

A Mini Project Report

On

“WINDOWS AUTHENTICATION BYPASSING”

Submitted in partial fulfillment of the
Requirements for the award of the degree of

Bachelor of Technology

In

Computer Science & Engineering-Cyber Security

By

M.JASWANTH – 20R21A6218

A.BHUVAN REDDY – 20R21A6201

E.HARSHITHA – 20R21A6212

A.RUBEN – 20R21A6203

Under the guidance of

Mr.B.Prabhanjan
Assistant Professor

Department of Computer Science & Engineering-Cyber Security



MLR

INSTITUTE OF TECHNOLOGY

(UGC AUTONOMOUS)

Affiliated to JNTUH, Approved by AICTE

Laxman Reddy Avenue, Dundigal, Hyderabad-500 043, Telangana, India



2022

Department of Computer Science & Engineering-Cyber Security

CERTIFICATE

This is to certify that the project entitled **“WINDOWS AUTHENTICATION BYPASSING”** has been submitted by **Meesala Jaswanth (20R21A6218), A Bhuvan Reddy (20R21A6201) and Eligeti Harshitha (20R21A6212) and Aerolla Ruben (20R21A6203)** in partial fulfillment of the requirements for the award of degree of Bachelor of Technology in Computer Science and Engineering - Cyber Security from Jawaharlal Nehru Technological University, Hyderabad. The results embodied in this project have not been submitted to any other University or Institution for the award of any degree or diploma.

Internal Guide

Head of the Department

External Examiner

Department of Computer Science & Engineering-Cyber Security

DECLARATION

We hereby declare that the project entitled “**WINDOWS AUTHENTICATION BYPASSING**” is the work done during the period from **August 2022 to December 2022** and is submitted in partial fulfillment of the requirements for the award of degree of Bachelor of Technology in Computer Science and Engineering from Jawaharlal Nehru Technology University, Hyderabad. The results embodied in this project have not been submitted to any other university or Institution for the award of any degree or diploma.

Meesala Jaswanth	20R21A6218
A Bhuvan Reddy	20R21A6201
Eligeti Harshitha	20R21A6212
Aerolla Ruben	20R21A6203

Department of Computer Science & Engineering-Cyber Security

ACKNOWLEDGEMENT

The satisfaction and euphoria that accompany the successful completion of any task would be incomplete without the mention of people who made it possible, whose constant guidance and encouragement crowned our efforts with success. It is a pleasant aspect that we now have the opportunity to express our guidance for all of them.

First of all, we would like to express our deep gratitude towards our internal guide **B. PRABHANJAN YADAV, Assistant Professor, Department of CSE-Cyber Security** for his support in the completion of our dissertation. We wish to express our sincere thanks to **Mr.K.Sai Prasad, HOD, and Department of CSE-Cyber Security** for providing the facilities to complete the dissertation.

We would like to thank all our faculty and friends for their help and constructive criticism during the project period. Finally, we are very much indebted to our parents for their moral support and encouragement to achieve goals.

Meesala Jaswanth	20R21A6218
A Bhuvan Reddy	20R21A6201
Eligeti Harshitha	20R21A6212
Aerolla Ruben	20R21A6203

Department of Computer Science & Engineering-Cyber Security

ABSTRACT

Windows Authentication Bypassing is an attack where attacker can go into others personal laptops or systems without knowing their password for their windows system. Bypassing is a thing which is not always detected and blocked, so it will be easy for the hacker to bypass windows authentication without the victim known. This leads to gathering information from the target, intrusion into important servers stealing confidential information. There are different types of methods can be used to bypass windows, such as using USB boot the system in your USB enter the boot according to bios by using this install a driver but will not and directly system goes to this pc, such as using CD boot the system in your CD enter the boot according to bios by using this install a driver but will not and directly system goes to this pc, by using command prompt and there are many other methods to bypass a windows. An attacker with a clear intention and purpose intends to steal information form a specific organization or a person. So it is not only important to enable security functions but to implement multilayered defence such as strengthen monitoring, this can decrease the chance of bypassing windows authentication.

LIST OF FIGURES

Figure Number	Name of the Figure	Page Number
1	Kon-Boot Loading	9
2	Proposed System Architecture	10
3	Bios Setup	13
4	USB connected to System	13
5	Boot from external device	14
6	Searching in Github	15
7	Kon-Boot Cracked version	15
8	Files Inside Zip file	16
9	Kon-Boot Installer	16
10	Select the USB drive	17
11	Kon-boot alert	17
12	Process in CMD	18

13	Confirmation pop up	18
14	Files Installed in USB	18
15	USB Bootable file	19
16	Alert for Administrator Access	19
17	Confirmation Pop up	20
18	USB consisting of Kon-boot Software	21
19	Bios Setup	21
20	Kon-boot Loading	22
21	Windows Login Page	22
22	Unlocked without Password	23

INDEX

Certificate	i
Declaration	ii
Acknowledgement	iii
Abstract	iv
List of Figures	v
Chapter 1	
Introduction	1
1.1 Overview	1
1.2 Purpose of the project	1
1.3 Motivation	2
Chapter 2	
Literature Survey	3
2.1 Existing System	3
2.2 Limitations of Existing System	4
Chapter 3	
Proposed System	6
3.1 Proposed System	6
3.2 Objectives of Proposed System	6
3.3 System Requirements	6
3.3.1 Software Requirements	6
3.3.2 Hardware Requirements	7
3.3.3 Functional Requirements	7
3.3.4 Non-Functional Requirements	7
Chapter 4	
System Design	8
4.1 Components Used in the Proposed System	8
4.2 Proposed System Architecture	10
4.3 How Does Kon-Boot work	11
4.4 How Exactly is Booting Process	12
4.5 How Does Booting from USB device work	12
4.5.1 How to Boot from a Usb Device	12

Chapter 5	15
Implementation	15
5.1 Steps to Download	15
Chapter 6	21
Results	21
Chapter 7	24
Conclusion	24
References	25

CHAPTER 1

INTRODUCTION

1.1 OVERVIEW

Windows Authentication Bypassing is an attack where attacker can go into others personal laptops or systems without knowing their password for their windows system. Bypassing is a thing which is not always detected and blocked, so it will be easy for the hacker to bypass windows authentication without the victim known. This leads to gathering information from the target, intrusion into important servers stealing confidential information. There are different types of methods can be used to bypass windows, such as using USB boot the system in your USB enter the boot according to bios by using this install a driver but will not and directly system goes to this pc, such as using CD boot the system in your CD enter the boot according to bios by using this install a driver but will not and directly system goes to this pc, by using command prompt and there are many other methods to bypass a windows.

1.2 PURPOSE OF THE PROJECT

The purpose of this project is to find a solution to unlock the computers or laptops without any password incase of forgotten the password. Ofcourse it is common to people to forget their passwords in long run. So, Windows authentication Bypassing plays a major role in this cases. The moto of this project is to spread awareness about the tool that can be used to bypass windows authentication. So it will help users to login with out any password and then reset the password. This can be used for both windows and mac.

1.3 MOTIVATION

Let us consider this Scenario. Suppose you bought a new laptop and Comfortably using it. Later you realized that some of your important documents were there in your old laptop. Ofcourse if we get used to new passwords, we will automatically forget old passwords, that's common. But what if at any cost you need those documents. Ofcourse you can get it repaired in a service centre. But if you are in no time, you only think of how to unlock it with out any password. And then Windows Bypassing comes into picture. It is an alternative to unlock a locked device. But it is not possible on our own. So we use third party software that is capable of changing the bios settings and unlock the system without any password. And this is achived by using some hard drive devices. Hence it is clear that, most of the users face this issue but can't resolve it. So it's useful for users to get to know about This tools.

