

Breaking Windows Password with Unshackle

@mmar



Unshackle is an open-source tool to bypass Windows and Linux user passwords from a bootable USB based on Linux.

This can be a perfect free alternative to **Kon Boot** which is a paid tool and provides similar functionality



Attacks

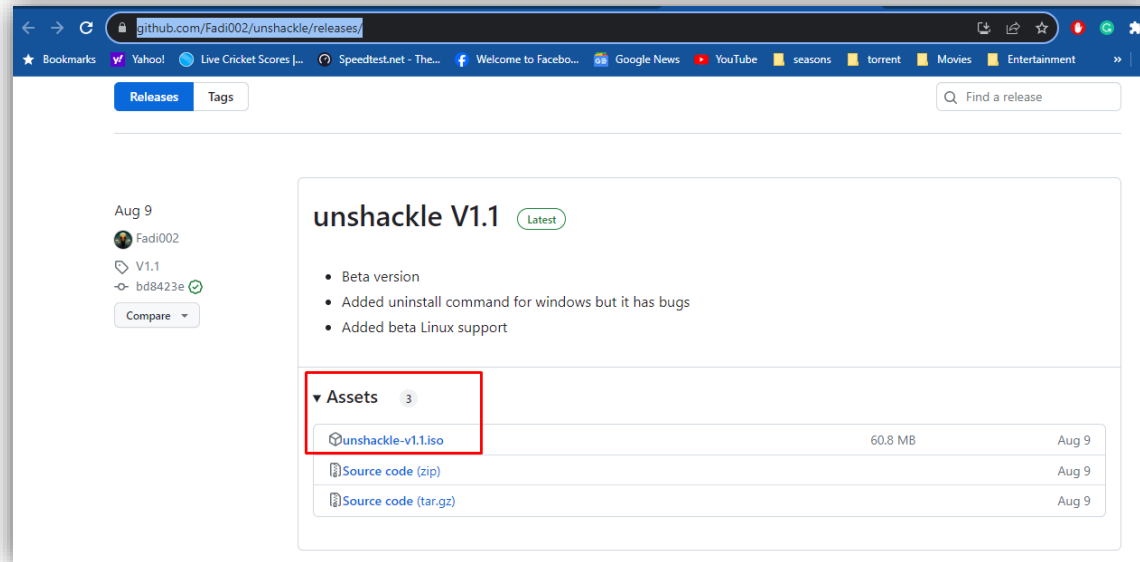
Scenario

- You have physical access to a system which is **password locked**. The tool can be used to quickly bypass the password

Step- 1

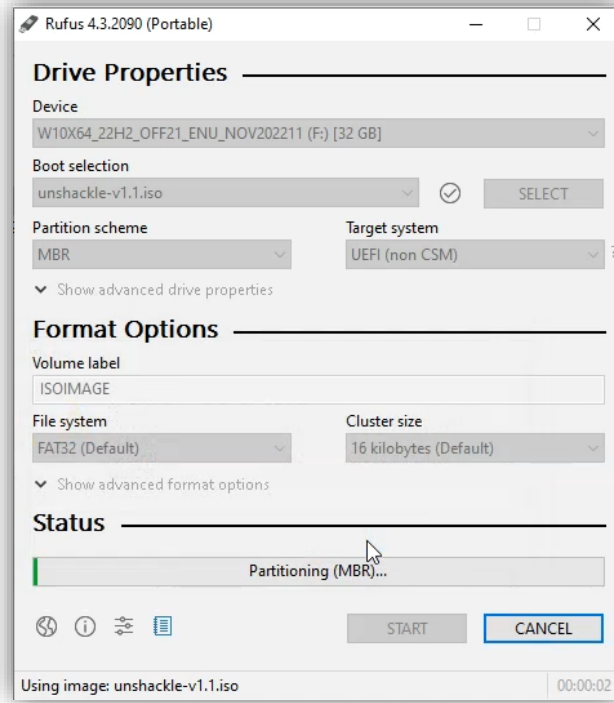
- ❖ Download the tool from the Github Repository

