Network Security Project

TMagen773637.S11.ZX305

Ron Nisinboym

September 22, 2025

Overview

Project Description:

This project is an automated network security testing tool that simplifies penetration testing by automating common tasks. It guides users through an easy setup, asking for a network range and credentials. The tool offers three operational modes—Scanning, Enumeration, and Exploitation—with adjustable intensity levels: Basic, Intermediate, Advanced or None. Depending on the selected level, the main script calls one of three scripts (basic.sh, intermediate.sh, or advanced.sh) to carry out the necessary tasks. By automating complex processes like service discovery, vulnerability assessment, and brute-forcing, the tool saves time and reduces manual effort, making domain enumeration faster and more efficient.

Technologies Used

- **Bash Scripting:** Used for automating the execution of commands, managing file paths, and automating the report generation.
- **Nmap:** Scans the network to identify active hosts and the versions of services running on them for vulnerability assessment.
- **Masscan (UDP Ports Scanning):** Uses Masscan to rapidly scan large networks for open UDP ports.
- **Nmap NSE**: Used for a wide range of tasks, including vulnerability detection, network discovery, and service enumeration.
- **Smbclient**: A tool for accessing and interacting with SMB (Server Message Block) shares on Windows networks, useful for file transfer, enumeration, and managing file permissions.
- **Rpcclient:** A tool for interacting with remote Windows systems using the SMB protocol, useful for querying Windows systems for information such as shares, users, and permissions.
- **Enum4linux:** A tool for gathering information from Windows machines over SMB, enabling enumeration of shares, users, groups, and passwords.
- **CrackMapExec:** A post-exploitation tool that automates common penetration testing tasks on Windows networks, such as SMB, RDP, and WinRM enumeration and exploitation.
- **Hashcat:** A password recovery tool that uses a wide variety of hashing algorithms and can perform brute-force, dictionary, and rule-based attacks to crack password hashes.
- **Enscript:** Converts text files into various formats like PostScript, HTML, or RTF, useful for formatting output from scripts or commands for easier readability or printing.
- **Ghostscript:** Interprets and processes PostScript and PDF files, useful for converting, printing, and manipulating these file formats in scripts or automated systems.
- **Python3:** A versatile programming language used for scripting, automation, and the development of custom tools for data processing, network communication, and vulnerability assessment.

Detailed Workflow

1. **Initial Setup:**

- The script begins by verifying that the user has root privileges.
- It checks if all required dependencies (tools) are installed on the system.
- The user is then prompted to provide the following inputs:
    - Network range
    - Active Directory (AD) credentials
    - Password list

2. **Main Menu:**
   After initialization, the user can choose the **"Help"** option to view more detailed information about the script's functionality before executing it with the **"Start"** option.

3. **Mode Level Configuration:**
   For each mode—**Scanning**, **Enumeration**, and **Exploitation**—the user is prompted to select an intensity level: **Basic**, **Intermediate**, **Advanced** or **None**. As the user selects higher levels, additional steps are incorporated into the process for more thorough testing and analysis.
   Once the mode level is selected, the script will continue automatically without requiring further input from the user, except in the case of the Intermediate or Advanced exploitation levels. In these cases, the user will need to specify a single password to perform password-spraying against identified Active Directory users.

4. **Log to PDF:**
   Throughout the execution of the script, all collected data is continuously appended to a text file. Once all modes have completed, the script automatically converts this text log into a PDF report, providing a neatly formatted summary of the results.

Design Principles

1. **Simplicity Over Decoration:** By reducing the use of bold colors, fancy fonts, and overly complex layouts, the script avoids visual clutter, providing an **"easy on the eyes" experience**.
2. **Clear, Readable Output**:
    a. The font choice is kept **simple and legible**, ensuring that the user can quickly read and interpret the different output, even over long periods of use.
    b. Colors are used sparingly, with only essential information (e.g. important information, warnings, errors and successes) highlighted using subtle color changes. This reduces eye strain while still providing the necessary emphasis on important results.

Credits

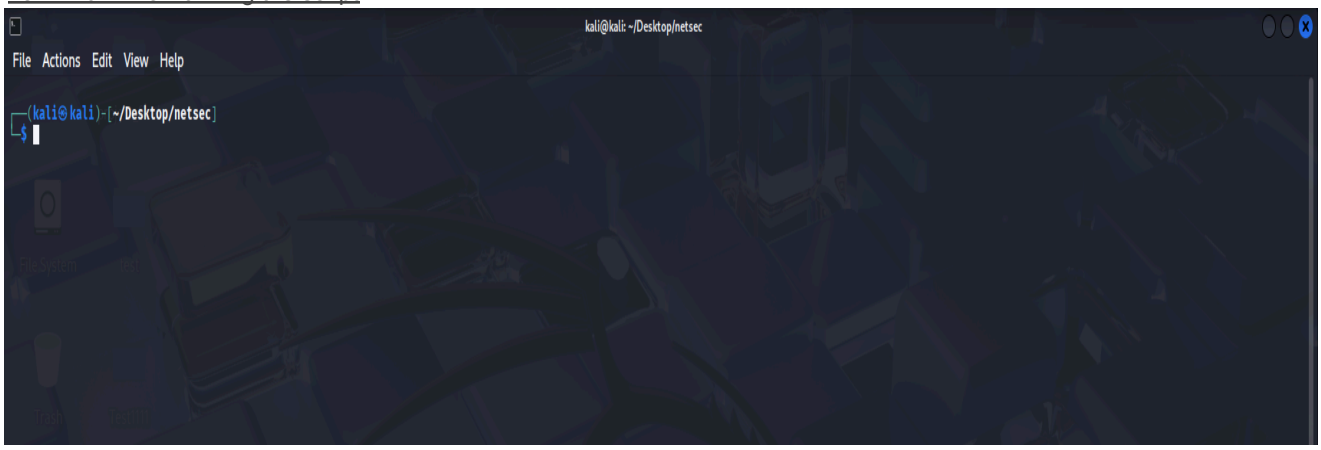
ChatGPT – The use of AI was made exclusively as a helping tool. Used to fix some of the errors and bugs occurring while writing the script, consulting in regards of the script's logic when more difficult steps were used(e.g., Booleans, complex text manipulations, arrays), asking for general information(e.g., "*Source*", PDF conversion, "pushd and popd"), things I struggled to remember(e.g., certain flags), and prettifying the code to make it more structured and readable. The choice of ChatGPT over Google, forums or other sources was made mostly to save time and get straight forward explanations for each piece of advice to keep learning from it.

