

**COURSE: OPERATING SYSTEM (SE102L)**

**PROGRAM:   
BS CYBER SECURITY   
SEMESTER:  
4TH  
BATCH:  
2023-SPRING  
DEPARTMENT:   
SOFTWARE ENGINEERING  
  
SUBMITTED BY:**MEMBER#1: **SAIRA GUL 2023s-BCYS-008**

MEMBER#2: **ZAINAB ARIF 2023s-BCYS-028  
  
  
SUBMITTED TO:**INSTRUCTOR**: MUHAMMAD WAQAR**

https://www.linkedin.com/in/zainabaarif?utm\_source=share&utm\_campaign=share\_via&utm\_content=profile&utm\_medium=android\_app

**PROJECT TITLE:**  
**Windows Operating Systems: “Windows 7 Bypass"**



### Introduction to Windows 7 Bypass

Windows 7, released in 2009, is widely known for its user-friendly interface and functionality. However, it also has notable security vulnerabilities, particularly in its password and login management systems. These vulnerabilities can be exploited using tools like the Command Prompt (CMD), allowing unauthorized access to the system.

This project focuses on demonstrating a Windows 7 bypass technique using administrative CMD commands and highlights its implications for system security.

### ****Objective of the Experiment****

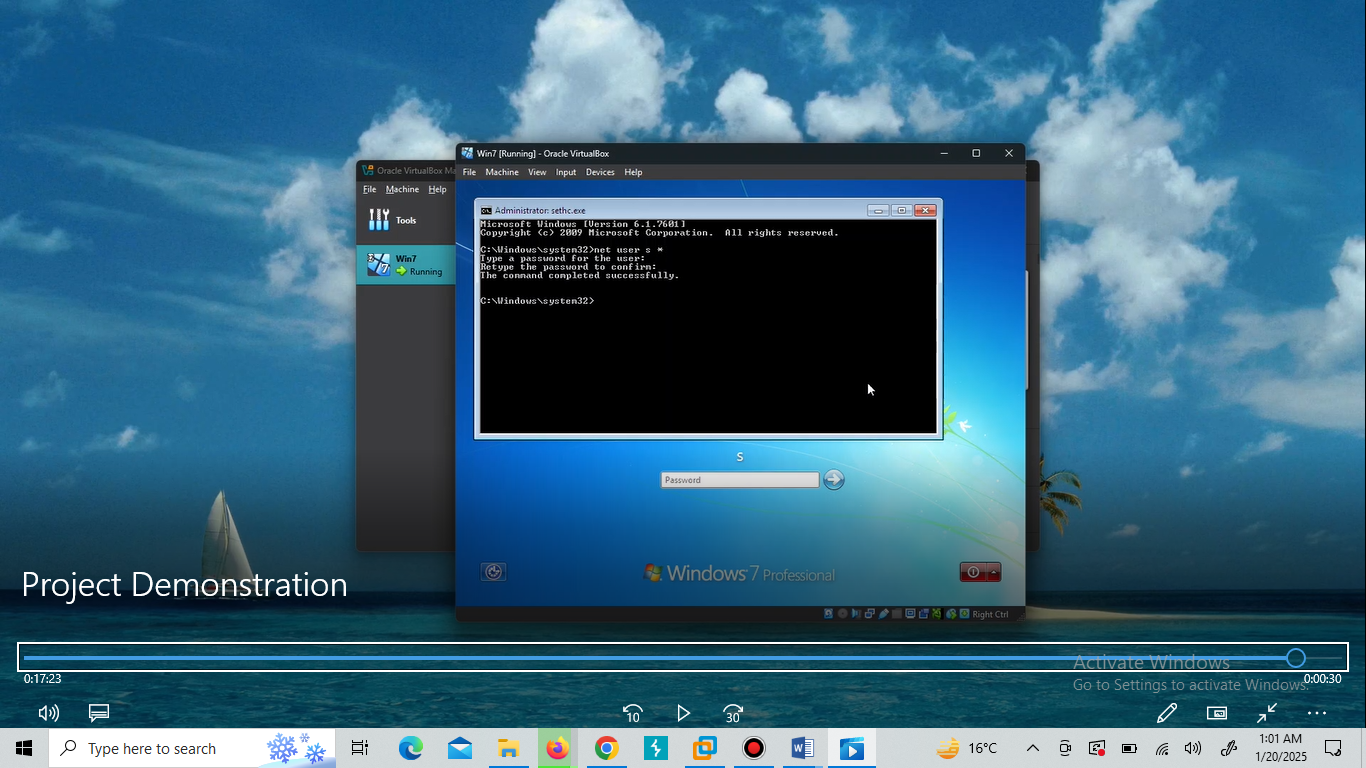
1. To demonstrate the Windows 7 password bypass process using CMD.
2. To analyze the security vulnerabilities exploited during the bypass.
3. To discuss recommendations for mitigating such vulnerabilities.

