S9L1

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) 3. Abilitare il Firewall sulla macchina Windows XP 4. Effettuate una seconda scansione con nmap, utilizzando ancora una volta lo switch –sV.

Traccia: Che differenze notate? E quale può essere la causa del risultato diverso? Requisiti: Configurate l'indirizzo di Windows XP come di seguito: 192.168.240.150 Configurate l'indirizzo della macchina Kali come di seguito: 192.168.240.100

Suggerimento: Se non siete certi di come abilitare il Firewall su Windows XP, seguite le istruzioni di seguito. 1. Cliccate sull'icona in basso a destra all'interno del rettangolo rosso in figura 2. Cliccate su Windows Firewall (rettangolo blu in figura) 3. Selezionate «DISATTIVATO» come in figura e cliccate su «OK»

Una volta avviata la nostra macchina Linux andremo direttamente ad aprire il terminale per scrivere il seguente comando:

sudo nano /etc/network/interfaces

Ci si presenterà davanti la schermata in Figura 1, questa schermata ci mostrerà l'attuale configurazione di rete e ci permetterà di configurarla a nostro piacimento.
Seguendo le indicazioni fornite dall'esercizio settiamo come di seguito la configurazione.

La nostra traccia ci chiede di settare la configurazione internet di entrambe le nostre macchine virtuali (Kali Linux - Windows XP).

Una volta avviata la nostra macchina Windows XP andremo direttamente al pannello di controllo > Rete e Connessione Internet > Connessione di rete

Successivamente andremo a usare il tasto destro su "Connessione alla rete locale"
Facciamo Click su "Proprietà" e poi Click su "Protocollo Internet (TCP / IP)"

Successivamente andremo ad usare il tasto “Proprietà” e ciò che ci troveremo davanti sarà una finestra come quella in Figura 2.
Andremo dunque a seguire le richieste della traccia per quel che riguarda la configurazione di rete così facendo:

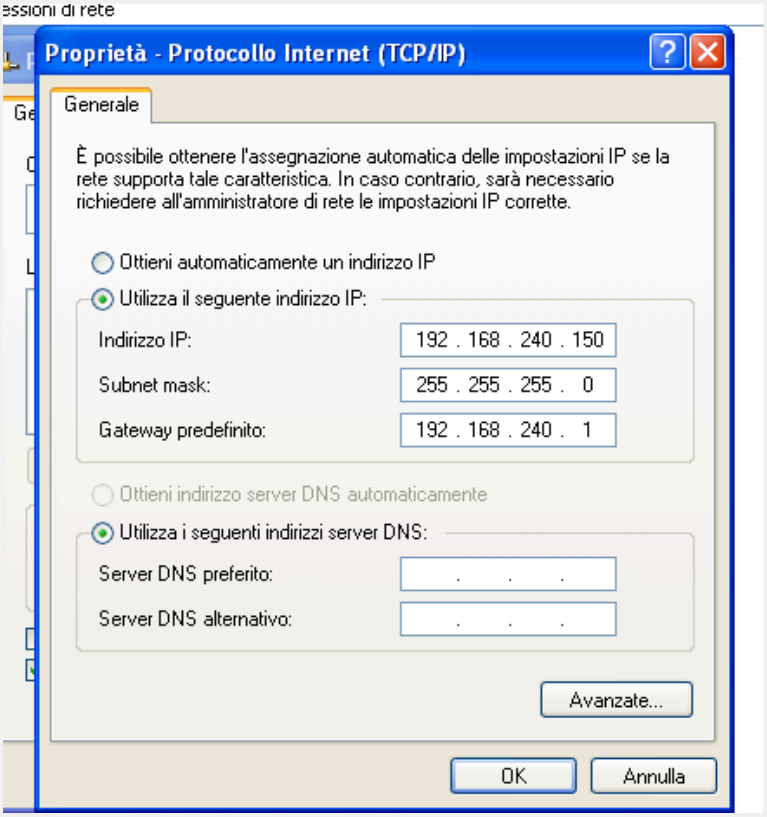

Figura 2

Subito dopo aver settato entrambe le macchine andremo a riavviarle, così da essere sicuri che le configurazioni siano utilizzate.
Una volta settate entrambe le configurazioni di rete eseguiremo un ping (Come da Figura 3) dalla macchina Kali Linux alla macchina Windows XP, così da accertarsi della corretta configurazione avvenuta.

