Caleb Javier

Professor Holden-Gouveia

CIS-245

3 November 2024

Assignment 8: Scripts for Security - Part 1

1. **Script for detecting unusual or suspicious IP activity**

To begin, we will note the things that must be focused on by the script in order to have the most effectiveness when detecting potential red flag activities. Things such as these may be: After hours access, excessive logins for a specific user (as mentioned in the instruction), or a sudden increase in failed login attempts, logins from IPs that are not from within a network, or a sudden and large number of attempts in a short span of time.

These are often indications of a potential brute-force attack and can prove a threat unless detected in time. For the purpose of functionality, this script will be made as a cron job so that it will run hourly in order to cover the widest possible range of potential attacks.

This can be done using the command **crontab -e**, which will allow the user to begin writing a new cron job. The process is very similar for both servers and both scripts have been attached. Begin by using **sudo crontab -e** to open the editor. If necessary, select the default text editor, which is typically **nano**. For CentOS it is **vi**. Following the format provided by the crontab display, we enter

**\* 6 \* \* \* /home/cjavier/scripts/file\_name.sh (This will allow for the script to run daily at 6 AM).**

Then press **Esc, then enter :wq** to save and quit.

This message should appear in the terminal.



1. **How else can the server be fortified with additional scripts/cron jobs?**

With cron jobs, automation is made extremely simple and effective. In this way, a tedious task such as reimplementing network rules or gathering IP/port/routing table data can be made extremely efficient. This is also a strong security measure because being able to have rules updated in a timely fashion while also being able to determine what comes in and out (such as the scripts designed in the networking and firewall labs) makes for a tightly-run server and provides the root user with as much information as they need as often as they need it. In a specific cron job, for example, could be an hourly report of which ports are open, which are receiving traffic, and automated rules to be set in place especially since they are able to be run after a reboot whereas iptables rules are not.

Works Cited

“Cron Jobs For Beginners | Linux Task Scheduling.” *YouTube*, Akamai Developer, www.youtube.com/watch?v=v952m13p-b4. Accessed 6 Dec. 2024.

L., Linas. “What Is a Cron Job: Understanding Cron Syntax and How to Configure Cron Jobs.” *Hostinger Tutorials*, 24 Sept. 2024, www.hostinger.com/tutorials/cron-job.

Staff, Editorial. “How Cron Job Scheduling Automation Simplifies Your Workflows: Activebatch Blog.” *Blog*, 2 May 2023, www.advsyscon.com/blog/cron-job-scheduling/.

user1129812user1129812 17311 gold badge11 silver badge66 bronze badges, and user9517user9517 117k2020 gold badges222222 silver badges305305 bronze badges. “Does Cron Job Remain in Effect after Computer Reboots?” *Server Fault*, 1 Jan. 1962, serverfault.com/questions/818606/does-cron-job-remain-in-effect-after-computer-reboots.