**Linux Commands**

|  |  |
| --- | --- |
| last -20 | Outputs last 20 logins including the hostname/IP where the user logged in from |
| ls -lart | time ordered list of files; pay attention to changes in /sbin, /bin, /usr/sbin, and /usr/bin |
| ps -ef  ps -aux | running processes |
| lsof -p [PID] | investigate suspicious process; shows all files and ports used by the process |
| lsof | grep IPv  lsof | grep LIST  lsof | grep ESTAB | files listening for a connection, or have an established connection |
| sort -nk3 -t: /etc/passwd | less | new accounts in sorted list by UID; check for any with UID < 500 |
| egrep ':0+:' /etc/passwd | unexpected UID 0 accounts |
| find / -nouser -print | orphaned files, indicator an attacker's temporary account has been deleted |
| find / -uid 0 -perm -4000 -print | unusual SUID root files |
| find / -name " " -print  find / -name ".. " -print  find / -name ". " -print | files named with dots and spaces to camouflage files |
| crontab -u root -l | unusual cron jobs scheduled by root |
| cat /etc/crontab ls /etc/cron.\* | unusual system-wide cron jobs |