PROTOCOLS(0;)
Timestamp: 1762721884   Host: 192.168.223.150 ()        Ports: 137/open/udp//netbios-ns//
Timestamp: 1762721921   Host: 192.168.223.150 ()        Ports: 56986/open/udp//unknown//
Timestamp: 1762722060   Host: 192.168.223.150 ()        Ports: 57417/open/udp//unknown//
Timestamp: 1762722100   Host: 192.168.223.128 ()        Ports: 41779/open/udp//unknown//
Timestamp: 1762722101   Host: 192.168.223.2 ()  Ports: 53/open/udp//domain//
# Masscan done at Sun Nov  9 21:02:16 2025

Basic Enumeration results: nmap -sV on each IP
```



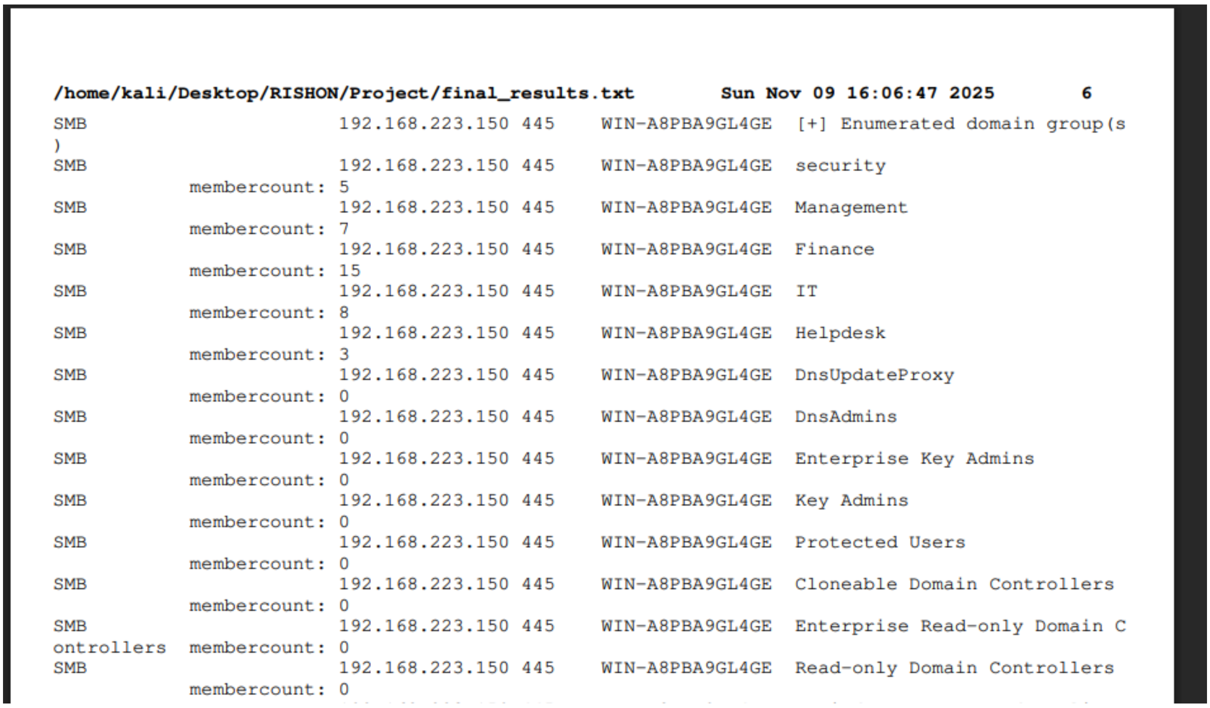
```
/home/kali/Desktop/RISHON/Project/final_results.txt       Sun Nov 09 16:06:47 2025       3
139/tcp open   netbios-ssn
445/tcp open   microsoft-ds
MAC Address: 00:0C:29:AD:5B:35 (VMware)

Host script results:
| nbstat: NetBIOS name: WIN-A8PBA9GL4GE, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:ad:5b:
35 (VMware)
| Names:
|   NETSEC<1c>           Flags: <group><active>
|   WIN-A8PBA9GL4GE<00>  Flags: <unique><active>
|   NETSEC<00>           Flags: <group><active>
|   WIN-A8PBA9GL4GE<20>  Flags: <unique><active>
|_  NETSEC<1b>           Flags: <unique><active>

# Nmap done at Sun Nov  9 16:04:04 2025 -- 1 IP address (1 host up) scanned in 0.24 seconds
# Nmap 7.95 scan initiated Sun Nov  9 16:04:02 2025 as: /usr/lib/nmap/nmap -Pn -p 445 --script
 smb-os-discovery.nse -oN /home/kali/Desktop/RISHON/Project/nse_scripts/os-discovery_192.168.2
23.150.txt 192.168.223.150
Nmap scan report for 192.168.223.150
Host is up (0.00049s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:AD:5B:35 (VMware)

Host script results:
| smb-os-discovery:
|   OS: Windows Server 2016 Standard 14393 (Windows Server 2016 Standard 6.3)
|   Computer name: WIN-A8PBA9GL4GE
|   NetBIOS computer name: WIN-A8PBA9GL4GE\x00
|   Domain name: netsec.local
|   Forest name: netsec.local
|   FQDN: WIN-A8PBA9GL4GE.netsec.local
|_  System time: 2025-11-09T13:04:02-08:00