CHAPTER 2

LITERATURE SURVEY

We conducted a thorough literature survey by reviewing existing systems that helps users unlocking their windows without password. Research papers, journals and publications have also been referred in order to prepare this survey.

2.1 EXISTING SYSTEM

[1] **PCUnlocker** is a Similar Software that is used to Reset and unlock forgotten Windows login password. When you lost your Windows password (including Administrator), Need to Log into a computer with an unknown password, Windows administrator account is disabled or the password has expired, Windows account was locked out by mistyping the password so many times then PCUnlocker can be used to Bypass Windows Authentication or Reset Windows password. This is Compatible with Windows 11, 10, 8, 7, Vista, XP and 2003/2008/2012/2016 Servers.

[2] **iSeePassword – Windows Password Recovery Pro** is another upgraded Software which has been developed to cope with PCUnlocker toolkit. When you wanted to Recover or reset all user, administrator passwords and other password, Reset Domain Administrator password, Reset passwords with a bootable USB drive, we use this software. Also for removing lost/forgotten local administrator and users password for Windows 10, 8, 7, Vista, XP and Windows Server 2000/2003.2008/2012 quickly and conveniently.

[3] **John the Ripper** is an Open Source password security auditing and password recovery tool available for many operating systems. John the Ripper jumbo supports hundreds of hash and cipher types, including for: user passwords of Unix flavors, macOS, Windows, web apps, groupware, database servers, network traffic captures, encrypted private keys, filesystems and disks are some examples.

[4] **iSunshare Windows 10 Password Genius** is the newest Windows 10 password recovery tool specialized for windows 10 to not only reset or remove windows 10 forgotten password, but also create new Windows 10 administrator account without data loss on locked computers. With iSunshare Windows 10 Password Genius, you can Easily remove Windows 10 local administrator and other local user password, Instantly reset Windows 10 domain administrator and other domain user password, Reset Windows 10 Microsoft account password with only one click. Compatible Settings are Windows XP/Vista/Win7/Win8/Win10/Win11(32 & 64 bit) and Servers 2000/2003/2008/2012/2016.

2.2 LIMITATIONS OF EXISTING SYSTEM

Concisely summarizing the disadvantages of the above implementations:

- All these Softwares are complex to use and not a user friendly tools. Thus Users get frustrated while using them.
- Some of the tools mentioned doesn't provide a 100% recovery. Thus there is no Guarantee that the tool or software works.
- PCUnlocker has'nt been updated since 2018 and also its not easy to reset or recover the forgotten password.
- As some of the softwares mentioned needs a usb for bootable device, it takes a longer time to complete the process.
- All these Softwares are Paid Softwares, The cost of these softwares ranges from \$15 - \$30. Hence normal people cannot afford them. There are no cracked versions available.
- And also there is a case where users may use hard disk encryption software like FileVault (Apple) / Bitlocker (Microsoft) / TrueCrypt or set BIOS/UEFI password. Hence these Softwares won't work.

CHAPTER 3

PROPOSED SYSTEM

3.1 PROPOSED SYSTEM

The proposed System is using Kon-Boot software that is capable of changing Bios settings. Kon boot is a third party platform that helps users in bypassing the windows authentication. It states itself as world's best remedy for forgotten passwords either windows or mac. Kon-Boot (aka kon boot, konboot) is a tool that allows accessing locked computer without knowing the user's password. Unlike other solutions Kon-Boot does not reset or modify user's password and all changes are reverted back to previous state after system restart. Kon boot also states that Kon-Boot is currently the only solution worldwide that can bypass Windows 10 passwords. Kon-Boot has been successfully used by military personnel, law enforcement, IT corporations and professionals, forensics experts, private customers. It has been on the market since 2009 and the free version was downloaded more than 50,00,000 times.

3.2 OBJECTIVES OF PROPOSED SYSTEM

The objectives of the proposed system include the following:

- To Bypass Windows Authentication.
- To Retrieve essential data from a device without knowing the password.
- To Spread the solution for windows bypassing.
- To Easily bypass using a usb in less than five minutes.

3.3 SYSTEM REQUIREMENTS

Here are the requirements for windows authentication bypassing.

3.3.1 SOFTWARE REQUIREMENTS

Below are the software requirements for windows authentication bypassing:

1. The required software is Kon-boot.
2. Github to search for mod versions.

3.3.2 HARDWARE REQUIREMENTS

Below are the hardware requirements to perform windows authentication bypassing:

1. Supported Operating System : Windows XP to Windows 11
2. Processor : Pentium III compatible processor (min)
3. Hard Drive (USB) : 10 Mb free space (min)
4. Other : Internet to download/ burn the file.

3.3.3 FUNCTIONAL REQUIREMENTS

- The system should be able to access the usb so that we need to add a bootable device while starting the system.
- Then we should configure the boot settings and change it to Boot with usb and then turn off Secure boot settings.
- After the change in settings, directly click on save changes and then you will be redirected to the windows page.
- The system should be able to bypass windows authentication, and this can be achieved only if the System doesn't have any BitLocker / FileFault.

3.3.4 NON-FUNCTIONAL REQUIREMENTS

Reliability

- Regardless of the number type of os, the system should be able to access the bootable file present in usb.
- System should be able to handle any exception properly.
- As for the output, the system should be able to provide a faster response.

CHAPTER 4

SYSTEM DESIGN

4.1 COMPONENTS USED IN THE PROPOSED SYSTEM

KON-BOOT (aka konboot, kon boot) is a software utility that allows users to bypass Microsoft Windows passwords and Apple macOS passwords (Linux support has been deprecated) without lasting or persistent changes to system on which it is executed. It is also the first reported tool capable of bypassing Windows 10 online (live) passwords and supporting both Windows and macOS systems. It is also a widely used tool in computer security, especially in penetration testing. Since version 3.5 Kon-Boot is also able to bypass Secure Boot feature. Kon-Boot was originally designed as a proof of concept, freeware security tool, mostly for people who tend to forget their passwords. The main idea was to allow users to login to the target computer without knowing the correct password and without making any persistent changes to system on which it is executed. First Kon-Boot release was announced in 2008 on Daily Dave mailing list. Version 1.0 (freeware) allowed users to login into Linux based operating systems and to bypass the authentication process (allowing access to the system without knowing the password). In 2009 author of this software announced Kon-Boot for Linux and 32-bit Microsoft Windows systems. This release provided additional support for bypassing Windows systems passwords on any Windows operating system starting from Windows Server 2008 to Windows 7. This version is still available as freeware Newest Kon-Boot releases are available only as commercial products and are still maintained. Kon-Boot works like a bootkit (thus it also often creates false positive alerts in antivirus software). It injects (hides) itself into BIOS memory. Kon-Boot modifies the kernel code on the fly (runtime), temporarily changing the code responsible for verification user's authorization data while the operating system loads.

