Name: Samarth Jain

USN: 4SU20CS081

Course: Cybersecurity

Trainer: Bharath Kumar

Date: 24/08/2023

Assignment Details

Assigned Date: 23/08/2023

Due Date: 24/08/2023

Topic: Exploitation (Gaining Access)

Introduction

Exploitation using Metasploit in Kali Linux is a pivotal technique in ethical hacking and penetration testing. Metasploit, a powerful open-source framework, empowers security professionals to identify vulnerabilities within systems and networks. By crafting and deploying exploit modules, analysts can assess an organization's defence mechanisms, aiding in the fortification of digital infrastructures. This introduction offers a glimpse into the dynamic realm of Metasploit-driven exploitation, enabling experts to proactively safeguard against potential cyber threats.

Content

Objectives

1. Create a text file with your name in Desktop of the Target machine
   Content: Name; USN number
2. Create a user with your name

Exploitation Steps/Phases

1. Find the vulnerabilities and record Vuln Name, Vuln Port Number, Vuln Code
2. Start & Initialize the Metasploit
3. Search & Import the Exploit script
4. Configure the script as per your target
5. Verify the details & execute

The Vulnerability to exploit

Name: 97833 - MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)

Description

Multiple remote code execution vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted packet, to execute arbitrary code. (CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148).

An information disclosure vulnerability exists in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit this, via a specially crafted packet, to disclose sensitive information. (CVE-2017-0147).

ETERNALBLUE, ETERNALCHAMPION, ETERNALROMANCE, and ETERNALSYNERGY are four of multiple Equation Group vulnerabilities and exploits disclosed on 2017/04/14 by a group known as the Shadow Brokers. WannaCry / WannaCrypt is a ransomware program utilizing the ETERNALBLUE exploit, and EternalRocks is a worm that utilizes seven Equation Group vulnerabilities. Petya is a ransomware program that first utilizes CVE-2017-0199, a vulnerability in Microsoft Office, and then spreads via ETERNALBLUE.

This module exploits the MS17-010 vulnerability in Windows systems, which is the vulnerability that was famously exploited by the **WannaCry ransomware**.

Solution

Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, 10, and 2016. Microsoft has also released emergency patches for Windows operating systems that are no longer supported, including Windows XP, 2003, and 8.

For unsupported Windows operating systems, e.g. Windows XP, Microsoft recommends that users discontinue the use of SMBv1. SMBv1 lacks security features that were included in later SMB versions. 10.0.2.4 11 SMBv1 can be disabled by following the vendor instructions provided in Microsoft KB2696547. Additionally, US-CERT recommends that users block SMB directly by blocking TCP port 445 on all network boundary devices. For SMB over the NetBIOS API, block TCP ports 137 / 139 and UDP ports 137 / 138 on all network boundary devices.

