ESERCITAZIONE W18D1(1)

EPICODE

Esercizio
Le 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.

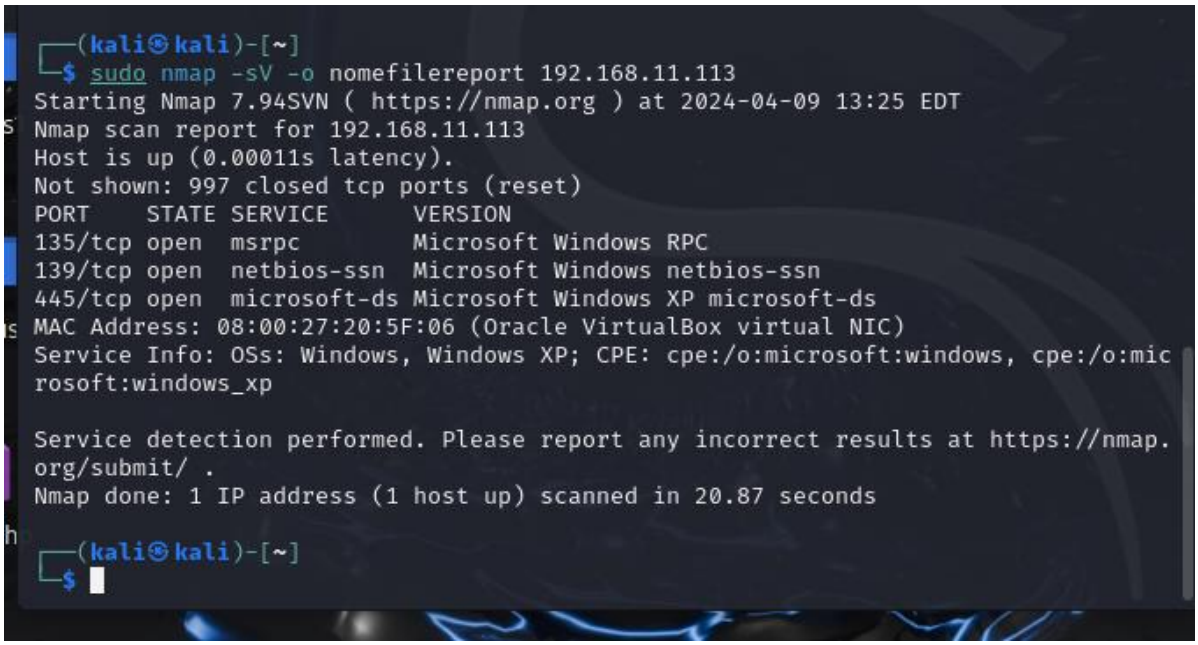
La macchina Windows XP in formato OVA che abbiamo utilizzato nella Unit 2 ha di **default il Firewall disabilitato.**

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.

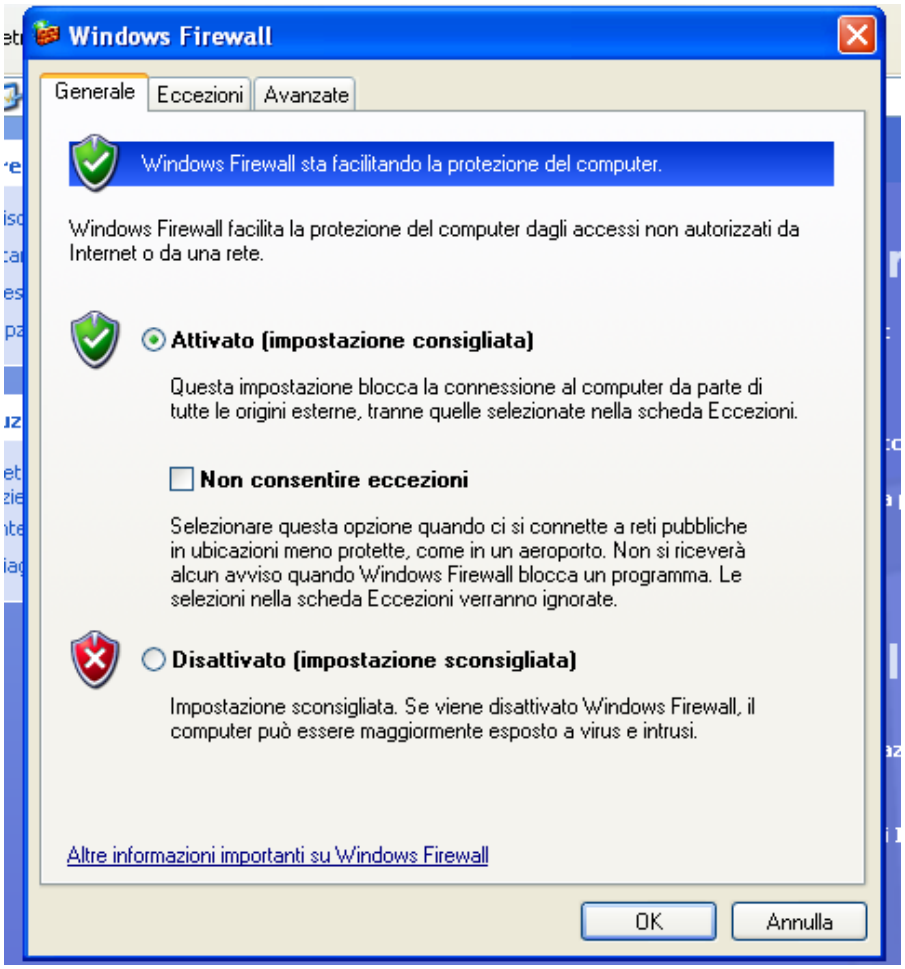
3

Scansione di nmap ,(senza firewall) sulla macchina Windows XP

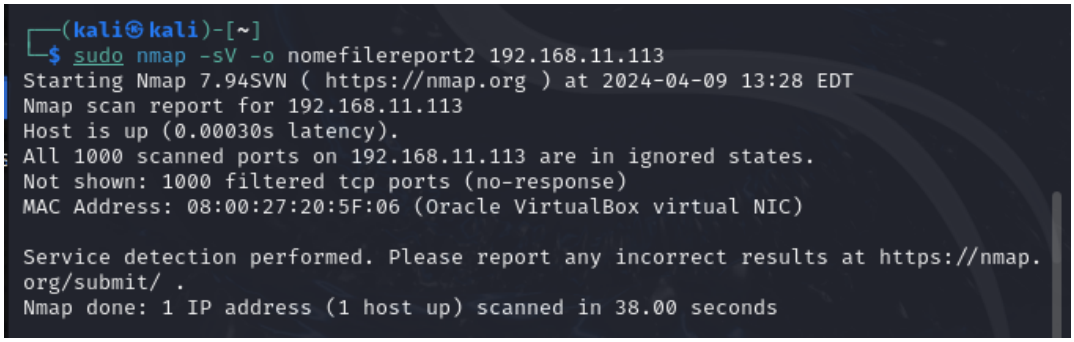


Dalla scansione possiamo vedere che ci sono 3 servizi in ascolto sulle porte TCP

Attivo il firewall per la prossima scansione



Scansione nmap su Windows XP (con firewall attivo)



Da questa scansione possiamo vedere che grazie al firewall tutte le porte sono filtrate, quindi bloccandone l'accesso