# SYSTEM HACKING WITH BOOTABLE DRIVES

An analytical demonstration of system access using bootable system utilities in a secure offline environment.

Name :-Prerna Bhashani
Institute : skillogic
Internship :- cybersecurity internship project

# INTRODUCTION

System security is a critical aspect of modern IT infrastructure. Organizations face increasing threats due to insecure systems, misconfigurations, and outdated security controls. To evaluate system security effectively, professionals often use bootable drives that allow testing in a controlled and isolated environment.

This project focuses on assessing system security using bootable drives in an offline environment to identify vulnerabilities without affecting the primary operating system.

# Problem Statement

- Organizations face several challenges in securing computer systems:
- Vulnerabilities in operating systems and applications
- Weak authentication mechanisms
- Poor visibility into system-level security flaws
- Compliance requirements such as GDPR and HIPAA
- Without regular security assessments, these weaknesses can lead to data breaches, unauthorized access, and financial losses.

# Solution Overview

- System hacking using bootable drives provides a solution by allowing security professionals to:
- Boot into a separate operating environment
- Perform security assessments without using the installed OS
- Analyze system configurations safely
- Conduct ethical penetration testing in an offline setup
- This approach ensures minimal risk to production systems while offering deep system-level visibility

# Project Objectives

- To understand bootable drive concept
- To demonstrate system access using bootable environment
- To analyze Windows security vulnerabilities
- To understand prevention techniques

# TOOLS AND TECHNOLOGIES USED

- Hiren BootCD PE
- Windows 10 Virtual Machine
- VirtualBox
- Bootable USB Creation Tool (Rufus)



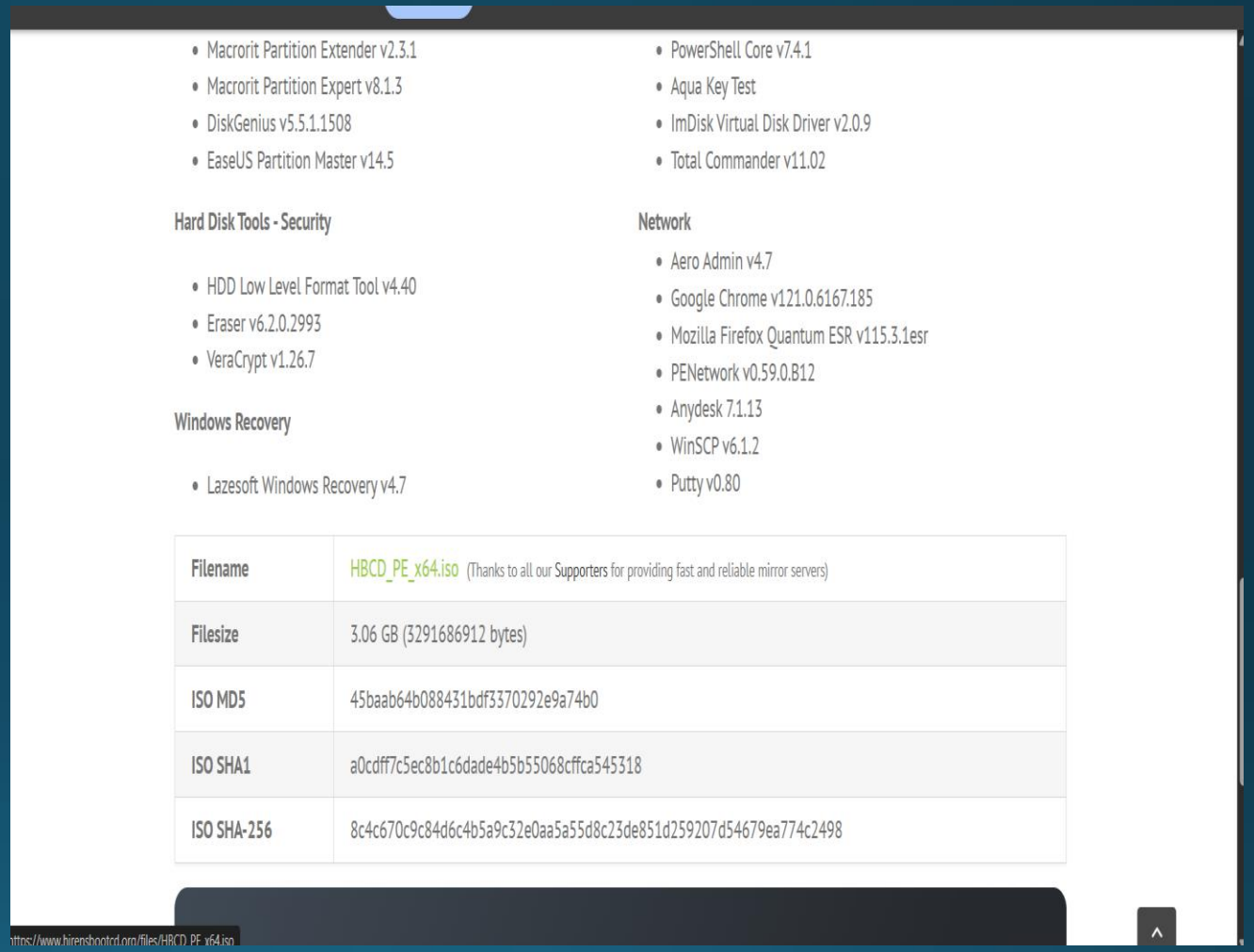


# WHAT IS BOOTABLE DRIVE?

A bootable drive contains operating system files that allow system to start independently from external storage. It bypasses the installed operating system and loads a separate working environment.