Risk factor: High

Vulnerability Port: 445

Vulnerability Code: CVE-2017-0143, MS17-010

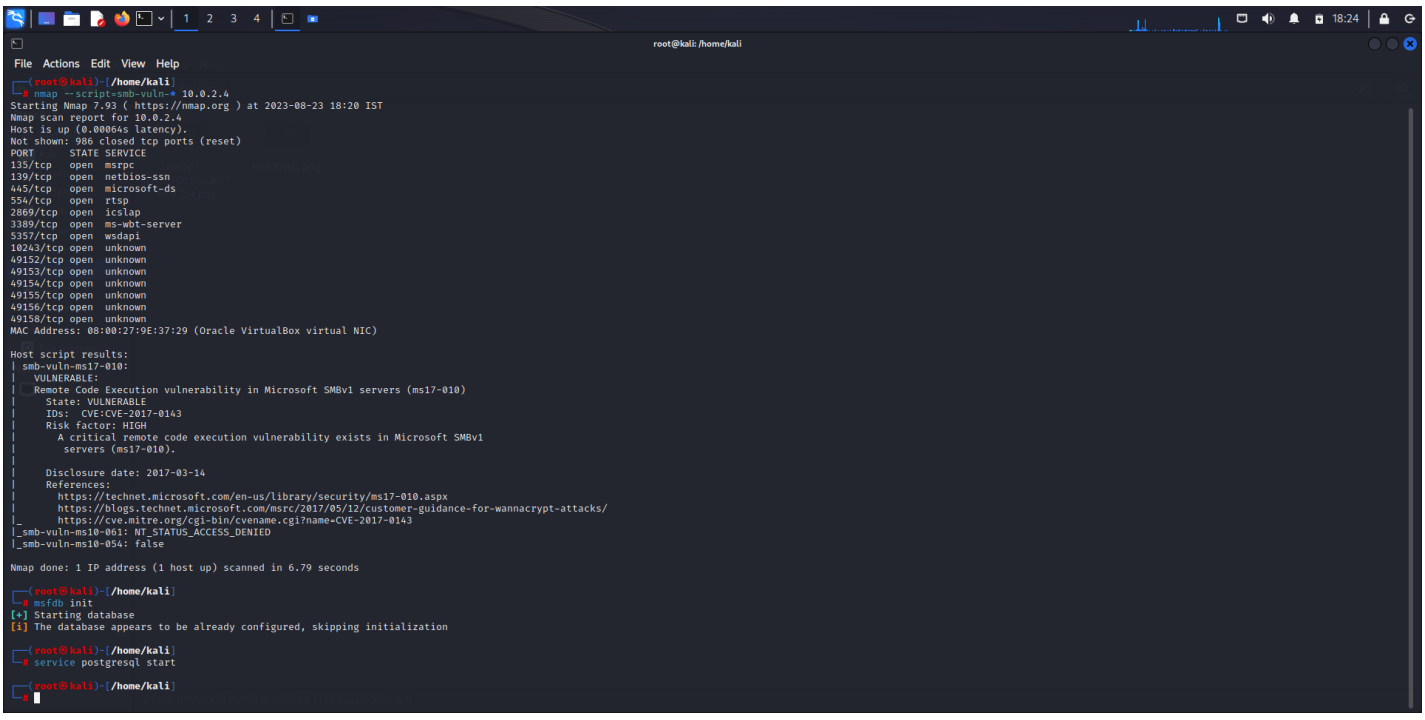
Exploitable with: CANVAS (true), Core Impact (true), Metasploit (true)

Steps to exploit the target machine and gain access

1. Command: #nmap –script=smb-vuln-* 10.0.2.4
   Syntax: #nmap –script=smb-vuln-* <Target IP address>
   Description:
   This is the **First phase of Exploitation**, that is Finding the Vulnerabilities.
   Vulnerability scanning if Nessus scan is not possible. Makes use of nmap tool.
   Note: It does provide a detailed analysis compared to Nessus tool.

2. Command: #msfdb init
   Description:
   This is the Second phase of Exploitation, that is Initialize the Metasploit database (Only written once)

3. Command: #service postresql start
   Description:
   PostgreSQL database server on a Linux-based system. PostgreSQL is a popular open-source relational database management system. To start the backend of the Metasploit.



4. Command: #msfconsole
   Description:
   Start Metasploit framework console, you'll access the command-line interface of the Metasploit Framework, which provides a variety of tools and modules for performing security assessments, vulnerability exploitation, and more.

5. Command: msf6> search 2017-0143
   Syntax: search <CVE code> or search <MS code> or search<Vuln Name>
   Description:
   This command should initiate a search within Metasploit's module database for any available modules related to the specified CVE identifier. If there are any relevant modules, the search results will be displayed, showing you the available exploits or auxiliary modules associated with that CVE.