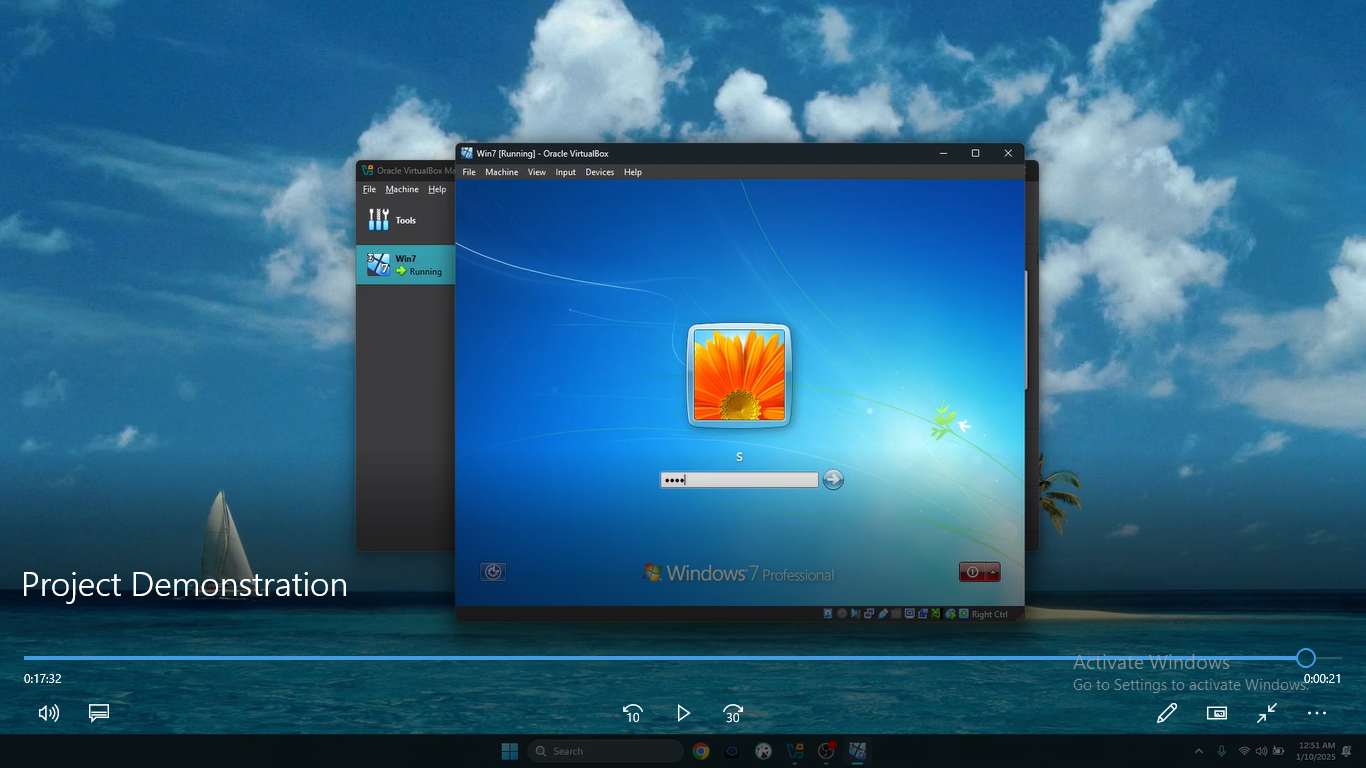
### ****Experiment Steps: Windows 7 Bypass****

#### **Setup**

1. Create an admin account and set a password unknown to others.
2. Goal: Reset admin password without knowing the original.

### ****Steps****

1. **Trigger Startup Repair**
   * Force shutdown during boot.
   * Select **Launch Startup Repair** when prompted.
2. **Access File Explorer**
   * Wait for diagnostics.
   * Click **View Problem Details** → Open file via Notepad → Access file explorer.
3. **Modify Sticky Keys**
   * Go to C:\Windows\System32.
   * Rename **sethc.exe** to sethc\_backup.exe.
   * Copy **cmd.exe** and rename it as sethc.exe.
4. **Open Command Prompt**
   * Restart and press **Shift key 5 times** on the login screen.
   * Command Prompt will open.
5. **Reset Password**
   * Type: net user <username> \* → Set a new password.
   * Close Command Prompt. 
6. **Login and Restore Sticky Keys**

Login using the new password. 

* + Restore sethc.exe by renaming sethc\_backup.exe.

Observe how the system allows the password change without any additional security checks or notifications.  
  


### ****Analysis of Vulnerabilities****

* **No Authentication for CMD Access:** Administrative Command Prompt does not require additional authentication to execute critical commands.
* **Weak Security Policies:** Windows 7 lacks robust mechanisms to prevent unauthorized password changes, making it susceptible to internal threats.
* **No Monitoring or Alerts:** Password changes via CMD are not logged or monitored, leaving system administrators unaware of potential breaches.

### ****Recommendations****

1. **Upgrade to Modern Operating Systems:** Transition to Windows 10 or later versions, which include advanced security policies and tools to prevent unauthorized access.
2. **Implement Two-Factor Authentication:** Add another layer of security to protect sensitive accounts from unauthorized changes.
3. **Restrict CMD Access:** Limit access to administrative tools like CMD to trusted users only.
4. **Enable Audit Logs:** Use system logging tools to monitor all administrative activities, including password changes.

### ****Conclusion****

The Windows 7 bypass experiment demonstrates significant vulnerabilities in its password management system. Exploiting these weaknesses can lead to unauthorized access, compromising system security.

Modern operating systems, such as Windows 10, have addressed these issues by incorporating stronger authentication mechanisms, CMD restrictions, and continuous updates. Users and organizations are encouraged to adopt secure practices and modern systems to mitigate risks and ensure data protection.

### ****Acknowledgments****

We thank our instructor, Muhammad Waqar, for his guidance and support throughout this project.

**CERTIFICATE COMPLETE WITH THIS COURSE:**   
  