# Nmap done at Sun Nov  9 16:04:02 2025 -- 1 IP address (1 host up) scanned in 0.28 seconds
# Nmap 7.95 scan initiated Sun Nov  9 16:04:03 2025 as: /usr/lib/nmap/nmap -Pn -p 445 --script
 smb-vuln-ms17-010.nse -oN /home/kali/Desktop/RISHON/Project/nse_scripts/vuln-ms17-010_192.168
.223.150.txt 192.168.223.150
Nmap scan report for 192.168.223.150
Host is up (0.00032s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:AD:5B:35 (VMware)
```



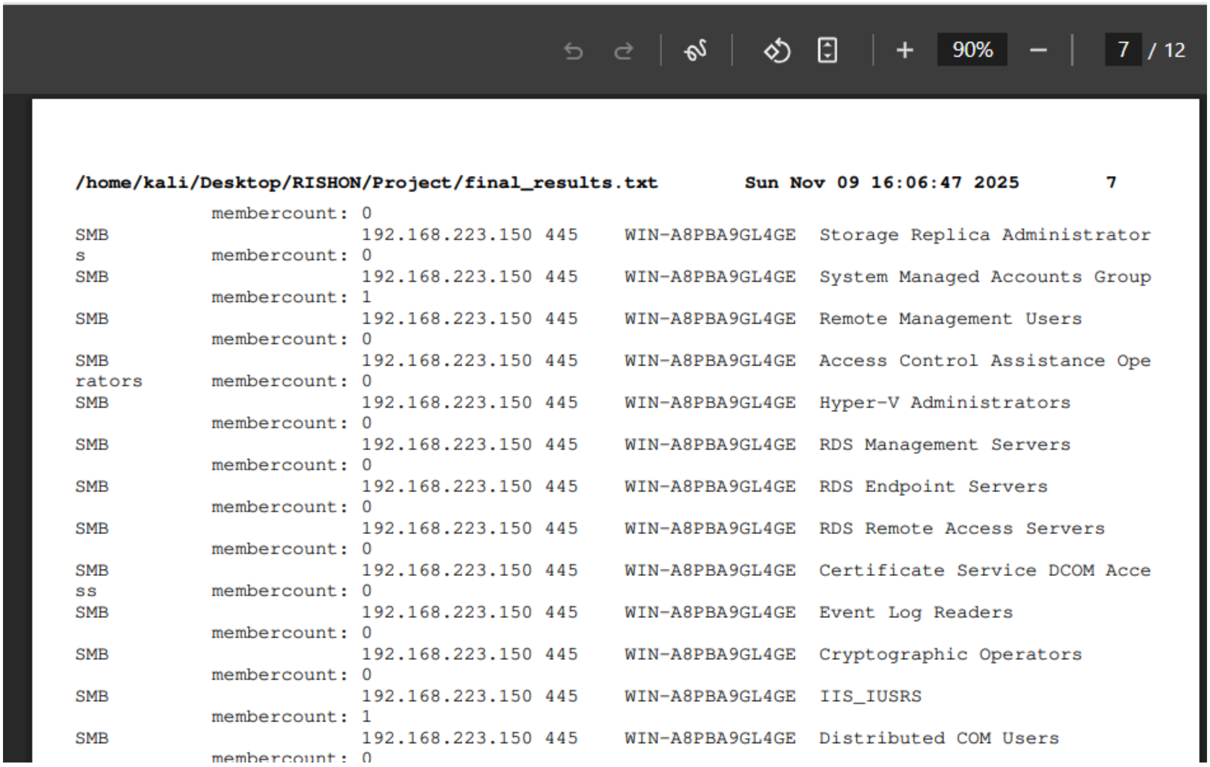
```
/home/kali/Desktop/RISHON/Project/final_results.txt       Sun Nov 09 16:06:47 2025       4
# Nmap done at Sun Nov  9 16:04:03 2025 -- 1 IP address (1 host up) scanned in 0.25 seconds
Advanced Enumeration results:
---- /home/kali/Desktop/RISHON/Project/groups_and_users/users.txt ----
SMB                      192.168.223.150 445    WIN-A8PBA9GL4GE  [*] Windows Server 2016 Stand
ard 14393 x64 (name:WIN-A8PBA9GL4GE) (domain:netsec.local) (signing:True) (SMBv1:True)
SMB                      192.168.223.150 445    WIN-A8PBA9GL4GE  [+] netsec.local\snufkin:Pass
word123! (Pwn3d!)
SMB                      192.168.223.150 445    WIN-A8PBA9GL4GE  [+] Enumerated domain user(s)
SMB                      192.168.223.150 445    WIN-A8PBA9GL4GE  netsec.local\snufkin
               badpwdcount: 4 desc:
SMB                      192.168.223.150 445    WIN-A8PBA9GL4GE  netsec.local\adminUser
               badpwdcount: 3 desc:
SMB                      192.168.223.150 445    WIN-A8PBA9GL4GE  netsec.local\neverExpireUser
               badpwdcount: 3 desc:
SMB                      192.168.223.150 445    WIN-A8PBA9GL4GE  netsec.local\disabledUser
               badpwdcount: 4 desc:
SMB                      192.168.223.150 445    WIN-A8PBA9GL4GE  netsec.local\hackadmin
               badpwdcount: 4 desc:
SMB                      192.168.223.150 445    WIN-A8PBA9GL4GE  netsec.local\hack3r
               badpwdcount: 4 desc:
SMB                      192.168.223.150 445    WIN-A8PBA9GL4GE  netsec.local\pentestme
               badpwdcount: 3 desc:
SMB                      192.168.223.150 445    WIN-A8PBA9GL4GE  netsec.local\Emily
               badpwdcount: 5 desc:
SMB                      192.168.223.150 445    WIN-A8PBA9GL4GE  netsec.local\Donna
               badpwdcount: 5 desc:
SMB                      192.168.223.150 445    WIN-A8PBA9GL4GE  netsec.local\Kimberly
               badpwdcount: 5 desc:
SMB                      192.168.223.150 445    WIN-A8PBA9GL4GE  netsec.local\Ashley
               badpwdcount: 5 desc:
SMB                      192.168.223.150 445    WIN-A8PBA9GL4GE  netsec.local\Sandra
               badpwdcount: 5 desc:
