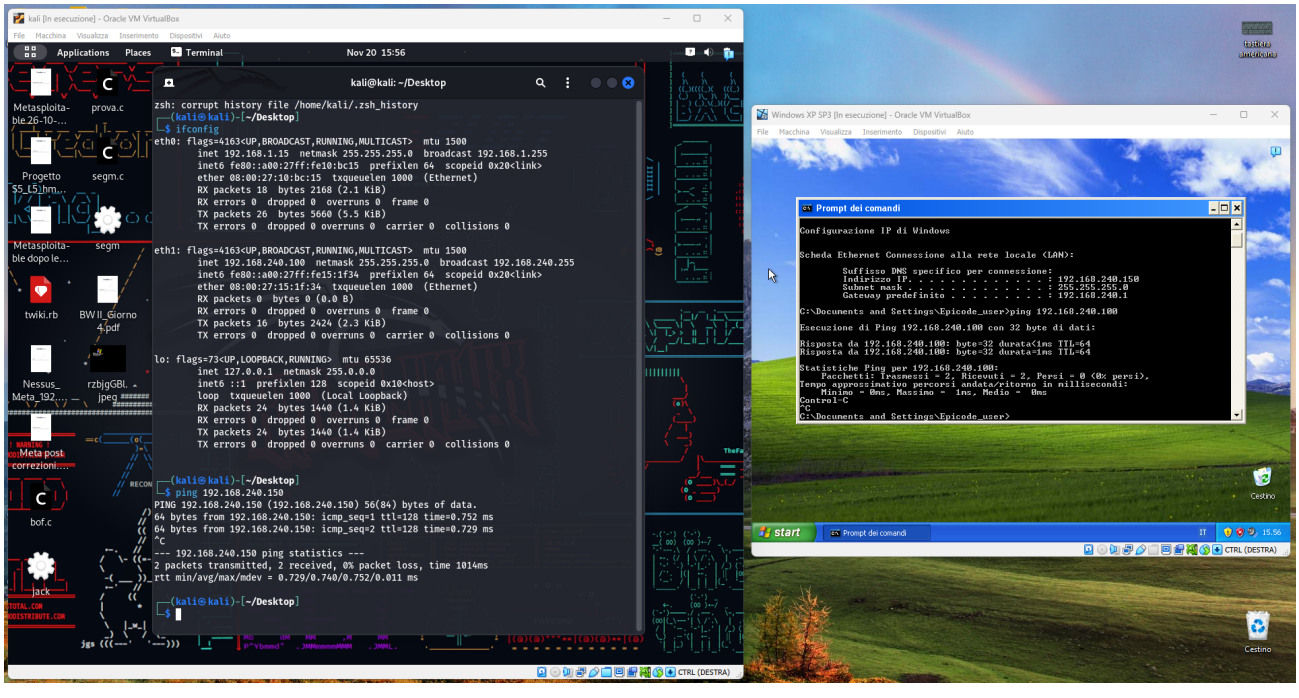
Pratica S9/L1

Security Operation: azioni preventive

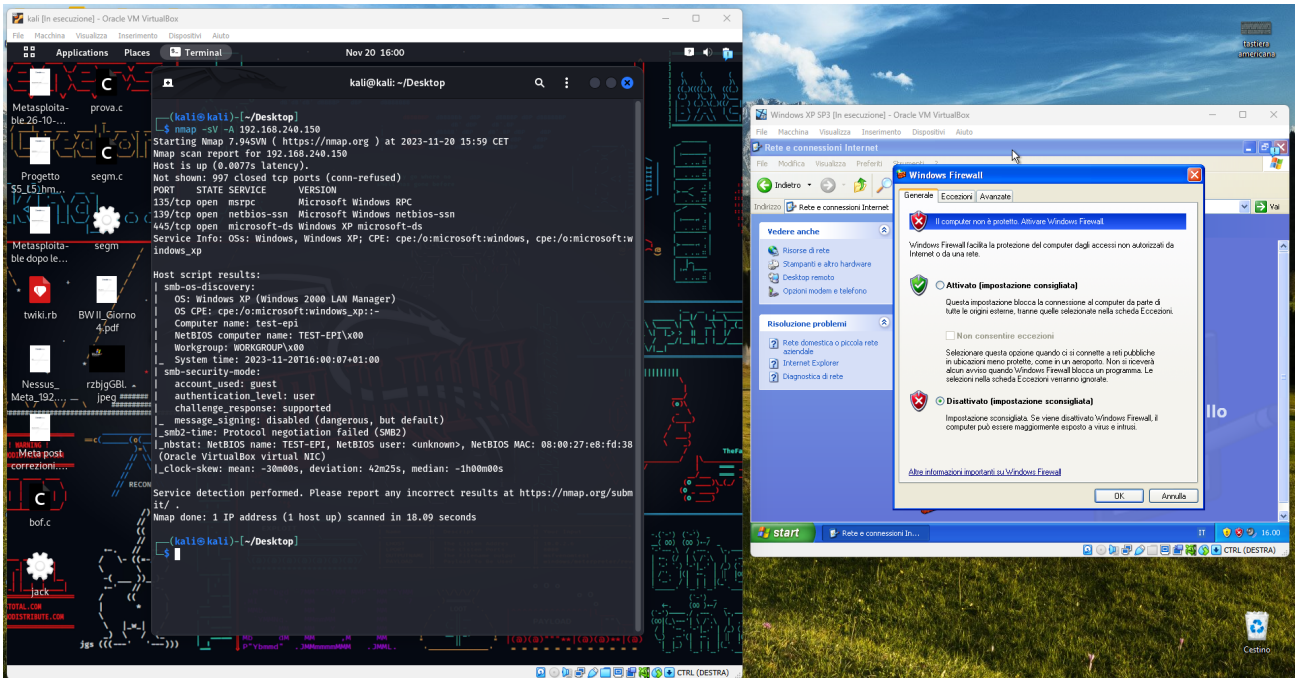
L’esercizio di oggi ha lo scopo di osservare quanto un firewall può influenzare una scansione dei servizi attivi su un host.

