

Презентация
на тему: «Разработка системы
аутентификации удаленных пользователей»

Студента: Титков В.В.

группы: ИТ-431М

ВВЕДЕНИЕ

- ▶ В представленной работе будет исследовано управление доступом и контроль аутентификации пользователей. Работа будет сосредоточена на сервере аутентификации, его преимуществах, функциональных возможностях и ролях в информационной безопасности.
- ▶ Целью работы является получение глубокого понимания принципов, преимуществ и возможностей сервера аутентификации, а также разработка рекомендаций для эффективного внедрения и использования в организации. Будут проведены эксперименты с использованием виртуальных сред и тестовых сценариев.

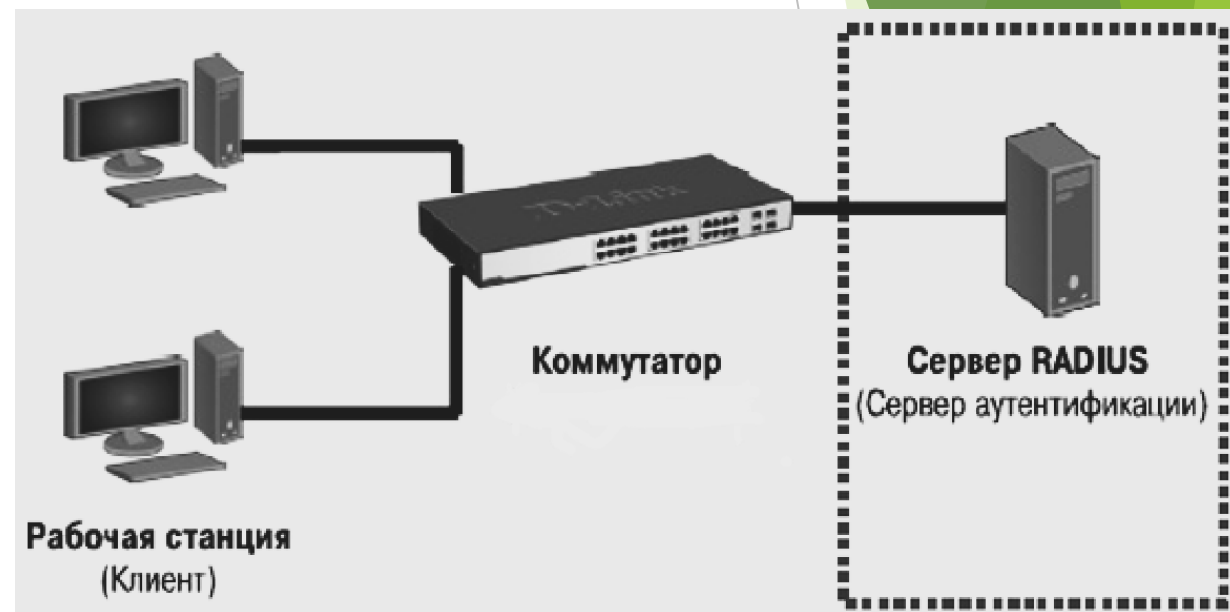
СЕРВЕР АУТЕНТИФИКАЦИИ

- ▶ Сервер аутентификации является центральным узлом, управляющим всеми процессами аутентификации для всех приложений, сервисов и ресурсов. Промышленные серверы аутентификации поддерживают разнообразные методы проверки подлинности, такие как, RADIUS, LDAP, простой пароль и другие.



СЕРВЕР АУТЕНТИФИКАЦИИ

- ▶ Каждый ресурс, использующий сервер аутентификации, может выбрать подходящий метод, соответствующий его потребностям, а администраторы имеют доступ к унифицированному интерфейсу для управления данными пользователей и гибким возможностям изменения, что позволяет бизнесу обеспечить надежную защиту доступа к сервисам.



ВЫБОР ОПЕРАЦИОННОЙ СИСТЕМЫ

- простота использования:
- поддержка и обновления
- высокая безопасность:
- бесплатность и открытость:



ВЫБОР ПРОТОКОЛА АУТЕНТИФИКАЦИИ

- ▶ При выборе сервера аутентификации были рассмотрены два протокола авторизации Tacsacs+ и Radius.
- ▶ RADIUS (Remote Authentication Dial-In User Service) - протокол, который использует UDP для связи. Он объединяет функции аутентификации и авторизации в своих пакетах, что делает его подходящим для таких сценариев, как аутентификация удаленного доступа.

