

REPORT



RAFAEL MANGO

requisiti

- *configurare l'indirizzo di windows xp come in seguito*
192.168.240.150
- *configurare l'indirizzo di Kali linux come in seguito*
192.168.240.100



Configurazione kali

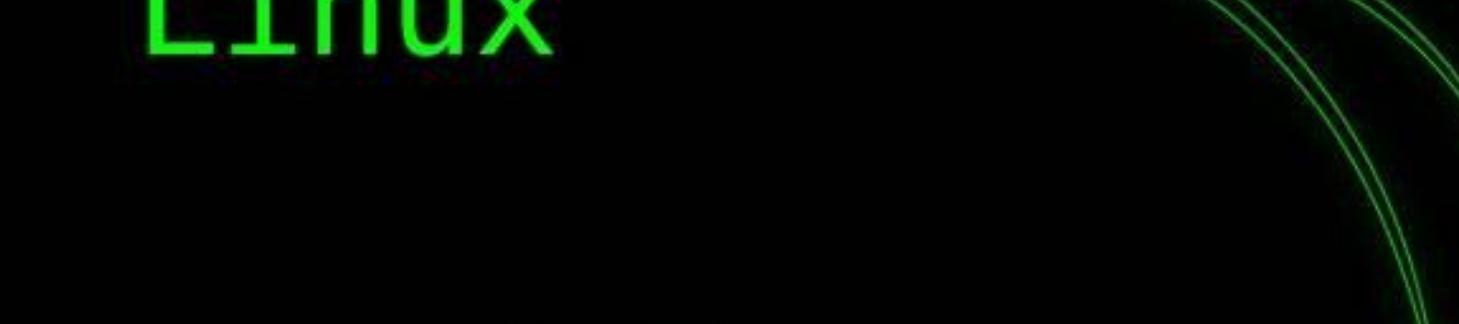
Per cambiare l'indirizzo IP di Kali, apriamo il terminale e utilizziamo il comando sudo per ottenere i privilegi necessari, quindi apriamo il file di configurazione /etc/network/interfaces utilizzando l'editor di testo nano. Una volta nel file, modificando l'indirizzo IP e le relative impostazioni di rete, salviamo le modifiche e chiudiamo l'editor. Successivamente, eseguiamo un riavvio della macchina per applicare le modifiche. Dopo il riavvio, possiamo verificare che le modifiche siano state effettuate correttamente utilizzando il comando ifconfig per visualizzare le nuove impostazioni di rete



Kali



Linux

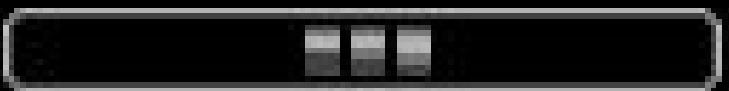


Helix

configurazione windows xp

Per cambiare l'indirizzo IP, avviamo selezionando il pulsante "Start" nella parte inferiore sinistra dello schermo e poi navighiamo in "Risorse del computer" > "Risorse di rete" > "Visualizza connessioni di rete". Qui, selezioniamo la connessione LAN e clicchiamo su "Cambia impostazioni connessione". Successivamente, andiamo su "Protocollo Internet TCP/IP", selezioniamo "Proprietà" e modifichiamo l'indirizzo IP come desiderato.

Dopo aver apportato le modifiche, riavviamo la macchina per assicurarci che siano state applicate correttamente. Per verificare che le modifiche siano state salvate e abbiano avuto effetto, apriamo il terminale e utilizziamo il comando ipconfig per visualizzare le nuove impostazioni di rete.



collegamento



andiamo a fare il ping dal terminale con il comando ping macchina terget che in questo caso e windows xp con indirizzo 192.168.240.150



andiamo a fare il ping con prompt comand il terminale di windows xp che troviamo in accessori aperto il terminale lanciamo il comando ping con l'indirizzo di kali 192.168.240.100



firewall

Una volta verificato che le due macchine comunicano andiamo accertiamoci che il Firewall di Windows sia disattivato e lanciamo la scansione verso il nostro target con lo switch –sV. La scansione ci riporta 3 servizi in ascolto rispettivamente sulle porte TCP 135,139,445

