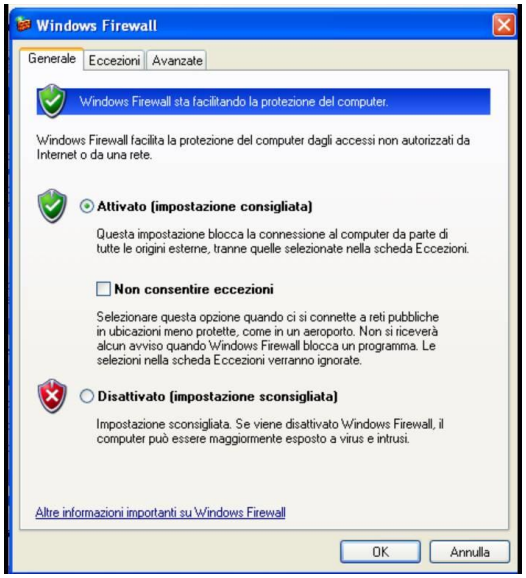
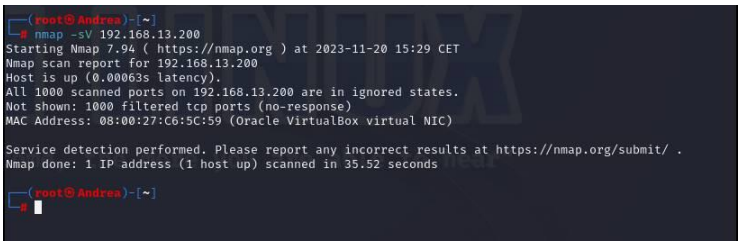
Esercizio 1 Settimana 9

Security Operations: azioni preventive

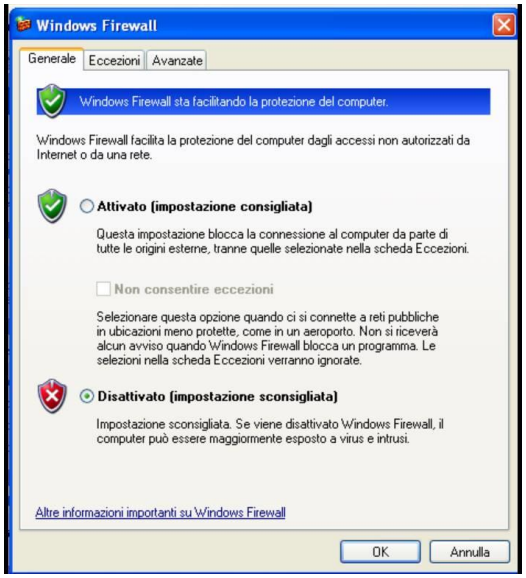
Tra le azioni preventive per ridurre la possibilità di attacchi, abbiamo esaminato quelle relative alla rete. Possiamo quindi andare ad attivare e/o configurare un Firewall che permetta solo a determinati indirizzi IP di generare del traffico non desiderato nella nostra rete.
Andiamo quindi ad effettuare una scansione con 'nmap' delle porte e dei relativi servizi attivi con lo switch '-sV' per la service detection sulla macchina Windows con e senza Firewall attivo.

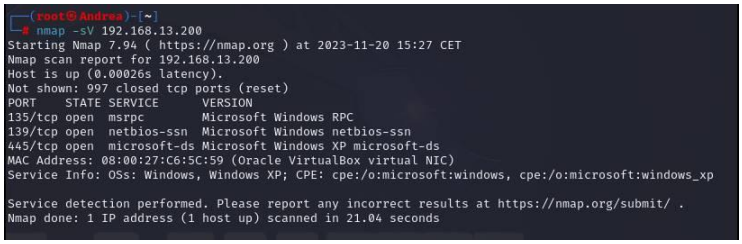
FIREWALL ON:





FIREWALL OFF:





Come possiamo notare, nella situazione con Firewall attivo ‘nmap’ non ci mostra in output alcuna informazione riguardo lo stato delle porte e i servizi attivi su di esse. Di contro ci comunica che tutte le porte scansionate su quell’IP sono in stato ‘filtered’: significa che per quelle determinate porte è impossibile determinarne lo stato (aperto, chiuso, etc.) a causa di restrizioni dovute, in questo caso, al Firewall.
Questa casistica potrebbe sorgere anche nel momento in cui l’utente disattivi il protocollo ICMP che permette la ricezione del ping; per poter distinguere le due casistiche (ICMP o Firewall) si potrebbe utilizzare lo switch ‘-Pn’ di ‘nmap’ per escludere il ping dalla scansione ed inviare le richieste direttamente senza prima preoccuparsi dello stato attivo o meno del target.
Caso contrario per la situazione di Firewall disattivato, dove ‘nmap’ ci restituisce le porte aperte e la relativa versione dei servizi attivi in quanto non ci sono limiti o restrizioni sulla macchina vittima.