While by default Kon-Boot bypasses Windows passwords it also includes some additional features that are worth noting:

- Kon-Boot can change Windows passwords due to embedded Sticky-Keys feature. For example after successful Windows boot with Kon-Boot user can tap SHIFT key 5 times and Kon-Boot will open a Windows console window running with local system privileges. Fully working console can be used for a variety of purposes. For example in case of changing Windows password following command can be used: `net user [username] [new password]` (selected user can be later added as new Windows administrator by typing: `net local group administrators [username] /add`). Similarly following command: `net user [username] *` will erase current Windows password for selected user.
- In the commercial Kon-Boot editions it is possible to use Automatic PowerShell Script Execution feature which automatically executes (after Windows boot) given PowerShell script with full system privileges. This feature can be used to automatize various tasks for example performing forensics data gathering task etc. To use this feature Windows needs to be installed in UEFI mode.

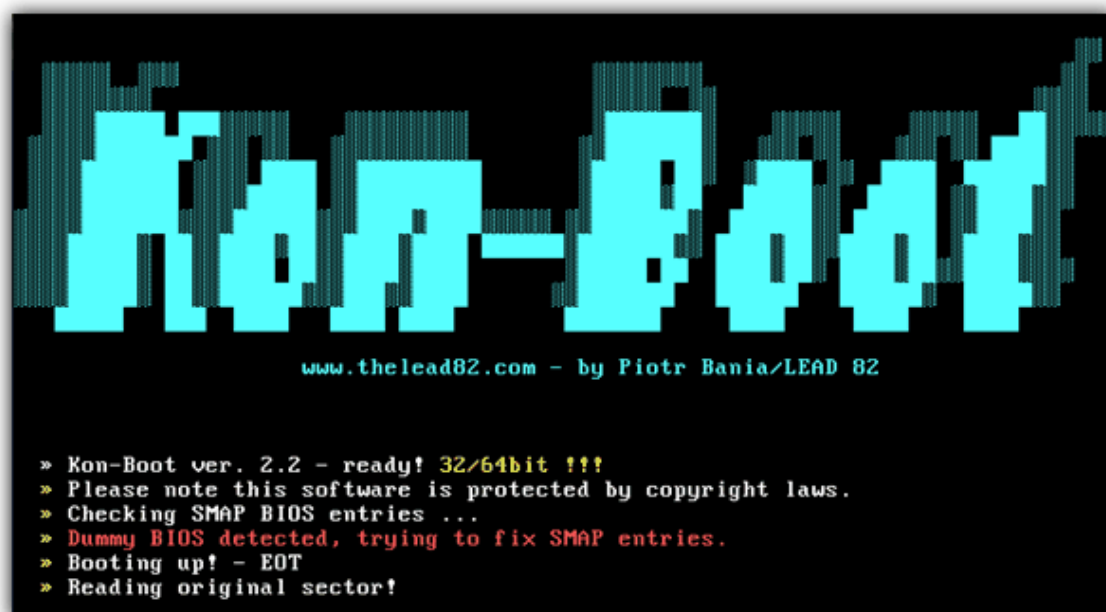


Figure 1: Kon-boot Loading

4.2 PROPOSED SYSTEM ARCHITECTURE

An architectural diagram outlines the system's components, their relationships, and system functionality. We are using USB to change the Bios settings. And these Bios settings are capable of unlocking the system without any password.

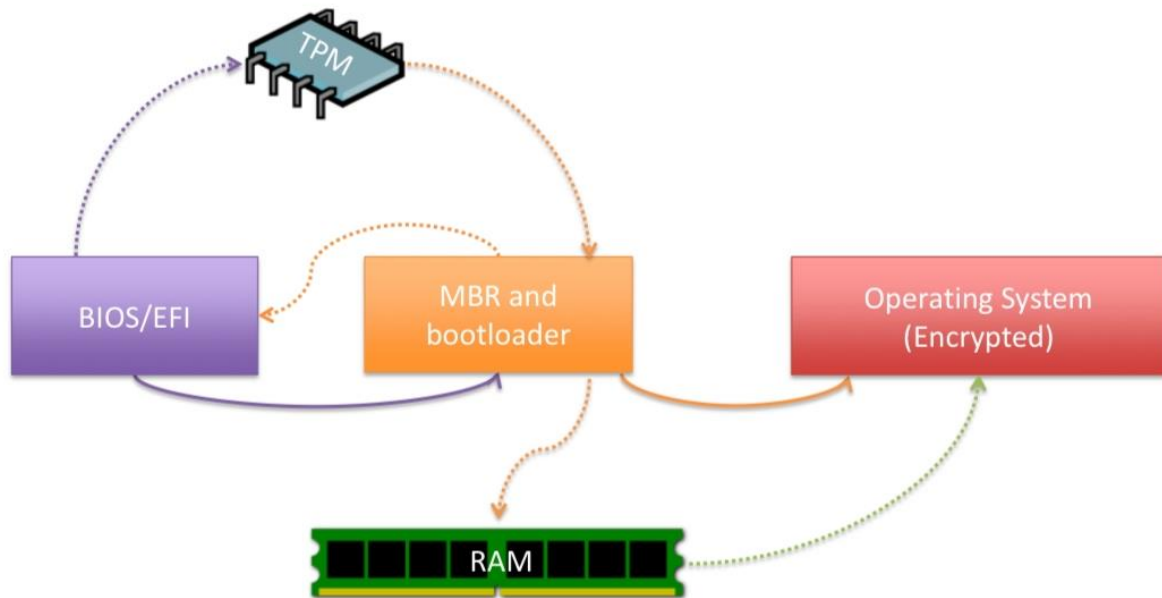


Figure 2 : Proposed System Architecture

Trusted Platform Module (TPM) technology is designed to provide hardware-based, security-related functions. A TPM chip is a secure crypto-processor that is designed to carry out cryptographic operations. The chip includes multiple physical security mechanisms to make it tamper-resistant, and malicious software is unable to tamper with the security functions of the TPM. Some of the key advantages of using TPM technology are that you can:

- Generate, store, and limit the use of cryptographic keys.
- Use TPM technology for platform device authentication by using the TPM's unique RSA key, which is burned into it.
- Help ensure platform integrity by taking and storing security measurements.

The most common TPM functions are used for system integrity measurements and for key creation and use. During the boot process of a system, the boot code that is loaded (including firmware and the operating system components) can be measured and recorded in the TPM. The integrity measurements can be used as evidence for how a system started and to make sure that a TPM-based key was used only when the correct software was used to boot the system. TPM-based keys can be configured in a variety of ways. One option is to make a TPM-based key unavailable outside the TPM. This is good to mitigate phishing attacks because it prevents the key from being copied and used without the TPM. TPM-based keys can also be configured to require an authorization value to use them. If too many incorrect authorization guesses occur, the TPM will activate its dictionary attack logic and prevent further authorization value guesses.

4.3 HOW DOES KON-BOOT WORK

The source code of Kon-boot has not been published by its author so it is not known what it does exactly to hack the operating system. However some hypothesis can be made based on known technologies to determine how it works. In general, bootkits basically hook the 0x13 interruption routine that is usually provided by the BIOS of the computer. The role of this routine is to read sectors from the hard disk and to load them into a given location in RAM memory. By hooking this routine, bootkits such as Kon-boot or Vbootkit modify directly the code of the operating system when it is copied into main memory, just before its execution.

4.4 WHAT EXACTLY IS THE BOOTING PROCESS

Before booting, let's grab out some facts. Your operating system (Windows/Linux/Mac), is stored on your hard drive / SSD, along with all the configurations. The operating system does not operate from the hard drive itself, because secondary storage devices are slow. So, the OS (which is also a program) is loaded to the main memory (RAM), which is fast, and can be processed by the CPU to perform various tasks as it does. So, booting involves loading the OS (precisely, kernel, a component of OS) to the main memory. When you power on your system, the first thing which fires up is the BIOS (with your manufacturer's logo on it). It is the BIOS which loads a small program from a special location on your hard drive (people call it MBR / boot partition), called the bootloader. It is now the bootloader, which is responsible for loading the kernel, and primary processes, which eventually load other processes, and you are landed to the login screen with a bunch of processes working in the background.

4.5 HOW DOES BOOTING FROM USB DEVICE WORK

There are lots of reasons you might want to boot from a USB device, like an external hard drive or a flash drive, but it's usually so you can run special kinds of software. When you boot from a USB device, what you're doing is running your computer with the operating system installed on the USB device. When you start your computer normally, you're running it with the operating system installed on your internal hard drive- windows, Linux, etc.

4.5.1 HOW TO BOOT FROM A USB DEVICE

Follow these easy steps to boot from a flash drive, an external hard drive, or some other bootable USB device.

- Change the BIOS boot order so the USB device option is listed first. The BIOS is rarely set up this way by default.

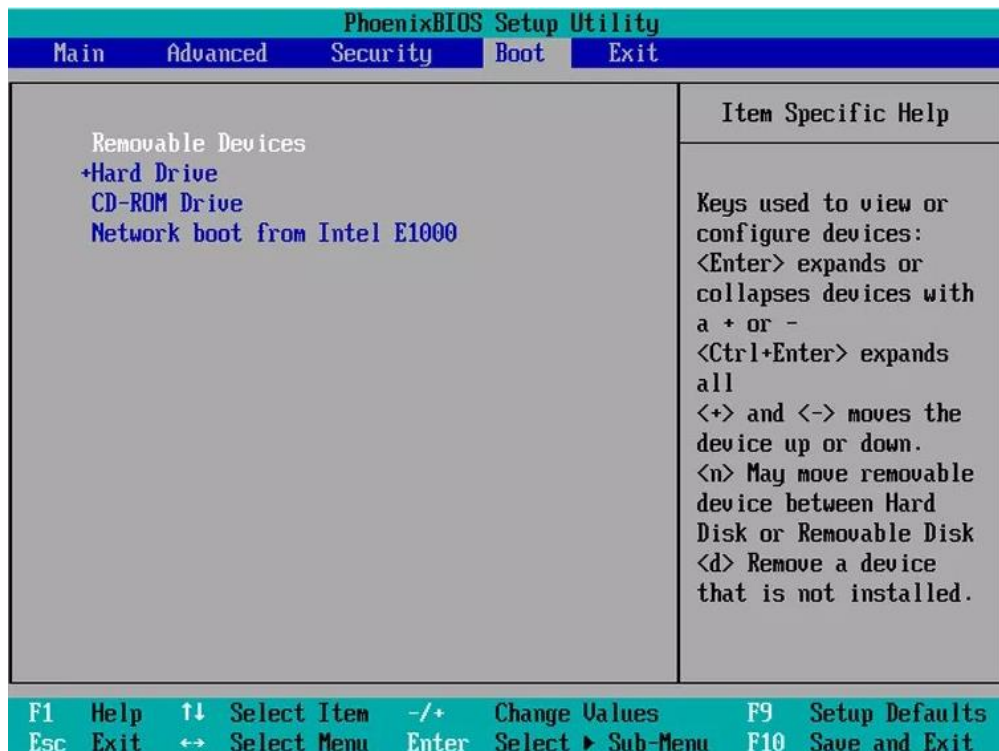


Figure 3 : Bios Setup

- If the USB boot option is not first in the boot order,, your PC will start "normally" (i.e., boot from your hard drive) without even looking at any boot information that might be on your USB device.
- Attach the USB device to your computer via any available USB port.

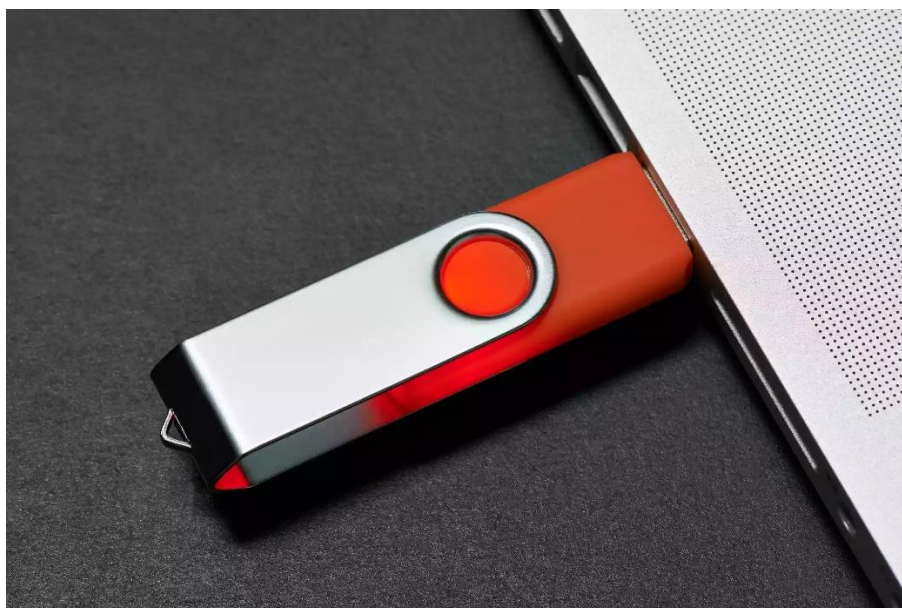


Figure 4 : USB connected to system

- Restart your computer.. Since you're not actually inside of the operating system at this point, restarting isn't the same as using normal restart buttons. Instead, BIOS should explain which key to press—such as F10 or F12—to save the boot order changes and restart the computer.
- Watch for a Press any key to boot from external device message.