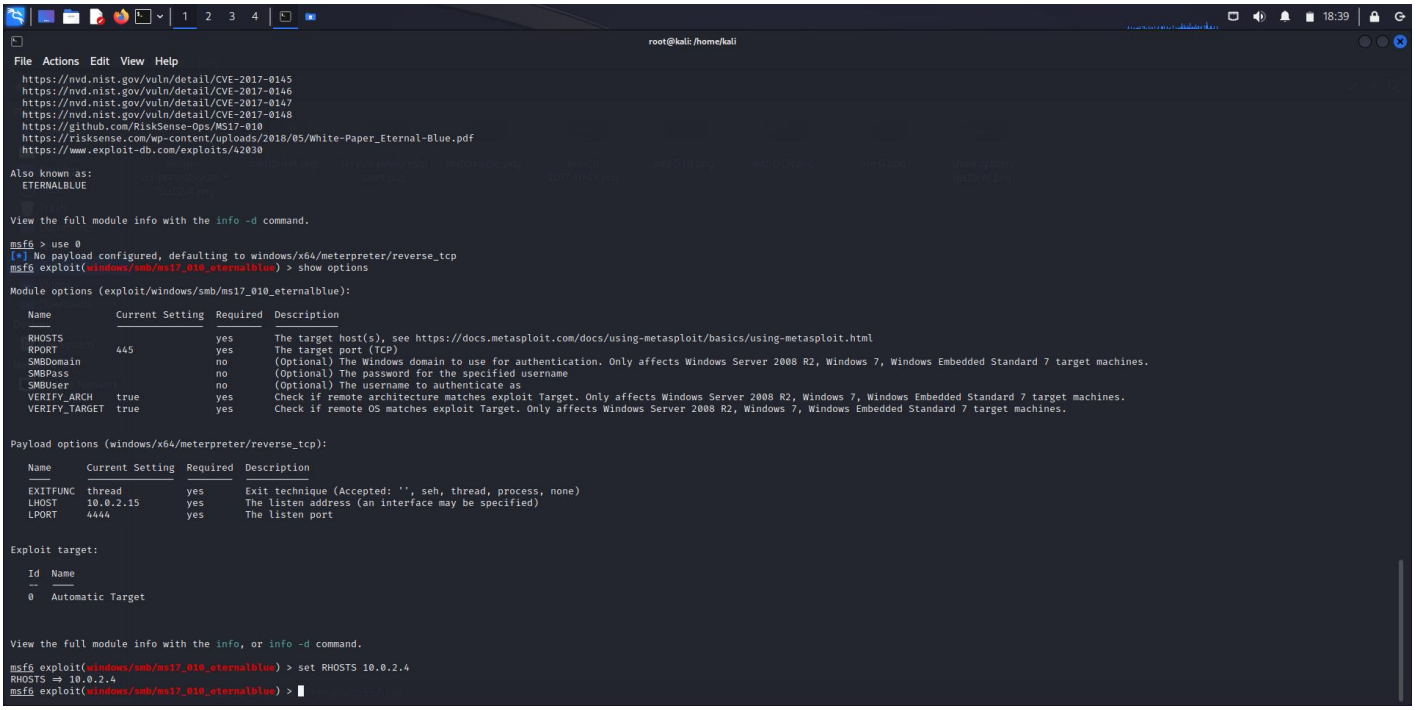
6. Command: msf6> info 0
   Syntax: info <id> or info <path>
   Description:
   Checks whether the script is compatible with the target (Platform, Architecture, Privilege). Finds the Available Targets and provides Basic Options. It used to display detailed information about a specific module. The module can be an exploit, auxiliary module, payload, or any other type of module available in Metasploit's module database.

7. Command: msf6> use 0
   Syntax: use <id>
   Description:
   This is the Third phase of Exploitation, that is Importing the Exploit Script.
   The use command is used to select a specific module from the Metasploit Framework's module database for further configuration and execution. The module index refers to the position of the module in the list of available modules. However, using just the module index might not be the most accurate way to select a module, as the indexes can change based on the state of the database.

8. Command: msf6 exploit(windows/smb/ms17_010_eternalblue) > show options
   Description:
   Checks the mandatory setting (Set Current Setting if Required: yes). The show options command is used to display the available configuration options for the selected module. These options allow you to customize the behavior of the exploit to suit your needs.
   Note: The below picture shows the options **BEFORE** setting the values.

9. Command: msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 10.0.2.4
   Syntax: set <option-name> <option-value/Current Setting value>
   Description:

In the context of Metasploit, RHOSTS stands for "Remote Hosts," and it is used to specify the IP address or IP range of the target system(s) you intend to exploit.



10. Command: msf6 exploit(windows/smb/ms17_010_eternalblue) > show options
    Note: The below picture shows the options **AFTER** setting the values.

11. Command: msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit
    Description:
    To execute the exploit. Executing the exploit command launches the selected module with the configured options. In this case, you're using the EternalBlue exploit module to attempt to exploit the MS17-010 vulnerability in Windows systems. If the exploit is successful, it may result in gaining unauthorized access to the target system.

