

# TABLE OF CONTENTS

|    |                                       |    |
|----|---------------------------------------|----|
| 01 | <b>Rootkit Introduction</b>           |    |
|    | Intro .....                           | 03 |
|    | Code .....                            | 04 |
|    | POC & Detection .....                 | 05 |
| 02 | <b>Understanding Protection Rings</b> |    |
|    | Intro .....                           | 06 |
|    | Code .....                            | 07 |
|    | POC & Detection .....                 | 08 |
| 03 | <b>Our Rootkit Structure</b>          |    |
|    | Intro .....                           | 09 |
|    | Code .....                            | 10 |
|    | POC & Detection .....                 | 11 |
| 04 | <b>Hiding Files and Directories</b>   |    |
|    | Intro .....                           | 12 |
|    | Code .....                            | 13 |
|    | POC .....                             | 14 |
| 05 | <b>Hiding Processes</b>               |    |

# TABLE OF CONTENTS

## 06 Hiding Registries

Intro ..... 03

Code and PoC ..... 05

## 07 Main EXE

## 09 Exercise

## 10 Conclusions