SMB                      192.168.223.150 445    WIN-A8PBA9GL4GE  netsec.local\Dorothy
```



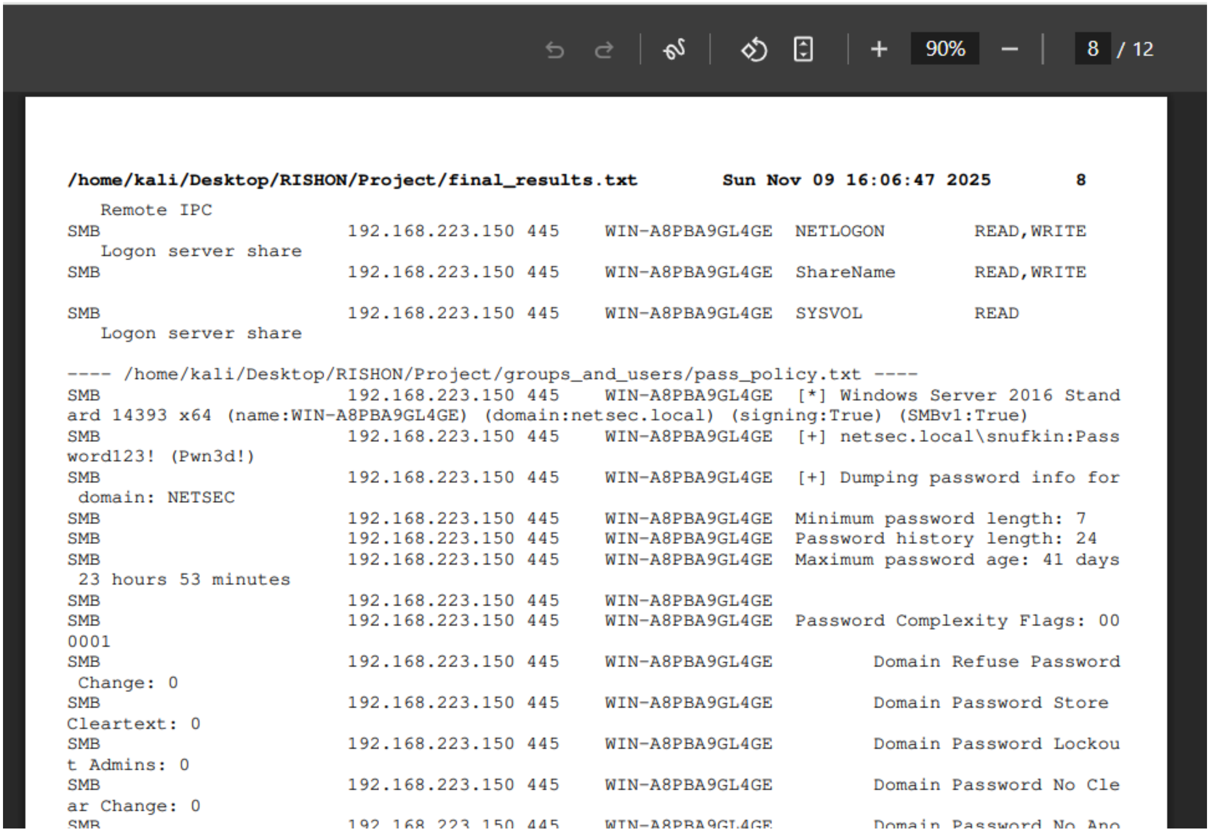
```
/home/kali/Desktop/RISHON/Project/final_results.txt       Sun Nov 09 16:06:47 2025       5
               badpwdcount: 5 desc:
SMB                      192.168.223.150 445    WIN-A8PBA9GL4GE  netsec.local\Brian
               badpwdcount: 5 desc:
SMB                      192.168.223.150 445    WIN-A8PBA9GL4GE  netsec.local\Kevin
               badpwdcount: 5 desc:
SMB                      192.168.223.150 445    WIN-A8PBA9GL4GE  netsec.local\George
               badpwdcount: 5 desc:
SMB                      192.168.223.150 445    WIN-A8PBA9GL4GE  netsec.local\Joshua
               badpwdcount: 5 desc:
SMB                      192.168.223.150 445    WIN-A8PBA9GL4GE  netsec.local\Kenneth
               badpwdcount: 5 desc:
SMB                      192.168.223.150 445    WIN-A8PBA9GL4GE  netsec.local\Andrew
               badpwdcount: 5 desc:
SMB                      192.168.223.150 445    WIN-A8PBA9GL4GE  netsec.local\Steven
               badpwdcount: 5 desc:
SMB                      192.168.223.150 445    WIN-A8PBA9GL4GE  netsec.local\Paul
               badpwdcount: 5 desc:
SMB                      192.168.223.150 445    WIN-A8PBA9GL4GE  netsec.local\Mark
               badpwdcount: 5 desc:
SMB                      192.168.223.150 445    WIN-A8PBA9GL4GE  netsec.local\Donald
               badpwdcount: 5 desc:
SMB                      192.168.223.150 445    WIN-A8PBA9GL4GE  netsec.local\Anthony
               badpwdcount: 5 desc:
```



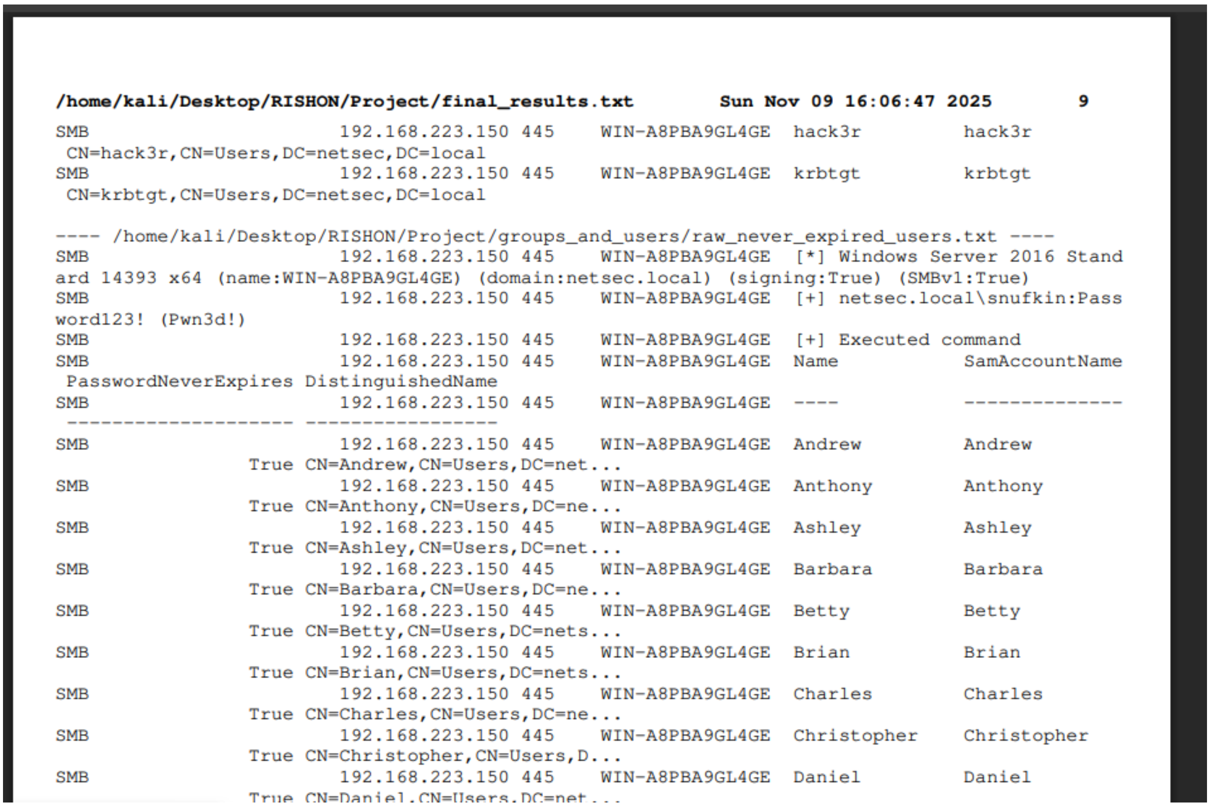
```
/home/kali/Desktop/RISHON/Project/final_results.txt       Sun Nov 09 16:06:47 2025       6
SMB                        192.168.223.150 445    WIN-A8PBA9GL4GE  [+] Enumerated domain group(s
)
SMB                        192.168.223.150 445    WIN-A8PBA9GL4GE  security
            membercount: 5
SMB                        192.168.223.150 445    WIN-A8PBA9GL4GE  Management
            membercount: 7
SMB                        192.168.223.150 445    WIN-A8PBA9GL4GE  Finance
            membercount: 15
SMB                        192.168.223.150 445    WIN-A8PBA9GL4GE  IT
            membercount: 8
SMB                        192.168.223.150 445    WIN-A8PBA9GL4GE  Helpdesk
            membercount: 3
SMB                        192.168.223.150 445    WIN-A8PBA9GL4GE  DnsUpdateProxy
            membercount: 0
SMB                        192.168.223.150 445    WIN-A8PBA9GL4GE  DnsAdmins
            membercount: 0
SMB                        192.168.223.150 445    WIN-A8PBA9GL4GE  Enterprise Key Admins
            membercount: 0