# About Hiren BootCD

Hiren BootCD is a recovery troubleshooting toolkit that provides access to system utilities, password reset tools, and disk management features.



- Macrorit Partition Extender v2.3.1
- Macrorit Partition Expert v8.1.3
- DiskGenius v5.5.1.1508
- EaseUS Partition Master v14.5

**Hard Disk Tools - Security**

- HDD Low Level Format Tool v4.40
- Eraser v6.2.0.2993
- VeraCrypt v1.26.7

**Windows Recovery**

- Lazesoft Windows Recovery v4.7

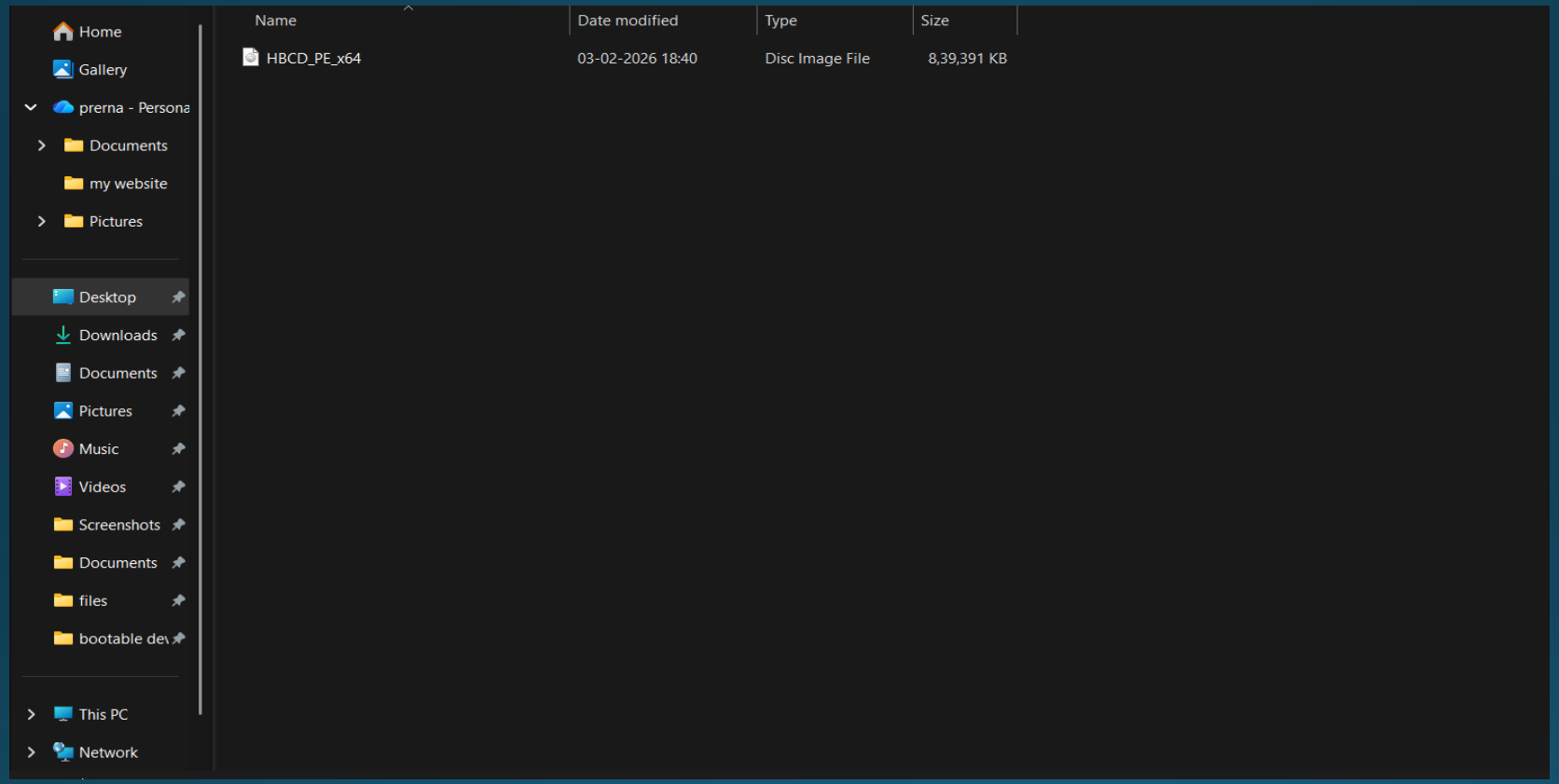
- PowerShell Core v7.4.1
- Aqua Key Test
- ImDisk Virtual Disk Driver v2.0.9
- Total Commander v11.02

