

## HONEYNET/HONEYPOT HOWTO

1. Install VMware Server.
2. Copy honeypot/ and Ubuntu/ from the DVD to your computer.
3. Open VMware, connect to localhost.
4. Open Ubuntu (monitoring) VM.
5. Start (boot-up) monitoring VM.
6. Login to Ubuntu with username: itladmin
7. Optional: `sudo /usr/local/bin/oinkmaster-update.sh`
8. Run `sudo snort -i eth0 -c /etc/snort/snort.conf`
9. In a separate terminal, run `sudo tail -f /var/log/snort/alert`
10. Open and boot the honeypot VM.
11. Wait for an attack.
12. After attack:
  - a. In the honeypot VM,
    - i. `cd C:\Program Files\tripwire\TFS\bin`
    - ii. `tripwire --check --report-file <report-filename>`
    - iii. `twprint --print-report --report-file <report-filename> -F <html|xml|classic> -o <outfile.><html|xml|classic>`