SMB                        192.168.223.150 445    WIN-A8PBA9GL4GE  Key Admins
            membercount: 0
SMB                        192.168.223.150 445    WIN-A8PBA9GL4GE  Protected Users
            membercount: 0
SMB                        192.168.223.150 445    WIN-A8PBA9GL4GE  Cloneable Domain Controllers
            membercount: 0
SMB                        192.168.223.150 445    WIN-A8PBA9GL4GE  Enterprise Read-only Domain C
ontrollers  membercount: 0
SMB                        192.168.223.150 445    WIN-A8PBA9GL4GE  Read-only Domain Controllers
            membercount: 0
```



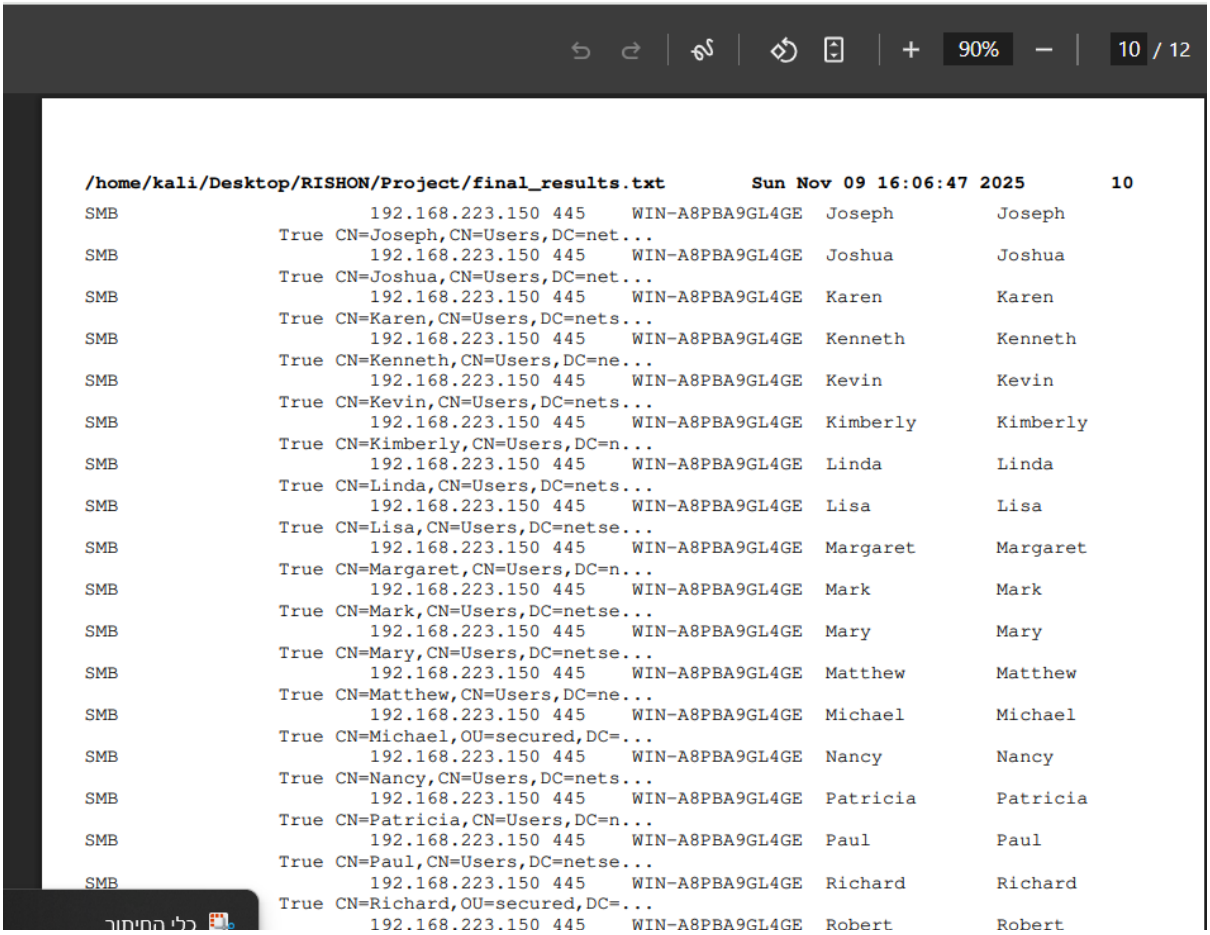
```
/home/kali/Desktop/RISHON/Project/final_results.txt       Sun Nov 09 16:06:47 2025       7
            membercount: 0
SMB                        192.168.223.150 445    WIN-A8PBA9GL4GE  Storage Replica Administrator
s           membercount: 0
SMB                        192.168.223.150 445    WIN-A8PBA9GL4GE  System Managed Accounts Group
            membercount: 1
SMB                        192.168.223.150 445    WIN-A8PBA9GL4GE  Remote Management Users
            membercount: 0
SMB                        192.168.223.150 445    WIN-A8PBA9GL4GE  Access Control Assistance Ope
rators      membercount: 0
SMB                        192.168.223.150 445    WIN-A8PBA9GL4GE  Hyper-V Administrators
            membercount: 0
SMB                        192.168.223.150 445    WIN-A8PBA9GL4GE  RDS Management Servers
            membercount: 0
SMB                        192.168.223.150 445    WIN-A8PBA9GL4GE  RDS Endpoint Servers
            membercount: 0
SMB                        192.168.223.150 445    WIN-A8PBA9GL4GE  RDS Remote Access Servers
            membercount: 0
SMB                        192.168.223.150 445    WIN-A8PBA9GL4GE  Certificate Service DCOM Acce
ss          membercount: 0
SMB                        192.168.223.150 445    WIN-A8PBA9GL4GE  Event Log Readers
            membercount: 0
SMB                        192.168.223.150 445    WIN-A8PBA9GL4GE  Cryptographic Operators
            membercount: 0
SMB                        192.168.223.150 445    WIN-A8PBA9GL4GE  IIS_IUSRS
            membercount: 1
SMB                        192.168.223.150 445    WIN-A8PBA9GL4GE  Distributed COM Users
            membercount: 0
```



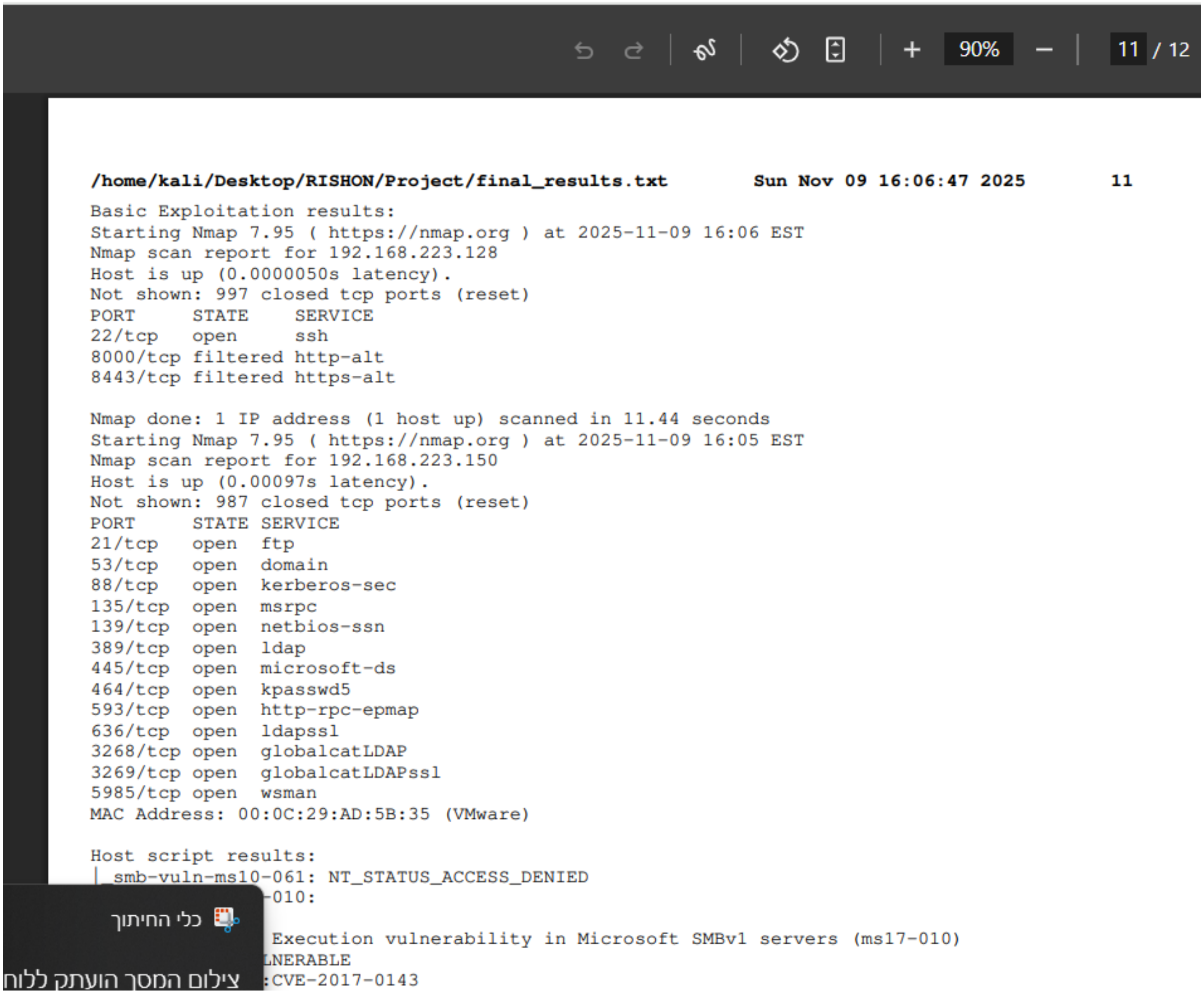
```
/home/kali/Desktop/RISHON/Project/final_results.txt       Sun Nov 09 16:06:47 2025       8
   Remote IPC
SMB                      192.168.223.150 445    WIN-A8PBA9GL4GE  NETLOGON        READ,WRITE
   Logon server share
SMB                      192.168.223.150 445    WIN-A8PBA9GL4GE  ShareName       READ,WRITE

