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:

● Assicuratevi che il Firewall sia disattivato sulla macchina Windows XP. Effettuate una scansione con nmap sulla macchina target (utilizzate lo switch –sV, per la service detection).

● Abilitare il Firewall sulla macchina Windows XP.

● Effettuate una seconda scansione con nmap, utilizzando ancora una volta lo switch –sV.

Che differenze notate? E quale può essere la causa del risultato diverso?

Che cos’è il firewall? Un dispositivo di filtraggio che regola pacchetti in entrata e in uscita. Utile per proteggere la rete

A close-up of a computer error

Description automatically generated

RISOLVIAMO LA TRACCIA

Se il firewall windows è disattivato possiamo tranquillamente scansionare ottenendo i seguenti output (per capire che il firewall è disattivato basta un semplice ping con esito positivo)

A screenshot of a computer program

Description automatically generated

Una volta abilitato il firewall come da consegna, lo scan -sV ci darà il seguente output

A screen shot of a computer code

Description automatically generated

Il firewall ha bloccato il ping quindi la nostra richiesta nmap non ha potuto completare la

Scansione, il servizio ci consiglia di eseguire una scansione con il comando -Pn ovvero effettuare

La scansione senza utilizzare protocollo ICMP

A computer screen shot of a program

Description automatically generated

Con questa scansione togliendo il ping nmap cercherà di scansionare la macchina vittima utilizzando

La stretta di mano a tre vie e ottenendo come risultato “host is up” ovvero sappiamo con certezza

Che la macchina vittima esiste, ma il firewall ci blocca qualsiasi altro tipo di comunicazione abusiva.

Un firewall, quando rifiuta pacchetti in entrata, sta effettivamente impedendo a determinati dati di passare attraverso la rete e raggiungere il sistema o la rete protetta. Questa azione di rifiuto si basa su regole predefinite configurate nel firewall. Le regole determinano quali pacchetti possono passare e quali devono essere bloccati.

Quando un pacchetto arriva al firewall, viene confrontato con queste regole. Se il pacchetto soddisfa i criteri specificati nelle regole, viene consentito; altrimenti, viene rifiutato. Le regole possono essere basate su vari criteri come indirizzi IP, porte, protocolli, o altri attributi del pacchetto.