Demonstrating Script Performance

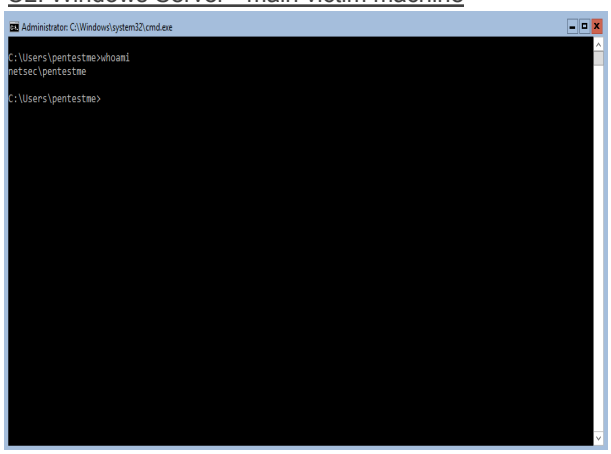
This script contains over 20 functions, making it impractical to document each one individually in this PDF. Instead, the report will focus on showcasing the program in action, highlighting key tasks and processes as they unfold.

Operating Systems Used -

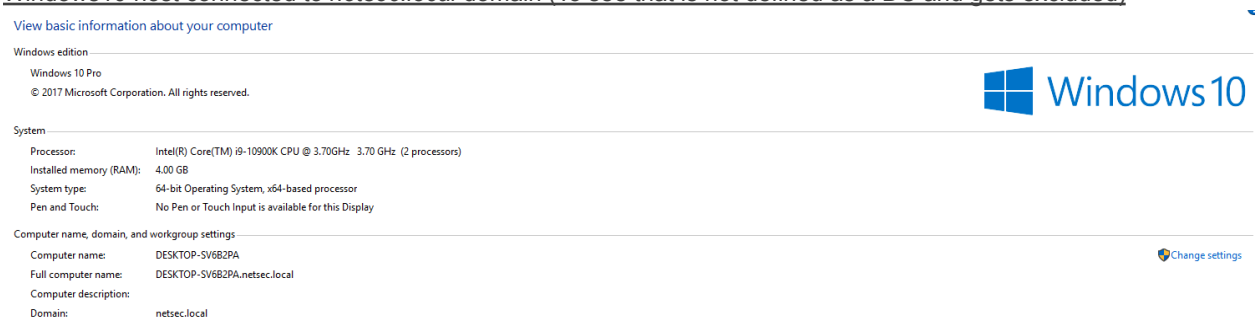
Kali Linux - For running the script



CLI Windows Server - main victim machine

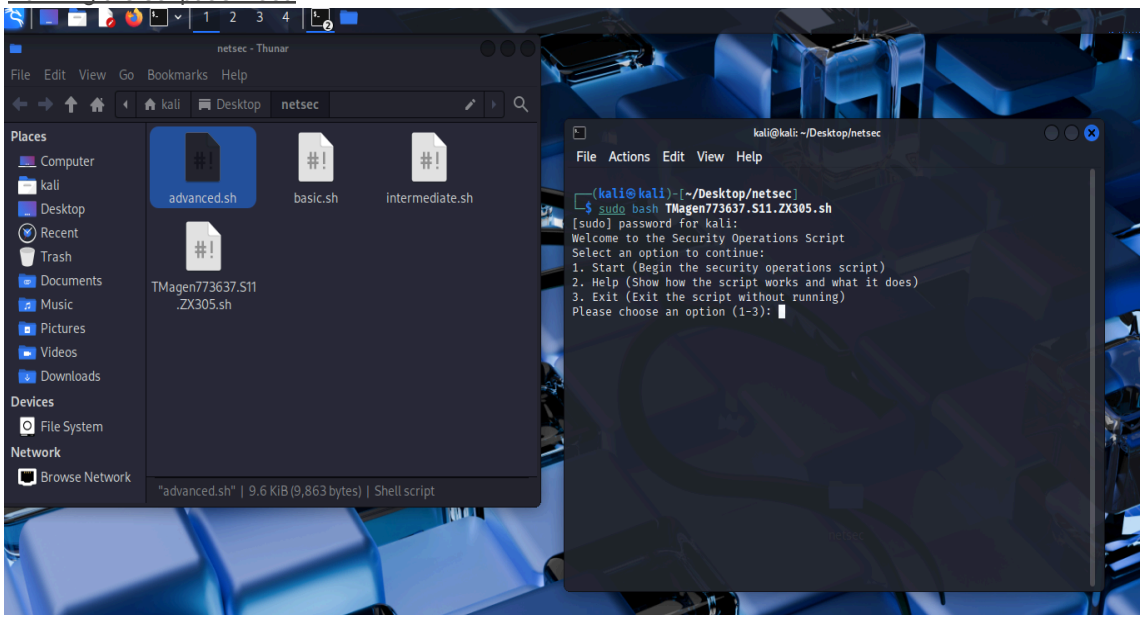


Windows10 host connected to *netsec.local* domain (To see that is not defined as a DC and gets excluded)