SMB                      192.168.223.150 445    WIN-A8PBA9GL4GE  SYSVOL          READ
   Logon server share

---- /home/kali/Desktop/RISHON/Project/groups_and_users/pass_policy.txt ----
SMB                      192.168.223.150 445    WIN-A8PBA9GL4GE  [*] Windows Server 2016 Stand
ard 14393 x64 (name:WIN-A8PBA9GL4GE) (domain:netsec.local) (signing:True) (SMBv1:True)
SMB                      192.168.223.150 445    WIN-A8PBA9GL4GE  [+] netsec.local\snufkin:Pass
word123! (Pwn3d!)
SMB                      192.168.223.150 445    WIN-A8PBA9GL4GE  [+] Dumping password info for
 domain: NETSEC
SMB                      192.168.223.150 445    WIN-A8PBA9GL4GE  Minimum password length: 7
SMB                      192.168.223.150 445    WIN-A8PBA9GL4GE  Password history length: 24
SMB                      192.168.223.150 445    WIN-A8PBA9GL4GE  Maximum password age: 41 days
 23 hours 53 minutes
SMB                      192.168.223.150 445    WIN-A8PBA9GL4GE
SMB                      192.168.223.150 445    WIN-A8PBA9GL4GE  Password Complexity Flags: 00
0001
SMB                      192.168.223.150 445    WIN-A8PBA9GL4GE         Domain Refuse Password
 Change: 0
SMB                      192.168.223.150 445    WIN-A8PBA9GL4GE         Domain Password Store
Cleartext: 0
SMB                      192.168.223.150 445    WIN-A8PBA9GL4GE         Domain Password Lockou
t Admins: 0
SMB                      192.168.223.150 445    WIN-A8PBA9GL4GE         Domain Password No Cle
ar Change: 0
SMB                      192.168.223.150 445    WIN-A8PBA9GL4GE         Domain Password No Ano
```



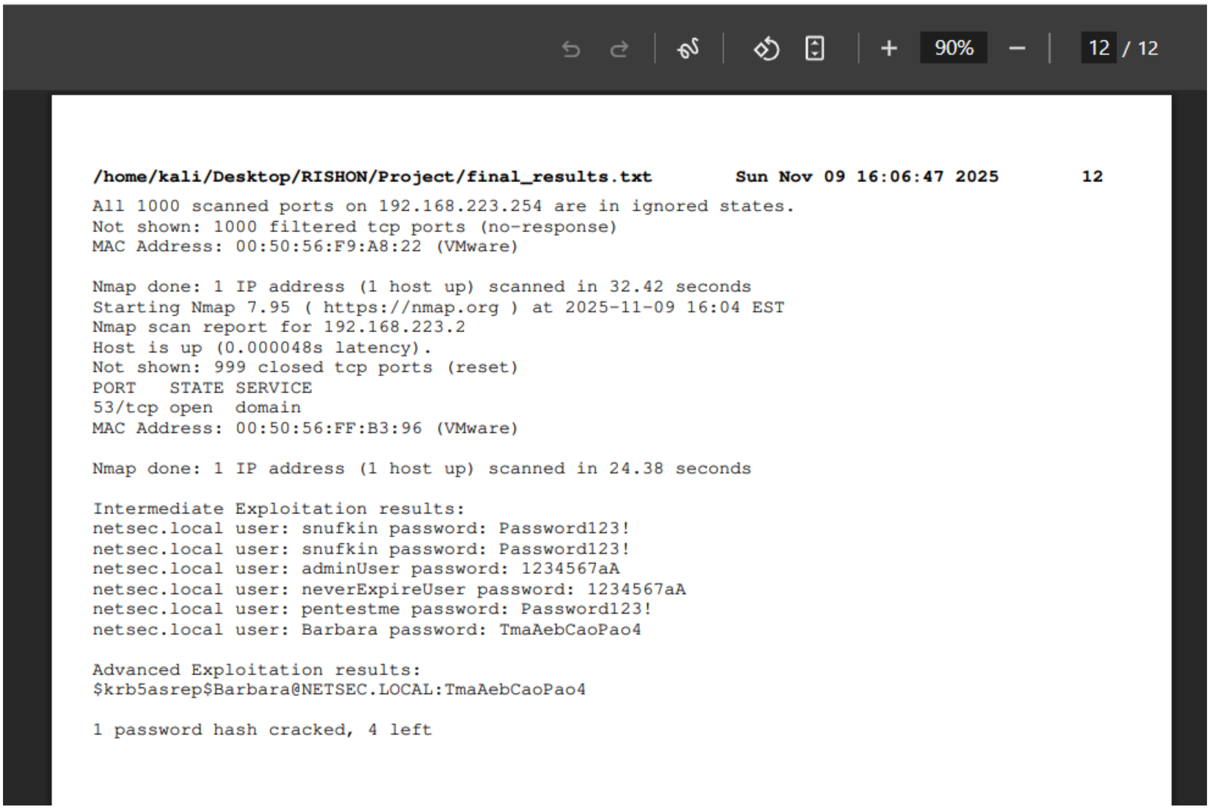
```
/home/kali/Desktop/RISHON/Project/final_results.txt       Sun Nov 09 16:06:47 2025       9
SMB                      192.168.223.150 445    WIN-A8PBA9GL4GE  hack3r          hack3r
 CN=hack3r,CN=Users,DC=netsec,DC=local
SMB                      192.168.223.150 445    WIN-A8PBA9GL4GE  krbtgt          krbtgt
 CN=krbtgt,CN=Users,DC=netsec,DC=local

---- /home/kali/Desktop/RISHON/Project/groups_and_users/raw_never_expired_users.txt ----
SMB                      192.168.223.150 445    WIN-A8PBA9GL4GE  [*] Windows Server 2016 Stand
ard 14393 x64 (name:WIN-A8PBA9GL4GE) (domain:netsec.local) (signing:True) (SMBv1:True)
SMB                      192.168.223.150 445    WIN-A8PBA9GL4GE  [+] netsec.local\snufkin:Pass
word123! (Pwn3d!)
SMB                      192.168.223.150 445    WIN-A8PBA9GL4GE  [+] Executed command
SMB                      192.168.223.150 445    WIN-A8PBA9GL4GE  Name            SamAccountName
 PasswordNeverExpires DistinguishedName
SMB                      192.168.223.150 445    WIN-A8PBA9GL4GE  ----            --------------
 -------------------- -----------------
SMB                      192.168.223.150 445    WIN-A8PBA9GL4GE  Andrew          Andrew
                 True CN=Andrew,CN=Users,DC=net...
SMB                      192.168.223.150 445    WIN-A8PBA9GL4GE  Anthony         Anthony
                 True CN=Anthony,CN=Users,DC=ne...
SMB                      192.168.223.150 445    WIN-A8PBA9GL4GE  Ashley          Ashley
                 True CN=Ashley,CN=Users,DC=net...
SMB                      192.168.223.150 445    WIN-A8PBA9GL4GE  Barbara         Barbara
                 True CN=Barbara,CN=Users,DC=ne...
SMB                      192.168.223.150 445    WIN-A8PBA9GL4GE  Betty           Betty
                 True CN=Betty,CN=Users,DC=nets...
SMB                      192.168.223.150 445    WIN-A8PBA9GL4GE  Brian           Brian
                 True CN=Brian,CN=Users,DC=nets...
SMB                      192.168.223.150 445    WIN-A8PBA9GL4GE  Charles         Charles
                 True CN=Charles,CN=Users,DC=ne...
SMB                      192.168.223.150 445    WIN-A8PBA9GL4GE  Christopher     Christopher
                 True CN=Christopher,CN=Users,D...
SMB                      192.168.223.150 445    WIN-A8PBA9GL4GE  Daniel          Daniel
                 True CN=Daniel,CN=Users,DC=net...
```