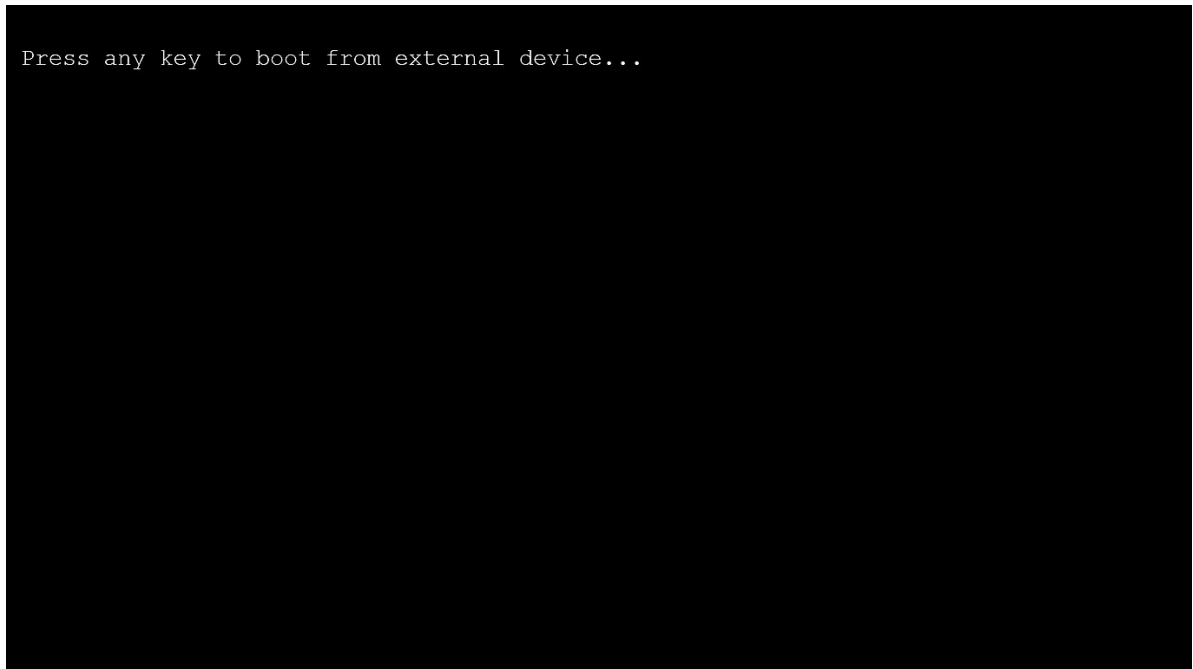


Figure 5 : Boot from external device

- You may be prompted with a message to press a key on some bootable devices before the computer boots from the flash drive or another USB device. If this happens, and you do nothing, your computer will check for boot information on the next boot device in the list in BIOS (see Step 1), which will probably be your hard drive.
- Your computer should now boot from the flash drive or USB based external hard drive.

CHAPTER 5

IMPLEMENTATION

Open Google Chrome and search for Cracked Versions. Obviously we know that, most of the cracked versions are present In Github. Hence First download Cracked Version of Konboot Software from Resources where Cracked Versions are available.

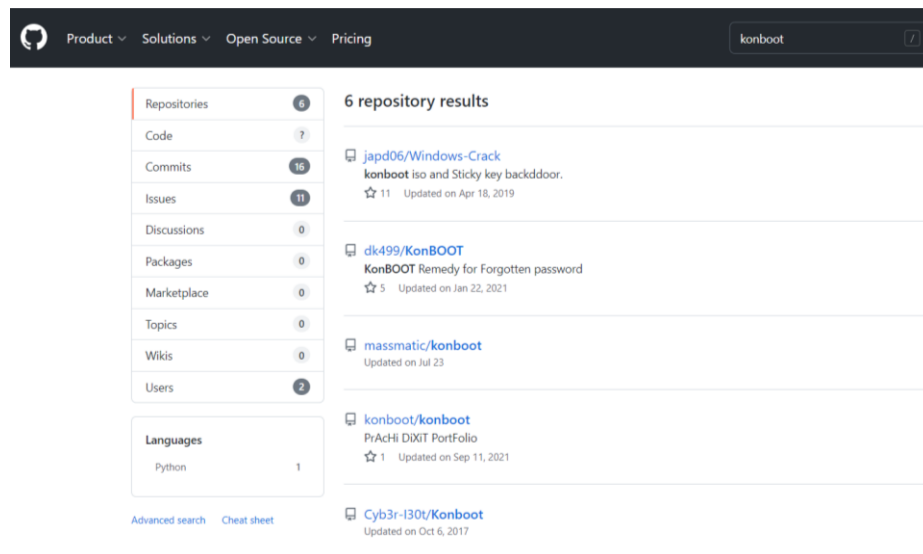


Figure 6 : Searching in Github

Steps to Download :

1. First, download Kon-Boot Cracked Version from below.

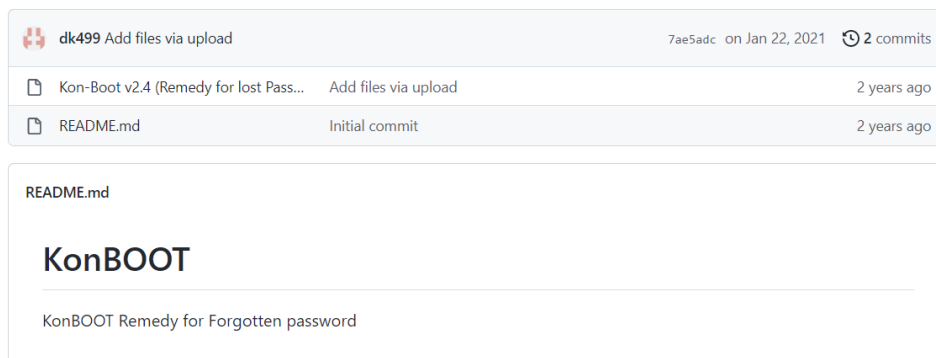


Figure 7 : Kon-Boot Cracked version

2. Extract the ZIP file using extract here option.

3. Now, you need to click on KonBootInstaller Application and run it.









 kon-bootCD	12/21/2022 9:35 AM	File folder	
 kon-bootFLOPPY	12/21/2022 9:35 AM	File folder	
 kon-bootUSB	12/21/2022 9:35 AM	File folder	
 eula	12/21/2022 9:35 AM	Text Document	8 KB
 formatcommands	12/21/2022 9:36 AM	Text Document	1 KB
 KonBootInstaller	12/21/2022 9:35 AM	Application	21 KB
 konbootWIN_guide	12/21/2022 9:35 AM	Microsoft Edge PD...	610 KB
 konlog	12/21/2022 9:36 AM	Text Document	3 KB

