Log analysis report

On July 6th a system administrator noticed unusual alerts during routine server maintenance: high CPU usage on an administrative server, unusual login patterns in authentication logs, and alerts from the intrusion detection system. An analysis was requested in order to draw conclusions from the prove that was delivered from the different security systems, where a lot of concerning actions and results were deduced, it can be say that the system was access by external people (hackers) that gain a privilege user permissions in order to modify, copy, or delete different data or movements realized by the same hackers to hide their track, by analyzing the time that each malicious action happened, the hacker was in the system for a long time, getting an approximately amount of 4 hours inside the system with access to everything. The high CPU usage can be explained because the system was receiving a lot of attempts to log in (807 exactly) and most of those attempts where between 2pm and 4pm. The hacker that gained access was making a lot of requests to the server as an administrative user, modifying users and files

The intrusion detection system receive three different level two (medium) severity alerts: Potentially bad traffic, the hacker try to use a malicious script that the IDS/IPS detected and registered, attempt information leak, the hacker tried to do requests about information with a unknow user, and device retrieving external IP, the hacker wanted to recognize the system and mapping it

- Auth.log: Is the file records login attempts and user management activities, the file recorded a total off 807 failed login attempts form different users, focusing on the users with the most access to the system. The difference of time between each request gives signal that the hacker was trying a brute force attack in order to gain credentials. The timeline of the actions where between the 00:05 and 17:05 but the most attempts to log in was from 14:05 to 17:05.
- Alerts.log: It logs monitor network traffic and flag suspicious activities based on known patterns or anomalies. From this file we got very important information that tells us what suspicious activities happens in the system because of some patterns, we found twenty-five level two severity alerts, there when some that alert the same, but most of the alerts where form the same IP which makes it more suspicious.
- Audit.log: It provides detailed records of specific monitored activities like file access or changes, system calls, command execution and other ones. The file gave some actions about removing and copying a large number of files, 630 of remove and 298 of copy to be exact, which means clearly that there was a hacker in the system that affected and compromised important data.

The attack was inside the network because of the IP of the attacker as 192.168.10.15, which means it was an internal network access

Before the brute force happen, there was already a user ‘attacker’ with privileges created that John had to erase around 12:22:54, this is associated with the local IP address used for the attack, meaning that the hacker already has scan and analyze the whole network and infrastructure.

The hacker started a brute force attack at 14:28:40 and try to compromise different accounts like root, user, guest, info, pi, oracle, and others in a very short amount of time

The first account compromised was the ‘admin’ account at 15:04:22, this account was found with weak credentials

The system dropped 858 connections for 46 minutes, indicating that the brute force attack used automatized tool and was way bigger than we thought at 15:16:41

When the hacker got to compromise different accounts, is clearly shown in the logs that some credentials were stolen by the access to the user ‘admin’ giving full control over the system from 15:04:22 to 15:21:00

The hacker knew the system’s users and passwords because we can see in the evidence that it got access to each user of the system

Stephanie user was created and escalated to root via sudo, by the user ‘admin’ that was compromised, at 15:25:07 from the ‘admin’ account

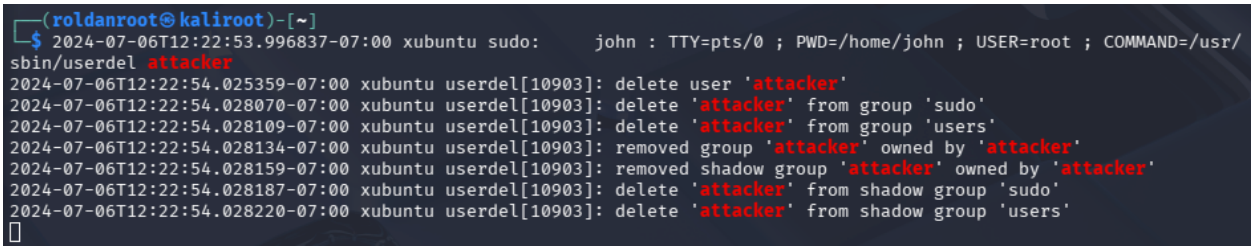
Some logs and movements were detected in the financial folder from the user Admin, which indicates that the data from the financial folder was compromised

The hacker deleted admin’s user from Stephanie user, at 16:16:49

The attacker first used and automated script to check credentials and gain access to different users, we know this because the same IP address (192.168.10.15) spend all the timeline making changes and trying making attempts by guessing different passwords and usernames. At the same time the hacker was scanning the mysql port (3306), we know this thanks to the alerts log that specifies the hour and the IP that did it, after the scan he started to scan the ssh in order to get some connection to the server remotely, then, thanks to filtering with SYSCALL in the Linux command lines, the hacker was removing data using the “rm” command to erase evidence and modifying permissions of some files which means that there is data that was compromised, when all the malicious activity was finished, the hacker clean up by removing some privilege access to different users.

