

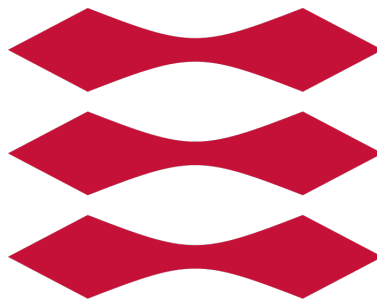
Exploiting known vulnerabilities,
misconfigurations and weaknesses in native
protocols to compromise Windows Active
Directory Domains with a focus on traceability
and ease of use.

Søren Fritzboøger - s153753

Vejledt af Henrik Tange

20. Januar 2019

DTU



Danmarks Tekniske Universitet

Abstract

Abstract here

Table of contents

1	Introduction	4
1.1	Problem definition	4
2	Credential gathering	4
2.1	Spoofing	4
2.1.1	NBNS - NetBIOS Name Resolution	4
2.1.2	LLMNR - Link-local Multicast Name resolution	4
2.2	Credential acquiring	4
2.2.1	Credential types	4
2.2.2	SMB	5
2.2.3	HTTP	5
3	Attack methods	5
3.1	LSASS secrets	5
3.1.1	Impacket wmiexec	5
3.1.2	Mimikatz	5
3.2	secretsdump	5
4	Reconnaissance	5
5	Implementation	5
5.1	Technologies	5
5.1.1	ASP.NET Core	5
5.1.2	SignalR	5
5.1.3	VueJS	5
5.2	Considerations	5
5.2.1	Modularity	5
5.2.2	Ease of use	5
5.2.3	Traceability	5
5.3	Storage	5
6	Discussion	5
6.1	Ethics	5
7	Conclusion	5

1 Introduction

1.1 Problem definition

2 Credential gathering

2.1 Spoofing

2.1.1 NBNS - NetBIOS Name Resolution

2.1.2 LLMNR - Link-local Multicast Name resolution

2.2 Credential acquiring

2.2.1 Credential types

LM

NT

NTLM

NetNTLMv1

NetNTLMv2

2.2.2 SMB

2.2.3 HTTP

3 Attack methods

3.1 LSASS secrets

3.1.1 Impacket wmiexec

3.1.2 Mimikatz

3.2 secretdump

4 Reconnaissance

5 Implementation

5.1 Technologies

5.1.1 ASP.NET Core

5.1.2 SignalR

5.1.3 VueJS

5.2 Considerations

5.2.1 Modularity

5.2.2 Ease of use

5.2.3 Traceability

5.3 Storage

6 Discussion

6.1 Ethics

7 Conclusion