**Network**

- Aero Admin v4.7
- Google Chrome v121.0.6167.185
- Mozilla Firefox Quantum ESR v115.3.1esr
- PENetwork v0.59.0.B12
- Anydesk 7.1.13
- WinSCP v6.1.2
- Putty v0.80

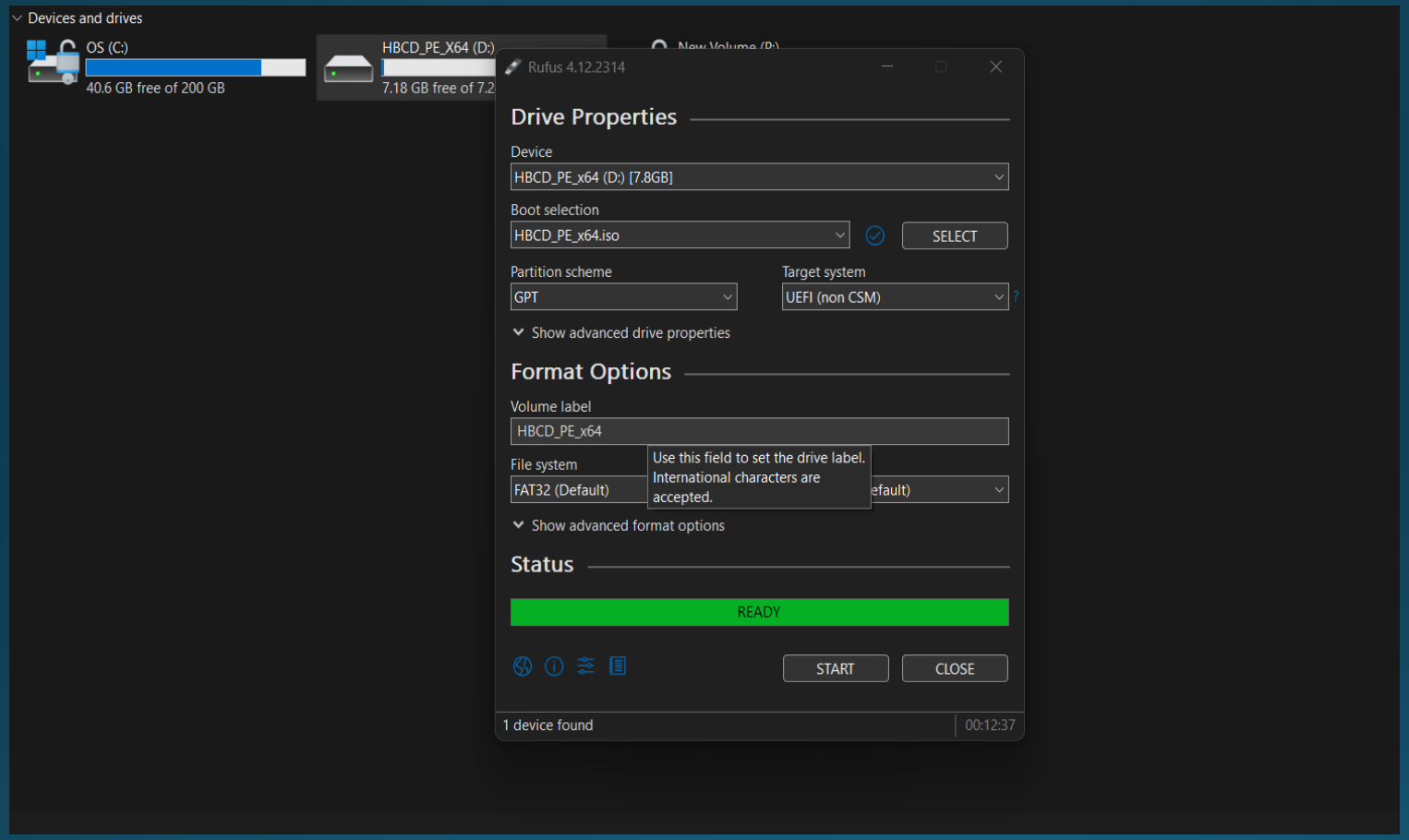
| | |
|---|---|
| **Filename** | HBCD_PE_x64.iso (Thanks to all our Supporters for providing fast and reliable mirror servers) |
| **Filesize** | 3.06 GB (3291686912 bytes) |
| **ISO MD5** | 45baab64b088431bdf3370292e9a74b0 |
| **ISO SHA1** | a0cdff7c5ec8b1c6dade4b5b55068cffca545318 |
| **ISO SHA-256** | 8c4c670c9c84d6c4b5a9c32e0aa5a55d8c23de851d259207d54679ea774c2498 |