ВЫБОР ПРОТОКОЛА АУТЕНТИФИКАЦИИ

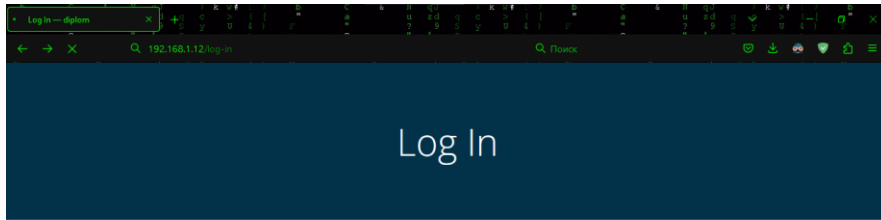
- ▶ TACACS+ (Terminal Access Controller Access Control System Plus) - это другой протокол аутентификации, авторизации и учета (AAA), который использует TCP для передачи данных. TACACS+ предоставляет расширенные возможности и преимущества по сравнению с RADIUS

ВЫБОР СЕРВЕРА АУТЕНТИФИКАЦИИ

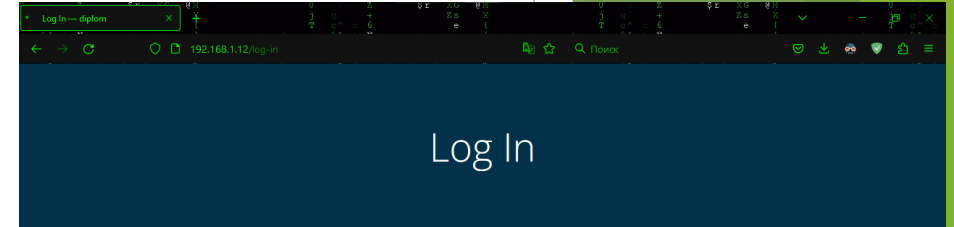
- ▶ Сервером аутентификации был выбран FreeRadius. Он предоставляет средства для проверки подлинности пользователей и авторизации доступа к сетевым ресурсам.
- ▶ Основные особенности и возможности FreeRADIUS:
- ▶ Гибкость и масштабируемость что позволяет настраивать различные методы аутентификации, включая пароли, сертификаты и тд.
- ▶ Поддержка множество модулей и расширений, которые позволяют добавлять дополнительные функциональные возможности.
- ▶ Безопасность:

FreeRADIUS
The world's most popular RADIUS Server

- ▶ Для сервера была так же разработана база данных, где хранятся учетные данные пользователей, а также разработан веб-сайт для демонстрации работы сервера аутентификации.

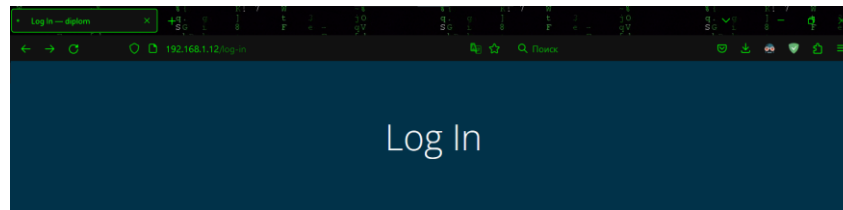


Логин или Email
Пароль
 Remember Me
[Log In](#)



ERROR: Invalid username or email. Забыли свой пароль?

Логин или Email
Пароль
 Remember Me
[Log In](#)



В настоящий момент вы вошли как user. [Выйти](#)

Заключение

- ▶ В ходе работы было проведено исследование, анализ и проектирование системы аутентификации и идентификации на основе сервера FreeRadius. Работа включала рассмотрение основных аспектов аутентификации, сравнение серверов FreeRadius и Tacsacs+, установку и настройку сервера FreeRadius, а также разработку веб-интерфейса для управления аутентификацией пользователей. Результатом работы стало создание надежной системы аутентификации на базе FreeRadius, обеспечивающей безопасность и контроль доступа пользователей в информационных системах.