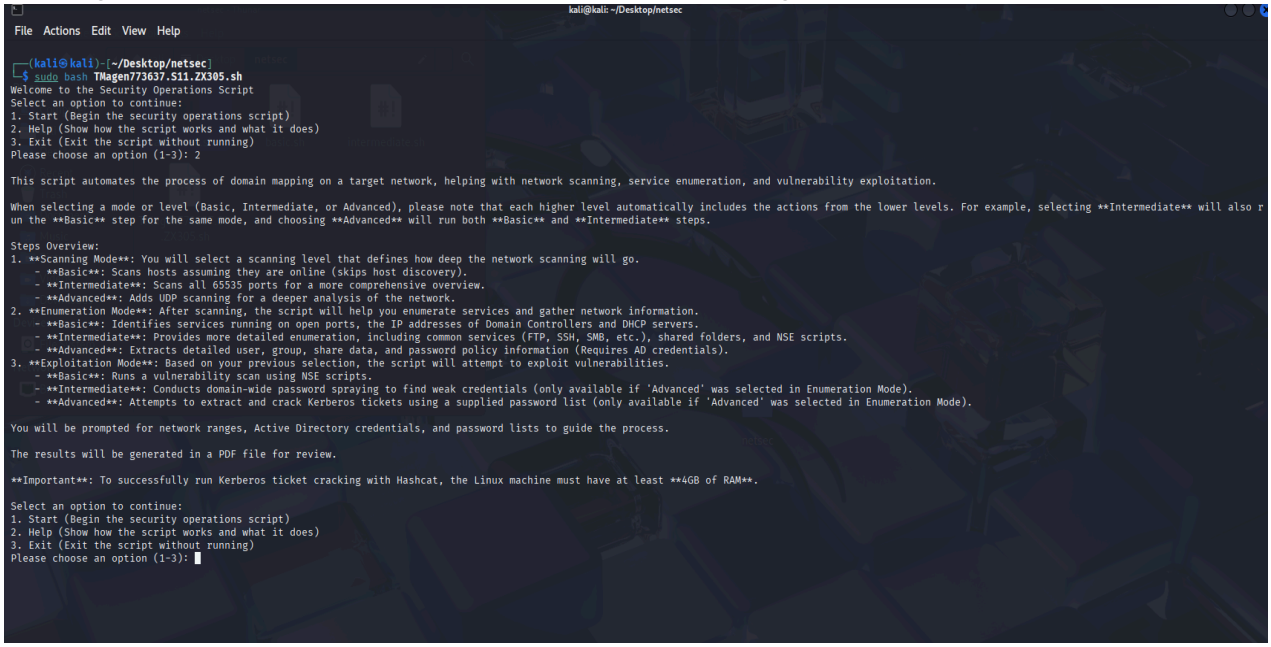


Running the script / “Help” -

Running the script as Root:

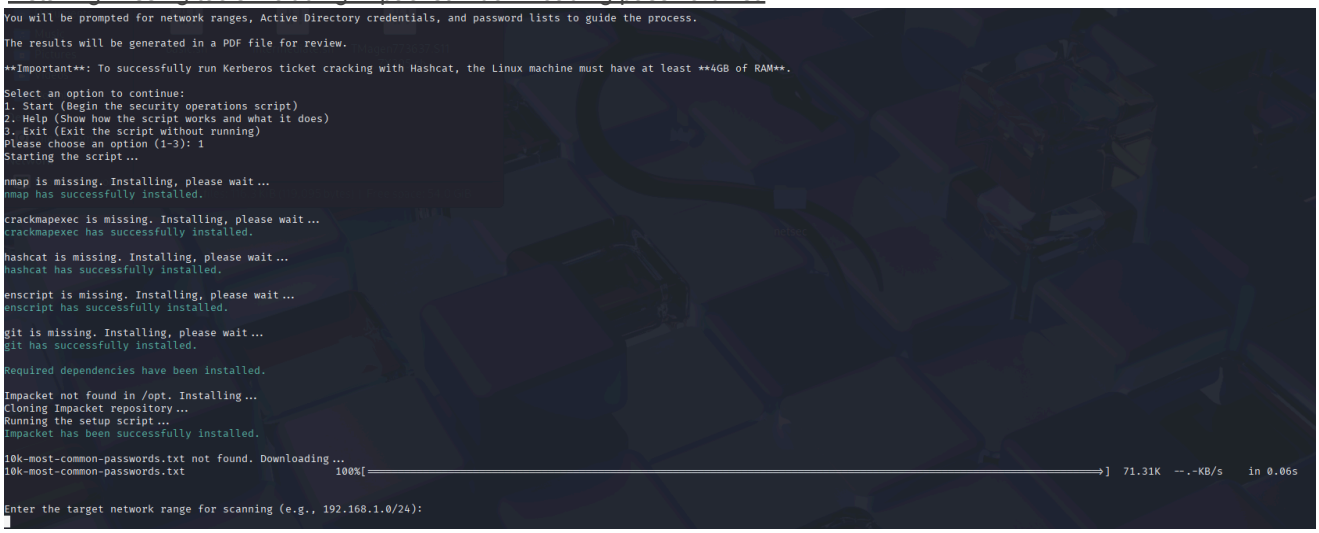


Choosing the *Help* option for more information about the script & returning to the main-menu:



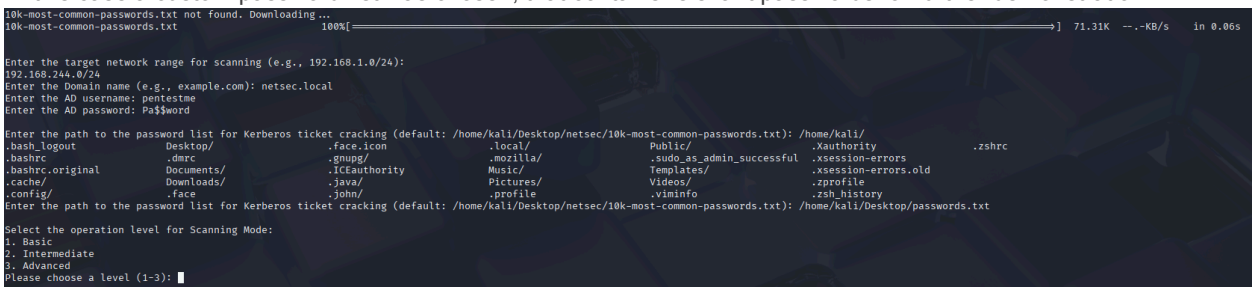
Starting the operations / Tools Installation -

Installing missing tools including impacket + downloading password-list:



Choosing the target network and filling Active-Directory credentials:

In this case a custom password-list was chosen, that contains relevant passwords for further demonstration.

