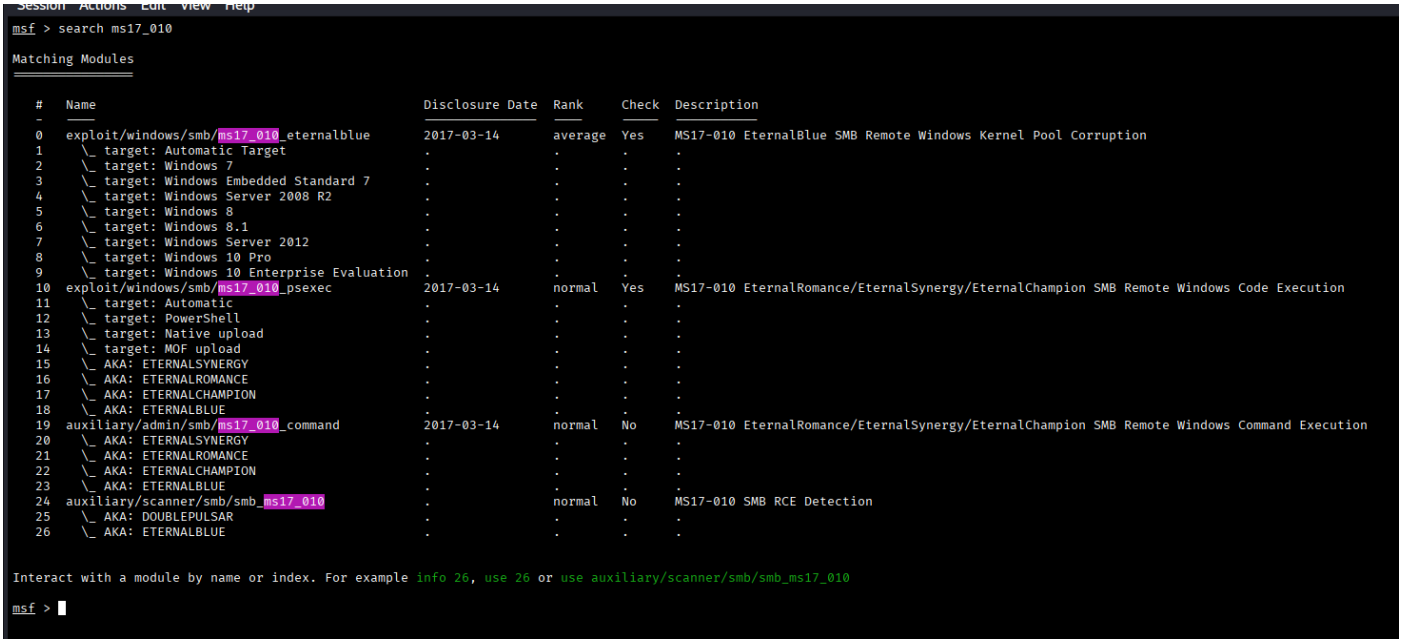
INDICE

INTRODUZIONE ED OBIETTIVO

INTRODUZIONE: Il presente report documenta l'attività di penetration testing condotta su un sistema Windows 7 vulnerabile alla CVE-2017-0144 (MS17-010), nota come EternalBlue. L'esercizio ha utilizzato il framework Metasploit per sfruttare la vulnerabilità nel protocollo SMBv1 e ottenere accesso remoto non autorizzato al sistema target.

OBIETTIVO: sfruttare la vulnerabilità MS17-010 per ottenere una sessione Meterpreter sul sistema target Windows e successivamente recuperare uno screenshot del desktop, individuare la presenza di webcam, e testare le funzionalità di keylogging.