# Step 1 : Downloading Hiren BootCD



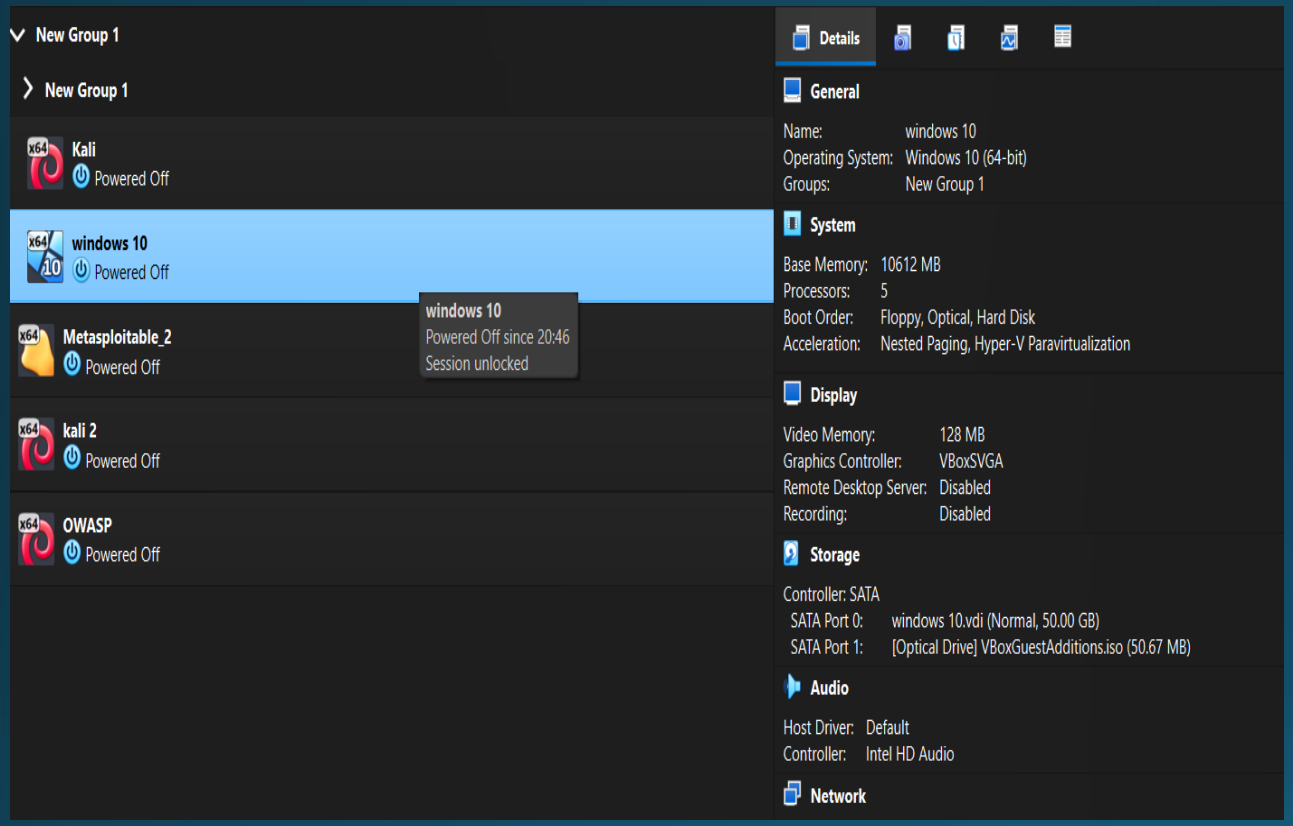

The Hiren BootCD ISO file was downloaded from the official website to ensure authenticity and security.

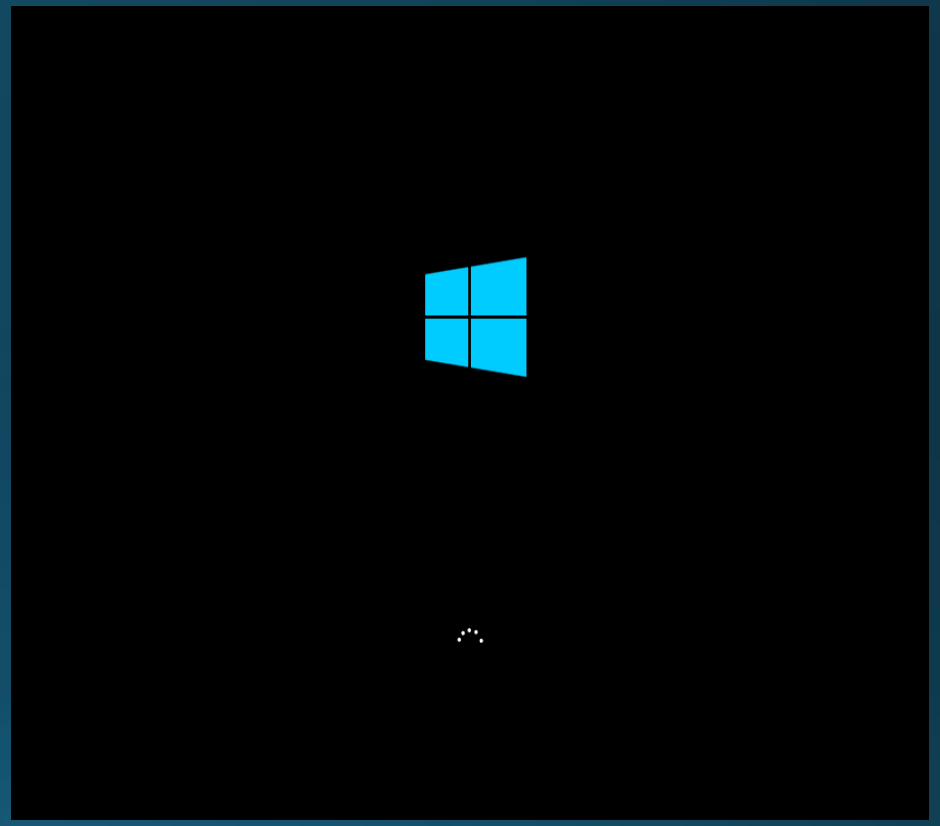
# Step 2 : Creating Bootable Drive




The ISO file was transferred to a USB drive using bootable creation tools (rufus) allowing the USB to function as a bootable device.

