Esercitazione WEEK 15 D1

Null session

Ettore Farris - 05/02/2024

Descrizione sintetica

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

- **Spiegare brevemente cosa vuol dire Null Session**

La null session è un tipo di vulnerabilità di Windows che consente di accedere a informazioni sensibili su sistemi windows (files, password ecc). Si verifica quando un client si connette a un server con sessione anonima

- **Elencare i sistemi che sono vulnerabili a Null Session**

Windows NT, Windows 2000, Windows XP e Windows Server 2003.

- **Questi sistemi operativi esistono ancora oppure sono estinti da anni e anni?**

Le vulnerabilità per i nuovi sistemi sono state eliminate. Sono presenti nei sistemi legacy. Probabilità ristretta di trovarla.

- **Elencare le modalità per mitigare o risolvere questa vulnerabilità. Commentare queste azioni di mitigazione, spiegando l'efficacia e l'effort per l'utente/azienda.**

Esistono diversi modi per risolvere il problema:

- Disabilitare files e stampanti: metodo efficace ma sconveniente se, ad esempio in una realtà aziendale, si usa la condivisione;
- Aggiornare Windows alla versione più recente: installare una patch rilasciata da Windows è efficace. Tuttavia potrebbe costringere l'azienda a cambiare l'hardware in funzione delle prestazioni;
- Disabilitare NETBios;
- Impostare delle regole firewall: buona pratica che deve essere implementata sempre
- Disattivare la sessione ospite: è un'ottima soluzione dato che la vulnerabilità fa leva sulle sessioni anonime;
- Usare software di sicurezza.