<https://github.com/Fadi002/unshackle/releases/>



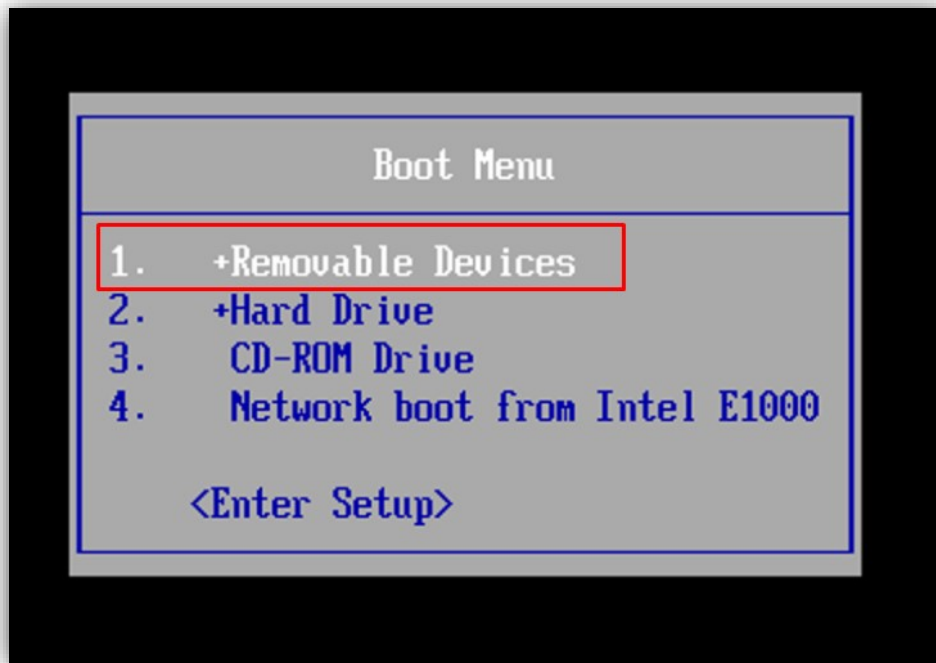
Step- 2

- ❖ Use rufus to make a bootable USB, You can also burn the ISO image to a CD/ DVD



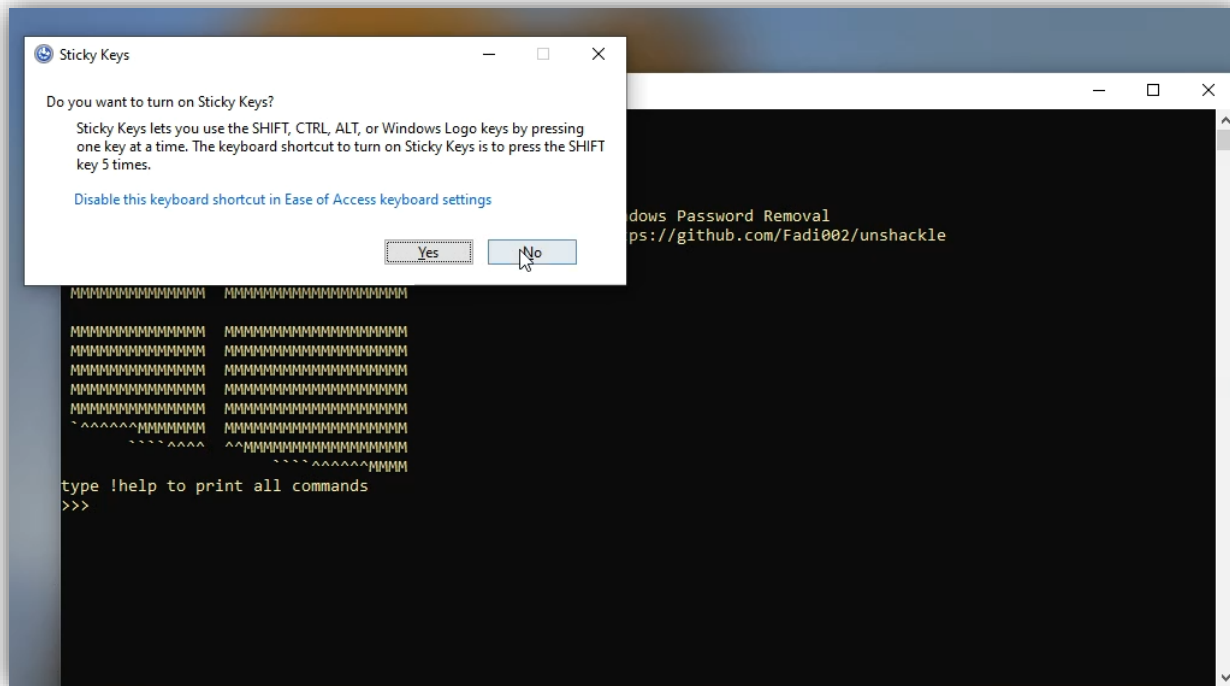
Step- 3

- ❖ Now on your PC, press esc or F12 (whatever your system supports and boot from USB



Step- 4

- ❖ On the Windows Login Screen, press shift 5 times, unshackle prompt will appear



Step- 5

- ❖ You can choose the option to clear password from the menu

```
!help - show this menu
!users - list all users
!change_password - change user account password
!remove_password - remove user account password
!restart - restart the pc
!poweroff - shutdown the pc
!clear - clear the console
!shell - open cmd here
!uninstall - remove unshackle
!exit - close the toolkit
>>> !users
Windows Users:
Administrator
DefaultAccount
Guest
Hassan
WDAGUtilityAccount
>>> !remove_password
Enter account username: Hassan
Type a password for the user:
Retype the password to confirm:
The command completed successfully.

done now just login with an empty password or restart
>>>
```




DEMO

A grayscale photograph of a calm sea with a small structure on the right and mountains in the background. The word 'THANKS' is overlaid in the center.

THANKS