12. Command: meterpreter> sysinfo
    Description: System information of the target computer. Command is using the Metasploit Framework's Meterpreter shell, which is a post-exploitation tool that allows you to interact with compromised systems after a successful exploit. The sysinfo command you've used is used to display system information about the compromised host.

13. Command: meterpreter> ifconfig
    Description:

In Metasploit's Meterpreter shell, the ifconfig command is used to display network interface information of the compromised system.

14. <u>Command</u>: meterpreter> getuid
<u>Description</u>:
Gives the UserID with which you have accessed. The getuid command in the Metasploit Framework's Meterpreter shell is used to retrieve information about the user privileges of the current session. It displays details about the user's identity, including their username, domain, and user ID (UID).

15. <u>Description</u>:

Entering the Desktop of the Target machine using a sequence of instructions through the meterpreter instructions like pwd(Present Working Directory), cd (Change Directory), ls (List of Files in pwd).

16. Command: meterpreter> shell
    Description:
    The shell command in Metasploit's Meterpreter shell is used to open a separate native shell on the compromised system. This command allows you to interact with the system as if you were using a regular command prompt or shell directly on the target.

17. Description
    With a sequence of commands create a file and fill the necessary information. Type the command as if you were accessing the native Command Prompt of the target machine.
    Command: C:\Users\windows7\Desktop> echo Name: Samarth Jain >> samarth.txt

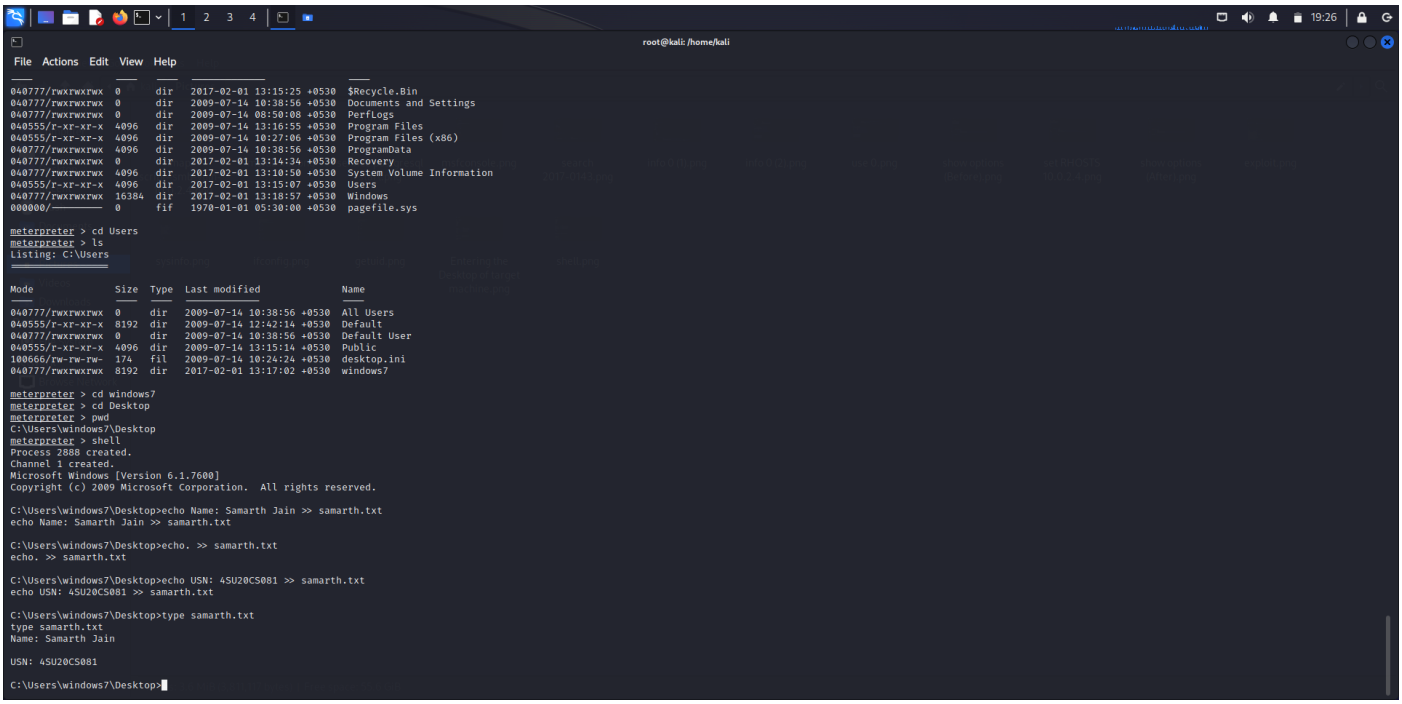
//Creates a file named “Samarth.txt” and stores the value typed.