# Step 3 : Setting Up Virtual Lab



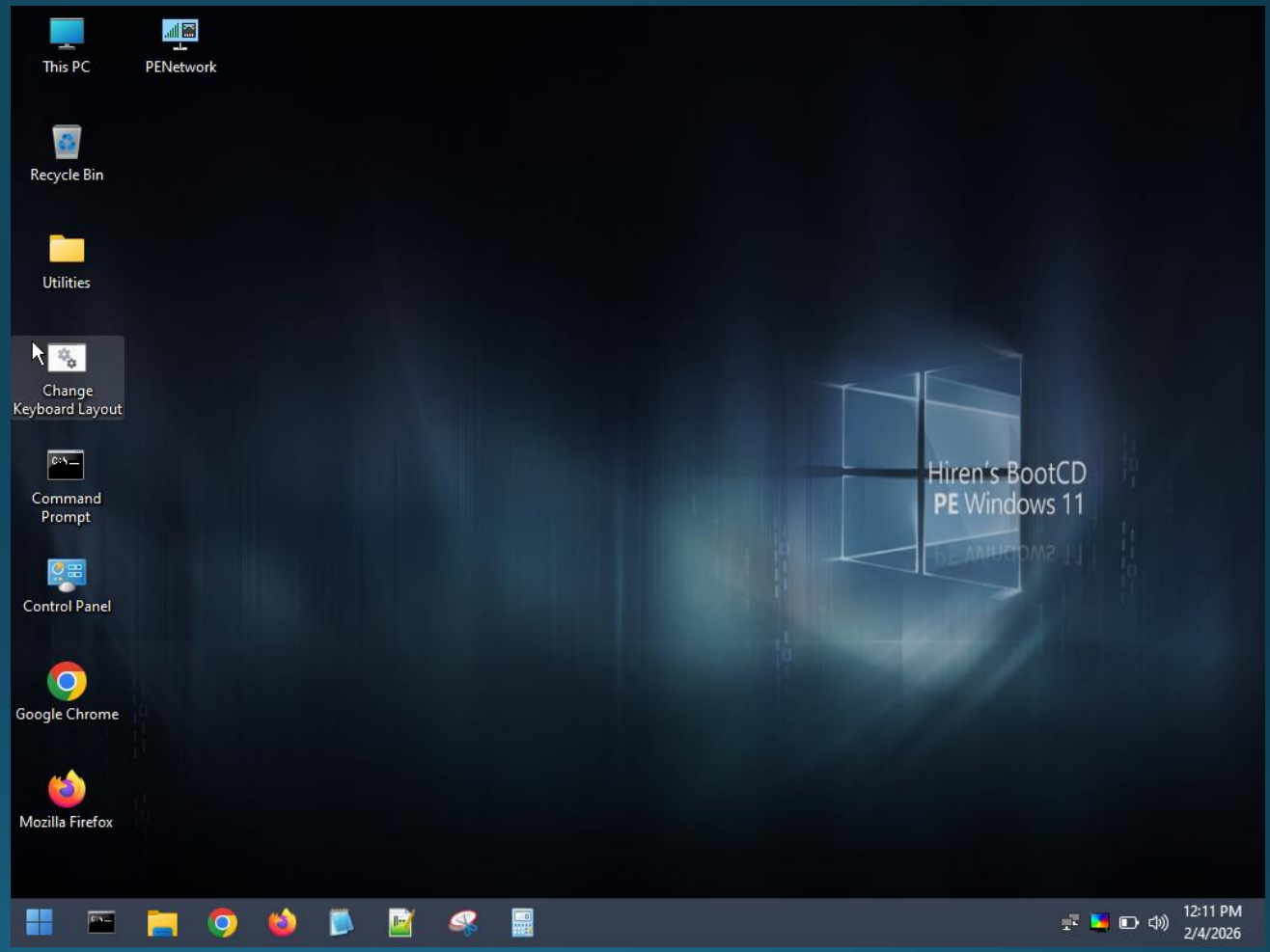



A Windows 10 virtual machine was created to safely test bootable drive access without affecting the main system.

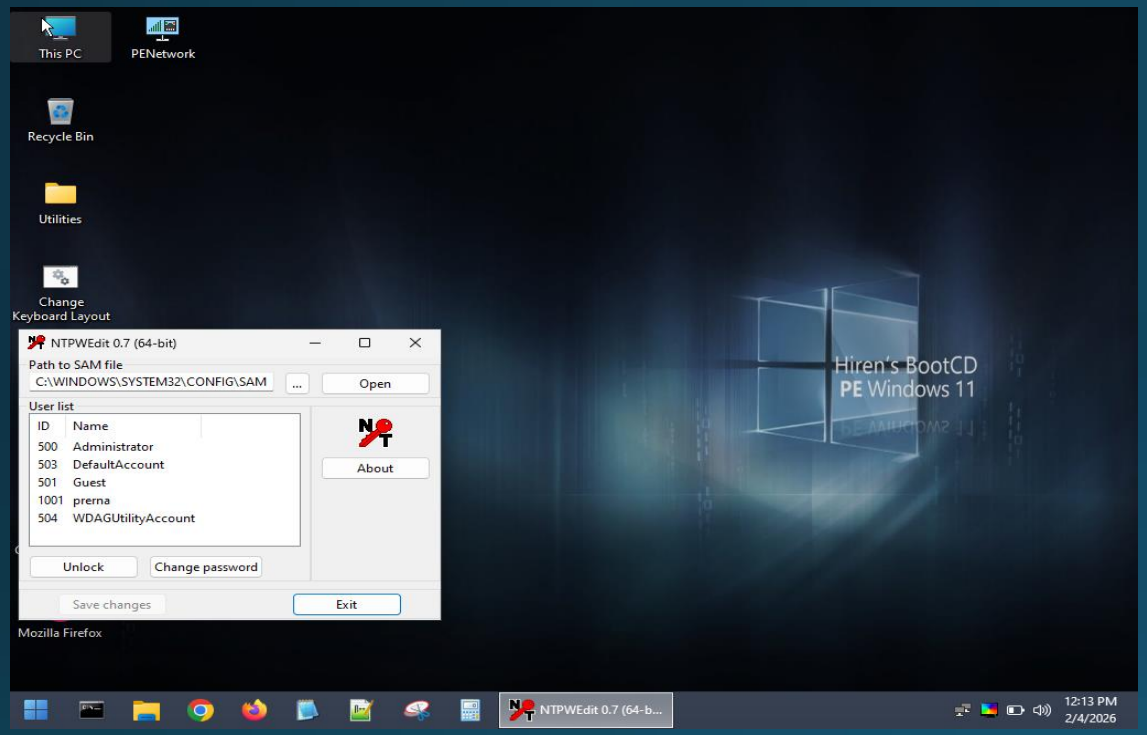
# Step 4 :Booting Hiren Enviornment

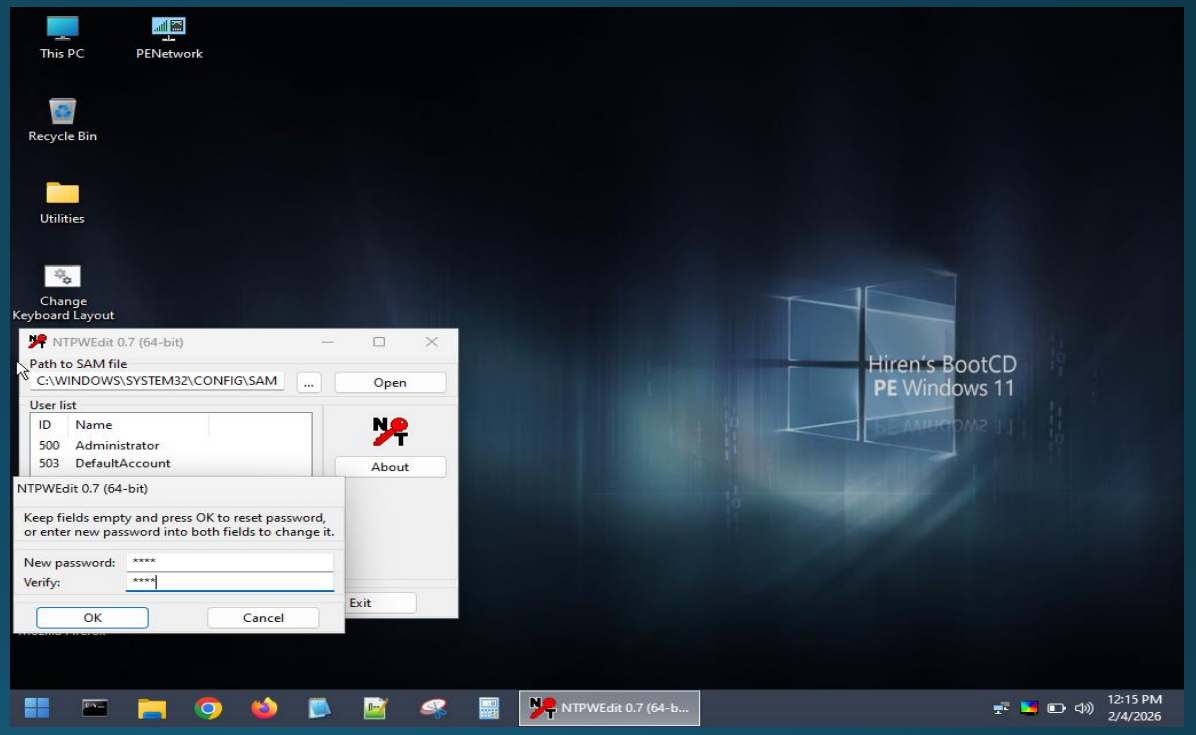
The virtual machine was started to perform testing.