```
/home/kali/Desktop/RISHON/Project/final_results.txt      Sun Nov 09 16:06:47 2025       10
SMB                     192.168.223.150 445    WIN-A8PBA9GL4GE  Joseph         Joseph
                 True CN=Joseph,CN=Users,DC=net...
SMB                     192.168.223.150 445    WIN-A8PBA9GL4GE  Joshua         Joshua
                 True CN=Joshua,CN=Users,DC=net...
SMB                     192.168.223.150 445    WIN-A8PBA9GL4GE  Karen          Karen
                 True CN=Karen,CN=Users,DC=nets...
SMB                     192.168.223.150 445    WIN-A8PBA9GL4GE  Kenneth        Kenneth
                 True CN=Kenneth,CN=Users,DC=ne...
SMB                     192.168.223.150 445    WIN-A8PBA9GL4GE  Kevin          Kevin
                 True CN=Kevin,CN=Users,DC=nets...
SMB                     192.168.223.150 445    WIN-A8PBA9GL4GE  Kimberly       Kimberly
                 True CN=Kimberly,CN=Users,DC=n...
SMB                     192.168.223.150 445    WIN-A8PBA9GL4GE  Linda          Linda
                 True CN=Linda,CN=Users,DC=nets...
SMB                     192.168.223.150 445    WIN-A8PBA9GL4GE  Lisa           Lisa
                 True CN=Lisa,CN=Users,DC=netse...
SMB                     192.168.223.150 445    WIN-A8PBA9GL4GE  Margaret       Margaret
                 True CN=Margaret,CN=Users,DC=n...
SMB                     192.168.223.150 445    WIN-A8PBA9GL4GE  Mark           Mark
                 True CN=Mark,CN=Users,DC=netse...
SMB                     192.168.223.150 445    WIN-A8PBA9GL4GE  Mary           Mary
                 True CN=Mary,CN=Users,DC=netse...
SMB                     192.168.223.150 445    WIN-A8PBA9GL4GE  Matthew        Matthew
                 True CN=Matthew,CN=Users,DC=ne...
SMB                     192.168.223.150 445    WIN-A8PBA9GL4GE  Michael        Michael
                 True CN=Michael,OU=secured,DC=...
SMB                     192.168.223.150 445    WIN-A8PBA9GL4GE  Nancy          Nancy
                 True CN=Nancy,CN=Users,DC=nets...
SMB                     192.168.223.150 445    WIN-A8PBA9GL4GE  Patricia       Patricia
                 True CN=Patricia,CN=Users,DC=n...
SMB                     192.168.223.150 445    WIN-A8PBA9GL4GE  Paul           Paul
                 True CN=Paul,CN=Users,DC=netse...
SMB                     192.168.223.150 445    WIN-A8PBA9GL4GE  Richard        Richard
                 True CN=Richard,OU=secured,DC=...
                        192.168.223.150 445    WIN-A8PBA9GL4GE  Robert         Robert
```