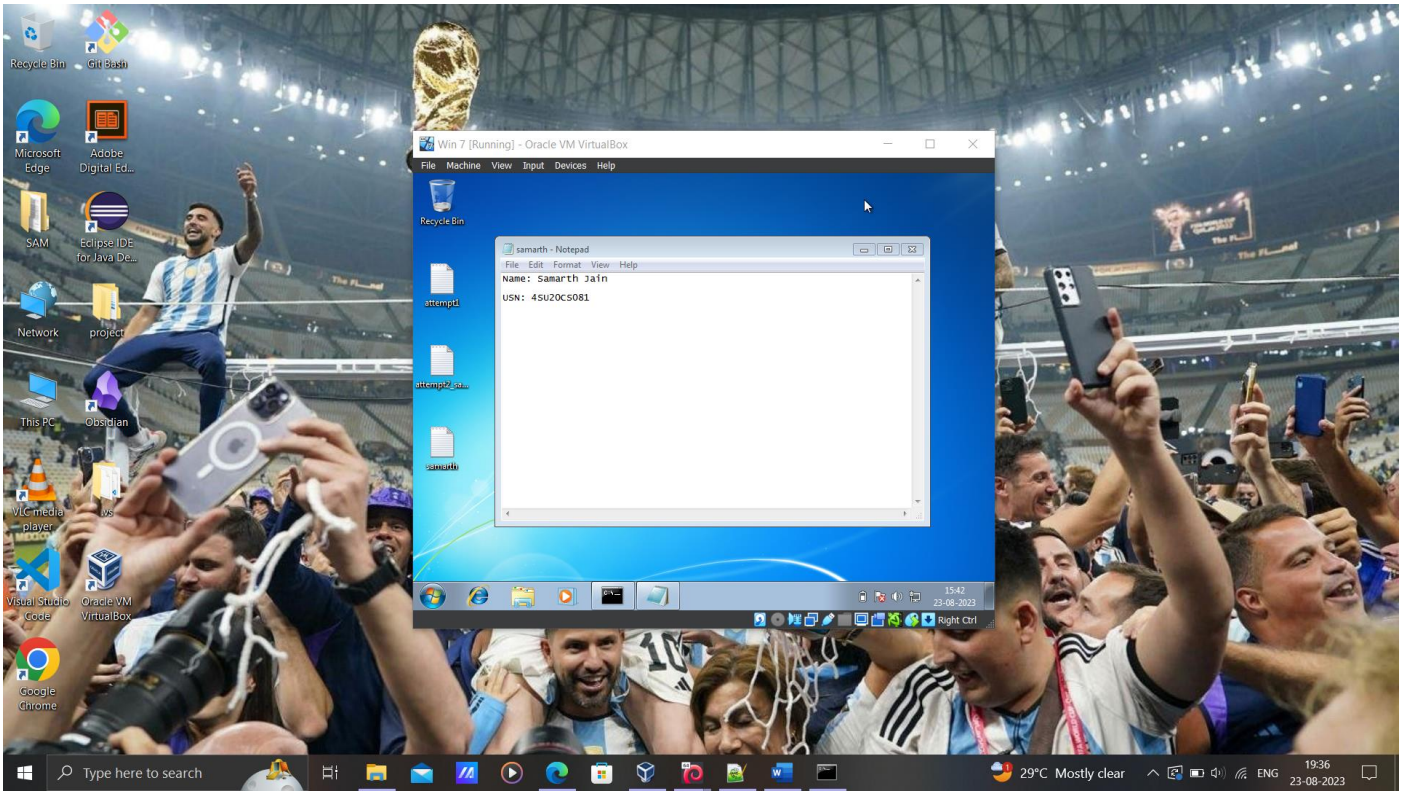
Command: C:\Users\windows7\Desktop> echo. >> samarth.txt