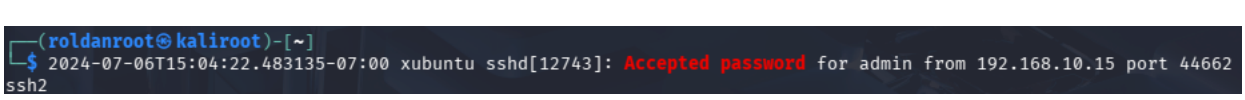
Evidence

A user called ‘attacker’ was erased before the brute force attack:



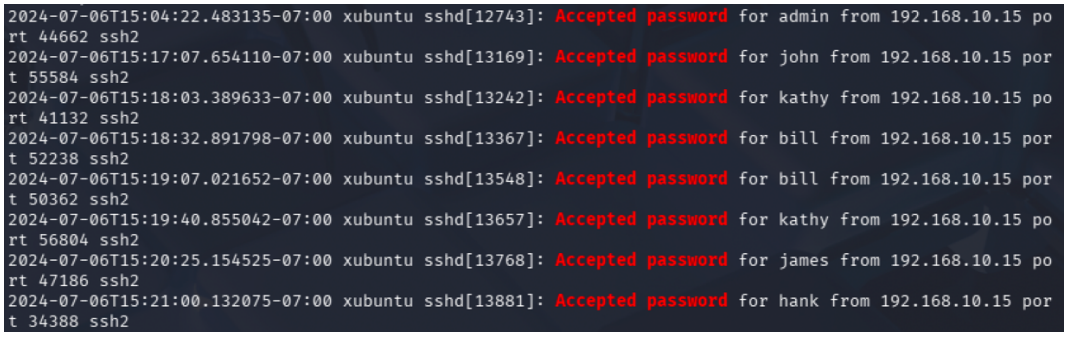
Start of the brute force attack and try to compromise different users:

First account compromised:

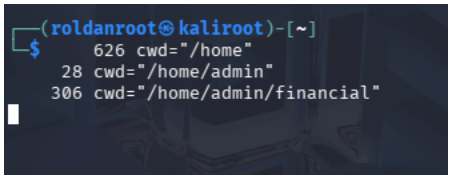


Connections dropped a clear example of a brute force attack happening:

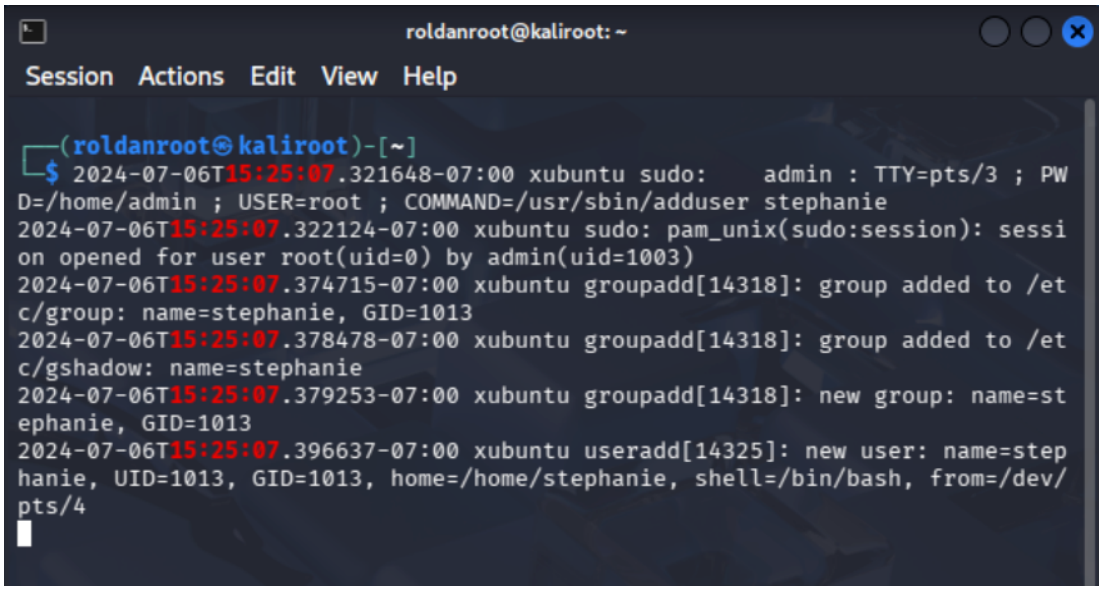
Access to other users, gaining full access over the system:



Movements on the financial admin folder:



Create and grant privileges to Stephanies user from the admin user:



Deleted user admin from everything: