**Security Operation: azioni preventive**

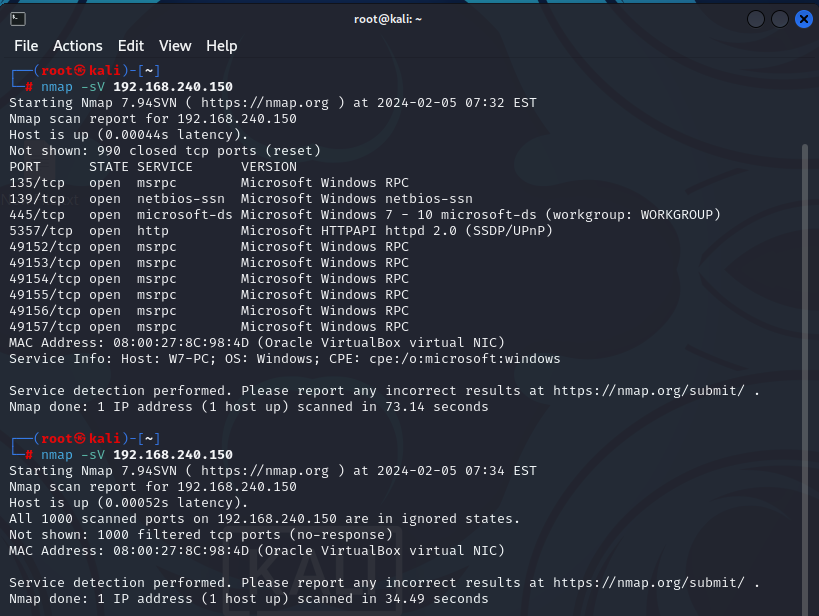
**Traccia:**

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 che abbiamo utilizzato 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.



Nella prima scansione, con il firewall disattivato, ci sono diverse porte aperte che indicano servizi in esecuzione, come il servizio RPC di Microsoft, NetBIOS, HTTP e altre porte associate a servizi di rete di Windows. Ciò mostra che la macchina è abbastanza esposta e potenzialmente vulnerabile agli attacchi, dato che vari servizi sono accessibili dall'esterno.

Nella seconda scansione, non si vedono porte aperte, indicando che il firewall è stato abilitato e configurato per bloccare l'accesso in ingresso a questi servizi. Questo suggerisce che il firewall sta efficacemente proteggendo la macchina bloccando le connessioni in entrata non autorizzate.

Rispondendo alla domanda numero 5 dell'esercizio, le differenze evidenti tra le due scansioni sono:

* La prima scansione mostra molte porte aperte, indicando che diversi servizi sono esposti e accessibili dall'esterno.
* La seconda scansione mostra tutte le porte in uno stato ignorato o filtrato, il che significa che il firewall sta bloccando l'accesso in ingresso a questi servizi.

La motivazione di queste differenze è chiaramente l'abilitazione del firewall tra la prima e la seconda scansione. Con il firewall attivato, i servizi che prima erano visibili e accessibili ora sono protetti, riducendo significativamente il profilo di attacco della macchina e migliorando la sua sicurezza generale.