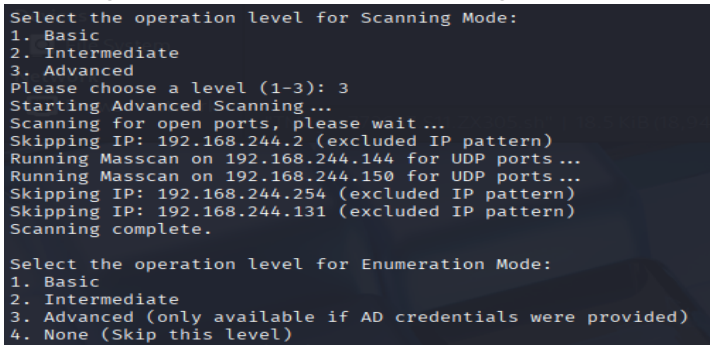


Modes & Levels -

Since each higher level includes all the steps from the previous levels, we'll focus on the execution of the **Advanced** level for each mode.
Lower level selections will be demonstrated later, at the "Error Handling" part.

Selecting **Advanced Scanning:**

Performing nmap and masscan, while excluding localhost and default VM IP's.

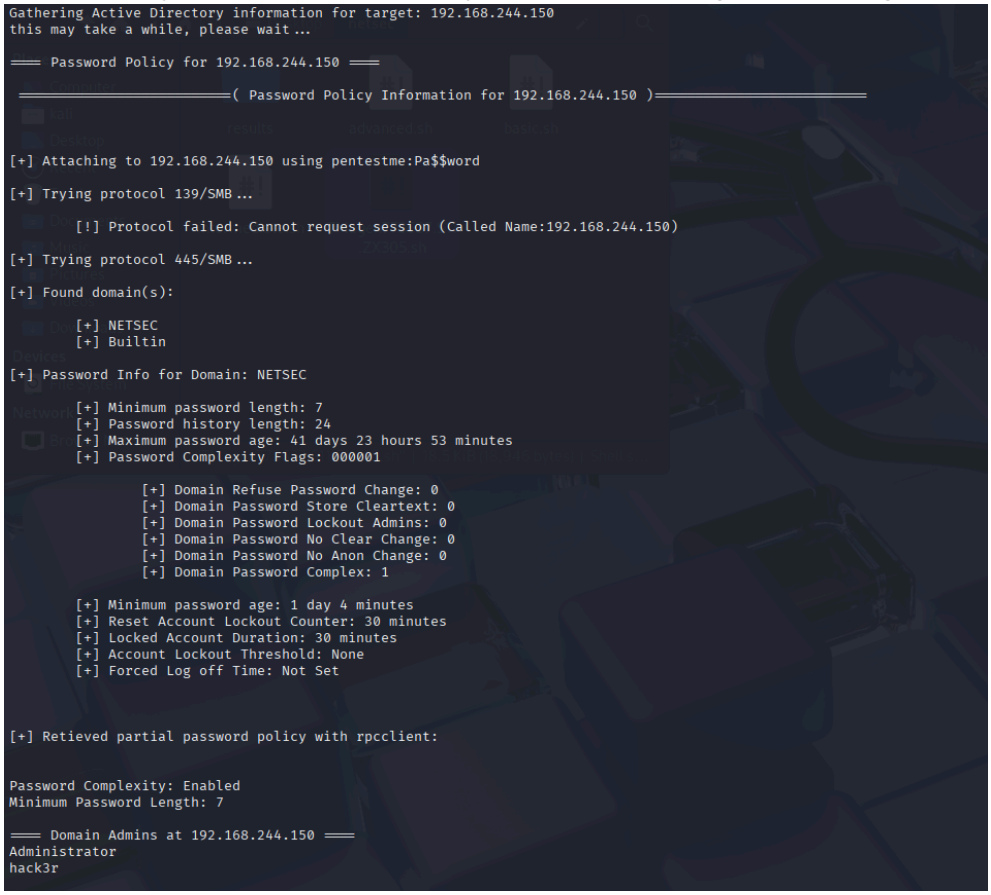


Selecting **Advanced Enumeration**:

Using the data gathered in the scanning stage to identify services and DC\DHCP addresses to further enumerate services, shared folders, SMB information and extract AD data including users, groups, and password policies via tools like rpcclient, enum4linux and different NSE scripts.

Domain Controller gets identified by relevant services running on each IP.

Password policy and Domain Admins displayed in the terminal along with appending to the final report.