Figure 8 : Files inside Zip File

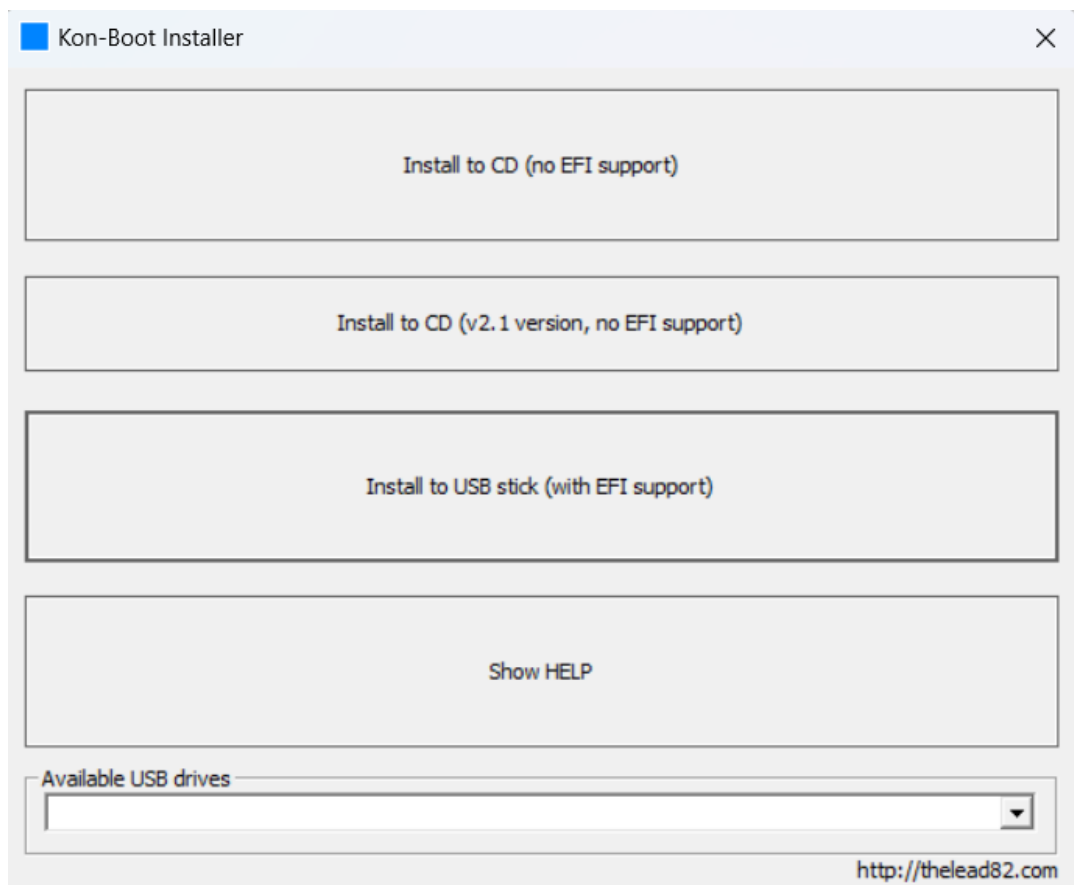


Figure 9 : Kon-Boot Installer

4. Now click on Available USB drives pop up and select the USB device you wants to use for booting the locked system.

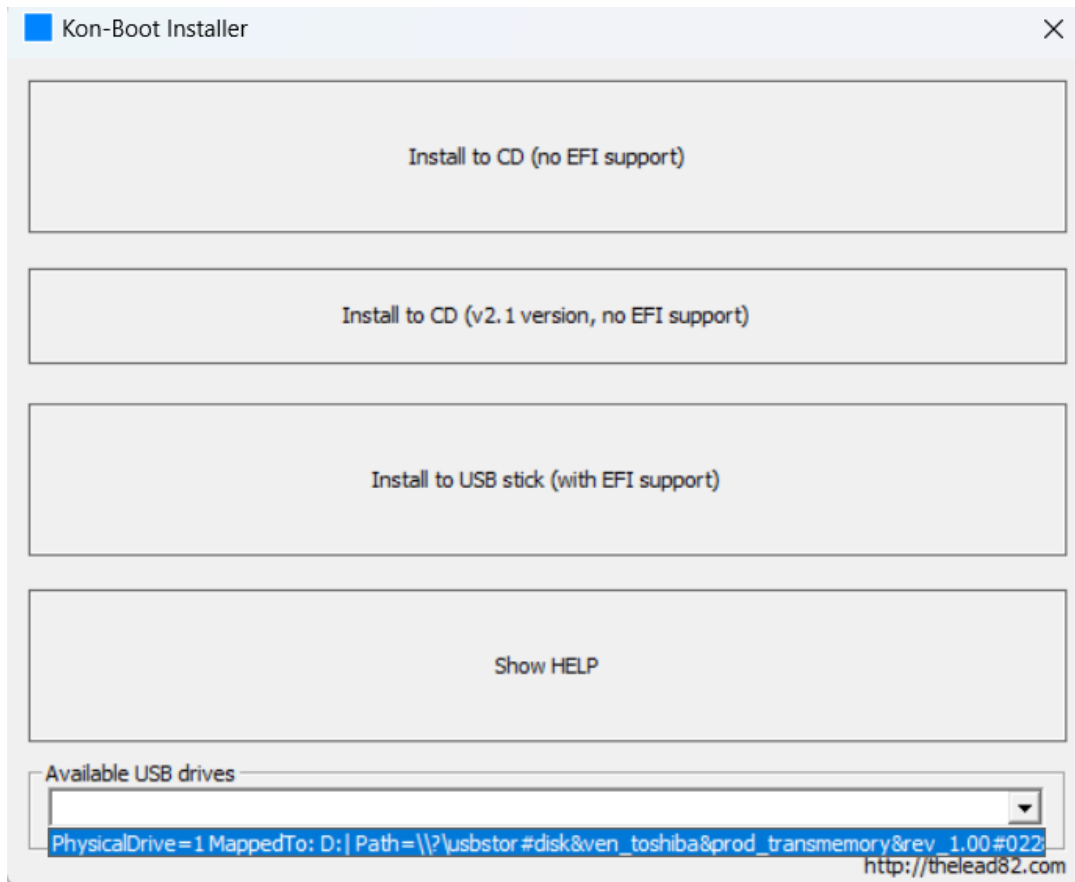


Figure 10 : Select the USB drive

5. Click on Install to USB stick(with EFI support) and Click on yes as shown below.

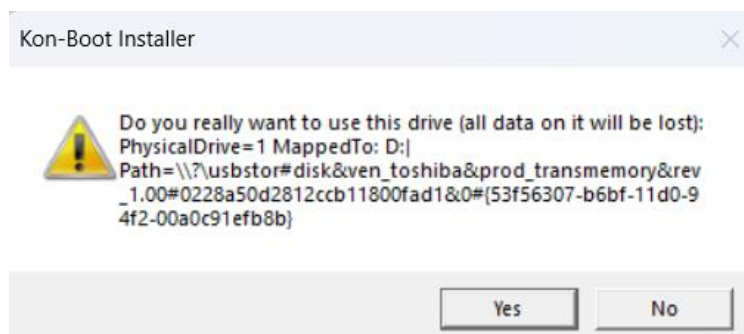


Figure 11 : Kon-boot alert

6. You will be redirected to Cmd and performs cleaning of disk and then installs the Kon-Boot bootable file to selected USB.

```
C:\Users\JASWANTH\Desktop\Kon-Boot v2.4 (Remedy for lost Password)\Kon-Boot v2.4

Microsoft DiskPart version 10.0.22621.1

Copyright (C) Microsoft Corporation.
On computer: LAPTOP-8AB00839

Volume 3 is the selected volume.

DiskPart succeeded in cleaning the disk.

DiskPart succeeded in creating the specified partition.

Partition 1 is now the selected partition.

DiskPart marked the current partition as active.

    0 percent completed
```

Figure 12 : Process in CMD

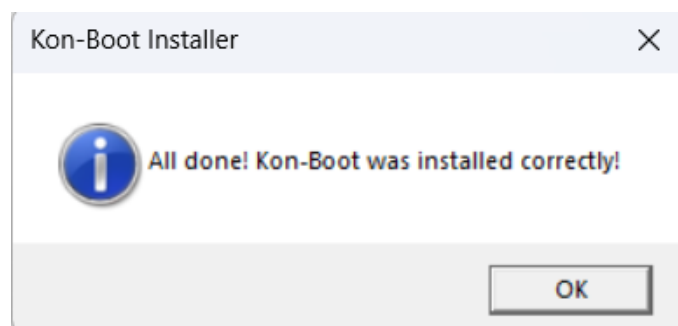


Figure 13 : Confirmation pop up

7. Kon boot files will be installed on the selected USB.

KONBOOT (D:) >				
	Name	Date modified	Type	Size
	EFI	12/21/2022 2:56 PM	File folder	
	grldr	12/21/2022 9:35 AM	File	210 KB
	konboot	12/21/2022 9:35 AM	Disc Image File	1,440 KB
	konbootOLD	12/21/2022 9:35 AM	Disc Image File	1,440 KB
	menu.lst	12/21/2022 9:35 AM	LST File	1 KB