//Creates a newline

Command: C:\Users\windows7\Desktop> echo USN: 4SU20CS081 >> samarth.txt

//Appends the text onto the file samarth.txt





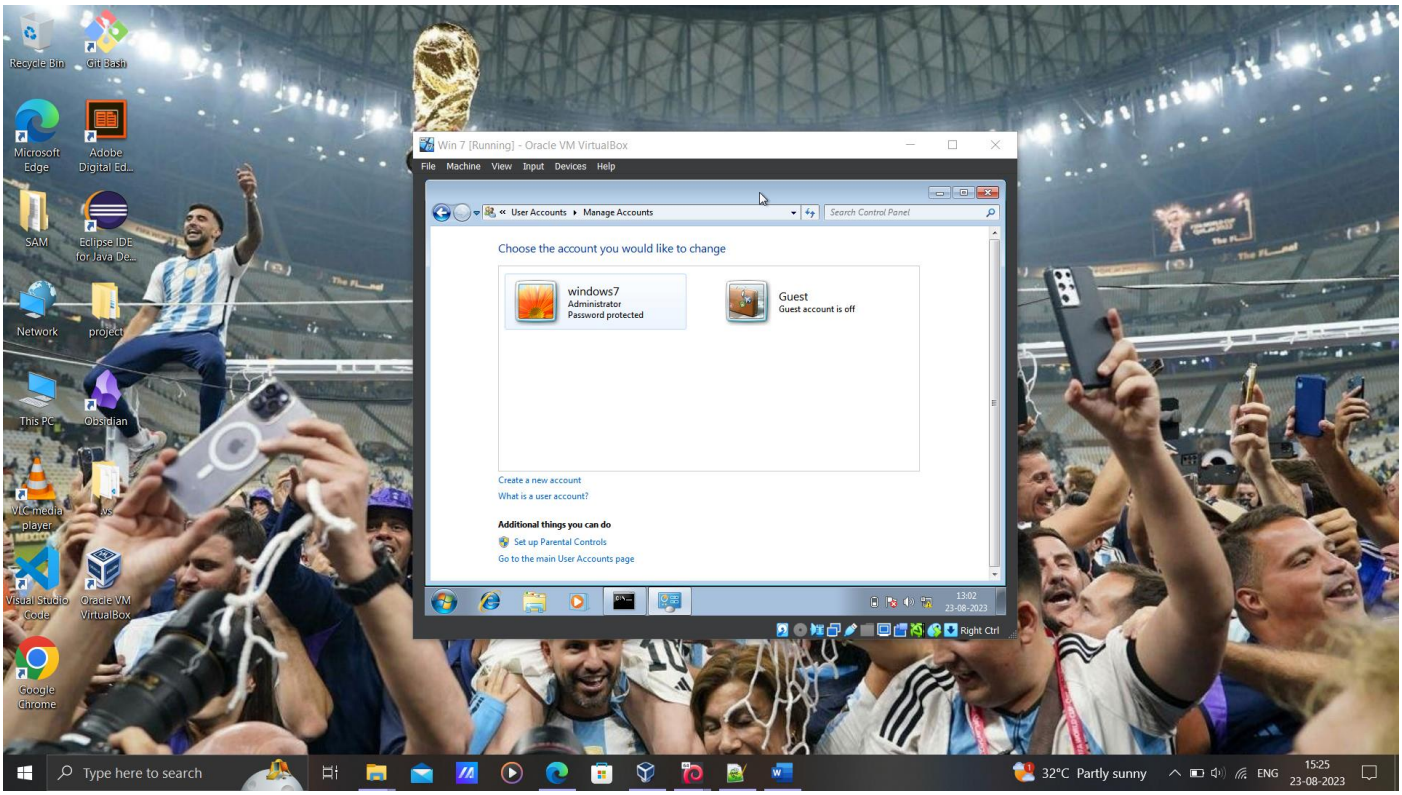
First Objective of the Assignment is Complete.

