Detailed Steps to Solve the Machine

Machine Information

Macro: File Permissions
Type: Shadow with world-writable permissions
Description: The machine has a /etc/shadow file with world-writable permissions, allowing any user to modify it. This can be exploited to change the root password and gain 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 192.168.1.1 is a live host, which we'll target in subsequent steps.
- **Output**: A list of active IP addresses, including the target machine at 192.168.1.1.

Step 2: Service Scanning with Nmap

Command: nmap -sV 192.168.1.1

Description:

- **Purpose**: Identify open ports and services running on the target machine (192.168.1.1).
- **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 192.168.1.1.
    - 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://192.168.1.1

Description:

- **Purpose**: Perform a brute-force attack to crack the SSH password for the user student on 192.168.1.1.
- **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 192.168.1.1.
    - This step aligns with the need to gain initial access to the machine.
- **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@192.168.1.1 -p 22

Description:

- **Purpose**: Establish an SSH connection to the target machine using the cracked credentials.
- **Details**:
    - Connect to 192.168.1.1 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 File Permissions

Command: ls -la /etc

Description:

- **Purpose**: List the files and their permissions in the /etc directory to identify if /etc/shadow has world-writable permissions.
- **Details**:
    - ls -la displays detailed file information, including permissions, for all files in /etc.
    - Executed on the target machine (192.168.1.1) via the SSH session.
    - This step confirms the machine's "shadow with world-writable permissions" characteristic.
- **Assumption**: The output shows that /etc/shadow has permissions like rw-rw-rw- (world-writable).

- **Output**: A list of files in /etc, with /etc/shadow showing world-writable permissions.

Step 6: Read the Shadow File

Command: cat /etc/shadow

Description:

- **Purpose**: View the contents of the /etc/shadow file to understand its structure and confirm write access.
- **Details**:
    - cat /etc/shadow displays the hashed passwords for all users, including root.
    - Executed on the target machine (192.168.1.1).
    - World-writable permissions allow the student user to read (and later modify) this file.
- **Assumption**: The file is readable, showing the current root password hash.
- **Output**: The contents of /etc/shadow, including the root user's password hash.

Step 7: Modify the Shadow File

Command: sed 's|^root:.*$|root:$y$j9T$LyUuW7eq0q8Ri37tZeZ2x.$V.v9W1nh7f57CR9ln4JYYVA7GJk.MNswwEW4bB2z7Y7:19821:0:99999:7:::|' /etc/shadow > /tmp/shadow_new

Description:

- **Purpose**: Replace the root user's password hash in /etc/shadow with a known hash to set a new password.
- **Details**:
    - sed is used to edit the /etc/shadow file by replacing the root user's line with a new one.
    - The new line sets the root password hash to a bcrypt hash corresponding to the password password.
    - The modified content is written to a temporary file /tmp/shadow_new.

    - This is possible due to the world-writable permissions on /etc/shadow.
- **Assumption**: The command successfully creates /tmp/shadow_new with the updated root password hash.
- **Output**: A new file /tmp/shadow_new containing the modified shadow file.

Step 8: Overwrite the Shadow File

Command: cat /tmp/shadow_new > /etc/shadow

Description:

- **Purpose**: Replace the original /etc/shadow file with the modified version.
- **Details**:
    - cat /tmp/shadow_new > /etc/shadow overwrites /etc/shadow with the contents of /tmp/shadow_new.
    - This updates the root password to password, as set in the previous step.
    - World-writable permissions allow the student user to perform this operation.
- **Assumption**: The command succeeds, updating /etc/shadow with the new root password hash.
- **Output**: The /etc/shadow file now contains the modified root password hash.

Step 9: Switch to Root User

Command: su -

Description:

- **Purpose**: Log in as the root user using the newly set password.
- **Details**:
    - su - prompts for the root password and starts a root shell.
    - Enter the password password (set in the modified /etc/shadow).
    - 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 10: Enter Root Password

Command: password

Description:

- **Purpose**: Provide the root password when prompted by su -.
- **Details**:
    - The password password is entered at the prompt from the su - command.
    - This authenticates the user as root, completing the escalation.
- **Assumption**: The password is accepted, granting root access.
- **Output**: Access to the root shell.

Step 11: 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 192.168.1.1.
    - The flag is the final objective of the machine.
- **Output**: The flag: bhRCN3tcGlp4V3hU.