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}')`