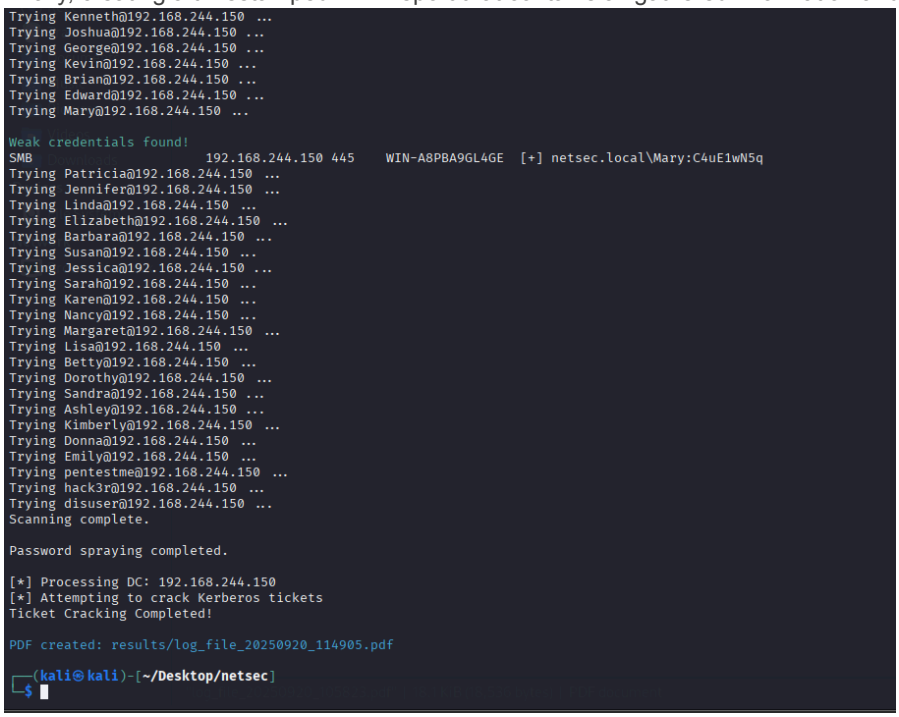


Selecting **Advanced Exploitation:**
Executing NSE Vulners against all services previously found to find specific vulnerabilities.

Next, the user asked to choose a password that will be used for password-spraying against discovered AD users while showing live progress and appending success to the log file.

Password-spraying the collected AD users with the use of *Crackmapexec*, targeting the SMB service.

Finishing password-spraying and attempting Kerberos ticket cracking by using Impacket's *GetNPUsers.py* script to extract AS-REP hashes and brute-forcing them with Hashcat.
Finally, creating a timestamped PDF report that contains all gathered information and exiting script.



Log file -

This part will showcase the log file:

PDF log file in the results folder.

1. Scanning mode:

All TCP and UDP ports scanning.

```
==== Nmap scan output for 192.168.244.0/24 ====

# Nmap 7.95 scan initiated Sat Sep 20 11:38:55 2025 as: /usr/lib/nmap/nmap -p- -Pn -T4 -oN nma
p_res.txt 192.168.244.0/24
Nmap scan report for 192.168.244.144
Host is up (0.00042s latency).
All 65535 scanned ports on 192.168.244.144 are in ignored states.
Not shown: 65535 filtered tcp ports (no-response)
MAC Address: 00:0C:29:1B:50:DA (VMware)

Nmap scan report for 192.168.244.150
Host is up (0.00034s latency).
Not shown: 65511 closed tcp ports (reset)
PORT      STATE SERVICE
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
9389/tcp  open  adws
47001/tcp open  winrm
49664/tcp open  unknown
49665/tcp open  unknown
49666/tcp open  unknown
49667/tcp open  unknown
49669/tcp open  unknown
49670/tcp open  unknown
49671/tcp open  unknown
49675/tcp open  unknown
49685/tcp open  unknown
49707/tcp open  unknown
MAC Address: 00:0C:29:E8:0D:53 (VMware)


==== End of Nmap scan results for 192.168.244.0/24 ====


==== Masscan UDP results for 192.168.244.0/24 ====

Discovered open port 64384/udp on 192.168.244.150
Discovered open port 137/udp on 192.168.244.150

==== End of Masscan UDP results for 192.168.244.0/24 ====
```

2. Enumeration Mode:

Service versions based on the previously found ports.

```
==== Nmap service version enumeration results ====

# Nmap 7.95 scan initiated Sat Sep 20 11:41:45 2025 as: /usr/lib/nmap/nmap -sV -p 53,88,135,13
9,389,445,464,593,636,3268,3269,5985,9389,47001,49664,49665,49666,49667,49669,49670,49671,4967
5,49685,49707 -oN /home/kali/Desktop/netsec/results/port_versions_192.168.244.150.txt 192.168.
244.150
Nmap scan report for 192.168.244.150
Host is up (0.00021s latency).

PORT      STATE SERVICE      VERSION
53/tcp    open  domain       (generic dns response: SERVFAIL)
88/tcp    open  kerberos-sec Microsoft Windows Kerberos (server time: 2025-09-20 15:42:00Z)
```

```
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: netsec.local, Si
te: Default-First-Site-Name)
445/tcp   open  microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds (workgroup:
NETSEC)
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http   Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
3268/tcp  open  ldap         Microsoft Windows Active Directory LDAP (Domain: netsec.local, Si
te: Default-First-Site-Name)
3269/tcp  open  tcpwrapped
5985/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
9389/tcp  open  mc-nmf       .NET Message Framing
47001/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49664/tcp open  msrpc        Microsoft Windows RPC
49665/tcp open  msrpc        Microsoft Windows RPC
49666/tcp open  msrpc        Microsoft Windows RPC
49667/tcp open  msrpc        Microsoft Windows RPC
49669/tcp open  msrpc        Microsoft Windows RPC
49670/tcp open  ncacn_http   Microsoft Windows RPC over HTTP 1.0
49671/tcp open  msrpc        Microsoft Windows RPC
49675/tcp open  msrpc        Microsoft Windows RPC
49685/tcp open  msrpc        Microsoft Windows RPC
49707/tcp open  msrpc        Microsoft Windows RPC
1 service unrecognized despite returning data. If you know the service/version, please submit
the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port53-TCP:V=7.95%I=7%D=9/20%Time=68CECB4E%P=x86_64-pc-linux-gnu%r(DNS-
SF:SD-TCP,30,"\0\.\0\0\x80\x82\0\x01\0\0\0\0\0\0\t_services\x07_dns-sd\x04
SF:_udp\x05local\0\0\x0c\0\x01");
MAC Address: 00:0C:29:E8:0D:53 (VMware)
Service Info: Host: WIN-A8PBA9GL4GE; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sat Sep 20 11:42:39 2025 -- 1 IP address (1 host up) scanned in 54.03 seconds

==== End of service version enumeration ====
```