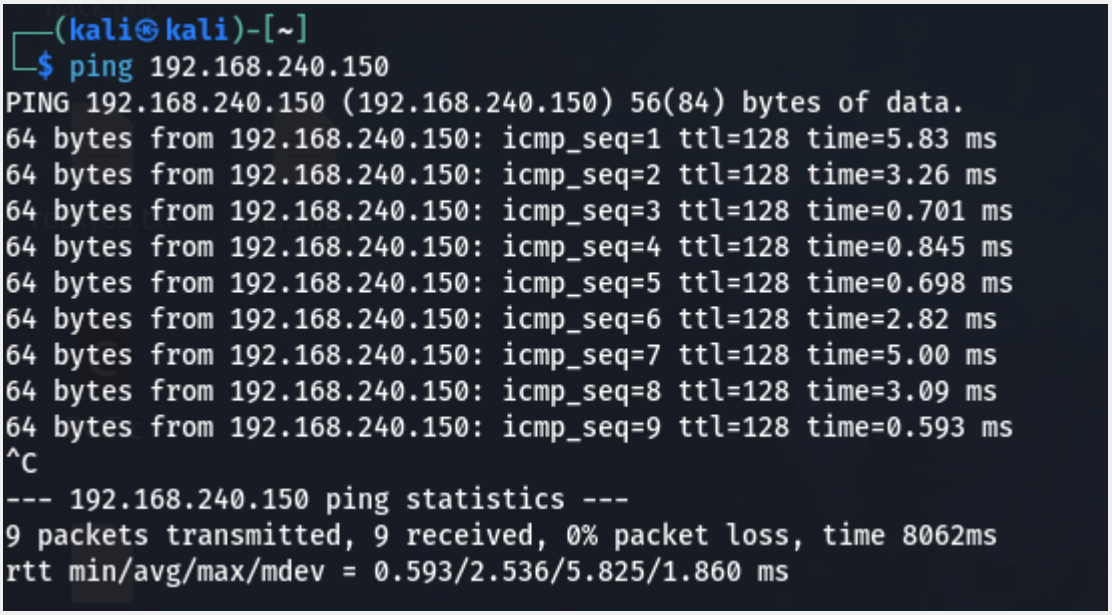

Figura 3

Come intuibile dalla Figura 3, il ping è andato a buon fine, ciò dimostra la possibilità che le due macchine si connettano.

Una volta testata la connessione andiamo ad eseguire il comando di NMAP:

nmap -sV 192.168.240.150

Come da Figura 4

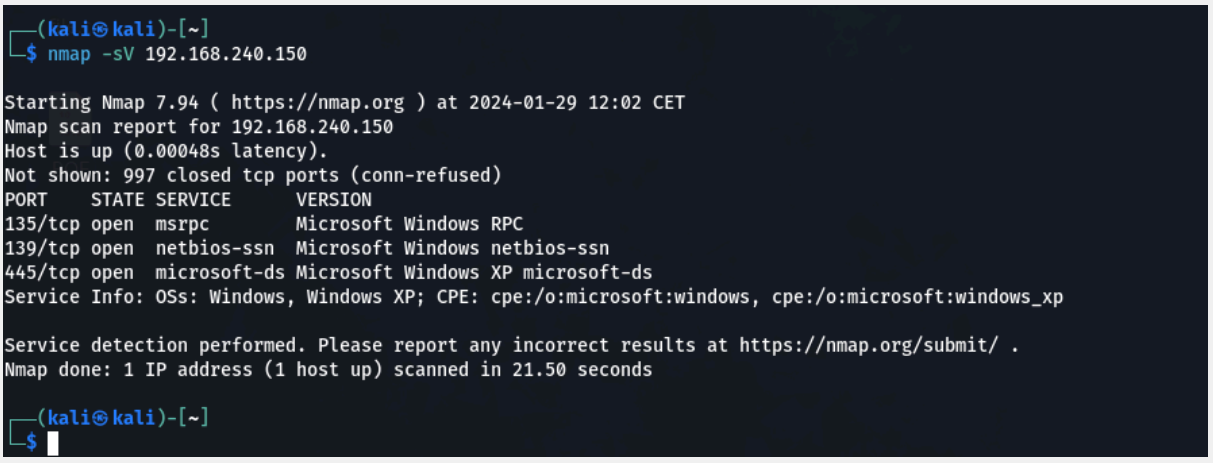

Figura 4

Come da Figura 4, notiamo diverse porte aperte e vulnerabilità.

