

Product ▾ Solutions ▾ Resources ▾ Open Source ▾ Enterprise ▾ Pricing

🔍

Sign in

Sign up

📁 redcanaryco / atomic-red-team

Public

🔔 Notifications

🍴 Fork

2.8k

★ Star

9.7k

<> Code

🕒 Issues 6

🔗 Pull requests 5

🎬 Actions

📖 Wiki

🛡 Security

📈 Insights

📁 Files

f339e7d

🔍

🔍 Go to file

> .github

> atomic\_red\_team

> atomics

> Indexes

> T1003.001

> T1003.002

> T1003.003

> T1003.004

> T1003.005

> T1003.006

> T1003.007

> T1003.008

> T1003

> T1006

> T1007

> T1010

> T1012

> T1014

> T1016

> T1018

> T1020

> T1021.001

> T1021.002

> T1021.003

> T1021.006

> T1027.001

> T1027.002

> T1027.004

> T1027

> T1030

> T1033

> T1036.003

> T1036.004

> T1036.005

> T1036.006

> T1036

atomic-red-team / atomics / T1136.001 / T1136.001.md 📄

🐙 CircleCI Atomic Red Team doc... Generate docs from job=genera... 7091fa8 · 2 years ago

🕒 History

PreviewCodeBlame256 lines (132 loc) · 6.26 KB

Raw📄⬇️☰

# T1136.001 - Local Account

## Description from ATT&CK

Adversaries may create a local account to maintain access to victim systems. Local accounts are those configured by an organization for use by users, remote support, services, or for administration on a single system or service. With a sufficient level of access, the `net user /add` command can be used to create a local account. On macOS systems the `dsc1 -create` command can be used to create a local account. Such accounts may be used to establish secondary credentialed access that do not require persistent remote access tools to be deployed on the system.

## Atomic Tests

- [Atomic Test #1 - Create a user account on a Linux system](#)
- [Atomic Test #2 - Create a user account on a MacOS system](#)
- [Atomic Test #3 - Create a new user in a command prompt](#)
- [Atomic Test #4 - Create a new user in PowerShell](#)
- [Atomic Test #5 - Create a new user in Linux with `root` UID and GID.](#)
- [Atomic Test #6 - Create a new Windows admin user](#)

## Atomic Test #1 - Create a user account on a Linux system

Create a user via useradd

**Supported Platforms:** Linux

**auto\_generated\_guid:** 40d8eabd-e394-46f6-8785-b9bfa1d011d2

**Inputs:**

Name	Description	Type	Default Value
username	Username of the user to create	String	evil_user

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

```
useradd -M -N -r -s /bin/bash -c evil_account #{username}
```

Page 1 of 4

- >  T1037.001
- >  T1037.002
- >  T1037.004
- >  T1037.005
- >  T1039
- >  T1040

Cleanup Commands:

```
userdel #{username}
```

## Atomic Test #2 - Create a user account on a MacOS system

Creates a user on a MacOS system with dscl

Supported Platforms: macOS

auto\_generated\_guid: 01993ba5-1da3-4e15-a719-b690d4f0f0b2

Inputs:

Name	Description	Type	Default Value
username	Username of the user to create	String	evil_user
realname	'realname' to record when creating the user	String	Evil Account

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

```
dscl . -create /Users/#{username}
dscl . -create /Users/#{username} UserShell /bin/zsh
dscl . -create /Users/#{username} RealName "#{realname}"
dscl . -create /Users/#{username} UniqueID "1010"
dscl . -create /Users/#{username} PrimaryGroupID 80
dscl . -create /Users/#{username} NFSHomeDirectory /Users/#{username}
```

Cleanup Commands:

```
dscl . -delete /Users/#{username}
```

## Atomic Test #3 - Create a new user in a command prompt

Creates a new user in a command prompt. Upon execution, "The command completed successfully." will be displayed. To verify the new account, run "net user" in powershell or CMD and observe that there is a new user named "T1136.001\_CMD"

Supported Platforms: Windows

auto\_generated\_guid: 6657864e-0323-4206-9344-ac9cd7265a4f

Inputs:

Name	Description	Type	Default Value
username	Username of the user to create	String	T1136.001_CMD
password	Password of the user to create	String	T1136.001_CMD!

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

```
net user /add "#{username}" "#{password}"
```

Cleanup Commands:

```
net user /del "#{username}" >nul 2>&1
```



## Atomic Test #4 - Create a new user in PowerShell

Creates a new user in PowerShell. Upon execution, details about the new account will be displayed in the powershell session. To verify the new account, run "net user" in powershell or CMD and observe that there is a new user named "T1136.001\_PowerShell"

Supported Platforms: Windows

auto\_generated\_guid: bc8be0ac-475c-4fbf-9b1d-9fffd77afbde

Inputs:

Name	Description	Type	Default Value
username	Username of the user to create	String	T1136.001_PowerShell

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

```
New-LocalUser -Name "#{username}" -NoPassword
```



Cleanup Commands:

```
Remove-LocalUser -Name "#{username}" -ErrorAction Ignore
```



## Atomic Test #5 - Create a new user in Linux with root UID and GID.

Creates a new user in Linux and adds the user to the root group. This technique was used by adversaries during the Butter attack campaign.

Supported Platforms: Linux

auto\_generated\_guid: a1040a30-d28b-4eda-bd99-bb2861a4616c

Inputs:

Name	Description	Type	Default Value
username	Username of the user to create	String	butter
password	Password of the user to create	String	BetterWithButter

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

```
useradd -g 0 -M -d /root -s /bin/bash #{username}
if [ $(cat /etc/os-release | grep -i 'Name="ubuntu"') ]; then echo "#{us
```



Cleanup Commands:

```
userdel #{username}
```



## Atomic Test #6 - Create a new Windows admin user

Creates a new admin user in a command prompt.

Supported Platforms: Windows

auto\_generated\_guid: fda74566-a604-4581-a4cc-fbbe21d66559

Inputs:

Name	Description	Type	Default Value
username	Username of the user to create	String	T1136.001_Admin
password	Password of the user to create	String	T1136_pass

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

```
net user /add "#{username}" "#{password}"
net localgroup administrators "#{username}" /add
```

Cleanup Commands:

```
net user /del "#{username}" >nul 2>&1
```