POC TASK

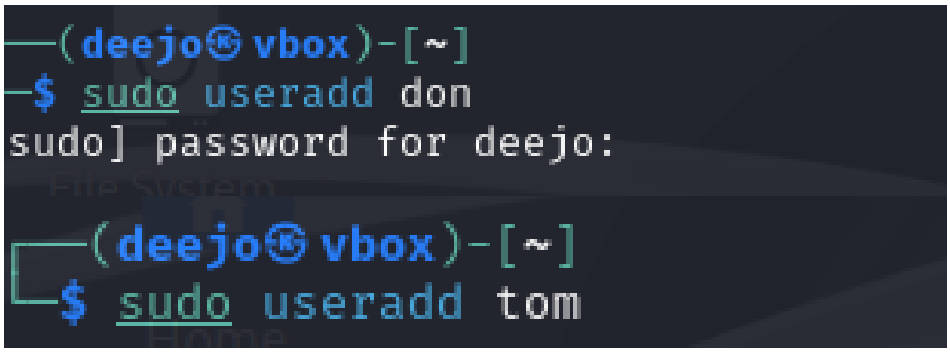
DHIRSSHIN.J

ADS - A

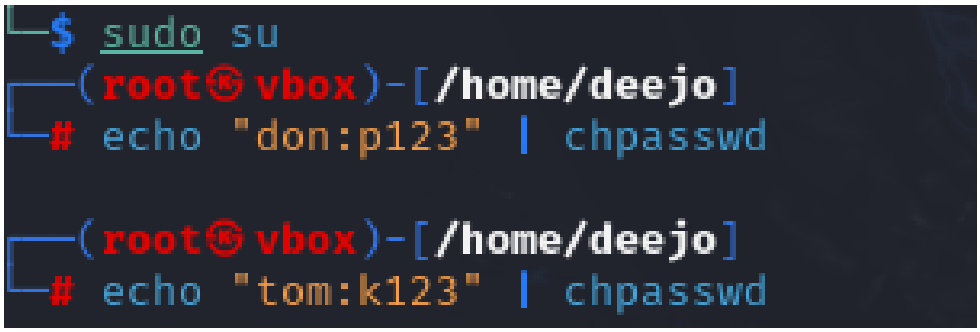
POC Task-1

1.Setup: Creating Users & Assigning Weak Permissions

Create a user: sudo useradd <username>

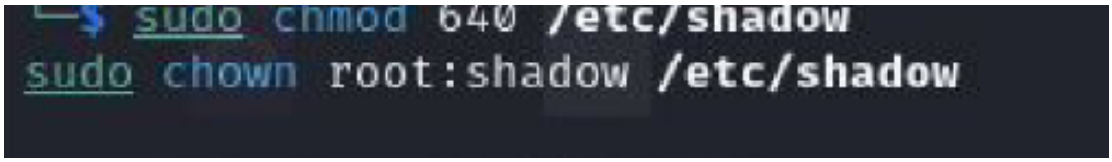


Set password: echo "user:pass" | sudo chpasswd



To ensure security, we must check file permissions, especially for sensitive files like /etc/shadow.Modifying its permissions to allow full access can expose passwords:

We examine the permissions of the password file to identify and exploit any misconfigurations.. We secure the password file by setting its permissions to 640 using the chmod command. This ensures that only the root user and members of the shadow group can access it. The root user's password remains viewable only under superuser privileges



Summary Of Steps

Step	Action	Command	
1	Create users	`useradd hacker` and `useradd victim`	
2	Set passwords	`echo "hacker:password123"	chpasswd`	
3	Misconfigure file permissions	`chmod 777 /etc/shadow`	
4	Verify file permissions	`ls -l /etc/shadow`	
5	Exploit as a low-privileged user	`su hacker` then `cat /etc/shadow`	
6	Fix file permissions	`chmod 640 /etc/shadow`	
7	Fix ownership	`chown root:shadow /etc/shadow`	
8	Restrict sudo access	`visudo`	