Torniamo sulla nostra macchina Windows Xp, come da Figura 5 andremo a configurare il Firewall sullo stato “Attivo”

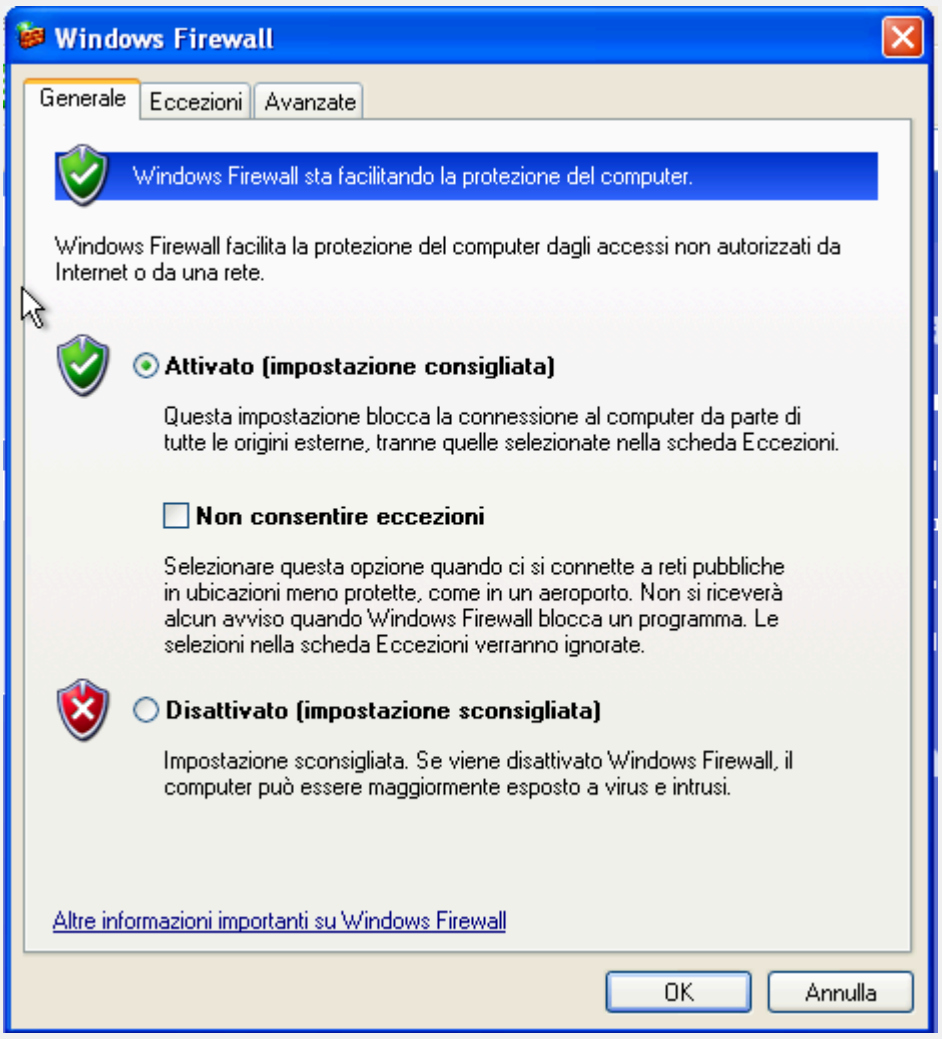

Figura 5

Successivamente all’attivazione del Firewall su Windows Xp notiamo come già il ping da Kali a Windows Xp non sia più facilmente avviabile.
Abbiamo mandato svariati pacchetti col risultato che nessuno di essi è stato ricevuto, come da Figura 6

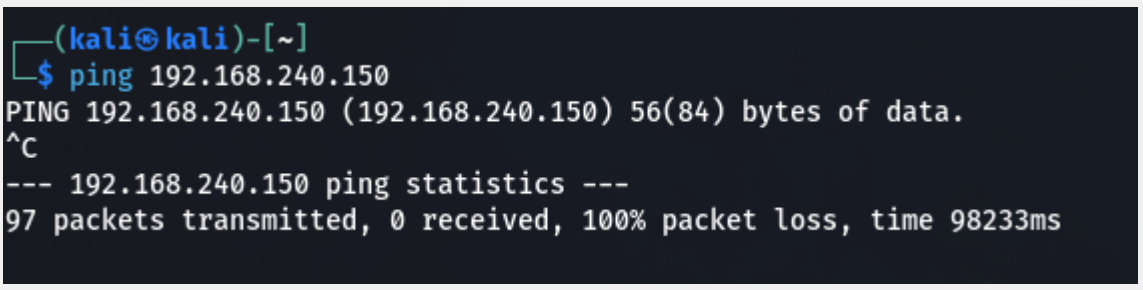

Figura 6

Come da Figura 7 andremo a inserire il nostro codice NMAP.

Questa volta non sono state individuate porte aperte su servizi attivi e vulnerabili:

Figura 7

Conclusioni:

La situazione iniziale implicava problemi di sicurezza in quanto nessun Firewall era presente dunque ogni connessione era permessa senza alcuna regola.
Una volta attivato il Firewall le connessioni sospette vengono bloccate, raggiungere i servizi vulnerabili è ora molto più difficile.
Il firewall è una protezione importante e necessaria alla fine della tutela della sicurezza sul nostro dispositivo