Timeline of Events and Actions Taken

July 6, 2024

12:07:54 - 12:07:57

- **User:** John
- **Action:** Elevated privileges using sudo to run /usr/bin/apt update.

12:08:31 - 12:08:35

- **User:** John
- **Action:** Elevated privileges using sudo to install auditd with /usr/bin/apt install auditd.

12:13:20 - 12:13:20

- **User:** John
- **Action:** Elevated privileges using sudo to set up audit rules with /usr/sbin/auditctl -w /home/admin/ -p wa -k admin_changes.

12:18:50 - 12:18:50

- **User:** Admin
- **Action:** Elevated privileges using sudo to delete a file with /usr/bin/rm financial_info-233.

12:19:24 - 12:19:24

- **User:** Admin
- **Action:** Elevated privileges using sudo to search audit logs with /usr/sbin/ausearch -k admin_changes.

12:20:35 - 12:20:35

- **User:** Admin
- **Action:** Elevated privileges using sudo to generate audit reports with /usr/sbin/aureport -f -i.

12:22:53 - 12:22:54

- **User:** John
- **Action:** Elevated privileges using sudo to delete the user attacker with /usr/sbin/userdel attacker.

14:28:42 - 15:20:19

- **Event:** Brute Force Attack

- **Details:** Numerous failed login attempts from 192.168.10.15 targeting various usernames (root, bob, test, guest, info, adm, mysql, user, administrator, oracle, ftp, pi, puppet, ansible, ec2-user, admin, vagrant, azureuser, john, bill, james). This high frequency of attempts suggests a potential brute force attack.

14:29:31 - 14:29:31

- **User:** John
- **Action:** Elevated privileges using sudo to open a root shell with /bin/bash.

15:25:07 - 15:25:21

- **User:** Admin
- **Action:** Elevated privileges using sudo to add a new user stephanie with /usr/sbin/adduser stephanie.

15:25:31 - 15:25:31

- **User:** Admin
- **Action:** Elevated privileges using sudo to add stephanie to the sudo group with /usr/sbin/usermod -aG sudo stephanie.

16:07:21 - 16:07:21

- **User:** Admin
- **Action:** Elevated privileges using sudo to delete a file with /usr/bin/rm financial_info-210.

16:10:29 - 16:14:32

- **User:** John
- **Action:** Elevated privileges using sudo to open a root shell with /bin/bash.

16:15:30 - 16:16:09

- **User:** Admin
- **Action:** Elevated privileges using sudo to open a root shell with /bin/bash.

16:16:34 - 16:17:14

- **User:** John
- **Action:** Elevated privileges using sudo to open a root shell with /bin/bash.

16:16:49 - 16:16:49

- **User:** John
- **Action:** Elevated privileges using sudo to delete the user admin with /usr/sbin/userdel admin.

16:57:03 - 16:57:03

- **User:** John
- **Action:** Elevated privileges using sudo to add a new user stephanie with /usr/sbin/adduser stephanie.

17:05:17 - 17:05:17

- **User:** John
- **Action:** Elevated privileges using sudo to view the auth log with /usr/bin/cat /var/log/auth.log.

Summary of Actions Taken

1. **User Additions and Deletions:**
    - Added: stephanie
    - Deleted: attacker, admin
2. **Privilege Elevation with sudo:**
    - John: Frequently used sudo for system updates, installing audit tools, setting up audit rules, deleting users, and opening root shells.
    - Admin: Used sudo for file deletions, searching audit logs, generating audit reports, adding users, and opening root shells.
3. **Concerning Commands:**
    - File Deletions: admin deleted files financial_info-233 and financial_info-210, which could be concerning if these files were important or sensitive.

Potential Security Concerns

- **Brute Force Attack:** High frequency of failed login attempts from 192.168.10.15 targeting multiple usernames. (got in)
- **Suspicious Activities:** Deletion of users attacker and admin, and the addition of stephanie multiple times.
- **File Deletions:** Deletion of financial files by admin could indicate malicious activity or an attempt to cover tracks.