Detailed Steps to Solve the Machine

Machine Information

Macro: Misconfigured Cron Job

Type: Cron job with root privileges and SETUID permissions

Description: The target machine (192.168.1.2) contains a cron job running as root that executes a world-writable script (/etc/secret.sh). This misconfiguration allows any user to modify the script, enabling privilege escalation by adding a user to the sudo group.

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:

  o Executed from a machine with IP 192.168.0.5.

  o nmap -sn conducts a host discovery scan without port scanning, checking the 256 IP addresses in the 192.168.1.0/24 range.

  o Identifies the target machine's IP address within the network.

• Assumption: The scan reveals 192.168.1.2 as a live host, targeted in subsequent steps.

• Output: A list of active IP addresses, including the target at 192.168.1.2.

Step 2: Service Scanning with Nmap

Command: nmap -sV 192.168.1.2

Description:

• Purpose: Identify open ports and services on the target machine (192.168.1.2).

• Details:

  o nmap -sV performs a service version scan to detect open ports and software versions.

  o Executed from 192.168.0.5, targeting 192.168.1.2.

  o 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://192.168.1.2

Description:

• Purpose: Brute-force the SSH password for the user student on 192.168.1.2.

• Details:

  o hydra attempts SSH logins using the username student.

  o -P /usr/share/wordlists/rockyou.txt.gz uses the rockyou.txt wordlist for password guessing.

  o Targets the SSH service on 192.168.1.2.

• Assumption: Hydra cracks the password, revealing password as the credential.

• Output: Cracked credentials: student:password.

Step 4: SSH Login

Command: ssh student@192.168.1.2 -p 22

Description:

• Purpose: Establish an SSH connection using the cracked credentials.

• Details:

  o Connects to 192.168.1.2 on port 22.

  o Uses username student and password password.

  o 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 World-Writable Files

Command: find / -type f -perm -o=w 2>/dev/null

Description:

• Purpose: Identify world-writable files to locate exploitable scripts.

• Details:

  o find / -type f -perm -o=w searches for files with world-writable permissions.

  o 2>/dev/null suppresses permission-denied errors.

  o Executed on 192.168.1.2 via SSH.

• Assumption: The output includes /etc/secret.sh, indicating it is world-writable.

• Output: A list of world-writable files, including /etc/secret.sh.

Step 6: Search for Secret Script

Command: grep -r '/etc/secret.sh' /etc/* 2>/dev/null

Description:

• Purpose: Confirm the presence of /etc/secret.sh in configuration files.

• Details:

  o grep -r recursively searches for references to /etc/secret.sh in /etc.

  o 2>/dev/null suppresses errors.

  o Suggests /etc/secret.sh is executed by a cron job.

• Assumption: The command finds references, indicating a cron job runs /etc/secret.sh.

• Output: Matches confirming /etc/secret.sh is used.

Step 7: Inspect Secret Script

Command: cat /etc/secret.sh

Description:

• Purpose: View the contents of /etc/secret.sh to understand its functionality.

• Details:

  o cat /etc/secret.sh displays the script's contents.

  o Executed on 192.168.1.2.

  o Confirms the script is world-writable and executed by a root cron job.

• Assumption: The script contains commands run as root.

• Output: Contents of /etc/secret.sh.

Step 8: Modify Secret Script

Command: echo "sudo usermod -aG sudo student" >> /etc/secret.sh

Description:

• Purpose: Append a command to /etc/secret.sh to add student to the sudo group.

• Details:

  o echo ... >> /etc/secret.sh appends the command.

  o usermod -aG sudo student grants student sudo privileges.

  o World-writable permissions allow modification.

• Assumption: The command is successfully appended.

• Output: Updated /etc/secret.sh with the new command.

Step 9: Wait for Cron Job Execution

Command: sleep 60

Description:

• Purpose: Wait for the cron job to execute the modified /etc/secret.sh.

• Details:

  o sleep 60 pauses execution for 60 seconds.

  o Allows the cron job, assumed to run periodically, to execute the script.

  o The cron job adds student to the sudo group.

• Assumption: The cron job runs within 60 seconds, granting sudo privileges.

• Output: None, but the student user gains sudo access.

Step 10: Switch to Student User

Command: su - student

Description:

• Purpose: Log in as the student user to verify sudo privileges.

• Details:

  o su - student switches to the student user.

  o Requires the student password, password.

  o Executed on 192.168.1.2.

• Assumption: The command succeeds, granting a student shell with sudo privileges.

• Output: A student user prompt.

Step 11: Enter Student Password

Command: password

Description:

• Purpose: Provide the student password when prompted by su -.

• Details:

  o The password password is entered at the prompt.

  o Authenticates the student user.

• Assumption: The password is accepted.

• Output: Access to the student shell.

Step 12: Retrieve the Flag

Command: sudo cat /root/flag

Description:

• Purpose: Read the contents of the flag file located at /root/flag.

• Details:

  o sudo cat /root/flag uses sudo privileges to access the root-only file.

  o Executed in the student shell on 192.168.1.2.

  o The flag is the final objective.

• Output: The flag: a84P5RP6aYJQKfQc.

Step 13: Enter Student Password for Sudo

Command: password

Description:

- Purpose: Provide the student password when prompted by sudo.
- Details:
  - The password password is entered at the sudo prompt.
  - Authenticates the sudo command to read /root/flag.
- Assumption: The password is accepted.
- Output: The flag is displayed.