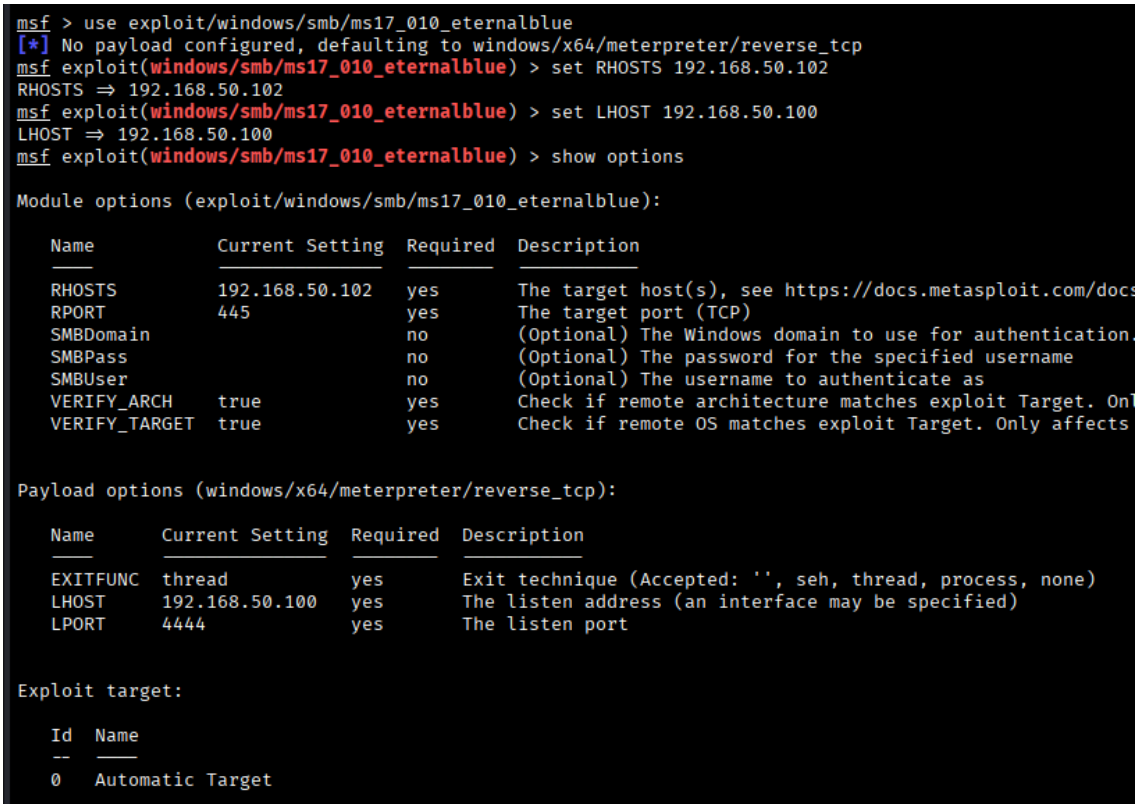


Dopo aver completato la configurazione dell'ambiente di laboratorio e verificato la connettività di rete tra la macchina attaccante e il sistema target tramite test di raggiungibilità (ping), è stato avviato Metasploit Framework attraverso l'interfaccia a riga di comando msfconsole.

Utilizzando il comando search MS17-010, sono stati identificati i moduli disponibili per lo sfruttamento della vulnerabilità. L'output ha mostrato diverse opzioni, tra cui:

- exploit/windows/smb/ms17_010_eternalblue - modulo di exploit per l'esecuzione remota di codice,
- exploit/windows/smb/ms17_010_psexec - modulo alternativo per l'esecuzione tramite SMB,
- auxiliary/scanner/smb/smb_ms17_010 - modulo ausiliario per la verifica della vulnerabilità.

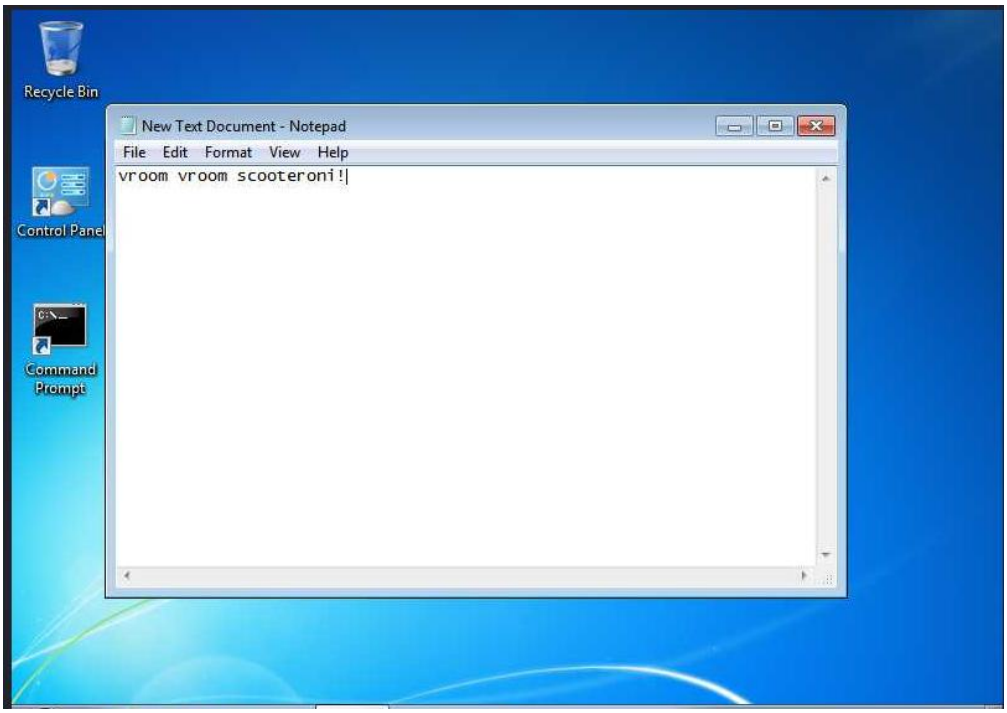
È stato selezionato il modulo exploit/windows/smb/ms17_010_eternalblue in quanto specificamente progettato per sistemi Windows 7 e in grado di fornire una sessione Meterpreter stabile con privilegi di sistema.



