# Esercitazione W15D1 - Pratica 1

# Null session

Fabio Benevento - 13/02/2024

## 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.

## Implementazione

Una Null Session è una connessione di rete anonima a un sistema Windows che non richiede credenziali di accesso, sfruttando tipicamente quella che è una vulnerabilità del servizio di share di Windows. Si tratta di una vulnerabilità che affligge per lo più i sistemi legacy come ad esempio Windows NT, 2000, XP, e versioni precedenti. Al giorno d'oggi è quindi molto più difficile riscontrarla in quanto nelle versioni più moderne di Windows sono stati introdotte contromisure per ridurre sensibilmente la vulnerabilità alle Null Session

### Modalità per Mitigare o Risolvere la Vulnerabilità

1. **Aggiornare il Sistema Operativo**

Le versioni affette dalla vulnerabilità citate precedentemente sono molto vecchie e non più supportate da Microsoft. E' quindi altamente consigliabile ove possible passare a versioni più recenti di Windows poiché comporta non solo la correzione della vulnerabilità Null Session, ma anche l'accesso a funzionalità di sicurezza aggiuntive e correzioni di bug.

2. **Disabilitare Null Session**

Nel Registro di sistema di Windows, è possibile disabilitare Null Session per ridurre il rischio.
Di seguito sono elencati i passaggi da eseguire:

- Premere Win + R per aprire la finestra di dialogo "`Esegui`"
- Digitare regedit e premere Invio per aprire l'Editor del Registro di Sistema.
- Individuare la voce `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa`.
- Creare o modifica la Chiave del Registro:
    - Clic destro su uno spazio vuoto nella finestra destra dell'Editor del Registro.
    - Selezionare "Nuovo" e poi "`Valore DWORD (32 bit)`".
    - Assegnare un nome ad esempio `RestrictAnonymous`.
    - Imposta il valore su 1 alla voce di registro inserita per disabilitare le Null Session.
- Riavvia il sistema affinché le modifiche abbiano effetto.

3. **Configurare le Autorizzazioni**

Limitare l'accesso alle risorse solo ai file/cartelle necessari e  solo agli utenti autorizzati.