**SECURITY OPERATION: AZIONI PREVENTIVE**

**INTRODUZIONE TEORICA**

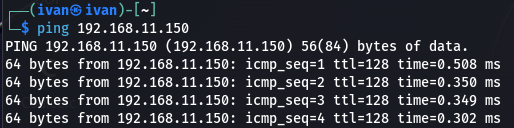
Firewall: dispositivo o software per proteggere una rete da minacce esterne, regolando la rete in entrata e in uscita.  
In questo caso Windows XP integra un firewall con filtraggio dinamico.  
Come vedremo nell’esercizio, il firewall di XP è dinamico, in quanto blocca le comunicazioni in entrata ma permette quelle in uscita.

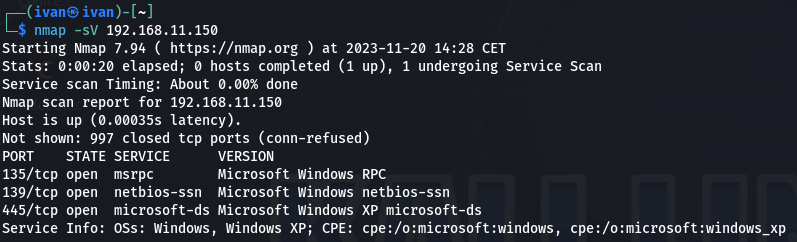
**ESERCIZIO**

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 ed effettuate una scansione con nmap sulla macchina target (utilizzate lo switch –sV, per la service detection).   
2) Abilitare il Firewall sulla macchina Windows XP ed effettuate una seconda scansione con nmap, utilizzando ancora una volta lo switch –sV.

**1) FW DISATTIVATO E SCANSIONE NMAP**

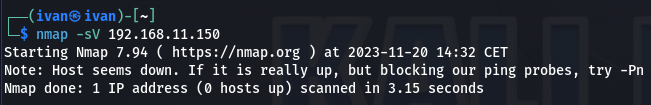
Abbiamo fatto pingare le due macchine.

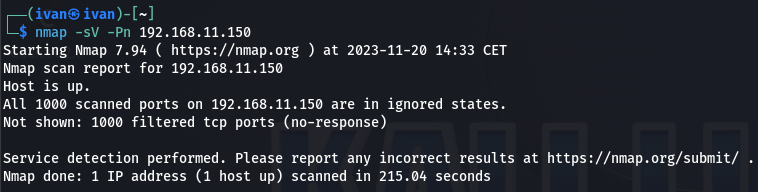


  
Successivamente abbiamo eseguito una scansione su Windows XP tramite NMAP. Con -sV siamo andati a vedere tutti i servizi e le corrispondenti versioni disponibili sulle porte di WinXP.

Siamo così riusciti ad ottenere le informazioni riguardanti le porte aperte di WinXP.

**2) FW ATTIVO E SCANSIONE NMAP**

Abbiamo attivato il firewall su WinXP e abbiamo avviato una scansione con NMAP.

Notiamo come NMAP ci dice che il target non esiste o che, probabilmente, esiste ma blocca i nostri ping.  
Proviamo quindi una scansione senza ping con -P.

In questo caso notiamo che rileva la macchina target “Host is up”, ma come risultiamo otteniamo tutte le sue porte filtrate.

**CONSIDERAZIONI**Che differenze notate? E quale può essere la causa del risultato diverso?  
  
Abbiamo notato come col firewall attivo, non riusciamo più ad ottenere le informazioni riguardanti le porte della macchina target.   
Questo è dovuto al fatto che il firewall blocchi molti servizi tra cui l’ICMP (è come se la macchina risultasse inesistente).  
Per questo motivo, tramite una scansione senza ping (3W HS), riusciamo a trovare la macchina target sulla rete, ma tutte le sue porte sono filtrate (potrebbero essere aperte ma NMAP non riesce a definirle al 100%).  
Tutto ciò è dovuto al firewall che funge da scudo analizzando tutto il traffico in entrata, respingendolo o accettandolo, a seconda del relativo funzionamento (es. Permit nell’ACL o in risposta ad una richiesta in uscita).