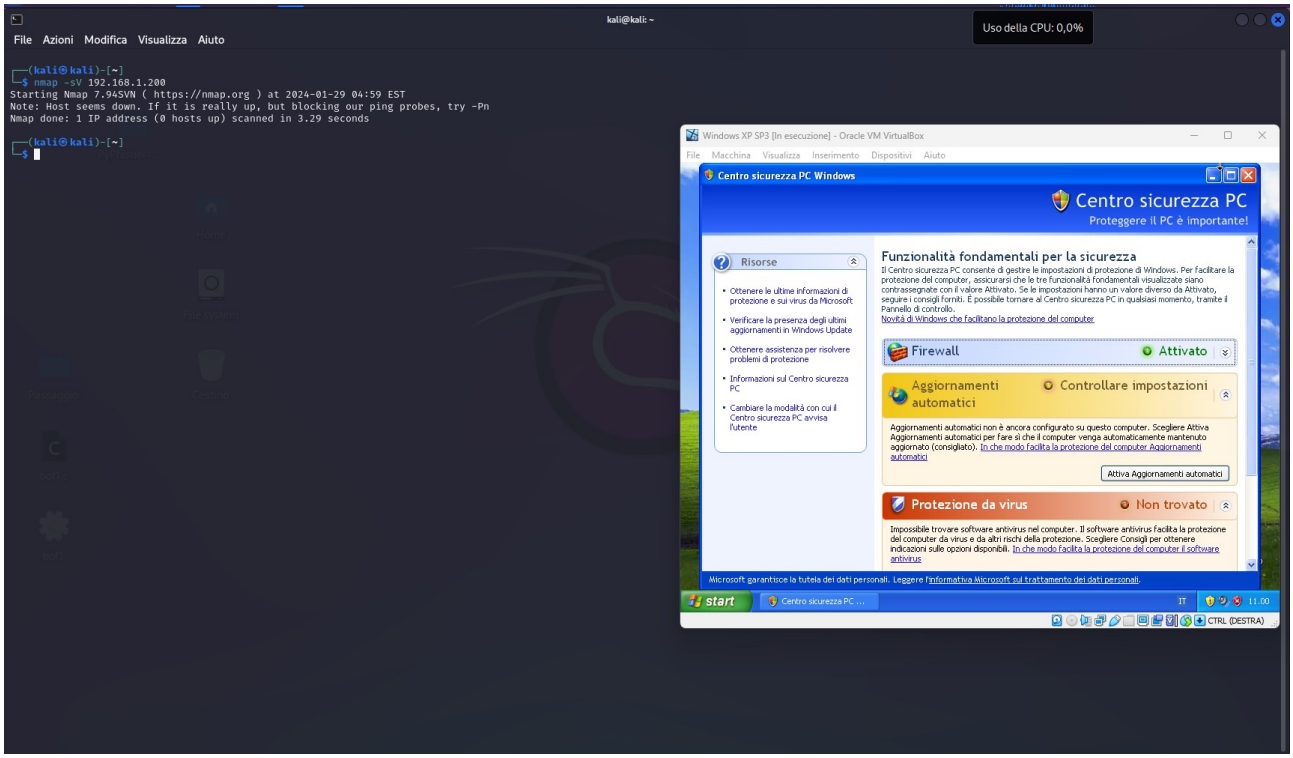
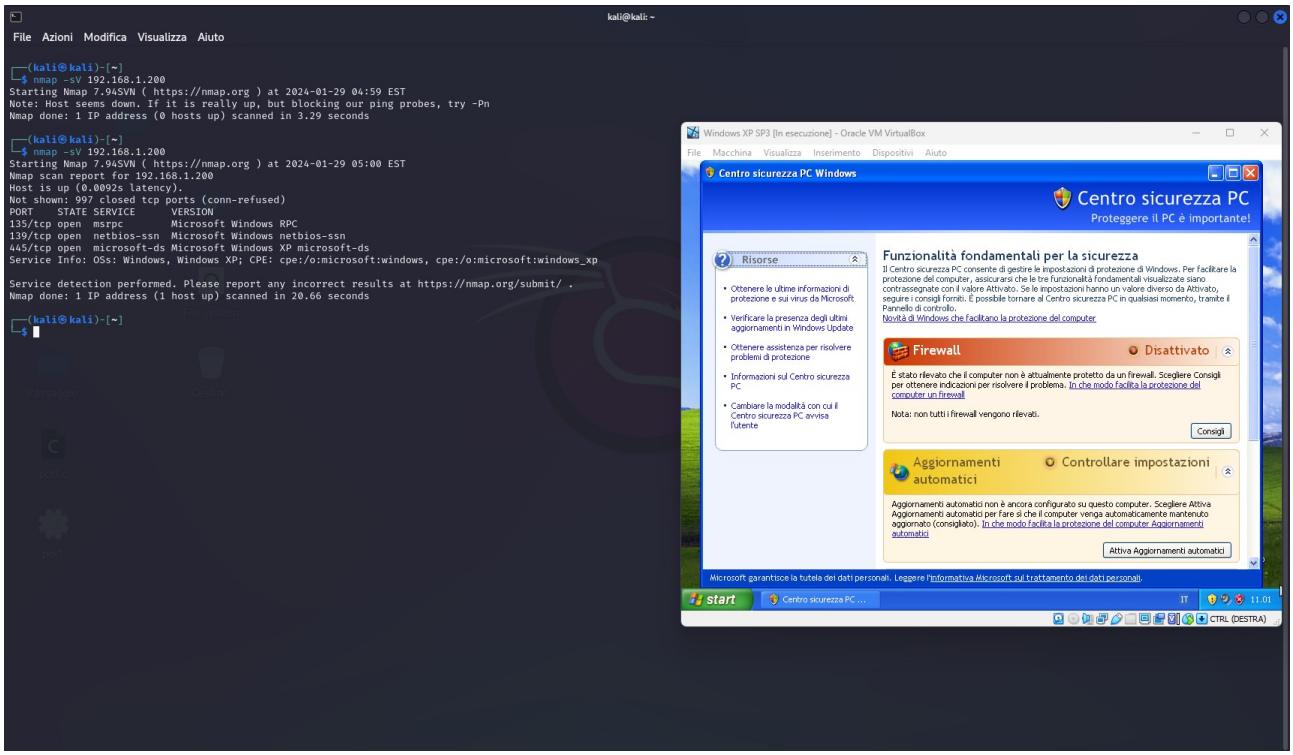
PRATICA S9/L1



