EPICODE

Security Operation: azioni preventive

Traccia:

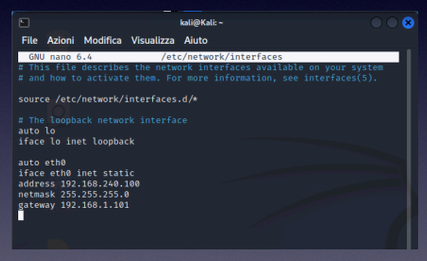
Durante la lezione teorica, abbiamo studiato le azioni preventive per ridurre la possibilità di attacchi provenienti dall'esterno.
Abbiamo visto che a livello di rete, possiamo attivare / configurare Firewall e regole per fare in modo che un determinato traffico, potenzialmente dannoso, venga bloccato.

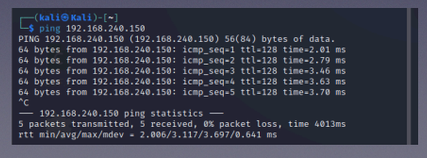
La macchina Windows XP in formato OVA che abbiamo utilizzato nella Unit 2 ha di default il Firewall disabilitato.

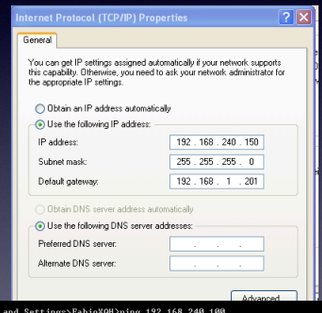
L'esercizio di oggi è verificare in che modo l'attivazione del Firewall impatta il risultato di una scansione dei servizi dall'esterno. Per questo motivo:

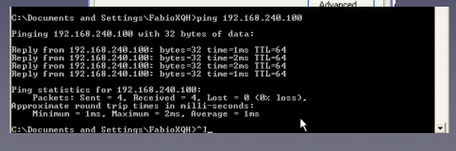
1. Assicuratevi che il Firewall sia disattivato sulla macchina Windows XP
2. Effettuate una scansione con nmap sulla macchina target (utilizzate lo switch –sV, per la service detection e -o nomefilereport per salvare in un file l'output)
3. Abilitare il Firewall sulla macchina Windows XP
4. Effettuate una seconda scansione con nmap, utilizzando ancora una volta lo switch –sV.
5. Trovare le eventuali differenze e motivarle.

Sono andato a configurare gli indirizzi IP di entrambe le macchine ai seguenti indirizzi:
-Kali 192.168.240.100
-Windows XP 192.168.240.150

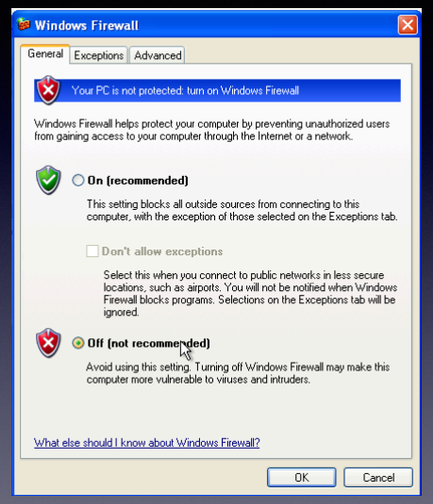




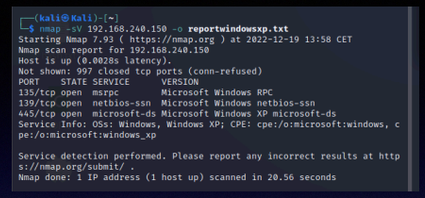


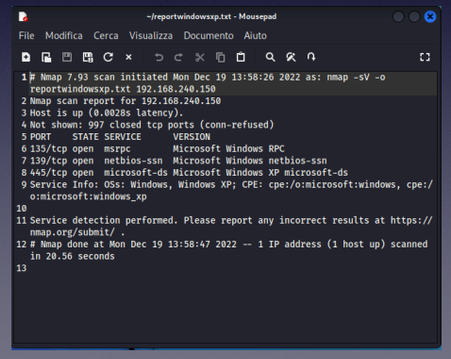


Fatto ciò sono andato a verificare lo stato del firewall su Windows, riscontrando che esso fosse disattivato.
Solo in questo modo la nostra macchina attaccante potrà effettuare una scansione con nmap come vedremo di seguito.

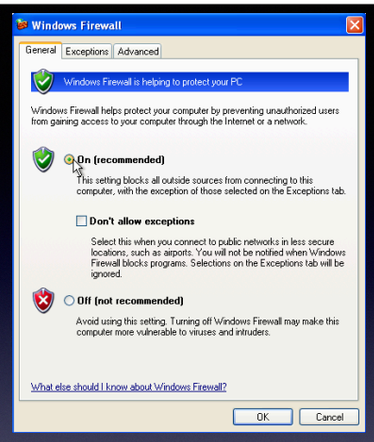


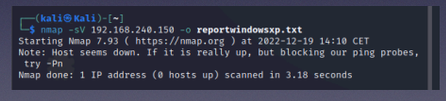
Infatti come risultato abbiamo ottenuto con comando “nmap -sV” la scansione porte e versione della macchina bersaglio.
In più ho creato un file (reportwindowsxp.txt) dove inserire il report della scansione appena effettuata, che ho associato con -o.

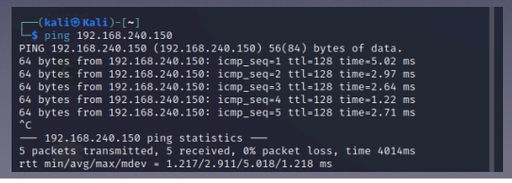


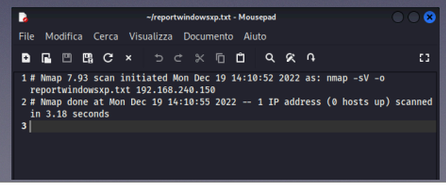


Ma adesso proviamo ad effettuare una scansione con firewall attivo e come risultato otteniamo l'esatto opposto, ovvero vi è comunicazione fra le macchine ma non è possibile effettuare alcuna scansione.

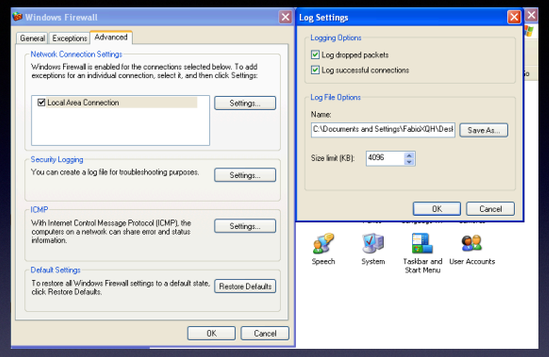


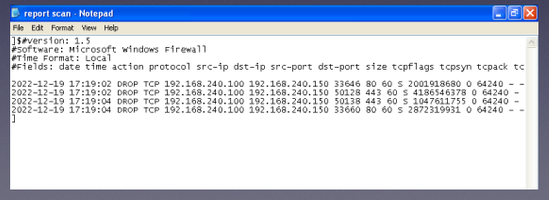






Una cosa in più che sono andato a configurare nelle opzioni avanzate del firewall, sono i log dei pacchetti in uscita e le connessioni con eventuali macchine. Ricevendo un report di tentativo di invio pacchetti tcp da macchina attaccante Kali, bloccati dal firewall.





Conclusioni:

Come abbiamo visto nella lezione teorica di oggi, possiamo dedurre che il firewall gioca un ruolo fondamentale per la sicurezza dei dati all'interno di un sistema informatico.
Pertanto occorre prestare la massima attenzione e assicurarsi di tenere sempre attivo il firewall onde evitare che qualche malintenzionato possa andare ad effettuare azioni malevole nella nostra rete.