Polenum

Polenum is a python script which uses the Impacted Library from CORE Security Technologies to extract the password policy information from a windows machine. This allows a non-windows (Linux, Mac OSX, BSD etc...) user to query the password policy of a remote windows box without the need to have access to a windows machine.

Supported OS:

Linux

How to do download GitHub repository?

https://github.com/wh1t3Fox/polenum.git

Copy this link and paste on terminal.

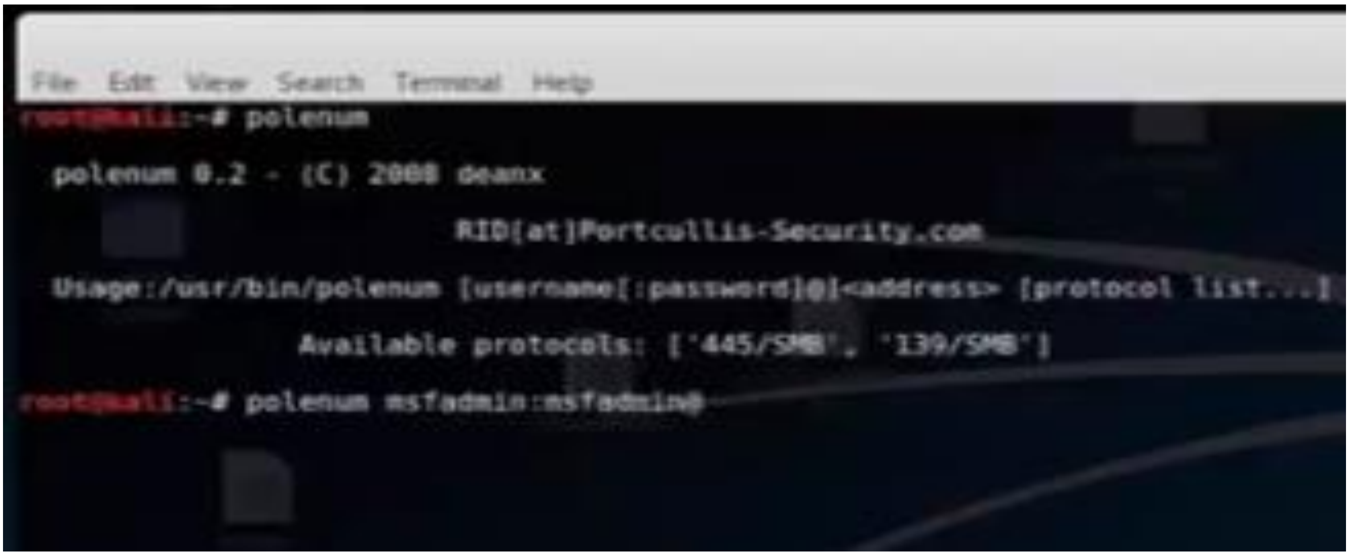
Key features

- Can extract password and associated information from a windows machine
- Will connect over a NULL or authenticated share
- Supports encrypted/signed sessions

How to Extract the Password policies from windows system?

