

# LINUX FORENSIC ARTIFACTS

|                                       |                       |
|---------------------------------------|-----------------------|
| Information - OS                      | /etc/os-release       |
| Information - Hostname                | /etc/hostname         |
| Information - Timezone                | /etc/timezone         |
| Information - Users                   | /etc/passwd           |
| Information - Groups                  | /etc/group            |
| Sudoers List                          | /etc/sudoers          |
| Password Hashes                       | /etc/shadow           |
| Bash Shell Configuration - User       | /home/<user>/.bashrc  |
| Bash Shell Configuration - System     | /etc/bash.bashrc      |
| Shell Configuration on Login - User   | /home/<user>/.profile |
| Shell Configuration on Login - System | /etc/profile          |
| DNS Configuration                     | /etc/hosts            |
| DNS Configuration                     | /etc/resolv.conf      |

|                                     |                            |
|-------------------------------------|----------------------------|
| Authentication Logs                 | /var/log/auth.log          |
| Authentication Logs                 | /var/log/secure            |
| User Sessions - Active              | /var/run/utmp              |
| User Sessions - History             | /var/log/wtmp              |
| Failed Login Attempts               | /var/log/btmp              |
| System Logs                         | /var/log/syslog            |
| System Logs                         | /var/log/message           |
| Network Interfaces                  | /etc/network/interface     |
| Startup Services Directory          | /etc/init.d/               |
| Cron Jobs - User Crontabs Directory | /var/spool/cron/crontabs/  |
| Cron Jobs - System Crontab          | /etc/crontab               |
| Command History - Bash              | /home/<user>/.bash_history |
| Command History - Vim               | /home/<user>/.viminfo      |