Keylogger/Backdoor Rootkit

Clemens BRUNNER
Michael FRÖWIS

October 27, 2015

Contents

1 Introduction

1.1 Kernel Modules

1.2 Kernel Rootkits

2 Implementation

2.1 Keylogging

2.2 Backdoor

2.3 Hiding

2.4 Networking and Activation

3 Conclusion