Discovering key services (e.g., FTP, SSH, SMB, WinRM, LDAP, RDP), and proceeding to shared folders enumeration followed by running three different NSE scripts for SMB enumeration (OS, Security Mode, Protocols)

```
==== Key service discovery ====

SMB service found at 192.168.244.150

[*] Enumerating SMB shares on 192.168.244.150...
# Nmap 7.95 scan initiated Sat Sep 20 11:42:39 2025 as: /usr/lib/nmap/nmap --script smb-enum-s
hares -p445 -oN results/smb_shares_192.168.244.150.txt 192.168.244.150
Nmap scan report for 192.168.244.150
Host is up (0.00041s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:E8:0D:53 (VMware)

Host script results:
| smb-enum-shares:
|   note: ERROR: Enumerating shares failed, guessing at common ones (NT_STATUS_ACCESS_DENIED)
|   account_used: <blank>
|   \\192.168.244.150\ADMIN$:
|     warning: Couldn't get details for share: NT_STATUS_ACCESS_DENIED
|     Anonymous access: <none>
|   \\192.168.244.150\C$:
|     warning: Couldn't get details for share: NT_STATUS_ACCESS_DENIED
|     Anonymous access: <none>
|   \\192.168.244.150\IPC$:
|     warning: Couldn't get details for share: NT_STATUS_ACCESS_DENIED
```

```
|     Anonymous access: READ
|   \\192.168.244.150\NETLOGON:
|     warning: Couldn't get details for share: NT_STATUS_ACCESS_DENIED
|_    Anonymous access: <none>

# Nmap done at Sat Sep 20 11:42:40 2025 -- 1 IP address (1 host up) scanned in 1.21 seconds

[*] Enumerating SMB OS and version on 192.168.244.150...
# Nmap 7.95 scan initiated Sat Sep 20 11:42:40 2025 as: /usr/lib/nmap/nmap --script smb-os-dis
covery -p445 -oN results/smb_os_192.168.244.150.txt 192.168.244.150
Nmap scan report for 192.168.244.150
Host is up (0.00040s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:E8:0D:53 (VMware)

Host script results:
| smb-os-discovery:
|   OS: Windows Server 2016 Standard Evaluation 14393 (Windows Server 2016 Standard Evaluation
 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: 2025-09-20T08:42:49-07:00
```

```
# Nmap done at Sat Sep 20 11:42:41 2025 -- 1 IP address (1 host up) scanned in 0.27 seconds

[*] Enumerating SMB security mode on 192.168.244.150...
# Nmap 7.95 scan initiated Sat Sep 20 11:42:41 2025 as: /usr/lib/nmap/nmap --script smb-securi
ty-mode -p445 -oN results/smb_security_192.168.244.150.txt 192.168.244.150
Nmap scan report for 192.168.244.150
Host is up (0.00060s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:E8:0D:53 (VMware)

Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: required

# Nmap done at Sat Sep 20 11:42:41 2025 -- 1 IP address (1 host up) scanned in 0.27 seconds

[*] Enumerating supported SMB protocols on 192.168.244.150...
# Nmap 7.95 scan initiated Sat Sep 20 11:42:41 2025 as: /usr/lib/nmap/nmap --script smb-protoc
ols -p445 -oN results/smb_protocols_192.168.244.150.txt 192.168.244.150
Nmap scan report for 192.168.244.150
Host is up (0.00037s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:E8:0D:53 (VMware)

Host script results:
| smb-protocols:
|   dialects:
|     NT LM 0.12 (SMBv1) [dangerous, but default]
|     2:0:2
|     2:1:0
|     3:0:0
|     3:0:2
|_    3:1:1

# Nmap done at Sat Sep 20 11:42:41 2025 -- 1 IP address (1 host up) scanned in 0.26 seconds
WinRM_HTTP service found at 192.168.244.150
LDAP service found at 192.168.244.150
LDAPS service found at 192.168.244.150

==== End of key service discovery ====
```

AD users and domain groups enumeration

```
[+] Scanning target IP: 192.168.244.150

==== Domain Users for 192.168.244.150 ====

Administrator
Guest
krbtgt
DefaultAccount
James
John
Robert
Michael
William
David
Richard
Joseph
Thomas
Charles
Christopher
Daniel
Matthew
Anthony
Donald
Mark
Paul
Steven
Andrew
Kenneth
Joshua
George
Kevin
Brian
Edward
Mary
Patricia
Jennifer
Linda
Elizabeth
Barbara
Susan
Jessica
Sarah
Karen
Nancy
Margaret
Lisa
Betty
Dorothy
Sandra
Ashley
Kimberly
Donna
Emily


Donna
Emily
```

```
pentestme
hack3r
disuser

==== Domain Groups for 192.168.244.150 ====

Enterprise Read-only Domain Controllers
Domain Admins
Domain Users
Domain Guests
Domain Computers
Domain Controllers
Schema Admins
Enterprise Admins
Group Policy Creator Owners
Read-only Domain Controllers
Cloneable Domain Controllers
Protected Users
Key Admins
Enterprise Key Admins
DnsUpdateProxy
Helpdesk
IT
Finance
Management
security

==== Domain Shares for 192.168.244.150 ====
```

Domain shares and password policy

```
==== Domain Shares for 192.168.244.150 ====


        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
        NETLOGON        Disk      Logon server share
        ShareName       Disk
        SYSVOL          Disk      Logon server share
Reconnecting with SMB1 for workgroup listing.
Unable to connect with SMB1 -- no workgroup available

==== Password Policy for 192.168.244.150 ====

 =========================( Password Policy Information for 192.168.244.150 )===============
==========


[+] Attaching to 192.168.244.150 using pentestme:Pa$$word

[+] Trying protocol 139/SMB...

        [!] Protocol failed: Cannot request session (Called Name:192.168.244.150)

[+] Trying protocol 445/SMB...

[+] Found domain(s):

        [+] NETSEC
        [+] Builtin

[+] Password Info for Domain: NETSEC

        [+] Minimum password length: 7
        [+] Password history length: 24
```



```
        [+] Maximum password age: 41 days 23 hours 53 minutes
        [+] Password Complexity Flags: 000001

                [+] 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: 1

        [+] Minimum password age: 1 day 4 minutes
        [+] 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: Enabled
Minimum Password Length: 7
```