Per il laboratorio di prova imposto una macchina virtuale Kali Linux ed una Windows XP, collegate tramite rete interna.

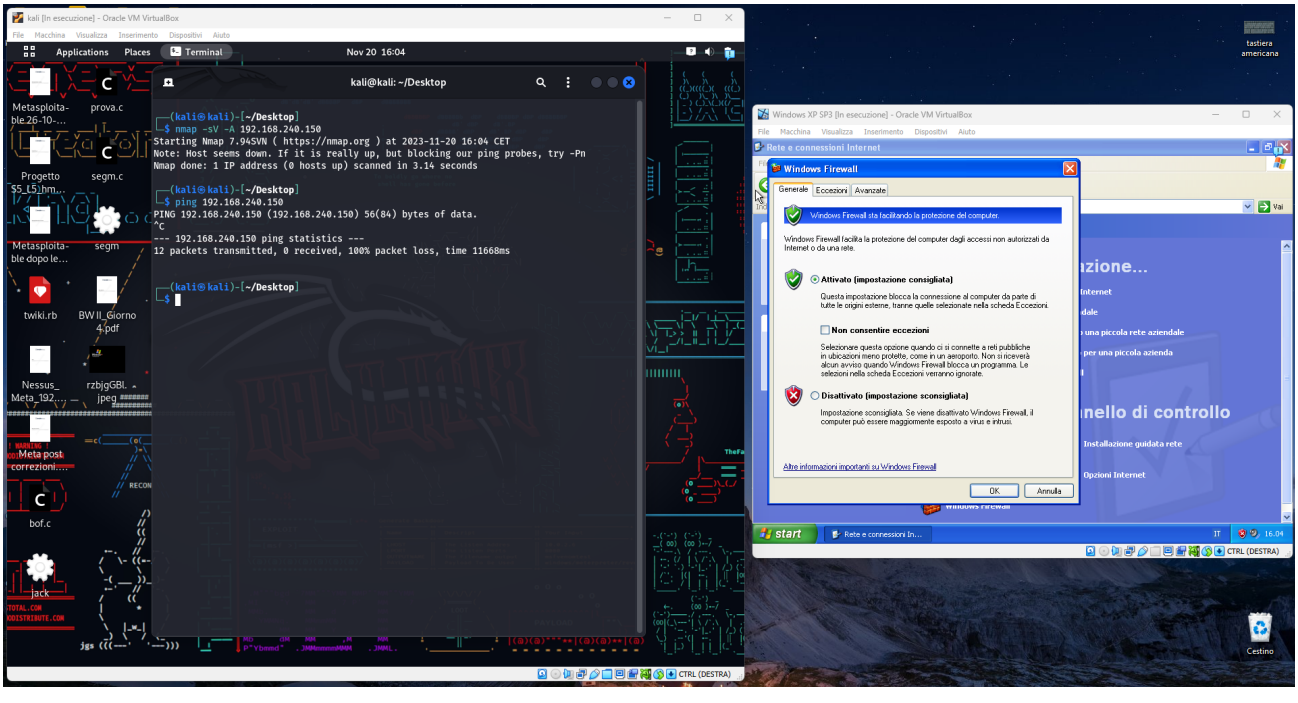


Una volta controllato che le due macchine siano in grado di comunicare, faccio partire una prima scansione con NMAP da Kali Linux verso Windows XP (NMAP è tra i tool più utilizzati dagli ethical hacker per la scansione di reti e servizi attivi sugli host, ci permette di avere una “mappa” fondamentale per comprendere come una determinata rete è organizzata, nonché dove indirizzarci per cercare e valutare eventuali vulnerabilità che possono essere sfruttate da malintenzionati).

Scansione con firewall disattivato.



Scansione con firewall attivato.



Come possiamo notare dalle due immagini sopra, il firewall fa una grande differenza quando si tratta di scansione dei servizi, una volta attivato non

permette di visionare alcuna porta/servizio, inoltre neanche il ping è possibile. Questo ci fa capire che già un basilare firewall software standard presente sul sistema operativo Windows XP, ormai obsoleto, rende per un attaccante la vita molto più difficile, non lasciando strada libera alla scansione e quindi facendolo navigare nel buio.