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 Fritzbøger - s153753
Vejledt af Henrik Tange

20. Januar 2019

Danmarks Tekniske Universitet

Abstract

Abstract here

Table of contents

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