|  |
| --- |
| Linux Backdoors |
| Technical Report |
| COMP 8505 |

|  |
| --- |
| Slade Solobay – A00769103  Zach Smoroden – A00768344  10/6/2014 |

Table of Contents

[Specification 2](#_Toc399407526)

[Design 2](#_Toc399407527)

[Psuedocode 2](#_Toc399407528)

[Usage 2](#_Toc399407529)

[Compilation 2](#_Toc399407530)

[Running the Program 2](#_Toc399407531)

[Output 2](#_Toc399407532)

[Testing 2](#_Toc399407533)

[Test System Information 2](#_Toc399407534)

[Test Cases 2](#_Toc399407535)

# Specification

The purpose of this assignment is to gain an understanding of Linux backdoors, specifically packet-sniffing backdoors. To aid in this a complete and working backdoor application will be created using the [**libpcap**](http://www.tcpdump.org/manpages/pcap.3pcap.html) library.

# Design

## Psuedocode

### mask.rb

initialize process name constants;

Mask Class

{

mask the process name (top/ps);

change the UID/GID to 0 (raise privs);

mask the process name (htop)

}

# Usage

## Compilation

## Running the Program

## Output

# Testing

## Test System Information

Operating System: Fedora 20

Byte Order: Little Endian

Architecture: x86\_64

Processors: 4

RAM: 4GB

## Test Cases