Team OM3N Boot2Root Write-Up

1. Chain Of Hacking

Goal: Gain root access and retrieve the flag

Steps Of Flag Retrieval:

1. Attach the b2r .vdi to a Kali VM as a **secondary disk** and mount it.
   lsblk
   sudo mount /dev/sdb1 /mnt/b2r
2. Searched for string “flag” using grep and found flag.txt in root folder
3. sudo cat /mnt/b2r/root/flag.txt
4. Flag – Obtained - SECE{ch41n_th3_m1st4k3s_n0t_c0mm4nds}

2. Tar-Pit

Goal: Gain root access and retrieve the flag

Steps Of Flag Retrieval:

1. Attach the b2r .vdi to a Kali VM as a **secondary disk** and mount it.
   sudo mount -o ro /dev/sdb2 /mnt/b2r
2. Searched for string “flag” using grep and found flag.txt in root folder
3. sudo cat /mnt/b2r/root/flag.txt
4. Flag – Obtained – SECE{b2r_sudo_tar_pwned}

3. Simplistic

Goal: Gain root access and retrieve the flag

Steps Of Flag Retrieval:

1. Attach the b2r .vdi to a Kali VM as a **secondary disk** and mount it.
   sudo mount -o ro /dev/ubuntu-vg/ubuntu-lv /mnt/lvmroot
2. Searched for files in root folder and found “root.txt”
3. sudo cat /mnt/b2r/root/root.txt
4. Flag – Obtained - SECE{r00t_v14_su1d_f1nd}

4. CyberSec

Same Method Used as Above Problems. Flag - SECE{Pyth0n_L1b_H1j4ck_1s_P0w3rful!}

5. Shadow Backup

Same Method Used as Above Problems. Flag - SECE{sudo_secure_path_is_not_your_friend}

6. Silent Trust

Goal: Gain root access and retrieve the flag

Steps Of Retrival:

1. Attach the b2r .vdi to a Kali VM as a **secondary disk** and mount it.
   sudo mount -o ro /dev/sdb1 /mnt/ghost
2. Seaeched for flag - sudo find /mnt/ghost -type f -iname '*flag*'
3. Found root.flag (Tried But Asked For More). Another User.flag (hidden inside CI cache)
4. sudo cat /mnt/ghost/home/devops/.cache/.ci/user.flag
5. Flag – Obtained - SECE{trust_is_the_first_vulnerability}