

Blue Team Ubuntu Machine

Install and configure Sguil Client

```
sudo apt update
sudo apt upgrade
```

```
cd ~/Downloads
wget https://github.com/bammv/sguil/archive/v0.9.0.tar.gz
```

```
cd /opt
sudo tar -xvzf ~/Downloads/v0.9.0.tar.gz
cd sguil-0.9.0/client
```

edit sguil.tk and under exec wish "\$0" "\$@" add the following line

```
cd /opt/sguil-0.9.0/client
```

```
sudo nano /opt/sguil-0.9.0/client/sguil.tk
```

so first 5 lines should appear as follows:

```
#!/bin/sh
# Run wish from users PATH \
exec wish "$0" "$@"
cd /opt/sguil-0.9.0/client
# $Id: sguil.tk,v 1.264 2012/09/05 00:38:45 bamm Exp $ #
```

Save and exit

Create a desktop shortcut

```
cd ~/Desktop
nano Sguil_Client.desktop
```

```
[Desktop Entry]
Version=1.0
Type=Application
Terminal=false
Icon=/opt/sguil-0.9.0/client/lib/images/sguil_logo_h.gif
Exec=sh /opt/sguil-0.9.0/client/sguil.tk
Name=Sguil Client
```

Save and exit

```
chmod a+x ~/Desktop/Sguil_Client.desktop
```

install Wireshark

```
sudo apt install wireshark
say Yes to Should non-superusers be able to capture packets?
```

Install and configure Network Miner

```
sudo apt install gnupg ca-certificates
```

```
sudo apt-key adv --keyserver hkp://keyserver.ubuntu.com:80 --recv-keys 3FA7E0328081BFF6A14DA29AA6A19B38D3D831EF
```

```
echo "deb https://download.mono-project.com/repo/ubuntu stable-bionic main" | sudo tee /etc/apt/sources.list.d/mono-official-stable.list
```

```
sudo apt update
```

```
sudo apt install mono-complete
```

```
Download Network miner from https://www.netresec.com/?download=NetworkMiner
```

```
sudo unzip ~/Downloads/NetworkMiner.zip -d /opt/ cd /opt/NetworkMiner
```

```
sudo chmod +x NetworkMiner.exe
```

```
sudo chmod -R go+w AssembledFiles/
```

```
sudo chmod -R go+w Captures/
```

```
#### Configure desktop shortcut for Network Miner ####
```

```
cd ~/Desktop
```

```
nano ssh_NetworkMiner.desktop
```

```
[Desktop Entry]
```

```
Version=1.0
```

```
Type=Application
```

```
Terminal=true
```

```
Icon=/home/labadmin/Pictures/NetworkMiner.png
```

```
Exec= mono NetworkMiner.exe --noupdatecheck
```

```
Name=Network Miner
```

```
Save and enter
```

```
chmod a+x ~/Desktop/NetworkMiner.desktop
```