Incident Response Checklist

Beforehand - Create initial process list  
 ps aux > "incident\_baseline.$(date +%F\_%R)"  
 chattr +i incident\_baseline.<date>

|  |  |
| --- | --- |
| Incident Response Process Upon Intrusion | |
| Purpose | Command |
| Create incident process list | ps aux > "incident.$(date +%F\_%R)" |
| Compare process lists | diff incident\_baseline.<date> incident.<date> |
| Check listening services | netstat -tulpn | tee "incident.net.$(date +%F\_%R)" |
| Check logs | tail /var/log/auth.log  tail /var/log/secure |
| Check bash history | tail /home/[username]/.bash\_history |
| Check SSH authorized\_keys | cat /home/[username]/.ssh/authorized\_keys |
| Kill SSH shells | fuser -k /dev/pts/[id]  kill $(ps aux | egrep "sshd:.\*[p]ts" | awk '{print $2}') |

Taking a screenshot in Linux / Mac:

Linux:

apt-get install imagemagick

Use xwininfo to get window id then,

import -window id directory/filename

Mac:

Press `command+Shift+4`, then drag mouse to crop screenshot window