Resoconto TEST Scansione Porte

A seguito di una scansione effettuata sulle porte del nostro server, è emerso che le porte numero 21 e 22 risultano aperte. Queste porte sono associate a servizi di rete comunemente utilizzati nei sistemi informatici che verranno analizzati e spiegati di seguito, con particolare dettaglio sui potenziali rischi di sicurezza a cui il server è esposto, e le eventuali misure di mitigazione da adottare.

- -Servizi associati alle porte numero 21 e 22- -

1. La porta 21 è riservata al servizio FTP (ovvero File Transfer Protocol), un protocollo di trasferimento utilizzato per la trasmissione di file tra dispositivi su una rete. FTP è un protocollo relativamente semplice e non cifrato, il che significa che le informazioni, inclusi username e password, viaggiano in chiaro.

   La presenza di questa porta aperta potrebbe consentire l'accesso non autorizzato ai file del server se il servizio non è configurato correttamente o se non vengono applicate misure di sicurezza adeguate. Inoltre, data la mancanza di cifratura, un attaccante potrebbe intercettare i dati trasmessi.

2. La porta 22 è utilizzata dal servizio SSH (ovvero Secure Shell), un protocollo sicuro per l'accesso remoto a macchine tramite un canale cifrato. SSH permette agli amministratori di sistema di gestire e controllare da remoto il server, garantendo un elevato livello di sicurezza grazie alla cifratura.

   Sebbene SSH sia generalmente considerato sicuro, la porta 22 rappresenta comunque un punto di accesso critico. Se la configurazione non è gestita in modo appropriato (ad esempio, tramite autenticazione a due fattori, chiavi SSH anziché password deboli o comuni), il server potrebbe essere vulnerabile a tentativi di attacco di brute force, tentativi di login non autorizzati, o vulnerabilità del software SSH.

Andiamo adesso ad analizzare un po' piu' nel dettaglio a quali Rischi di Attacco e' esposto il server alla luce di quanto appena preso in analisi.

Di seguito vengono riportati i rischi a cui espone l' apertura della porta numero 21:

- **Intercettazione dei Dati**: Dato che FTP non utilizza la crittografia, un attaccante potrebbe intercettare traffico non cifrato, acquisendo credenziali o dati sensibili.
- **Attacchi Man-in-the-Middle (MitM)**: Un malintenzionato potrebbe inserire se stesso tra la connessione FTP del client e del server per alterare o acquisire file.
- **Accesso non autorizzato**: Se le credenziali di autenticazione non sono sufficientemente robuste o se il servizio FTP non è ben configurato, un attaccante potrebbe ottenere accesso ai file del server.

Seguono adesso i rischi comportati dall' apertura della porta numero 22:

- **Attacchi di Brute Force**: Un attaccante potrebbe tentare di indovinare le credenziali SSH eseguendo attacchi di forza bruta, soprattutto se le password sono deboli o non sufficientemente robuste.
- **Esposizione a Vulnerabilità Note**: Se il software SSH o la configurazione non sono aggiornati, il server potrebbe essere vulnerabile a exploit che prendono di mira versioni obsolete o mal configurate.
- **Escalation dei Privilegi**: Nel caso un attaccante riesca a ottenere l'accesso SSH, potrebbe tentare di aumentare i propri privilegi e prendere il controllo completo del server.

In quanto parte integrante e fondamentale del nostro ruolo, sebbene la risoluzione dei problemi sia un punto cruciale riteniamo che la vera chiave nella protezione dei sistemi e dei clienti risieda piu' nella prevenzione delle minacce. Per questo motivo, procederemo a suggerire alcune misure che consentiranno all'utente di rendere piu' difficile un successo in caso di attacco da parte di terzi.

Porta numero 21 - FTP (File Transfer Protocol)

1. **Disabilitare FTP a favore di FTPS o SFTP**: FTPS (FTP Secure) o SFTP (SSH File Transfer Protocol) forniscono cifratura dei dati e maggiore sicurezza rispetto a FTP. Si raccomanda vivamente di migrare verso questi protocolli
2. **Limitare l'accesso**: Configurare firewall o controlli di accesso per limitare l'accesso alla porta 21 solo a indirizzi IP autorizzati.
3. **Monitoraggio e Logging**: Abilitare il monitoraggio e la registrazione degli accessi FTP per identificare tentativi di accesso sospetti e lasciare che eventuali tentativi fraudolenti vengano analizzati da un team di specialisti (Rimando alla sezione "Cybersecurity Team" di TigerBytes®)

Porta numero 22 - SSH (Secure Shell)

1. **Autenticazione a chiave pubblica**: Implementare l'uso di chiavi SSH anziché password, poiché è molto più sicuro contro gli attacchi di brute force.
2. **Autenticazione a due fattori (2FA)**: Attivare l'autenticazione a due fattori per SSH al fine di aggiungere un ulteriore livello di sicurezza.
3. **Intrusion Detection System (IDS)**: Implementare un sistema di rilevamento delle intrusioni per monitorare i tentativi di accesso non autorizzato.

Conclusioni

Le porte 21 (FTP) e 22 (SSH) aperte rappresentano un potenziale rischio per la sicurezza del server. Tuttavia, con un'adeguata configurazione dei servizi, politiche di accesso stringenti e l'adozione di protocolli sicuri come SFTP e autenticazione a due fattori, è possibile prevenire e ridurre efficacemente la maggior parte dei rischi associati a queste porte.

Raccomandiamo di intraprendere immediatamente le azioni correttive sopra descritte per migliorare la sicurezza del server e proteggere l'infrastruttura da potenziali attacchi, affidandovi ancora una volta al miglior team in circolazione.

Jacopo Cianfrini

Security Specialist

TigerBytes S.r.l.

Via delle Tigri, 15 - 00100 Roma, Italia

Telefono: +39 06 12345678

Fax: +39 06 87654321

Email: j.cianfrini@tigerbytes.it

Sito web: www.tigerbytes.it