Figure 14 : Files Installed in USB

8. Now open kon-bootUSB file and double click on usb_install_RUNASADMIN.

Name	Date modified	Type	Size
EFI	12/21/2022 9:35 AM	File folder	
USBFILES	12/21/2022 9:35 AM	File folder	
COPYING	12/21/2022 9:35 AM	File	18 KB
grubinst	12/21/2022 9:35 AM	Application	61 KB
konboot_usb	12/21/2022 9:35 AM	Application	55 KB
README	12/21/2022 9:35 AM	Text Document	1 KB
temp_file	12/21/2022 9:35 AM	Text Document	1 KB
USB_INSTALL	12/21/2022 9:35 AM	VBScript Script File	3 KB
USB_INSTALL_DIFF	12/21/2022 9:35 AM	VBScript Script File	4 KB
<u>usb_install_RUNASADMIN</u>	12/21/2022 9:35 AM	Windows Batch File	1 KB
usb_install? NFFDADMIN	12/21/2022 9:35 AM	Windows Batch File	1 KB

Figure 15 : USB bootable file

9. Next again you will be redirected to Command Prompt. Click on Ok.

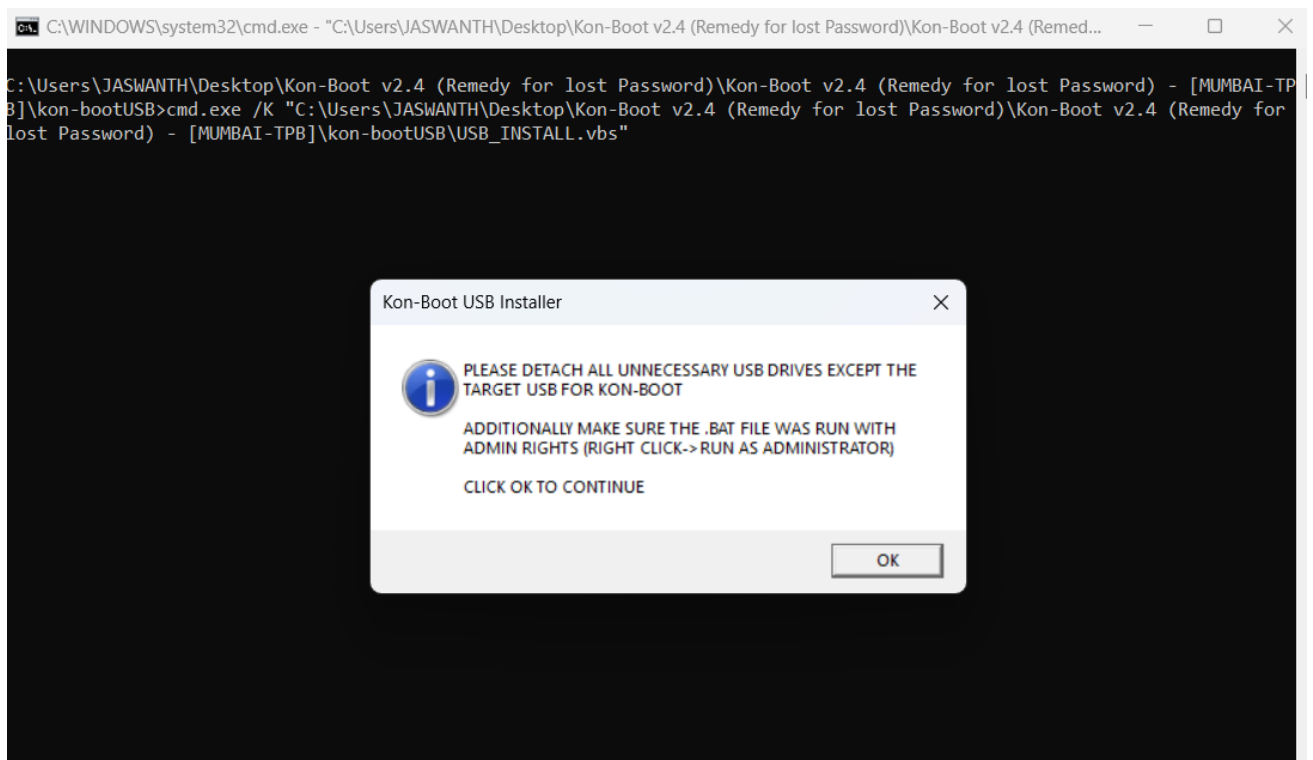


Figure 16 : Alert for Administrator Access

10. Now you are ready with the software installed on the USB.

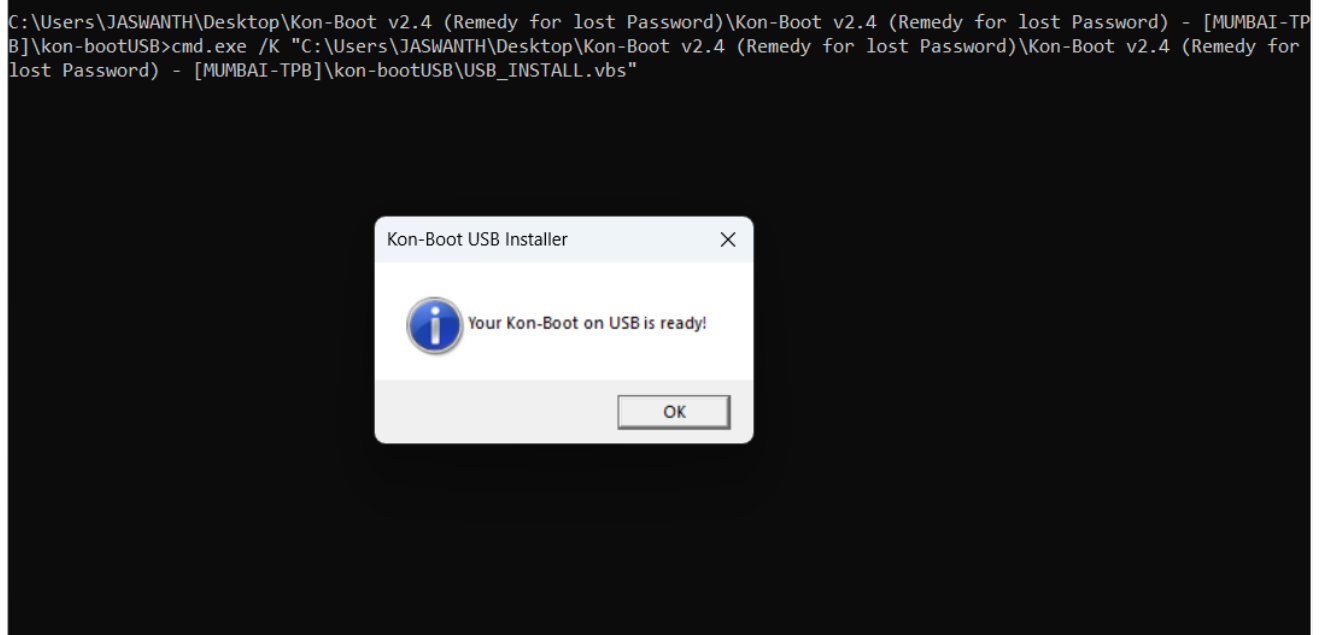


Figure 17 : Confirmation pop up

CHAPTER 6

RESULTS

Step 1 : After installing Kon-boot software to the USB, insert the USB to the locked system.



