

Report – Port Scanning e analisi dei servizi di rete

Questo programma viene utilizzato per effettuare una scansione delle porte TCP su un host specifico, con l'obiettivo di individuare quali servizi risultano accessibili dalla rete.

La scansione delle porte rappresenta uno dei primi passi nell'analisi della superficie di attacco di un sistema, poiché consente di capire quali punti di ingresso sono esposti.

All'avvio viene richiesto l'indirizzo IP del sistema da analizzare e un intervallo di porte. Per ogni porta compresa nel range indicato viene tentata una connessione TCP, utilizzando un timeout breve per mantenere la scansione rapida e controllata.

In base all'esito della connessione è possibile stabilire se la porta risulta aperta o chiusa.

Quando una porta risulta aperta, il programma verifica se è associata a un servizio noto per essere particolarmente sensibile o frequentemente bersaglio di attacchi.

In questi casi viene fornita un'indicazione chiara del servizio tipico e del potenziale rischio, permettendo di identificare rapidamente situazioni che meritano maggiore attenzione.

Durante l'esecuzione, i risultati vengono mostrati direttamente a console, con un'evidenziazione visiva delle porte considerate più critiche.

Allo stesso tempo, tutte le informazioni vengono salvate in un file di testo che riporta il target analizzato, il range di porte, l'orario di inizio e di fine della scansione, oltre all'esito per ciascuna porta.

Nel complesso, questo strumento permette di ottenere una visione chiara e immediata dell'esposizione dei servizi di rete di un sistema. La semplicità di utilizzo e la struttura ordinata dell'output lo rendono particolarmente adatto a contesti di analisi interna, verifica delle configurazioni e attività preliminari di sicurezza.