Comando “nmap –sV 192.168.1.200” con Windows Firewall Attivo



Comando “nmap –sV 192.168.1.200” con Windows Firewall Disattivo

PRATICA S9/L1

La differenza principale tra una scansione dei servizi con Nmap su una macchina

Windows XP con firewall disattivato e una con firewall attivato sono:

Firewall disattivato:

Se il firewall è disattivato, Nmap può rilevare e identificare facilmente i servizi in ascolto sulla macchina. La scansione sarà più completa, poiché non ci sono restrizioni imposte dal firewall che impediscano a Nmap di comunicare con i servizi.

Firewall attivato:

Con un firewall attivato, la scansione potrebbe essere più limitata. Il firewall può bloccare le richieste di Nmap verso alcuni o tutti i servizi in ascolto sulla macchina. In tal caso, Nmap potrebbe non essere in grado di rilevare alcuni servizi o ottenere informazioni complete su di essi.

Risposta ai pacchetti di probing:

Alcuni firewall possono reagire in modo diverso ai pacchetti di probing inviati da Nmap. Alcuni potrebbero ignorarli completamente, mentre altri potrebbero rispondere con informazioni limitate o generiche. Questo può influenzare la precisione delle informazioni raccolte durante la scansione.

Porte aperte e chiuse:

Un firewall può influire sullo stato delle porte, aprendo o chiudendo porte in base alla configurazione delle regole. Ciò significa che una porta che è aperta con firewall disattivato potrebbe apparire come chiusa durante una scansione con firewall attivato, se il firewall blocca il traffico verso quella porta specifica.

Possibili falsi positivi/negativi:

A causa delle regole del firewall, possono verificarsi falsi positivi (porte segnalate come aperte quando sono chiuse) o falsi negativi (porte segnalate come chiuse quando sono aperte) durante una scansione con firewall attivato.