

TABLE OF CONTENTS

01	Process Token Extraction and Substitution	
	Intro	03
	Code	04
	POC & Detection	05
02	Process Token Impersonation	
	Intro	06
	Code	07
	POC & Detection	08
03	Escalate Privileges Token Manipulation	
	Intro	09
	Code	10
	POC & Detection	11
04	Escalate Privileges via FodHelper	
	Intro	12
	Code	13
	POC	14
05	Access Token Creation	

TABLE OF CONTENTS

06 SID Spoofing

Intro 03

Code and PoC 05

07 Token Lockdown

09 Exercise

10 Conclusions