```
/home/kali/Desktop/RISHON/Project/final_results.txt       Sun Nov 09 16:06:47 2025       11
Basic Exploitation results:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-09 16:06 EST
Nmap scan report for 192.168.223.128
Host is up (0.0000050s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE    SERVICE
22/tcp    open     ssh
8000/tcp filtered http-alt
8443/tcp filtered https-alt

Nmap done: 1 IP address (1 host up) scanned in 11.44 seconds
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-09 16:05 EST
Nmap scan report for 192.168.223.150
Host is up (0.00097s latency).
Not shown: 987 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
53/tcp    open  domain
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
3268/tcp open  globalcatLDAP
3269/tcp open  globalcatLDAPssl
5985/tcp open  wsman
MAC Address: 00:0C:29:AD:5B:35 (VMware)

Host script results:
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
                -010:

                 Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
                LNERABLE
                :CVE-2017-0143
```



```
/home/kali/Desktop/RISHON/Project/final_results.txt       Sun Nov 09 16:06:47 2025       12
All 1000 scanned ports on 192.168.223.254 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:F9:A8:22 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 32.42 seconds
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-09 16:04 EST
Nmap scan report for 192.168.223.2
Host is up (0.000048s latency).
Not shown: 999 closed tcp ports (reset)
PORT    STATE SERVICE
53/tcp open  domain
MAC Address: 00:50:56:FF:B3:96 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 24.38 seconds

Intermediate Exploitation results:
netsec.local user: snufkin password: Password123!
netsec.local user: snufkin password: Password123!
netsec.local user: adminUser password: 1234567aA
netsec.local user: neverExpireUser password: 1234567aA
netsec.local user: pentestme password: Password123!
netsec.local user: Barbara password: TmaAebCaoPao4

Advanced Exploitation results:
$krb5asrep$Barbara@NETSEC.LOCAL:TmaAebCaoPao4

1 password hash cracked, 4 left
```