- Bootable environment was loaded in the testing virtual lab setup.
- Hiren BootCD interface was successfully launched.
- The external boot environment allowed access to system recovery and password reset tools.



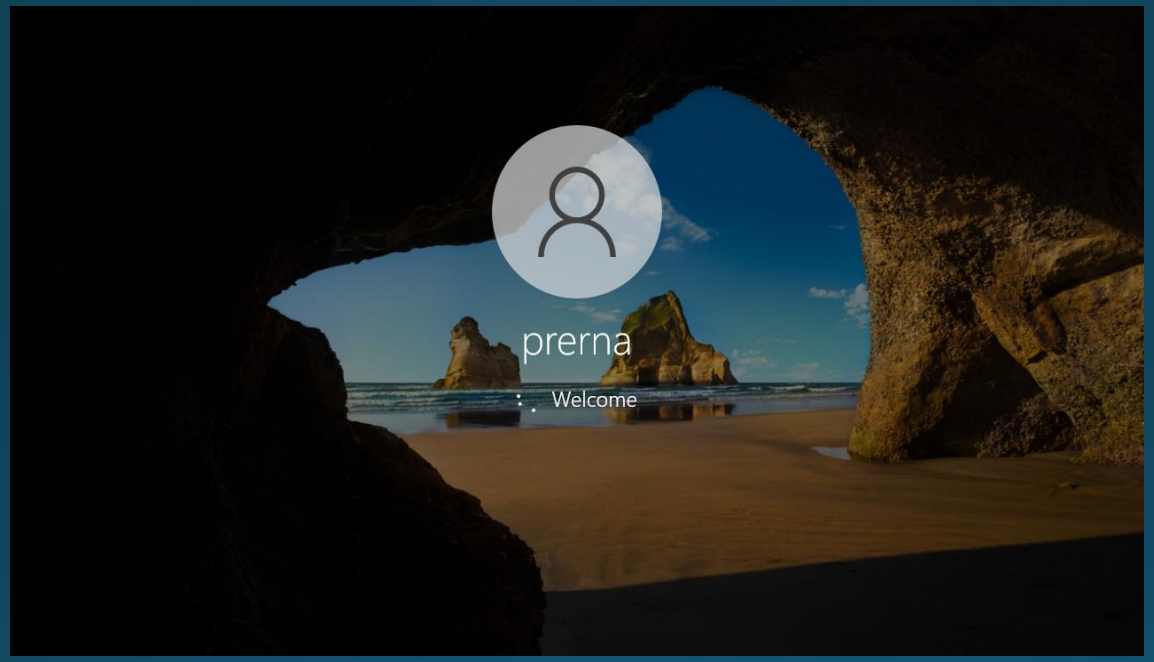
# Step 5: Password Reset Demonstration




Using Hiren Boot tools, the Windows login password was reset demonstrating how external boot environments can bypass system authentication.

