Immagine che contiene testo, schermata, Carattere, documento

Descrizione generata automaticamente

Immagine che contiene testo, Carattere, schermata, ricevuta

Descrizione generata automaticamente

Immagine che contiene testo, schermata, Carattere

Descrizione generata automaticamente

Immagine che contiene testo, schermata, Carattere

Descrizione generata automaticamente

Immagine che contiene testo, schermata, Carattere

Descrizione generata automaticamente

Immagine che contiene testo, schermata, Carattere, logo

Descrizione generata automaticamente

Immagine che contiene testo, schermata, Carattere

Descrizione generata automaticamente

La differenza nei risultati delle scansioni Nmap tra una configurazione senza firewall e una con firewall attivato può essere attribuita alle azioni di filtraggio del firewall stesso. Ecco una breve sintesi del motivo per cui ciò avviene e le cause principali:

\*\*Senza Firewall:\*\*

- In assenza di un firewall attivo, Nmap può esaminare apertamente le porte della macchina target e identificare i servizi in esecuzione su di esse.

- Nmap riceve risposte chiare (aperte, chiuse o non risposte) dalla macchina target, consentendo una scansione dettagliata delle porte.

\*\*Con Firewall Attivato:\*\*

- Quando il firewall è attivato, può filtrare o bloccare il traffico in arrivo su determinate porte.

- Il firewall può scegliere di "mettere in attesa" o ignorare (Dropping) i pacchetti di scansione senza fornire una risposta chiara, rendendo difficile per Nmap determinare lo stato effettivo delle porte.

- Il filtraggio silenzioso è un'opzione comune per limitare l'informazione fornita agli eventuali attaccanti sulla configurazione della rete.

\*\*Cause Principali:\*\*

- \*\*Politiche di Sicurezza:\*\* Il firewall è configurato per implementare politiche di sicurezza che limitano la visibilità della rete e riducono le informazioni fornite durante una scansione.

- \*\*Filtraggio Silenzioso:\*\* Il firewall può optare per il filtraggio silenzioso, dove ignora o ritarda le risposte senza notificare esplicitamente del blocco. Ciò è fatto per ostacolare gli sforzi degli attaccanti nell'ottenere dettagli sulla configurazione della rete.

In sintesi, l'attivazione del firewall introduce un livello di opacità nell'analisi delle porte e dei servizi sulla macchina target, complicando la comprensione del suo stato effettivo durante una scansione Nmap. Questo è un aspetto comune nelle strategie di sicurezza per limitare le informazioni disponibili agli attaccanti.