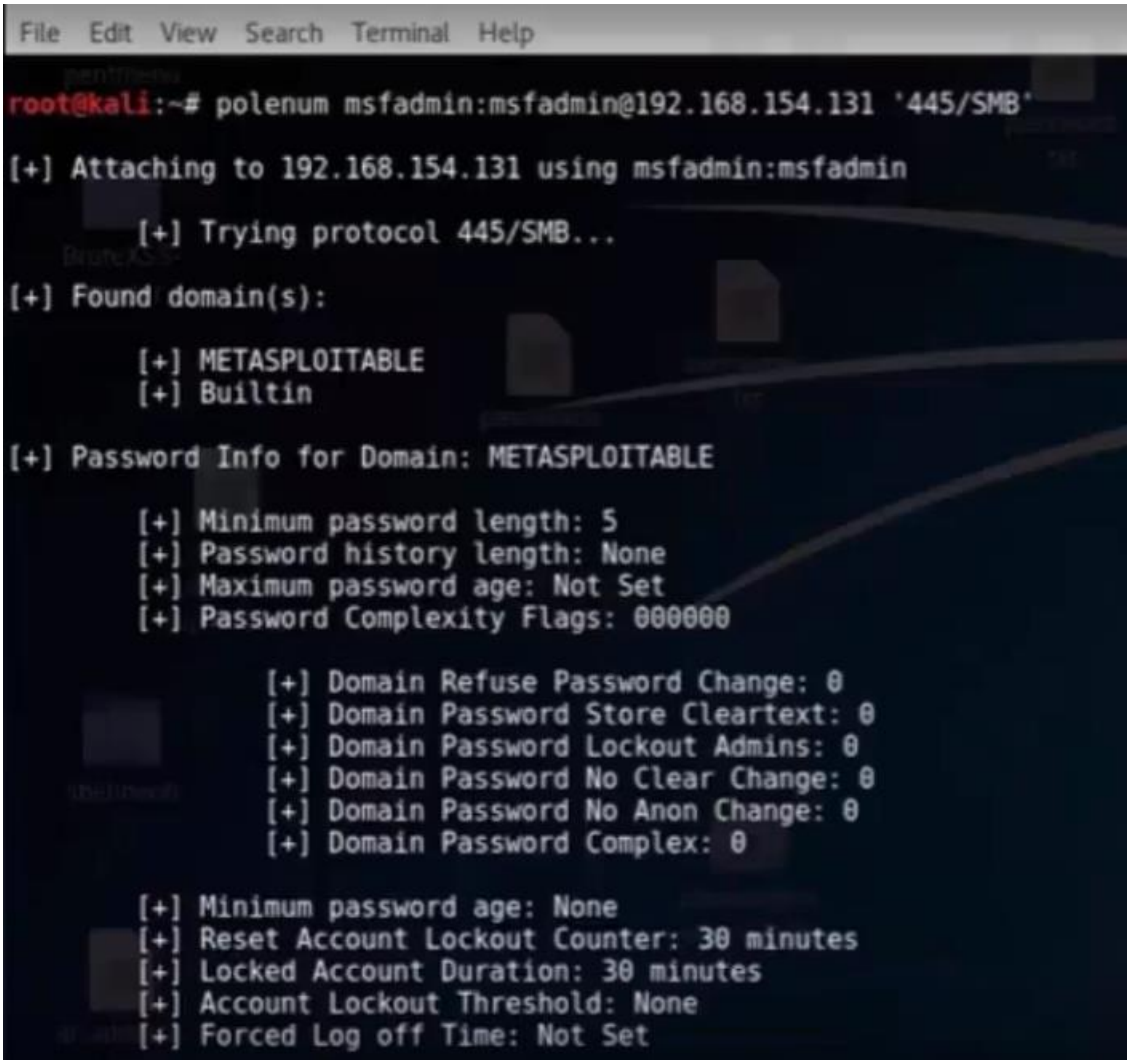
Step 1: Open Kali Linux and then click on terminal

Step 2: Type Polenum on terminal



```
root@kali:~# polenum

 polenum 0.2 - (C) 2008 deanx

                     RID[at]Portcullis-Security.com

 Usage:/usr/bin/polenum [username[:password]@]<address> [protocol list...]

                 Available protocols: ['445/SMB', '139/SMB']

root@kali:~# polenum msfadmin:msfadmin@
```

Step 3: Type polenum msfadmin:msfadmin@192.168.154.131 '445/SMB'



```
root@kali:~# polenum msfadmin:msfadmin@192.168.154.131 '445/SMB'

[+] Attaching to 192.168.154.131 using msfadmin:msfadmin

        [+] Trying protocol 445/SMB...

[+] Found domain(s):

        [+] METASPLOITABLE
        [+] Builtin

[+] Password Info for Domain: METASPLOITABLE

        [+] Minimum password length: 5
        [+] Password history length: None
        [+] Maximum password age: Not Set
        [+] Password Complexity Flags: 000000

                [+] Domain Refuse Password Change: 0
                [+] Domain Password Store Cleartext: 0
                [+] Domain Password Lockout Admins: 0
                [+] Domain Password No Clear Change: 0
                [+] Domain Password No Anon Change: 0
                [+] Domain Password Complex: 0

        [+] Minimum password age: None
        [+] Reset Account Lockout Counter: 30 minutes
        [+] Locked Account Duration: 30 minutes
        [+] Account Lockout Threshold: None
        [+] Forced Log off Time: Not Set
```