18. Command: C:\Users\windows7\Desktop> net user Samarth mudryk10 /add

    Syntax: net user <Username> <Password> /add

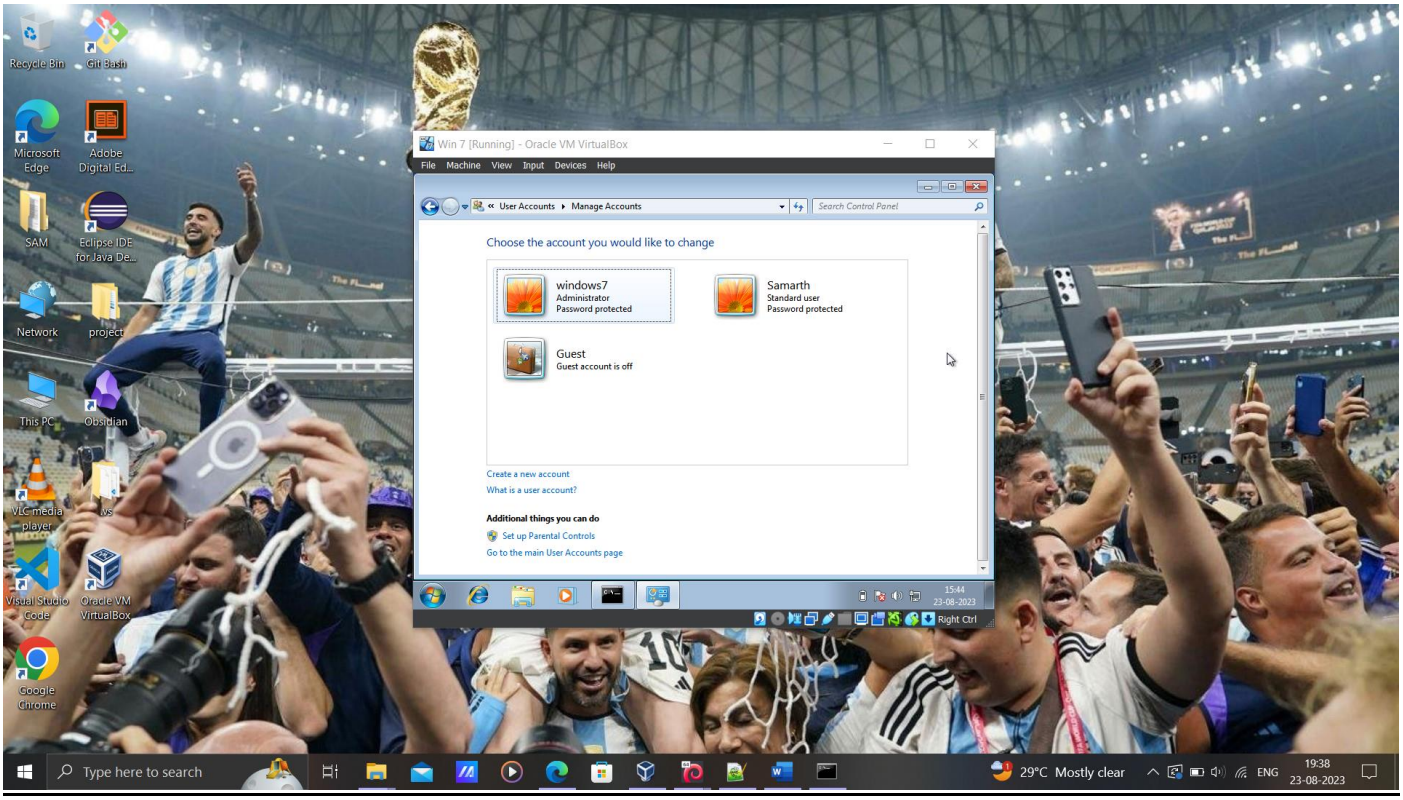
    Description:

The command provided, net user username password /add, is used to add a new user to the Windows system using the "net user" command.



The above figure shows the Users present in the target machine **BEFORE** the command is executed.

The below figure shows the Users present in the target machine **AFTER** the command is executed.



Second Objective of the Assignment is Complete.

Analysis

The report aims to analyze the execution of two specific objectives. Firstly, it involves the creation of a text file containing personal information, including the name and USN number, to be placed on the Desktop of the Target machine.

Conclusion

In conclusion, the undertaken tasks have provided valuable insights into file manipulation and user administration on the target machine. The successful creation of a personalized text file on the Desktop demonstrates proficiency in managing file systems programmatically. Additionally, the establishment of a user account with the same name underscores the control over user management aspects. These achievements collectively highlight the practical application of system-level commands and contribute to a deeper comprehension of system operations.