Domain Admin accounts, Disabled accounts and Never-Expired accounts identified by RID and hexadecimal acb, carved with enum4linux.

```
==== Domain Admins at 192.168.244.150 ====

Administrator
hack3r

==== Disabled Accounts at 192.168.244.150 ====

Charles
disuser
krbtgt

==== Never-Expired Accounts at 192.168.244.150 ====

Barbara
James
Jennifer
Joseph
Matthew
```

3. Exploitation Mode:

NSE Vulnerability scan against discovered ports.

```
==== Nmap vulnerability scan results ====

# Nmap 7.95 scan initiated Sat Sep 20 11:43:24 2025 as: /usr/lib/nmap/nmap -p 53,88,135,139,38
9,445,464,593,636,3268,3269,5985,9389,47001,49664,49665,49666,49667,49669,49670,49671,49675,49
685,49707, --script=vuln -oN results/nmap_vuln_scan_192.168.244.150.txt 192.168.244.150
Nmap scan report for 192.168.244.150
Host is up (0.00020s latency).

PORT      STATE SERVICE
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
9389/tcp  open  adws
```

```
47001/tcp open  winrm
49664/tcp open  unknown
49665/tcp open  unknown
49666/tcp open  unknown
49667/tcp open  unknown
49669/tcp open  unknown
49670/tcp open  unknown
49671/tcp open  unknown
49675/tcp open  unknown
49685/tcp open  unknown
49707/tcp open  unknown
MAC Address: 00:0C:29:E8:0D:53 (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
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-a
ttacks/
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|_      https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
|_smb-vuln-ms10-054: false

# Nmap done at Sat Sep 20 11:46:08 2025 -- 1 IP address (1 host up) scanned in 164.76 seconds

==== End of vulnerability scan results ====
```

Successful password-spraying attempts with Crackmapexec against previously discovered AD users.

```
==== Password spraying results ====


Weak credentials found:
SMB                     192.168.244.150 445    WIN-A8PBA9GL4GE  [+] netsec.local\Richard:C4uE
1wN5q

Weak credentials found:
SMB                     192.168.244.150 445    WIN-A8PBA9GL4GE  [+] netsec.local\Mark:C4uE1wN
5q

Weak credentials found:
SMB                     192.168.244.150 445    WIN-A8PBA9GL4GE  [+] netsec.local\Mary:C4uE1wN
5q

==== End of password spraying results ====
```

Successful Hashcat Kerberos ticket cracking attempts after carving the hashes by using the Impacket script.

```
==== Cracked Tickets for 192.168.244.150 ====

$krb5asrep$23$Matthew@NETSEC.LOCAL:0b2c6c1c8af01c95e2206d7f70e51491$603467665fb65f01716ba86789
92e7ab6113f64f52ccb64621f12239655b7ea6764e178179a73606c10bee86eefdae0848106e6de045882e23356b68
c0c871c624a5b73a7b02965aa2877aa80217db90b31b65a76228c23ed82d5c46155a53580c8b277c0f0fe3b1484b38
78c7a50d4aa58063a62168c36300a74f63c3346d61fb47dff295ab941765f7a675df75c0ab0fb3c0219829aeef334e
7e7968f654cc72d8eb15567200321b9e120fdbf83d4c0f05ef44b0bbb1dfc34fca7cc113c433decd1881898dac7854
7e662b4f0496a387303ac5fe95cfe80282f12b7f91cc4ea44285587e8e484b318e678b:ReinaAgustine55
$krb5asrep$23$Barbara@NETSEC.LOCAL:6223d2e6585b4e8ed3cdaab7d8d359d9$f8690138ad8dc16dd4cff4b3fc
2690f59acadc3c90ee4cf0f2b3744fffa6bf148714994ea1b597b0e04989eb5336d8fc53f446a3b7bb7f552d7053b9
```

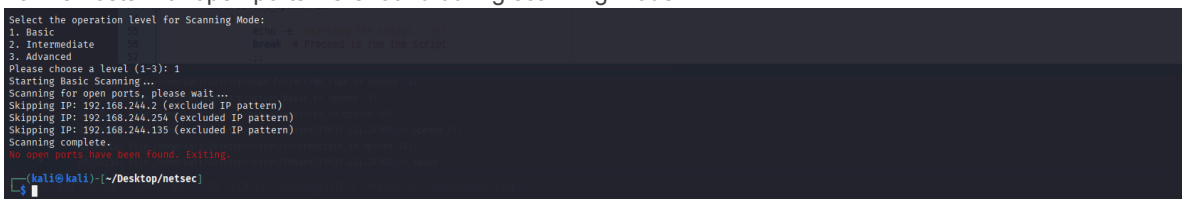
```
31574487e8b99f310aa1e37ab46c639640d55e64438625adc53c48fbc8161a510589b2e9780010cb02c0fe25a9552b
1787c51269ab0668dae1007a52476fa038e6e63443874bd893abcf1328a1e9de05ab724198d970421877628cf1a297
d1f39066e42180b30cae25aa6ccc8766b4283f81fe7d33549adb1e9c318ed2af9a6896f42627aa9f4bb2686caf4808
07bcad6db094f49f735f01edb887c76438ea469988b0e6b5f99c60855aa8d5ef0ef575:TmaAebCaoPao4
```