Si è proceduto alla configurazione dei parametri necessari all'esecuzione dell'exploit. Sono stati definiti l'indirizzo del sistema target (ip 192.168.50.102) e l'indirizzo locale di ascolto della macchina attaccante (IP 192.168.50.100) utilizzato per ricevere la connessione di ritorno.

Prima di procedere, è stato effettuato un controllo per assicurarsi che tutti i parametri obbligatori fossero correttamente valorizzati e coerenti con l'architettura del sistema target. Dopo aver verificato l'assenza di incongruenze nella configurazione, l'exploit è stato avviato, dando inizio alla fase di sfruttamento controllato della vulnerabilità

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



Come prima verifica del controllo remoto acquisito, è stata utilizzata la funzionalità di cattura dello schermo per acquisire uno screenshot del desktop della macchina compromessa. L'immagine è stata salvata automaticamente sulla macchina attaccante e mostra chiaramente l'ambiente grafico del sistema Windows 7 in esecuzione, confermando l'accesso effettivo e il pieno controllo della sessione.
Questa operazione rappresenta una prova concreta dell'avvenuta compromissione e costituisce una tipica attività di verifica non distruttiva condotta durante le fasi di post-exploitation.

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

Successivamente è stata effettuata una verifica della presenza di dispositivi di acquisizione video sul sistema compromesso, utilizzando le funzionalità di enumerazione hardware disponibili ma l'operazione non ha rilevato alcun dispositivo webcam disponibile sul sistema target.

```
meterpreter > sysinfo
Computer        : AJEJE-PC
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : it_IT
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x64/windows
meterpreter >
```

è stata eseguita un'ulteriore operazione di raccolta delle informazioni di sistema del target e tramite l'apposita funzionalità di interrogazione del sistema, sono stati ottenuti i principali dati identificativi della macchina compromessa, tra cui il nome del computer, la versione del sistema operativo, l'architettura a 64 bit, la lingua di sistema e il contesto di rete di appartenenza.

Le informazioni raccolte confermano che il sistema target corrisponde all'ambiente previsto per l'esercizio e che la sessione Meterpreter è stata stabilita correttamente, consentendo l'accesso in lettura ai dati di sistema senza effettuare modifiche o azioni distruttive.

```
Session  Actions  Edit  View  Help
meterpreter > shell
Process 1828 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::49fd:6a60:8bf6:63b1%11
   IPv4 Address. . . . . . . . . . . : 192.168.50.102
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Tunnel adapter isatap.{9A4546A2-0F0C-44EF-B9F7-1835CEA8DAD3}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Windows\system32>
```

Per finire è stato aperto un canale di shell interattiva sul sistema compromesso, consentendo l'interazione diretta con l'ambiente operativo Windows attraverso l'interfaccia a riga di comando nativa.

L'accesso alla shell è stato verificato mediante un controllo della configurazione di rete del sistema, che ha confermato la corrispondenza dell'indirizzo IP con quello della macchina target (192.168.50.102). Questo riscontro dimostra inequivocabilmente che il controllo è stato effettivamente ottenuto sul sistema corretto e che attraverso la shell è possibile eseguire qualsiasi comando disponibile sul sistema operativo compromesso.

CONCLUSIONE

L’esercizio ha consentito di simulare in modo completo e controllato lo sfruttamento della vulnerabilità, dimostrando l’intero flusso operativo dalla fase di configurazione e verifica fino alle attività di post-exploitation.

L’ottenimento della sessione Meterpreter ha permesso di confermare il pieno controllo remoto del sistema target attraverso operazioni non distruttive, quali l’acquisizione dello screenshot del desktop, la verifica dell’assenza di dispositivi di acquisizione video e la raccolta delle informazioni di sistema e di rete.

Le attività svolte hanno evidenziato come una vulnerabilità non corretta possa consentire l’accesso remoto e l’interazione approfondita con il sistema compromesso, anche in assenza di credenziali valide.