

POSUDEK OPONENTA DIPLOMOVÉ PRÁCE

Student: BC. TOMÁŠ DRLÝ

Oponent: Ing. Ladislav Vyskočil

Studijní program: **Informační technologie**
Specializace: **Kybernetická bezpečnost**
Akademický rok: **2024/2025**

Téma diplomové práce: Manipulace s Active directory pomocí protokolu Kerberos a její detekce

Hodnocení práce:

Cílem diplomové práce bylo popsat problematiku manipulace s Active directory pomocí protokolu Kerberos a následně možnosti její detekce, k jehož dosažení bylo třeba naplnit několik bodů, jejichž přesná specifikace byla součástí zásad uvedených v zadání práce. Všechny body zadání diplomové práce byly splněny v plném rozsahu. Diplomant popisované problematice dobře rozumí. Diplomová práce je na vysoké odborné úrovni, je přehledně strukturována a jednotlivé části na sebe logicky navazují. Text práce je zpracován srozumitelně. Po jazykové stránce nebyly nalezeny žádné pravopisné, nebo stylistické chyby. Po formální stránce je práce vhodným způsobem řazena do logických celků a doplněna upřesňujícími komentáři i odkazy na odpovídající literární či elektronické zdroje. V diplomové práci autor uvádí přiměřené množství obrázků, tabulek, zdrojových kódů a příloh k objasnění popisované problematiky.

V teoretické části byly podrobně popsány principy adresářových služeb, historie a vývoj služby Active directory, její funkcionalita a ukládání objektů a hesel. Dále byl v této části proveden velmi rozsáhlý rozbor protokolů LDAP a Kerberos, se zaměřením na strukturu a typy zpráv a jejich využití v komunikaci mezi klientem a serverem.

V praktické části byla provedena přehledná analýza protokolu Kerberos a procesu komunikace při ověřování klienta. Dále byla implementována manipulace protokolu Kerberos, která byla realizována pomocí MITM (Man In The Middle) útoku. Následně byly popsány i rozsáhlé testy těchto manipulací. Diplomant také navrhl a vytvořil vlastní skener na uživatelské účty, který z odpovědi serveru dokáže určit, jací uživatelé se v doméně nachází a v jakém stavu je jejich účet. Závěr praktické části je věnován obraným opatřením, které by měly zamezit manipulaci se zprávou Kerberos a obraně proti skenování.

Přínosem práce je přehledný a podrobný popis dané problematiky, kdy diplomová práce může sloužit jako vzorový návod pro mnohá řešení v praxi. Diplomová práce se jeví jako zdařilá a splňující svůj cíl, a proto ji doporučuji předložit k obhajobě.

Otázka k obhajobě: Jak bude pokračovat Váš další výzkum v této oblasti?



Celkové hodnocení práce:

Známku uvede oponent dle svého uvážení dle klasifikační stupnice ECTS:

A – výborně, B – velmi dobře, C – dobře, D – uspokojivě, E – dostatečně, F – nedostatečně.

Stupeň F znamená též „nedoporučuji práci k obhajobě“.

Předloženou diplomovou práci doporučuji k obhajobě a navrhuji hodnocení

A - výborně.

V případě hodnocení stupněm „F – nedostatečně“ uveďte do připomínek a slovního vyjádření hlavní nedostatky práce a důvody tohoto hodnocení.

Datum

2. 6. 2025

Podpis oponenta diplomové práce