Error Handling -

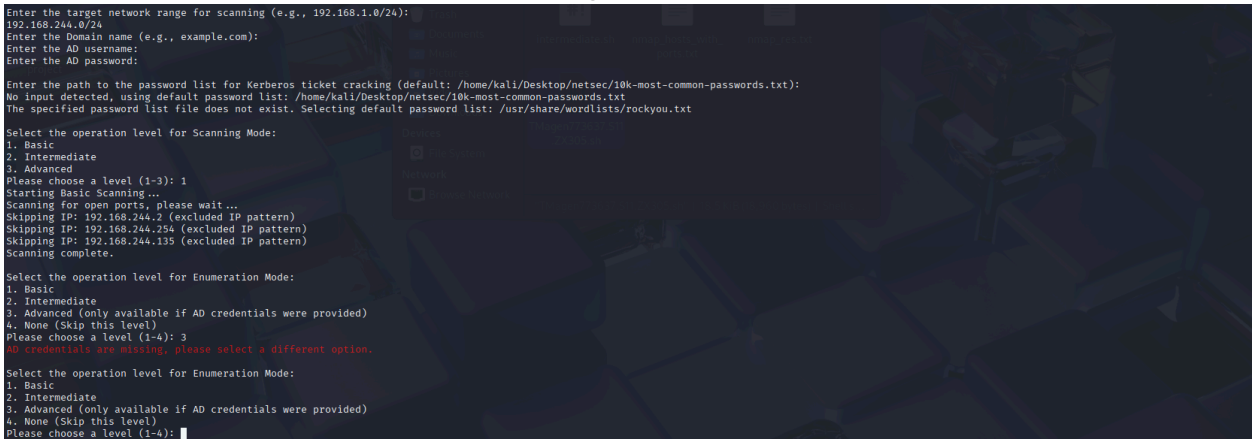
This section will go through different occurrences of incorrect input by the user and lower level modes selection.

Root privilege and invalid network range format handling.
Additionally, AD credentials were not provided by the user (Will be handled on the Enumeration stage).

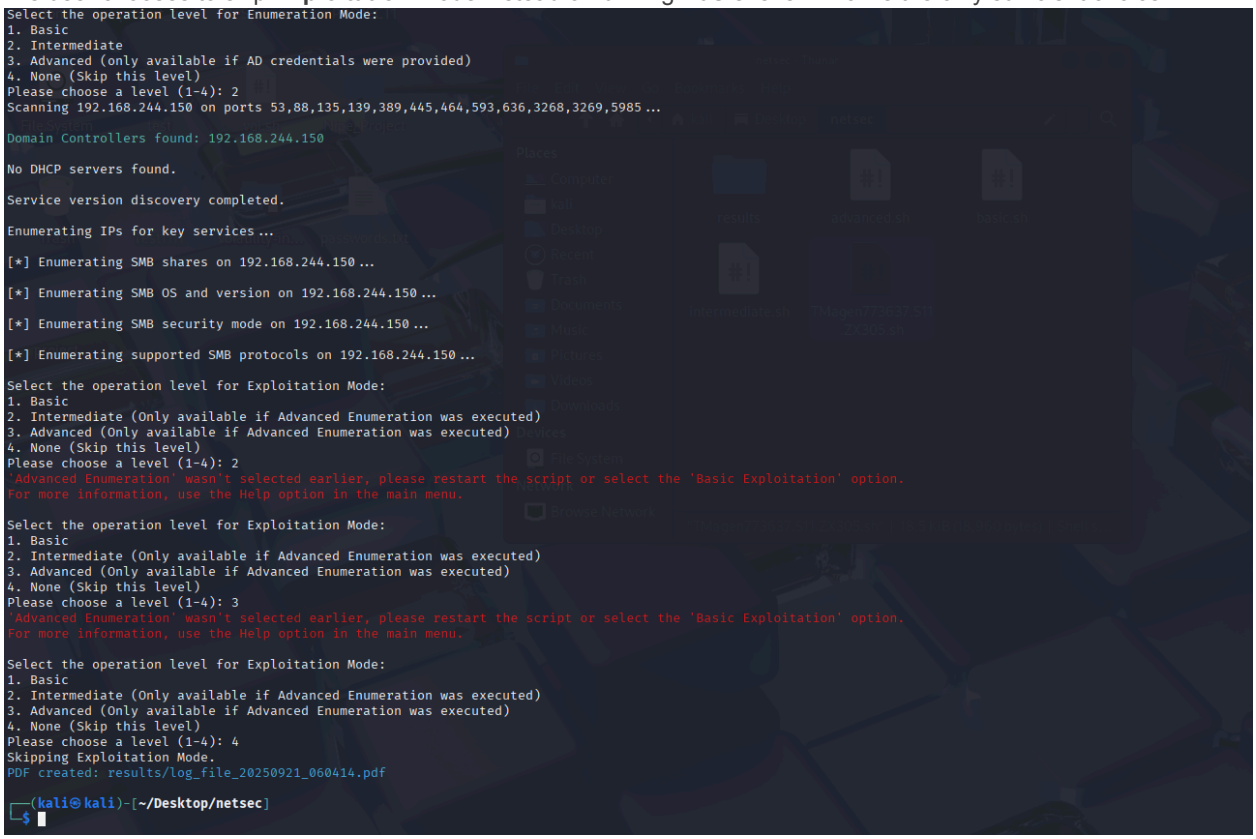
No live hosts with open ports were found during scanning mode.



Running the script the same way but with live remote hosts with open ports.
Advanced Enumeration is unable to run due to missing AD credentials.



Choosing **Intermediate Enumeration** instead.
Intermediate and **Advanced Exploitation** modes unable to run due to missing data that is carved only by **Advanced Enumeration** (e.g., AD users for password-spraying that happens when at least **Intermediate** level was chosen for exploitation).
The user chooses to skip **Exploitation** mode instead of running **Basic** level which is the only sufficient choice.



New log file added to the results folder.

A shorter log file, based on the user's limited execution of the script.

```
PORT     STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:E8:0D:53 (VMware)

Host script results:
| smb-protocols:
|   dialects:
|     NT LM 0.12 (SMBv1) [dangerous, but default]
|     2:0:2
|     2:1:0
|     3:0:0
|     3:0:2
|_    3:1:1

# Nmap done at Sun Sep 21 06:03:51 2025 -- 1 IP address (1 host up) scanned in 0.28 seconds
```

```
WinRM_HTTP service found at 192.168.244.150
LDAP service found at 192.168.244.150
LDAPS service found at 192.168.244.150

==== End of key service discovery ====
```