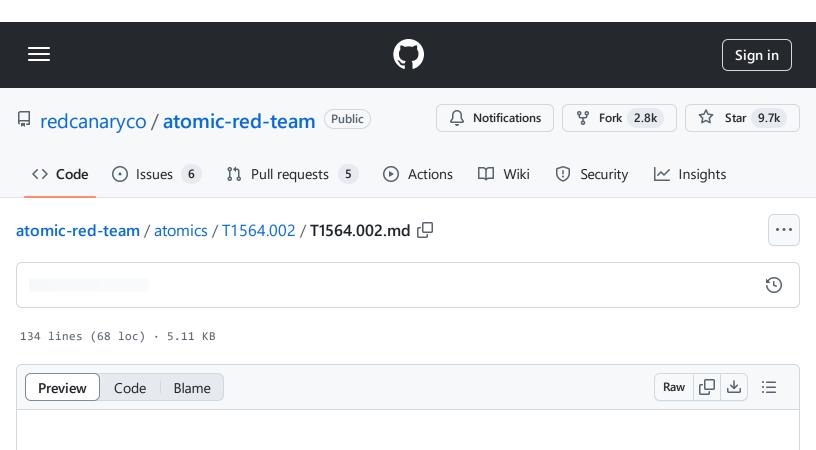
atomic-red-team/atomics/T1564.002/T1564.002.md at 40b77d63808dd4f4eafb83949805636735a1fd15 · redcanaryco/atomic-red-team · GitHub - 31/10/2024 20:16 https://github.com/redcanaryco/atomic-red-team/blob/40b77d63808dd4f4eafb83949805636735a1fd15/atomics/T1564.002/T1564.002.md



# T1564.002 - Hidden Users

# **Description from ATT&CK**

Administrators may use hidden users to hide the presence of user accounts they create or modify. Administrators may want to hide users when there are many user accounts on a given system or if they want to hide their administrative or other management accounts from other users. In macOS, adversaries can create or modify a user to be hidden through manipulating plist files, folder attributes, and user attributes. To prevent a user from being shown on the login screen and in System Preferences, adversaries can set the userID to be under 500 and set the key value Hide500Users to TRUE in the /Library/Preferences/com.apple.loginwindow plist file. (Citation: Cybereason OSX Pirrit) Every user has a userID associated with it. When the Hide500Users key value is set to TRUE, users with a userID under 500 do not appear on the login screen and in System Preferences. Using the command line, adversaries can use the dscl utility to create hidden user accounts by setting the IsHidden attribute to 1. Adversaries can also hide a user's home folder by changing the chflags to hidden.(Citation: Apple Support Hide a User Account)

Adversaries may similarly hide user accounts in Windows. Adversaries can set the HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\SpecialAccounts\UserList Registry key value to 0 for a specific user to prevent that user from being listed on the logon screen.(Citation: FireEye SMOKEDHAM June 2021)(Citation: US-CERT TA18-074A)

On Linux systems, adversaries may hide user accounts from the login screen, also referred to as the greeter. The method an adversary may use depends on which Display Manager the distribution is currently using. For example, on an Ubuntu system using the GNOME Display Manger (GDM), accounts may be hidden from the greeter using the gsettings command (ex: sudo -u gdm gsettings set org.gnome.login-screen disable-user-list true).(Citation: Hide GDM User Accounts) Display Managers are not anchored to specific distributions and may be changed by a user or adversary.

### **Atomic Tests**

- Atomic Test #1 Create Hidden User using UniqueID < 500</li>
- Atomic Test #2 Create Hidden User using IsHidden option
- Atomic Test #3 Create Hidden User in Registry

## Atomic Test #1 - Create Hidden User using UniqueID < 500

Add a hidden user on macOS using Unique ID < 500 (users with that ID are hidden by default)

Supported Platforms: macOS

**auto\_generated\_guid:** 4238a7f0-a980-4fff-98a2-dfc0a363d507

### Inputs:

Name	Description	Type	Default Value
user_name	username to add	String	APT

Attack Commands: Run with sh! Elevation Required (e.g. root or admin)

Q

#### **Cleanup Commands:**

Q

### Atomic Test #2 - Create Hidden User using IsHidden option

Add a hidden user on macOS using IsHidden optoin

Supported Platforms: macOS

auto\_generated\_guid: de87ed7b-52c3-43fd-9554-730f695e7f31

### Inputs:

Name	Description	Туре	Default Value
user_name	username to add	String	APT

Attack Commands: Run with sh! Elevation Required (e.g. root or admin)

Q

### Cleanup Commands:

Q

# Atomic Test #3 - Create Hidden User in Registry

atomic-red-team/atomics/T1564.002/T1564.002.md at 40b77d63808dd4f4eafb83949805636735a1fd15 · redcanaryco/atomic-red-team · GitHub - 31/10/2024 20:16 https://github.com/redcanaryco/atomic-red-team/blob/40b77d63808dd4f4eafb83949805636735a1fd15/atomics/T1564.002/T1564.002.md

Adversaries may similarly hide user accounts in Windows. Adversaries can set the HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\SpecialAccounts\UserList Registry key value to 0 for a specific user to prevent that user from being listed on the logon screen. Reference <a href="https://attack.mitre.org/techniques/T1564/002/">https://attack.mitre.org/techniques/T1564/002/</a> and <a href="https://thedfirreport.com/2022/07/11/select-xmrig-from-sqlserver/">https://thedfirreport.com/2022/07/11/select-xmrig-from-sqlserver/</a>

Supported Platforms: Windows

auto\_generated\_guid: 173126b7-afe4-45eb-8680-fa9f6400431c

#### Inputs:

Name	Description	Туре	Default Value
user_password	Password for new user account	String	At0micRedTeam!
user_name	Username	String	AtomicOperator

Attack Commands: Run with command\_prompt! Elevation Required (e.g. root or admin)

NET USER #{user\_name}\$ #{user\_password} /ADD /expires:never
REG ADD "HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\SpecialAccount:

### **Cleanup Commands:**