Incident Response Report

Incident #

Team #

March 23, 2024

## Introduction

The attack began through a breach on [machine]. Attackers changed the sudoers settings and installed a disruptive program that ran after running sudo.

## Triggers

Team # noticed the attack when they ran sudo, and recognized a program called “hollywood” disrupting their activities.

## Timeline

15:11 – Attackers log in to [ip] with default credentials.

15:12 – Attackers allow all users to run password-less sudo.

15:14 – Attackers install hollywood.

## Source

Team # found that the attack came through SSH from IP address [ip].

## Incident classification

Unauthorized access, malware.

## Scope

The incident affected the [machine] system. The attack disrupted Team # from hardening, threat hunting, and checking status of services. This would also prevent users from carrying out the necessary tasks for organization operations. It also allows users to run sudo commands without passwords.

## Response actions

Team # continued to run Ctrl+C in the terminal until they were able to temporarily stop hollywood, then went into bash.rc and deleted hollywood. Then, the team updated iptables rules to drop traffic from IP address [ip], and changed the /etc/sudoers file, and changed the passwords for all users on Web.

## Root cause analysis

The root cause of the incident was failure to change default credentials, allowing attackers to obtain access to Web. While Team # did change credentials for users such as jack.rover and root, they failed to change passwords for all uses. As a result, the attackers successfully accessed the system through spraying credentials.

## Recommendations

To prevent similar incidents in the future, default credentials for all users should be changed to strong passwords with a large length and character size and updated regularly to prevent the success of brute-force and compromised credential methods. There should also be a rule or policy to prevent the installation of malicious programs such as hollywood, as well as changes to /etc/sudoers file.

## Conclusion

With some users on the Web system still requiring default credentials, attackers were able to access the system and install malware. This resulted in disruption of Team #’s efforts to monitor and secure the [machine] system. To mediate this, default credentials for all users on the system should be changed to strong passwords and measures to prevent the installation of malware and changes to sudo settings should be implemented.