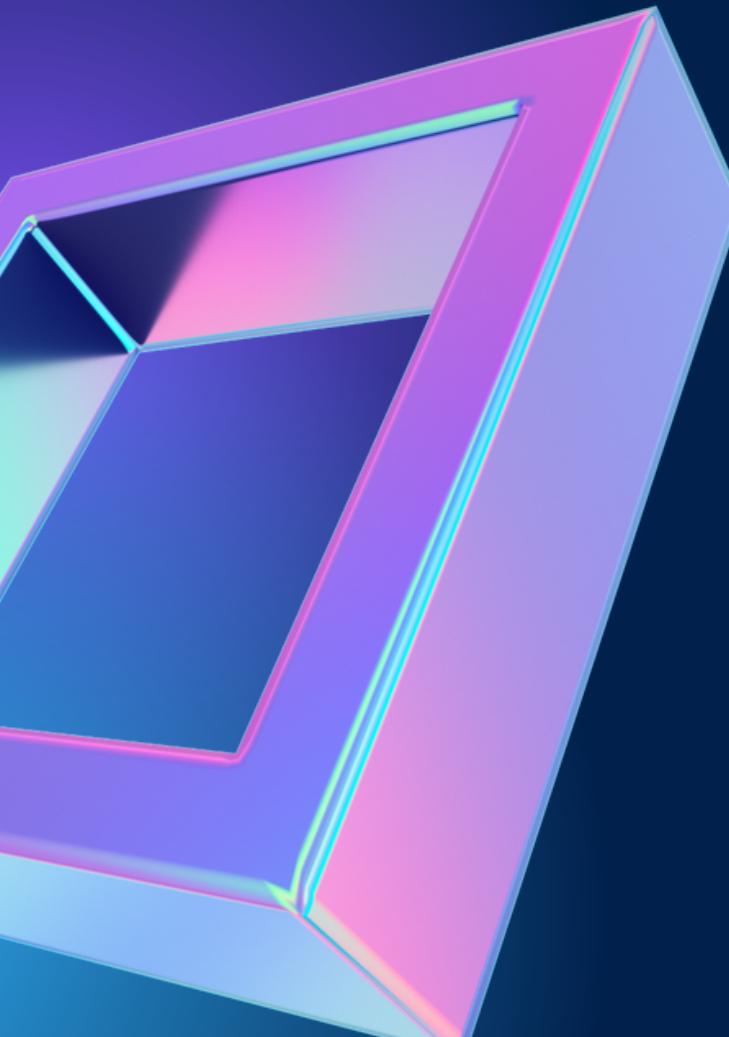
Attiviamo il Firewall di Windows XP e procediamo nuovamente alla scansione.

Dopo aver eseguito la scansione, abbiamo ricevuto un risultato che indica che la macchina potrebbe non essere accesa, oppure se è accesa, sta impedendo l'individuazione dell'host da parte di nmap. Di conseguenza, ci viene consigliato di utilizzare il parametro –Pn. Questa indicazione suggerisce che il firewall potrebbe bloccare il traffico in ingresso con il protocollo ICMP (il ping). Per superare questo problema, decidiamo di utilizzare lo switch –Pn per evitare di inviare il ping e procedere direttamente con la scansione dei servizi.

Con l'utilizzo dello switch –Pn, la scansione salta il ping e procede direttamente alla scoperta dei servizi. In questa occasione, tutte le porte sembrano essere filtrate, il che significa che non hanno risposto alle richieste dello scanner. È evidente che il Firewall sta impedendo l'accesso alle porte. Quando una porta risulta filtrata, significa che lo scanner non riceve alcuna risposta – in generale, non è possibile determinare con certezza se una porta filtrata sia aperta o chiusa

Conclusioni

L'attivazione del Firewall su Windows XP sta effettivamente impedendo la scansione dei servizi attivi sulla macchina da parte di soggetti esterni. È noto che questi servizi presentano vulnerabilità, poiché sono stati sfruttati durante i test effettuati con Metasploit nell'Unità 2. Possiamo quindi concludere che il Firewall, in modo preventivo, sta riducendo il rischio di attacchi provenienti dall'esterno, bloccando l'accesso esterno ai servizi che utilizzano le porte TCP 135, 139 e 445.



Thank You