

# NULL SESSION

## ATTACCHI ALLE RETI(2)

### 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?

---

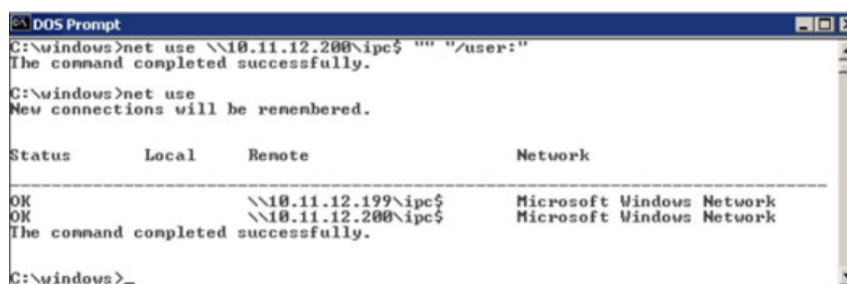
### COSA VUOL DIRE NULL SESSION

Una sessione di Windows può essere utilizzata per produrre una sessione nulla, utilizzando un nome e una password vuoti.

Una sessione nulla, come qualsiasi altro processo, ha un proprio difetto di sicurezza che è stato identificato come vulnerabile agli attacchi di alcuni criminali informatici spietati. L'utente malintenzionato può sfruttare la vulnerabilità legata alla sessione nulla per connettersi a una condivisione IPC (Inter-Process Communication) non protetta del sistema Windows anche a distanza o tramite Internet.

I ladri malintenzionati troveranno abbastanza semplice sfruttare un PC Windows non sicuro digitando codici specifici nella riga di comando di Windows. Secondo la ricerca, l'attaccante dovrà solo digitare "net use IP addressipc\$" e "/user:" al prompt dei comandi per ottenere l'accesso alla macchina.

esempio:



```
C:\windows>net use \\10.11.12.200\ipc$ "" /user:"
The command completed successfully.

C:\windows>net use
New connections will be remembered.

Status      Local      Remote      Network
-----
OK           \\10.11.12.199\ipc$  Microsoft Windows Network
OK           \\10.11.12.200\ipc$  Microsoft Windows Network
The command completed successfully.

C:\windows>
```

### ELENCARE I SISTEMI CHE SONO VULNERABILI A NULL SESSION

Questo tipo di attacco è più difficile da eseguire quando i clienti utilizzano versioni più recenti del sistema operativo però sistemi operativi come

- Windows 2.x
- Windows OS/2
- Windows 3.1x
- Windows NT

- Windows 95
- Windows 98
- Windows Me
- Windows XP
- Windows 2000

contengono difetti che li rendono più soggetti ad attacchi.

### **QUESTI SISTEMI OPERATIVI ESISTONO ANCORA OPPURE SONO ESTINTI?**

Questi sistemi operativi si possono oramai definire obsoleti dunque sono sempre meno usati ma non del tutto estinti in quanto la maggior parte degli utenti ha optato per sistemi operativi sempre più recenti. Il problema con le versioni di Windows vecchie e fuori produzione va oltre l'installazione di software più recente. Un altro problema infatti, è che Microsoft ha già tagliato il supporto per questi sistemi, un processo chiamato "fine del ciclo di vita".

- Windows XP ha raggiunto la fine del ciclo di vita nel 2014
- Windows Vista ha raggiunto la fine del ciclo di vita nel 2017
- Windows 7 nel 2020
- Anche Windows 8.1 e Windows 10 stanno raggiungendo questa fase rispettivamente nel 2023 e nel 2025

#### Tuttavia, cosa succede se il PC viene utilizzato in un ambiente aziendale?

Microsoft offre un po' di margine di manovra per gli utenti per l'aggiornamento in questi scenari specifici poiché sa che gli aggiornamenti in questo spazio sono considerevolmente più difficili. Anche questo, tuttavia, ha un limite.

- Nel caso di Windows 7, le edizioni speciali del sistema operativo stanno ancora ricevendo aggiornamenti.
- Le edizioni con contratto multilicenza di Windows 7 Professional ed Enterprise riceveranno gli aggiornamenti di sicurezza fino al 10 gennaio 2023.
- Windows Embedded Standard 7 riceverà aggiornamenti fino al 10 ottobre 2023
- Windows Embedded POSReady 7 riceverà aggiornamenti fino al 2024.

### **MODALITA' PER MITIGARE O RISOLVERE QUESTE VULNERABILITA'**

- Aggiornare a versioni più recenti di Windows
- Utilizzare firewall
- Limitare connessioni anonime