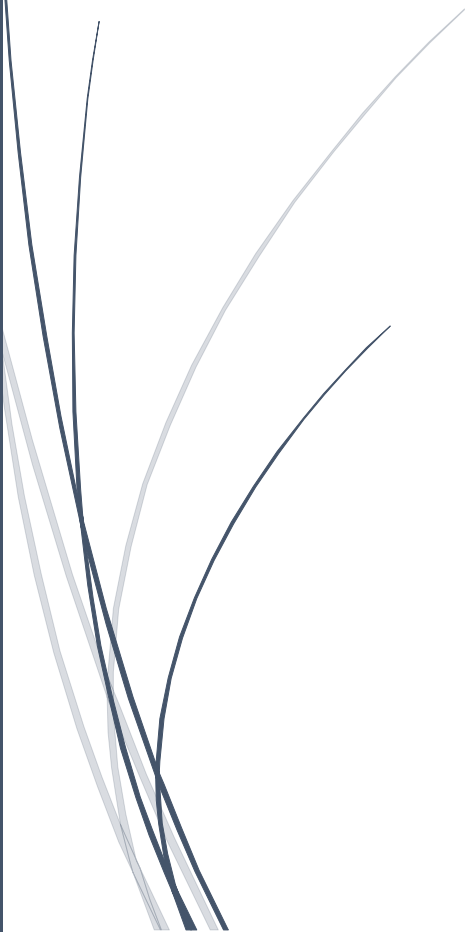


A dark blue vertical bar runs down the left side of the slide. A blue arrow points to the right from this bar, containing the date.

27/05/2024

# Vulnerability Assessment Null Session

Esercizio Modulo 4 - Week 15 – D1  
[Orazio Ciccozzi](#)

Several thin, curved lines in dark blue and light grey originate from the bottom left corner and sweep upwards and to the right, creating a sense of movement or a stylized graphic element.

Sommario

Introduzione ..... 2

Cosa vuol dire Null Session..... 2

Sistemi che sono vulnerabili a Null Session..... 3

Modalità per mitigare o risolvere questa vulnerabilità..... 3

## Introduzione

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

- 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.

## Cosa vuol dire Null Session

**la vulnerabilità "null session" di Windows permette a un utente malintenzionato di accedere a risorse di sistema condivise senza dover autenticarsi.**

Normalmente, quando si accede a una risorsa di rete condivisa su Windows, è necessario autenticarsi con un nome utente e una password. Tuttavia, in passato, era possibile sfruttare una falla nel sistema per accedere a queste risorse senza credenziali valide. Questa falla era chiamata "null session" perché l'utente malintenzionato non doveva fornire alcuna informazione di autenticazione, creando di fatto una sessione nulla.

**Le conseguenze dello sfruttamento di questa vulnerabilità potevano essere gravi:**

- **Ricognizione della rete:** un malintenzionato poteva utilizzare una sessione nulla per enumerare le risorse di rete disponibili, come cartelle condivise, stampanti e utenti.
- **Accesso non autorizzato:** in alcuni casi, era possibile accedere alle risorse di rete condivise anche senza diritti di accesso espliciti.
- **Aumento dei privilegi:** un malintenzionato poteva sfruttare la vulnerabilità null session per ottenere privilegi più elevati sul sistema.

Tuttavia, è importante notare che le sessioni nulle possono presentare problemi di sicurezza. Ad esempio, un hacker potrebbe sfruttare una sessione nulla per accedere in lettura/scrittura ai computer della rete. Questo potrebbe consentire all'hacker di inserire codice dannoso o altri materiali su computer senza password. Inoltre, l'hacker potrebbe tentare di decifrare le password degli utenti utilizzando l'elenco delle risorse e dei nomi utente generati durante una sessione nulla. Anche se la protezione tramite password è attiva, se l'hacker riesce a indovinare la password, potrebbe causare danni durante la sessione

## Sistemi che sono vulnerabili a Null Session

In passato, la vulnerabilità "null session" era presente in diverse versioni di sistemi Microsoft Windows. Tra le più colpite troviamo:

Windows NT 4.0

Windows 2000

Windows XP

Windows Server 2003

È importante sottolineare che Microsoft ha rilasciato patch per correggere la vulnerabilità null session in tutte queste versioni. È fondamentale installare queste patch per proteggere i sistemi Windows da questo tipo di attacco.

Anche se la vulnerabilità non è più un problema per i sistemi aggiornati, è comunque utile conoscerla per comprendere meglio i rischi associati alla sicurezza informatica e per implementare adeguate misure di protezione.

## Modalità per mitigare o risolvere questa vulnerabilità

Per mitigare questi rischi, gli amministratori di rete possono disabilitare le sessioni nulle. Ogni sistema operativo ha un processo leggermente diverso per farlo, ma gli utenti possono chiedere aiuto al personale IT per configurare i propri computer e affrontare questo potenziale exploit di sicurezza

Inoltre Microsoft ha rilasciato diverse patch per correggere la vulnerabilità null session. È importante installare queste patch per proteggere i sistemi Windows da questo tipo di attacco.

Oltre all'installazione delle patch, è possibile adottare altre misure per mitigare il rischio di attacchi basati su sessioni nulle:

Disabilitare le condivisioni di rete non necessarie.

Limitare l'accesso alle condivisioni di rete solo agli utenti e ai gruppi che ne hanno bisogno.

Utilizzare firewall e software antivirus per proteggere il sistema da intrusioni esterne.