Getting Started

This will guide you through using the Im Blue repository to set up a host with incident response software.

Downloads

The repository can be downloaded as a zip file from a shortened domain.

Linux

```
wget ir.scriptingis.life -O master.zip && unzip master.zip && cd Im-Blue-master
```

Windows

Windows users can download the file with a web browser and unzip the file through the file explorer.

Ansible

Linux

Ansible uses SSH keys to control clients. You'll need to add the public key to the `authorized_keys` file for each user. `curl -L pub.scriptingis.life >> authorized_keys`

Windows

There is a PowerShell script in `Im-Blue-master/Scripts/Powershell/Ansible-Setup.ps1`. Right click the script and select *Run with PowerShell*.

Other Software

Linux

Maltrail

Maltrail is a two part sensor and server written in Python which listens for malicious traffic and logs it.

Setup

To run the sensor on boot, edit `/etc/rc.local`. Add the line `cd $INSTALL_DIR && python sensor.py &` below everything except if the `exit 0` at the end. To run the sensor now, enter a screen session with the `screen` command then run `python sensor.py &`. Leave the shell with `Ctrl + A, D`. This keeps the program running until the system reboots.

Windows

Glasswire

Glasswire is a Windows program that alerts when an application connects to the internet for the first time.

Setup

Run `Im-Blue-master/Programs/GlassWireSetup.exe` and click *Next* until it's installed and running.