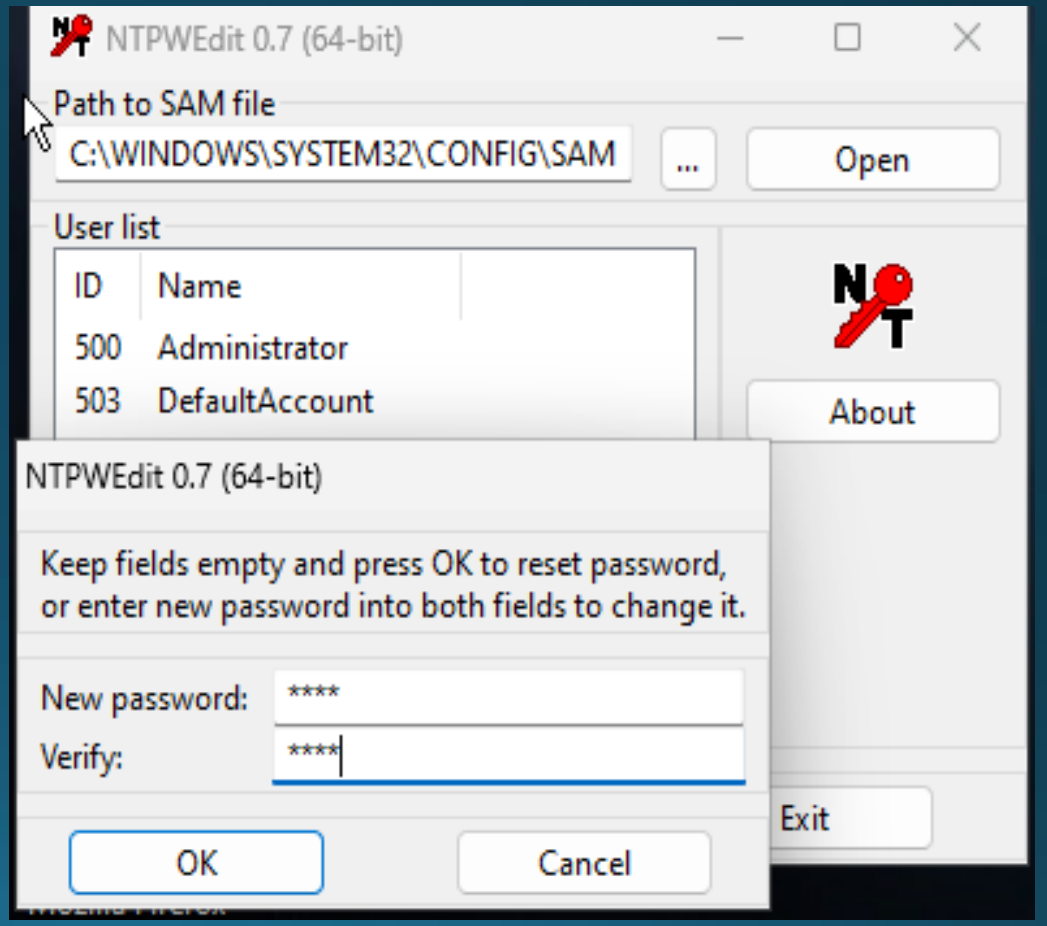
# Step 6 : System Access Verification




After resetting the password, the system was restarted and successfully accessed using the newly created password.

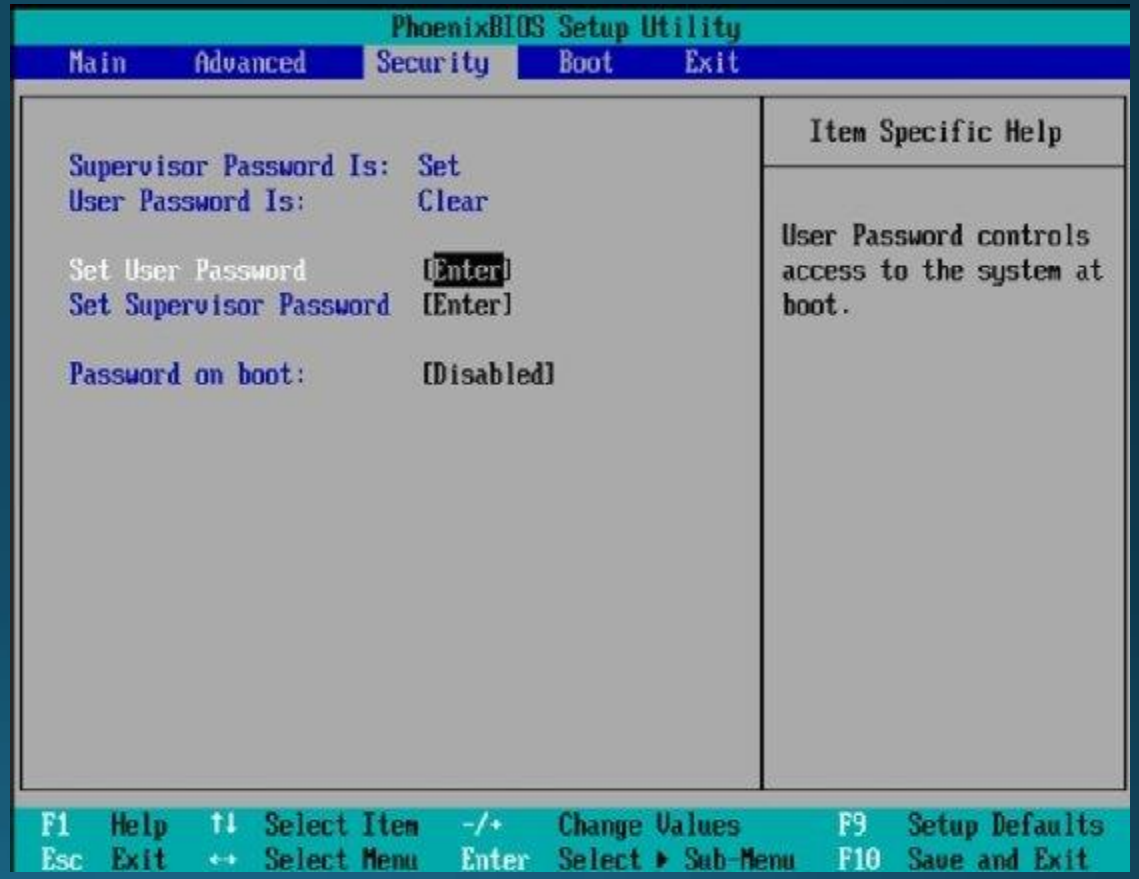
# Security Risks Identified

- Unauthorized system access
- Password bypass possibility
- Data exposure risk
- Physical security vulnerability



# Prevention Techniques

- BIOS password protection
- Secure Boot enable
- Disable external boot devices
- Disk encryption (BitLocker)



# CONCLUSION

Bootable drives provide powerful system recovery and testing

capabilities. However, they can also bypass system security.

Proper preventive measures must be implemented to protect

systems from unauthorized access.