**Port Scanning: ragioni, rischi e consigli per la sicurezza**

**Perché il Port Scanning?**

La scansione delle porte è un processo importante per proteggere le reti aziendali. Implica la scansione delle porte di un server o di un dispositivo di rete per determinare quali porte sono aperte. Questo processo ci consente di avere un'idea chiara di dove è possibile accedere ai nostri sistemi, identificare eventuali vulnerabilità e adottare le misure di sicurezza necessarie per proteggerli.

**Cosa serve sapere di avere delle porte aperte?**

Sapere quali porte sono aperte aiuta a contrastare possibili attacchi dall’esterno e dall’interno. Questi attaccanti possono utilizzarle le porte aperte come punti di ingresso. Ecco come possono essere utilizzate:

Ricognizione: gli aggressori eseguono la scansione delle porte per identificare i servizi in esecuzione e le versioni del software in esecuzione per identificare le vulnerabilità note.

Sfruttamento delle vulnerabilità: una volta identificate le porte aperte, gli aggressori possono sfruttare vulnerabilità specifiche nei servizi in esecuzione su tali porte. Ad esempio, un server Web sulla porta MYSQUL (3306) potrebbe presentare vulnerabilità che possono essere sfruttate per ottenere accesso non autorizzato.

Backdoor: le porte aperte possono essere utilizzate per stabilire un accesso coerente al sistema compromesso. Cioè, si crea un modo per aggirare le politiche di autenticazione e ottenere l'accesso a un sistema. Gli aggressori installano backdoor sui sistemi compromessi per consentire l'accesso continuo anche dopo che le vulnerabilità originali sono state risolte.

**Cosa serve chiudere le porte? E quali?**

La chiusura delle porte si basa su servizi essenziali per l'operatività dell'azienda. In generale è consigliabile:

Chiudere le porte non necessarie: qualsiasi porta aperta rappresenta un potenziale pericolo. Se un servizio non è affatto necessario, è buona norma disabilitarlo e chiudere la porta associata.

Filtrare le porte sensibili: per i servizi critici che devono rimanere aperti, è possibile utilizzare le regole del firewall per limitare l'accesso solo agli indirizzi IP attendibili.

Monitorare le porte aperte: mantenere un elenco aggiornato delle porte aperte e monitorare eventuali modifiche può aiutare a identificare attività sospette

**Perché abbiamo utilizzato TCP invece di UDP**

Abbiamo scelto di concentrarci sulla scansione delle porte TCP per diversi motivi:

Affidabilità: TCP (Transmission Control Protocol) è uno standard di connessione e garantisce l'affidabilità dei dati trasmessi. Ciò significa che possiamo ottenere una risposta chiara e deterministica sul fatto che un servizio sia in ascolto su una porta.

Riduzione dei falsi positivi: le scansioni TCP tendono ad essere più accurate delle scansioni UDP, riducendo il numero di falsi positivi. Le porte UDP aperte potrebbero non rispondere affatto, rendendo difficile sapere con certezza se un servizio è in esecuzione.

Funzionalità estese: molti servizi fondamentali per le applicazioni aziendali, come HTTP, HTTPS, FTP e SSH, utilizzano il protocollo TCP. Pertanto, una scansione TCP fornisce un quadro chiaro dei principali servizi in esecuzione sulla rete.

**Considerazioni finali**

La scansione delle porte è fondamentale per mantenere la sicurezza della rete aziendale. L’identificazione delle porte aperte ci consente di valutare i rischi associati e di mitigarli implementando adeguate misure di sicurezza. Mantenere un ambiente di sicurezza solido implica non solo chiudere le porte non necessarie, ma anche monitorare continuamente l’attività di rete e aggiornare regolarmente il software per correggere eventuali vulnerabilità.

**Conclusione**

L'obiettivo finale è proteggere l’azienda da potenziali minacce utilizzando le informazioni ottenute dalla scansione delle porte per rafforzare le difese della rete. Un approccio alla sicurezza, combinato con pratiche di gestione delle vulnerabilità, ci aiuta a mantenere un ambiente IT sicuro e solido.



