Detailed Steps to Solve the Machine

Machine Information

Name: AC
Type: SETUID bit misuse and environment variable exploitation
Description: The target machine (192.168.1.4) has a SETUID binary (/etc/updater) with a misconfigured environment variable, allowing execution of arbitrary commands as root. This vulnerability enables privilege escalation to gain root access and retrieve the flag located at /root/flag.
Objective: Gain root access to the target machine and retrieve the flag 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**:
    - Executed from a machine with IP 192.168.0.5.
    - nmap -sn conducts a host discovery scan without port scanning, checking the 256 IP addresses in the 192.168.1.0/24 range.
    - Identifies the target machine's IP address within the network.
- **Assumption**: The scan reveals 192.168.1.4 as a live host, targeted in subsequent steps.
- **Output**: A list of active IP addresses, including the target at 192.168.1.4.

Step 2: Service Scanning with Nmap

Command: nmap -sV 192.168.1.4
Description:

- **Purpose**: Identify open ports and services on the target machine (192.168.1.4).
- **Details**:

    - nmap -sV performs a service version scan to detect open ports and software versions.
    - Executed from 192.168.0.5, targeting 192.168.1.4.
    - Identifies services like SSH, critical for the attack vector.
- **Assumption**: The scan confirms port 22 (SSH) is open, running OpenSSH.
- **Output**: A report listing open ports, with port 22 (SSH) as a potential entry point.

Step 3: Password Cracking with Hydra

Command: hydra -l student -P /usr/share/wordlists/rockyou.txt.gz ssh://192.168.1.4
Description:

- **Purpose**: Brute-force the SSH password for the user student on 192.168.1.4.
- **Details**:
    - hydra attempts SSH logins using the username student.
    - -P /usr/share/wordlists/rockyou.txt.gz uses the rockyou.txt wordlist for password guessing.
    - Targets the SSH service on 192.168.1.4.
- **Assumption**: Hydra cracks the password, revealing password as the credential.
- **Output**: Cracked credentials: student:password.

Step 4: SSH Login

Command: ssh student@192.168.1.4 -p 22
Description:

- **Purpose**: Establish an SSH connection using the cracked credentials.
- **Details**:
    - Connects to 192.168.1.4 on port 22.
    - Uses username student and password password.
    - Grants shell access as the student user.

- **Assumption**: The SSH connection is successful.
- **Output**: An active SSH session on the target machine.

Step 5: Find SETUID Binaries

Command: find / -type f -perm /4000
Description:

- **Purpose**: Identify files with the SETUID bit set, which may allow privilege escalation.
- **Details**:
    - find / -type f -perm /4000 searches for files with the SETUID bit enabled.
    - Executed on 192.168.1.4 via SSH.
- **Assumption**: The output includes /etc/updater, indicating it is a SETUID binary.
- **Output**: A list of SETUID binaries, including /etc/updater.

Step 6: Execute SETUID Binary

Command: /etc/updater
Description:

- **Purpose**: Run the SETUID binary to explore its functionality and potential vulnerabilities.
- **Details**:
    - /etc/updater is executed on 192.168.1.4.
    - The binary likely uses an environment variable (e.g., PATH) insecurely, allowing manipulation to execute arbitrary commands as root.
- **Assumption**: The binary runs but does not immediately grant root access, suggesting further exploitation is needed.
- **Output**: The binary's output, possibly indicating it calls another command.

Step 7: Exploit Environment Variable Misuse

Command: 7
Description:

- **Purpose**: Exploit the SETUID binary's misuse of environment variables to gain a root shell.
- **Details**:
    - The command 7 likely represents a step where the environment variable (e.g., PATH) is manipulated to point to a custom script or binary.
    - For example, creating a malicious script named 7 in a user-controlled directory and prepending it to PATH before running /etc/updater.
    - The SETUID binary executes the malicious perpetrators as root, granting a root shell.
- **Assumption**: The manipulation succeeds, and /etc/updater executes the malicious script, spawning a root shell.
- **Output**: A root shell prompt.

Step 8: 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 flag file's contents.
    - Executed in the root shell on 192.168.1.4.
    - The flag is the final objective.
- **Output**: The flag: cBs3wWG4UBds9LSv.

Final Answer

Flag: cBs3wWG4UBds9LSv