

МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ФАКУЛЬТЕТ РАДИОФИЗИКИ И КОМПЬЮТЕРНЫХ
ТЕХНОЛОГИЙ

Кафедра телекоммуникаций и информационных технологий

ПОДГАЙСКИЙ
Максим Александрович

**БЕЗОПАСНОСТЬ ACTIVE DIRECTORY: УГРОЗЫ,
УЯЗВИМОСТИ, МОДЕЛИ НАРУШИТЕЛЕЙ**

Аннотация к дипломной работе

Научный руководитель – старший преподаватель Е.Е. Попко

Минск, 2022

РЕФЕРАТ

Дипломная работа: 75 с., 44 рис., 23 источника

АКТИВНЫЙ КАТАЛОГ, СЛУЖБА КАТАЛОГОВ, БЕЗОПАСНОСТЬ СЛУЖБЫ КАТАЛОГОВ, УГРОЗЫ, УЯЗВИМОСТИ, МОДЕЛИ НАРУШИТЕЛЕЙ, АТАКИ, ACTIVE DIRECTORY, GOLDEN TICKET, KERBEROS, NTLM, LDAP, AD, AD DS

Цель данной дипломной работы – исследование безопасности службы каталогов, разработка модели нарушителя и создаваемых злоумышленником угроз.

Для достижения цели был проведен анализ структуры службы каталогов, исследуя её структурно-функциональные характеристики и взаимосвязи между ними, рассмотрены возможные способы атак, которые могут совершить нарушители, описаны уязвимости, которые они эксплуатируют и построены модели нарушителя. Также реализована и продемонстрирована одна из возможных атак, с последующим описанием рекомендаций по её предотвращению.

РЭФЕРАТ

Дыпломная работа: 75 с., 44 мал., 23 крыніцы

АКТЫЎНЫ КАТАЛОГ, СЛУЖБА КАТАЛОГАЎ, БЯСПЕКА СЛУЖБЫ КАТАЛОГАЎ, ПАГРОЗЫ, УРАЗЛІВАСЦІ, МАДЭЛІ ПАРУШАЛЬНІКАЎ, АТАКІ, ACTIVE DIRECTORY, GOLDEN TICKET, KERBEROS, NTLM, LDAP, AD, AD DS

Мэта дадзенай дыпломнай працы – даследаванне бяспекі службы каталогаў, распрацоўка мадэлі парушальніка і ствараемых зламыснікам пагроз.

Для дасягнення мэты быў праведзены аналіз структуры службы каталогаў, даследуючы яе структурна-функцыянальныя характарыстыкі і ўзаемасувязі паміж імі, разгледжаны магчымыя спосабы нападаў, якія могуць здзейсніць парушальнікі, апісаны ўразлівасці, якія яны эксплутуюць і пабудаваны мадэлі парушальніка. Таксама рэалізавана і прадэманстравана адна з магчымых нападаў, з наступным апісаннем рэкамендацый па яе прадухіленні.

ABSTRACT

Thesis: 75 p., 44 fig., 23 sources

ACTIVE DIRECTORY, DOMAIN SERVICES, ACTIVE DIRECTORY SECURITY, THREATS, VULNERABILITIES, VIOLATOR MODELS, ATTACKS, GOLDEN TICKET, KERBEROS, NTLM, LDAP, AD, AD DS

The purpose of this thesis is to study the security of the active directory, develop a model of the intruder and the threats created by the attacker.

To achieve the goal, an analysis of the structure of the directory service was carried out, examining its structural and functional characteristics and the relationship between them, possible methods of attacks that violators can make were considered, the vulnerabilities that they exploit were described, and models of the intruder were built. One of the possible attacks was also implemented and demonstrated, followed by a description of recommendations for its prevention.