Detailed Steps to Solve the Machine

Machine Information

Macro: Sudo
Type: Weak user password with sudo power
Description: The machine has a user account with a weak password that can be cracked, and this user has sudo privileges, allowing escalation to root access.

Objective

The goal is to gain root access to the target machine and retrieve the flag located at /root/flag.

Step-by-Step Process

Step 1: Network Discovery with Nmap

Command: nmap -sn 192.168.1.0/24

Description:

- **Purpose: Perform a ping scan to identify live hosts on the 192.168.1.0/24 subnet.**
- **Details:**
    - **The command is executed from a machine with IP 192.168.0.5.**
    - **nmap -sn performs a host discovery scan (ping scan) without port scanning, checking which IP addresses in the 192.168.1.0/24 range (256 addresses) are active.**
    - **This step helps identify the target machine's IP address within the network.**
- **Assumption: The scan reveals that 192.168.1.0 (or a specific IP in the range) is a live host, which we'll target in subsequent steps.**
- **Output: A list of active IP addresses, including the target machine.**

Step 2: Service Scanning with Nmap

Command: nmap -sV 192.168.1.0

Description:

- **Purpose: Identify open ports and services running on the target machine (192.168.1.0).**
- **Details:**
    - **nmap -sV performs a service version scan, detecting open ports and the software versions running on them.**
    - **Executed from 192.168.0.5, targeting the IP 192.168.1.0.**
    - **This step is critical to identify services like SSH, which is implied as the attack vector based on later commands.**
- **Assumption: The scan reveals that port 22 (SSH) is open, running a version of OpenSSH.**
- **Output: A report listing open ports, with port 22 (SSH) confirmed as a potential entry point.**

Step 3: Password Cracking with Hydra

Command: hydra -l student -P /usr/share/wordlists/rockyou.txt.gz ssh://192.168.1.0

Description:

- **Purpose: Perform a brute-force attack to crack the SSH password for the user student on 192.168.1.0.**
- **Details:**
    - **hydra is a password-cracking tool used to attempt SSH logins.**
    - **-l student specifies the username student.**
    - **-P /usr/share/wordlists/rockyou.txt.gz uses the rockyou.txt wordlist, a common list of leaked passwords, to guess the password.**
    - **The target is the SSH service on 192.168.1.0.**
    - **This aligns with the machine's description of a "weak user password."**
- **Assumption: Hydra successfully cracks the password, revealing password as the credentials for the student account.**

- **Output: The cracked credentials: student:password.**

Step 4: SSH Login

Command: ssh student@192.168.1.0 -p 22

Description:

- **Purpose: Establish an SSH connection to the target machine using the cracked credentials.**
- **Details:**
    - **Connect to 192.168.1.0 on port 22 (default SSH port).**
    - **Use the username student and password password.**
    - **This grants access to the student account on the target machine.**
- **Assumption: The SSH connection is successful, providing a shell as the student user.**
- **Output: An active SSH session on the target machine.**

Step 5: Check Sudo Privileges

Command: sudo -l

Description:

- **Purpose: List the sudo privileges available to the student user.**
- **Details:**
    - **sudo -l displays the commands the student user can run with elevated privileges.**
    - **Executed on the target machine (192.168.1.0) via the SSH session.**
    - **This step confirms the machine's "sudo power" characteristic.**
- **Assumption: The output shows that student can run commands as root (e.g., (ALL) ALL or specific commands without a password).**
- **Output: A list of sudo permissions, confirming root-level access is possible.**

Step 6: Escalate to Root

Command: sudo -i

Description:

- **Purpose: Gain a root shell by leveraging the student user's sudo privileges.**
- **Details:**
  - **sudo -i starts an interactive root shell.**
  - **Based on the previous step, student has sufficient sudo privileges to execute this command.**
  - **This escalates the session from the student user to the root user.**
- **Assumption: The command succeeds, granting a root shell.**
- **Output: A root prompt (root@machine).**

Step 7: Retrieve the Flag

Command: cat /root/flag

Description:

- **Purpose: Read the contents of the flag file located at /root/flag.**
- **Details:**
  - **cat /root/flag displays the contents of the flag file.**
  - **Executed in the root shell on 192.168.1.0.**
  - **The flag is the final objective of the machine.**
- **Output: The flag: Ey8C7gOdzaKxTNqp.**