M4_W15D1

Nella lezione teorica abbiamo visto la **Null Session**, vulnerabilità che colpisce Windows

Traccia

- Spiegare brevemente cosa vuol dire Null Session
- Elencare i sistemi che sono vulnerabili a Null Session
- Questi sistemi operativi esistono ancora oppure sono estinti da anni e anni?
- Elencare le modalità per mitigare o risolvere questa vulnerabilità
- Commentare queste azioni di mitigazione, spiegando l'efficacia e l'effort per l'utente/azienda.

Null Session: Connessione con un sistema Windows che non richiede alcuna credenziale di autenticazione, fornendo un accesso a determinate risorse condivise sul sistema.
Una Null Session permette ad un utente di connettersi ad un sistema e ai suoi endpoint per riuscire a recuperare informazioni quali: File Condivisi, Stampanti, Server, ecc.
Successivamente accediamo al file condiviso tramite un'autenticazione anonima (" ").
E' possibile ottenere accesso amministrativo o visualizzare in maniera limitata i file condivisi.

I sistemi Windows che supportano la Null Session includono le versioni precedenti di Windows come Windows NT, 2000, Server-2003, XP Professional.
Alcuni sistemi Legacy potrebbero ancora esistere in ambienti aziendali o in contesti specifici dove non è stato effettuato un aggiornamento del sistema operativo.

Elencare le modalità per mitigare o risolvere questa vulnerabilità:
- **Aggiornare il sistema operativo.**
- **Configurare autorizzazioni di accesso.**
- **Monitorare e registrare l'attività di rete.**
- **Formazione degli utenti.**
- **Utilizzo VPN.**
- **Crittografare i dati sensibili.**

Aggiornare il sistema operativo: Assicurarsi di utilizzare versioni supportate e aggiornate di Windows, che includono patch di sicurezza e correzioni di vulnerabilità note.

Configurazione Autorizzazioni di accesso: Principio del privilegio minimo (assegna agli utenti solo i privilegi necessari); Utilizzo Access Control Lista (ACL); Utilizzo Network Access Control (NAC).

Monitorare e registrare l'attività di rete: utilizzo Firewall, sistemi IDS/IPS

Formazione degli utenti: fornire formazione agli utenti sulla sicurezza informatica.
Utilizzo VPN: Crittografia dei dati per impedire lo sniffing dei dati in transito; Anonimato e mascheramento dell'indirizzo IP per rendere più difficile individuare e sfruttare potenziali vulnerabilità Null Session.

Crittografare i dati sensibili: Utilizzo protocolli come SSL/TLS, SSH, FTPS, HTTPS.