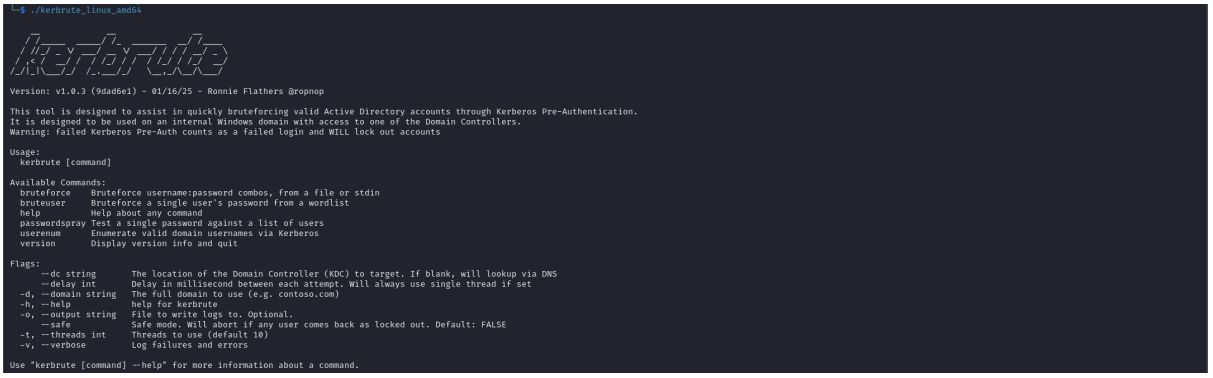
# Kerbrute

**Intro**

Kerbrute is a tool written in **GO program** language and it will work taking advantage of the **AS Req** (**Authentication Services request)** to make **users enumeration, brute force attack, password spaying** and **other techniques**.

**Installation**

To install Kerbrute we just have to download this tool from **ropnot** repo from **github**. The link is [Releases · ropnop/kerbrute](), specifically the binary ***kerbrute_linux_amd64***. Then we will give it execute permission with **chmod** ***kerbrute_linux_amd64*** and we are going to be able to use kerbrute with the command **./kerbrute_linux_amd64**

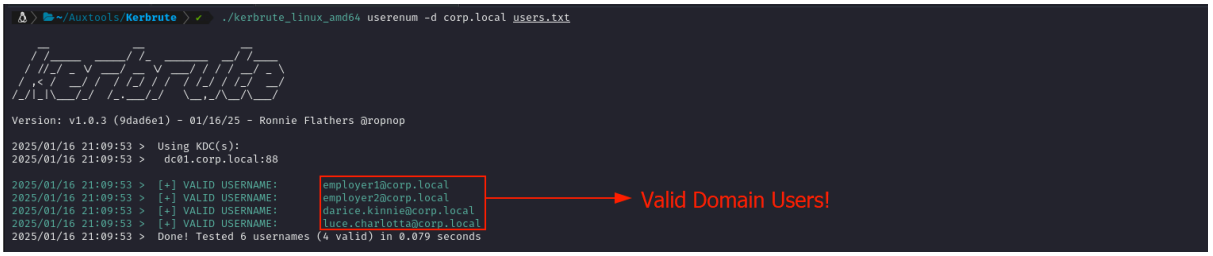



## Kerbrute on action

### Users enumeration

To make an user enumeration with kerbrute we are going to use those commands **1) userenum** to tell it which action we are going to execute, **2) -d domain.local** to pass it the domain that we are auditing and finally and finally, **3)** an **username dictionary** to make the attack. Is very easy to create a list of usernames because in an AD environment those names follow a pattern of **name.lastname.** The command going to be:

**./kerbrute userenum -d domain.local users.txt**



## 🏋️ Brute force attack with Kerbute

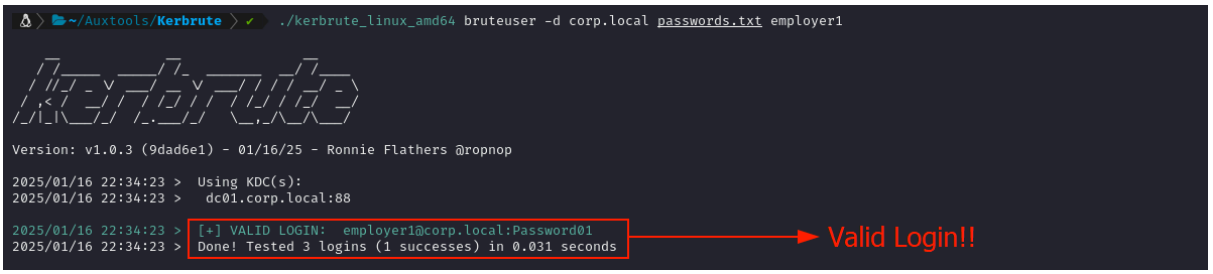
As it name says, the main use of Kerburte is to perform ***Brute Forces*** attack against **Kerberos protocol** in different ways. That we Going to see next

⚠️ **WARNING!!** ⚠️: *All these attacks must be carried out with great caution because they generate security events and abusing them can cause a user or the entire domain to be blocked due to failed login attempts.*

## 👥🔨 Brute Users

With the command we are going to use the command **bruteuser** we can perform an attack on a unique user following for a **password dictionary** and a **Valid Username.** The command is:

**./kerbute bruteuser -d local.domian dictionary.txt user.name**




## 🔒🔨 Brute Force

The Buteforce attack will consist of using a **file.txt with a list** t*hat combines username and password* in the format **user:password** to test the Kerberos authentication. The command going to fallow the next parameters:

**./kerbute -d domain.local burteforce user_pass.txt**

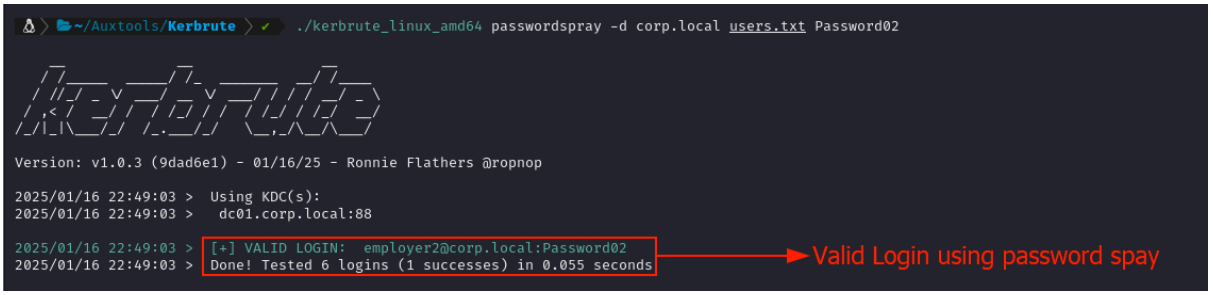

## 🔒🚿 PasswordSpaying

With Kerbrute we also can perform a **password spaying attack** using **a list of users** following for a **unique password** that will be used for all the users on the list. We can

investigate which passwords are common in an AD environment or, based on our information gathering, use those passwords that we think are going to be useful.

The command to perform this attack is:

**./kerbute passwordspay -d domain.local users.txt The.password**




**Conclusion**: Kerbute is a tool that is going to be useful to enumerate users and perform brute force attacks abusing the kerberos protocol.

But it is a tool that must be used ***very responsibly*** because if used indiscriminately it could be harmful to the infrastructure of the domain we are auditing.