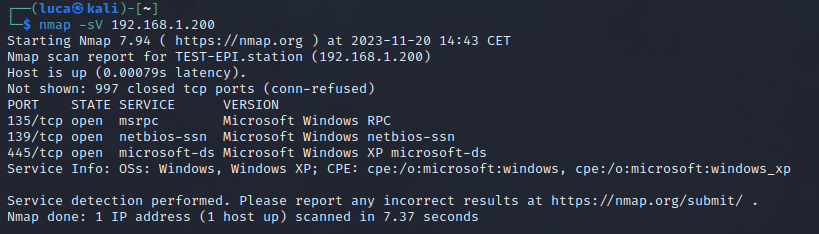
Verifica e considerazioni sulla scansione da kali a WinXP con e senza Firewall

Oggi andremo a vedere come e perché l’attivazione del Firewall su WindowsXP influisca sulla scansione tramite il tool di Nmap con Kali.

* Firewall disabilitato:

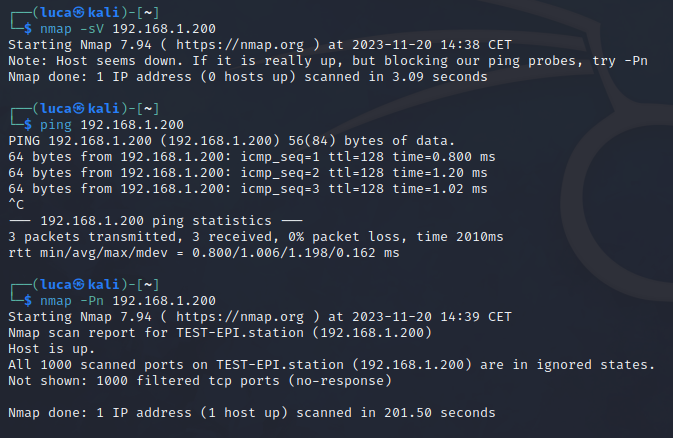


La mancanza di un firewall sulla macchina Windows XP semplifica la scansione e la comunicazione con i servizi aperti. Senza un firewall che blocchi le porte, Nmap è in grado di raggiungere e analizzare tutte le porte aperte senza ostacoli. Il sistema operativo e le versioni che presenta nei servizi aperti rendendolo vulnerabile.

Un esempio dello scambio di pacchetti che avverrà sarà il seguente:

Nmap invierà un pacchetto TCP SYN alla porta di destinazione. Questo pacchetto è utilizzato per stabilire una connessione iniziale se la porta è aperta la macchina di destinazione risponderà con un pacchetto TCP SYN/ACK, indicando che è pronta ad accettare la connessione quindi Nmap invierà un pacchetto TCP RST per interrompere la connessione senza completarla. Questo è noto come "scansione a tre vie".

* Firewall abilitato:



Il firewall di Windows XP, se configurato correttamente, filtra il traffico di rete in arrivo e in uscita, bloccando le connessioni non autorizzate limitando l'accesso solo a chi ne ha il diritto. Contribuisce a creare una barriera difensiva che migliora la confidenzialità, l'integrità e la disponibilità dei tuoi dati.

Ora, parlando di firewall attivo e non attivo, possiamo considerare come questi concetti si applicano in tema CIA (Confidentiality, Integrity, Availability)

Senza Firewall (Non Attivo):

1. Confidenzialità:

Rischio maggiore di accesso non autorizzato. Le porte possono essere aperte, rendendo il sistema più esposto a intrusioni. Il rischio di accessi non autorizzati è maggiore, poiché non esiste un meccanismo per verificare l'identità.

2. Integrità:

Maggior rischio di manipolazione dei dati da parte di terzi, poiché non ci sono restrizioni sul traffico in ingresso. Non c'è registrazione o tracciamento delle attività di rete.

3. Disponibilità:

Il sistema potrebbe essere più vulnerabile ad attacchi che compromettono la disponibilità, poiché non ci sono misure per filtrare o limitare il traffico.

Con Firewall (Attivo):

1. Confidenzialità:

Riduzione del rischio di accesso non autorizzato poiché il firewall può limitare l'accesso a determinate porte e servizi, può essere configurato per richiedere l'autenticazione prima di consentire l'accesso.

2. Integrità:

Minore rischio di manipolazione dei dati in quanto il firewall può bloccare o filtrare traffico sospetto, può generare log dettagliati delle attività di rete e avere maggiori possibilità di individuare e rispondere rapidamente a comportamenti anomali o attività sospette.

3. Disponibilità:

Migliorata poiché il firewall può mitigare attacchi che mirano a sopraffare il sistema con traffico non necessario come DOS o DDOS.