Security Operation: azioni preventive

Davide Diglio

Traccia

L'esercizio di oggi è verificare in che modo l'attivazione del Firewall impatta il risultato di una scansione dei servizi dall'esterno. Per questo motivo:

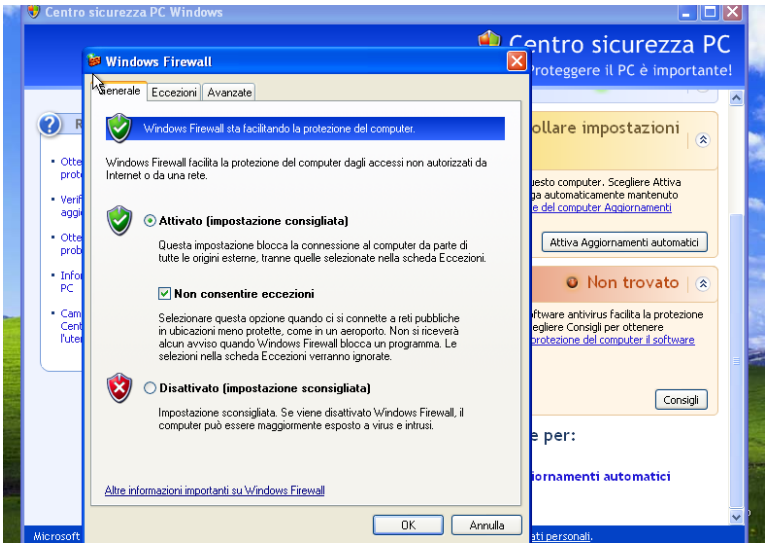
- Assicuratevi che il Firewall sia disattivato sulla macchina Windows XP.
- Effettuate una scansione con nmap sulla macchina target (utilizzate lo switch –sV).
- Abilitare il Firewall sulla macchina Windows XP.
- Effettuate una seconda scansione con nmap (utilizzando ancora una volta lo switch –sV).

Svolgimento

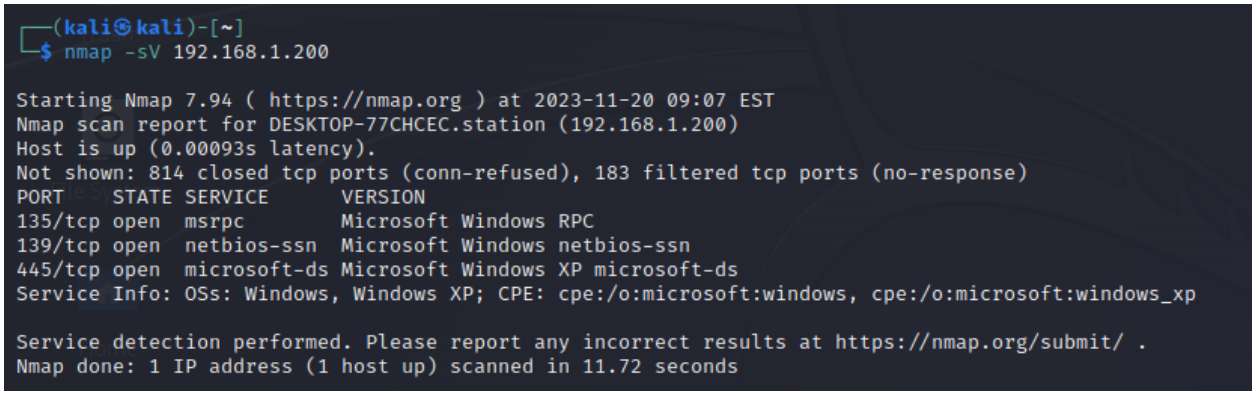
Parte I

In questo esercizio dobbiamo capire come impatta il Firewall sulla scansione dei servizi dall'esterno. Utilizziamo le due macchine virtuali, che sono: Windows XP e Kali.

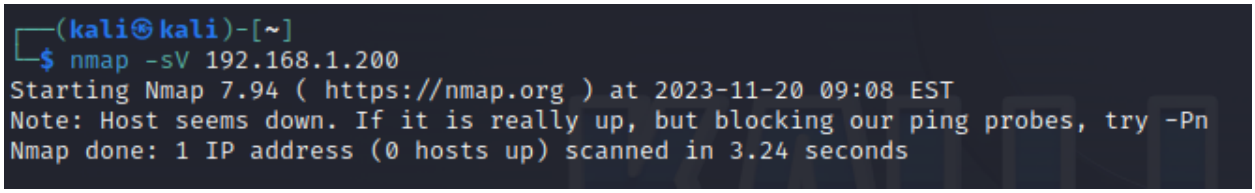
Sulla macchina Windows XP si deve disattivare il Firewall prima di fare la scansione, andando su Windows Firewall.



Dopo aver disattivato il Firewall sulla macchina Windows XP, nella macchina Kali andiamo a scansionare con il comando “nmap -sV 192.168.1.200” la macchina target.



Subito dopo abbiamo attivato il Firewall e rifatto la scansione sulla macchina.



Notiamo in questo esercizio se il Firewall è disattivato la scansione nmap può far vedere le porte aperte e i servizi attivi, questo comporta di avere più possibilità di attacchi. Abilitando il Firewall si può non rilevare queste informazioni, perché il Firewall filtra e blocca il traffico di rete.