Account Manipulation

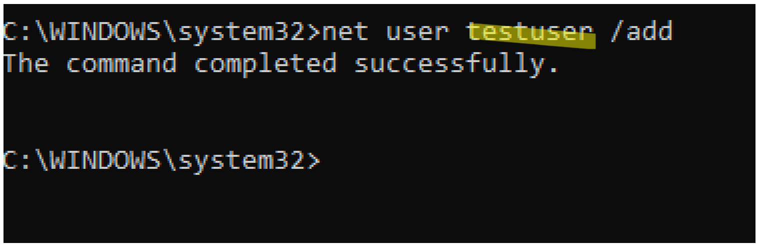
MITRE ATT&CK technique T1136.001: Create Account - Local Account

Technique: This technique shows how to create local accounts, which gives adversaries access to your system facilitating persistence and it can also lead to privilege escalation.

Environment: Windows 10 Home 22H2

Tools:

- Command Line (Run as administrator): net user (username) /add
- Command is used to add new users.

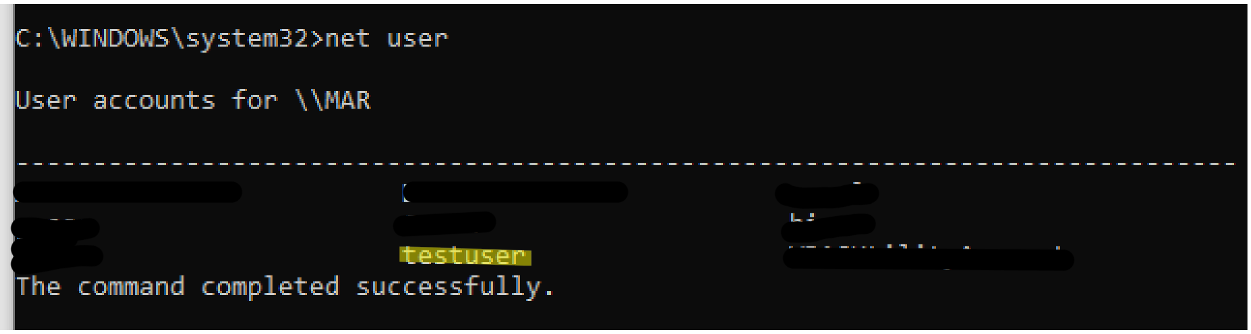


```
C:\WINDOWS\system32>net user testuser /add
The command completed successfully.


C:\WINDOWS\system32>
```

Verification:

Command: net user



```
C:\WINDOWS\system32>net user

User accounts for \\MAR

-------------------------------------------------------------------------------
[redacted]                    [redacted]                    [redacted]
[redacted]                    [redacted]                    [redacted]
[redacted]                    testuser                      [redacted]
The command completed successfully.
```

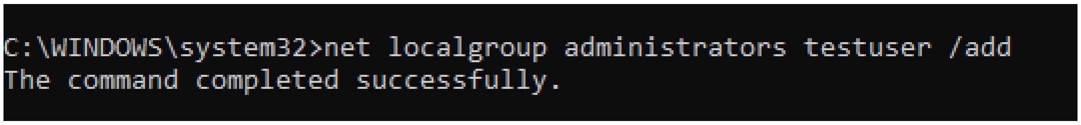
Conclusion:

Adding a new account is a highly usable technique for maintaining access in a system, especially when combined with a technique like privilege escalation. However, since it’s logged in and users have visibility on monitored systems, an anti-forensic technique would be to clear command line history and remove the entries from the log files such as /var/log/auth.log can help adversaries to cover their traces.

Bonus:

Tools:

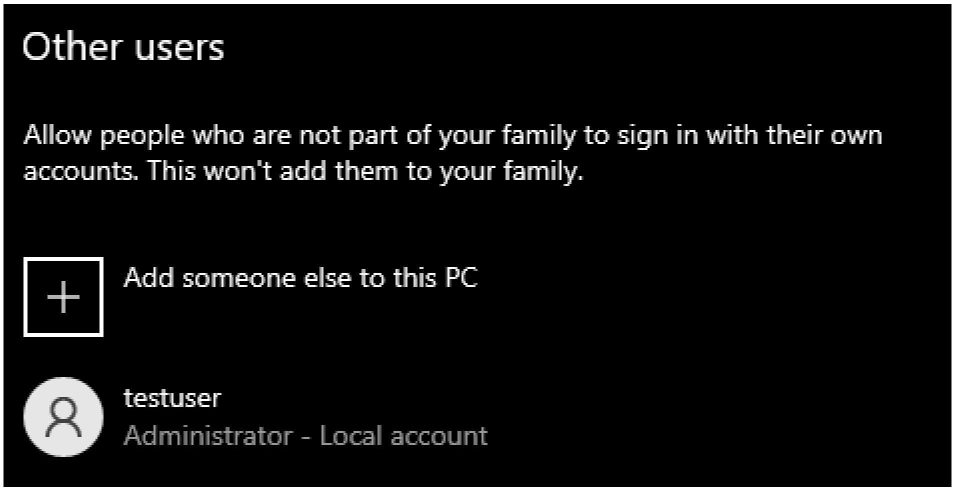
- Command Line (Run as administrator): net localgroup administrators (username) /add
- Command is used to add users to the administrator group.



```
C:\WINDOWS\system32>net localgroup administrators testuser /add
The command completed successfully.
```

Verification:

- Settings > Accounts> Family& other users



Other users

Allow people who are not part of your family to sign in with their own accounts. This won't add them to your family.

testuser
Administrator - Local account