Figure 18 : USB containing Kon-boot Software

Step 2 : While the system is Starting, click on F12 button to enter into Bios Setup. After entering Bios setup, click on Booting settings.



Figure 19 : Bios Setup

Step 3 : Now boot using CD-ROM, So the Kon-boot tool that was installed in the USB will be used to boot the system..



Figure 20 : Kon-boot Loading

Step 4 : Next The windows will turn on automatically and ask for password. Just click on Enter.

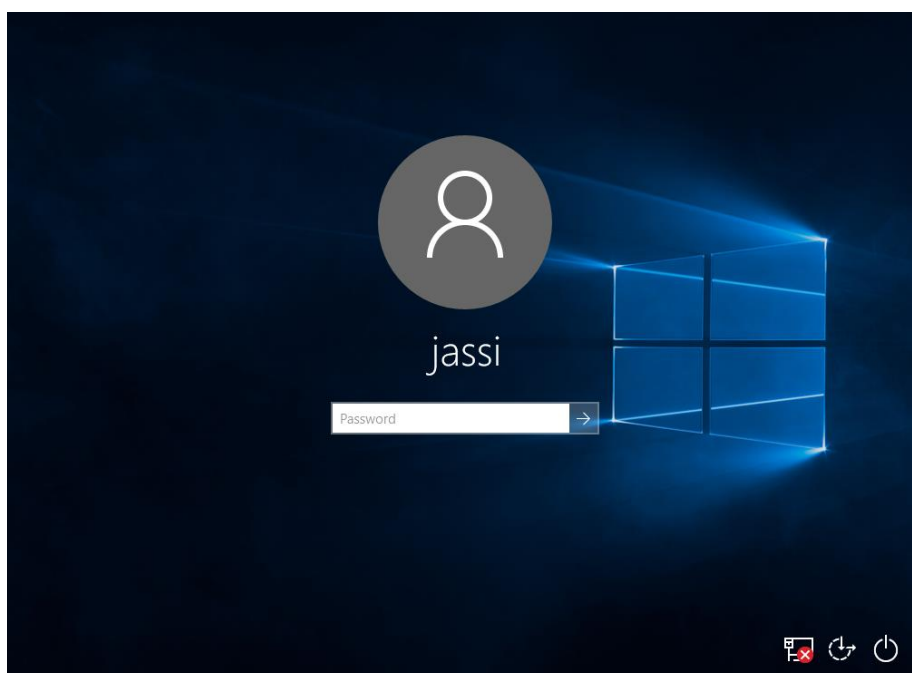


Figure 21 : Windows Login Page

Step 5 : The windows password is Bypassed Automatically, and it will get us logged into system.

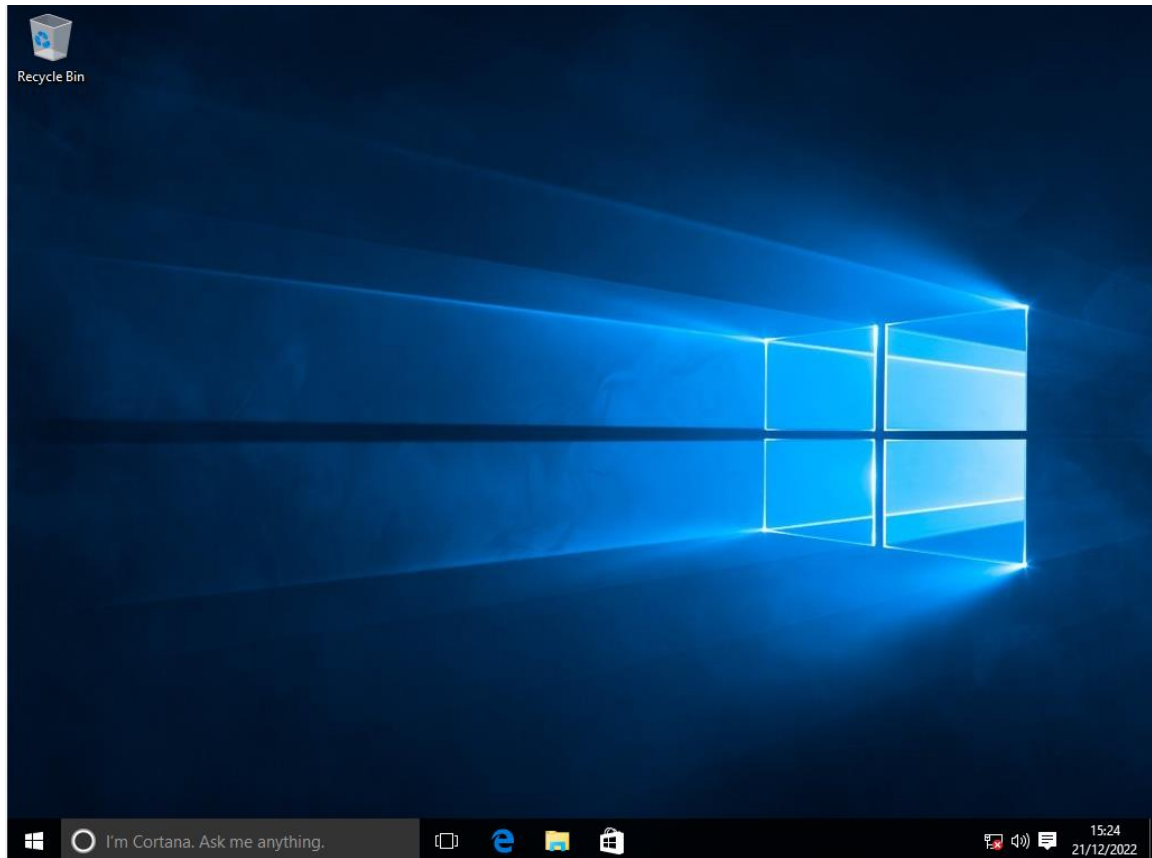


Figure 22 : Unlocked without password

CHAPTER 7

CONCLUSION

Windows authentication is the most useful feature that Verifies that whether the user is Legitimate user or not. It will give access only if the user is a authorized user. Inorder to provide Security for the users, Windows keeps on updating its authorization techniques. But There are some tools that can be used to Bypass windows authentication very easily. Inorder to bypass windows there are many Softwares that are capable of changing Bios Settings and booting settings. These softwares will configure the Bios settings to start from USB or USB thumb drive (FAT32 filesystem). There is also a big Enemy for these softwares. These Techniques wont work if the system has enabled Full disk encryption and BIOS password. And also BitLocker recovery for windows will stop the User from accessing Bios settings.

REFERENCES

- [1] <https://nvd.nist.gov/vuln/detail/CVE-2022-26913>
- [2] <https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-26913>
- [3] <https://www.techtarget.com/whatis/definition/trusted-platform-module-TPM>
- [4] <https://agrtech.com.au/windows/bypass-windows-password-using-kon-boot/>
- [5] <https://itoolab.com/windows-password/kon-boot-review/>
- [6] <https://crackitems.com/kon-boot-crack/>
- [7] <https://github.com/dk499/KonBOOT>
- [8] <https://kon-boot.com/>
- [9] <https://www.blackhat.com/docs/eu-15/materials/eu-15-Haken-Bypassing-Local-Windows-Authentication-To-Defeat-Full-Disk-Encryption.pdf>
- [10] <https://en.wikipedia.org/wiki/Kon-Boot>