Day 15 - Remote Desktop Protocol

Remote Desktop Protocol

RDP (Remote Desktop Protocol) è un protocollo sviluppato da Microsoft che permette di connettersi e controllare da remoto un altro computer tramite un'interfaccia grafica. Viene comunemente utilizzato per amministrare server e fornire accesso remoto a desktop e applicazioni.
Il protocollo utilizza la porta TCP 3389.

Perché si usa RDP:
•Amministrazione remota di server e PC.
•Accesso a desktop e applicazioni da qualsiasi posizione.
•Supporto e manutenzione a distanza.
Rischi principali:
•Vulnerabilità agli attacchi brute force.
•Possibili exploit di vulnerabilità del protocollo.
•Rischio di accessi non autorizzati se non configurato correttamente.

Come trovare server con servizio RDP esposto?

Shodan

Cosa è: Shodan è un motore di ricerca per dispositivi connessi a Internet che indicizza le informazioni sui servizi esposti.
Ricerca di RDP: Inserendo port:3389 nella barra di ricerca, puoi trovare server con il servizio RDP attivo. I risultati mostrano indirizzi IP, posizioni geografiche e dettagli del sistema operativo. È possibile visualizzare screenshot delle interfacce di accesso RDP, fornendo un'idea di come è configurato il server.

Censys

Cosa è: Censys è una piattaforma di ricerca che analizza e raccoglie dati sui dispositivi e servizi esposti su Internet.
Ricerca di RDP: Utilizzando port:3389, puoi ottenere una lista di indirizzi IP con RDP esposto, assieme a dettagli come versioni del software e certificati SSL.

Come proteggersi?

Disabilita RDP
Disabilitare il servizio RDP sui server quando non è necessario. Dopo aver disabilitato RDP, puoi utilizzare Shodan e Censys per verificare che il servizio non sia più esposto e accessibile.
Utilizza l'Autenticazione Multi-Fattore (MFA)
Implementare l'autenticazione multi-fattore per aggiungere un ulteriore strato di sicurezza. Questo richiede un secondo fattore di autenticazione oltre alla password, riducendo significativamente il rischio di accessi non autorizzati.
Restringi l'Accesso con Regole del Firewall
Configurare il firewall per limitare l'accesso al servizio RDP solo a indirizzi IP specifici. Mettere i server dietro una VPN crea un tunnel sicuro per l'accesso remoto, garantendo che solo gli utenti autorizzati possano connettersi al server tramite la VPN, riducendo l'esposizione diretta a Internet.

Come proteggersi?

Utilizza Password Sicure
Adottare password complesse di almeno 15 caratteri, che includano lettere maiuscole, minuscole, numeri e caratteri speciali. Gestire l'accesso privilegiato con strumenti di gestione delle password per garantire che le credenziali siano sicure e aggiornate.
Non Utilizzare Account Predefiniti
Evitare di utilizzare account predefiniti, come "Administrator". Prestare attenzione a possibili attacchi di credential dumping e credential stuffing, dove le credenziali rubate vengono utilizzate per accedere a più sistemi. Cambiare i nomi degli account e utilizzare pratiche di gestione delle credenziali sicure.