Пентест - Реальный взгляд на информационную безопасность

Ципорин Павел Игоревич
директор Департамента информационных технологий и цифрового развития Ханты-Мансийского автономного округа – Югры

Тестирование на проникновение — метод оценки безопасности компьютерных систем средствами моделирования атаки злоумышленника (возможность проверить способна ли система защиты найти и предотвратить попытку взлома ИС).

Цели: Выявить слабые места в системе (найти уязвимости). Обойти существующий комплекс СЗИ.

Кейс: кратчайший путь злоумышленника для захвата управления устройствами в инфраструктуре организации

1. Скомпрометировать сервер веб-ресурса «portalname».ru

2. Извлечь пароль пользователя «Username».

3. Используя полученную учетную запись, извлечь пароль пользователя.

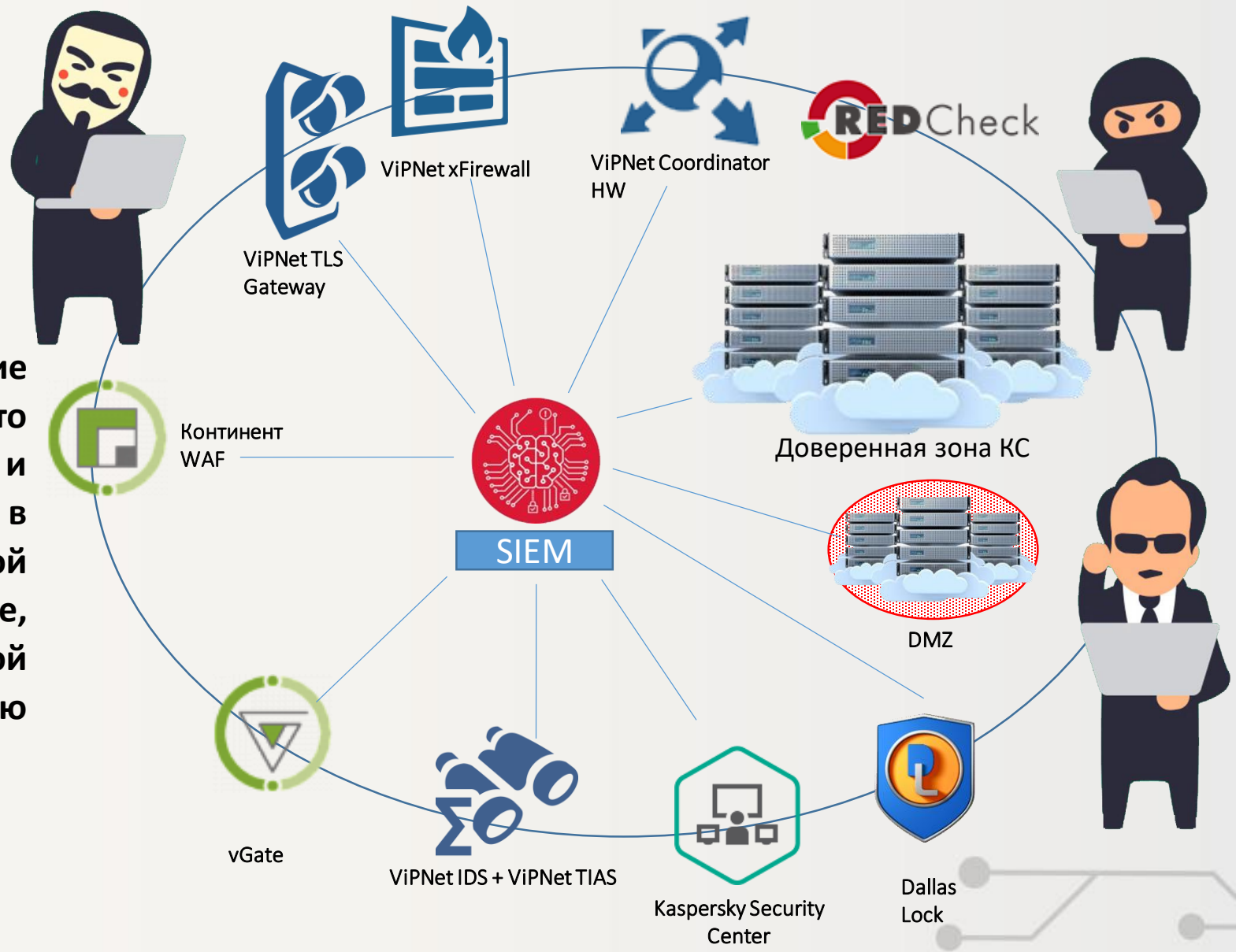
4. Провести атаку **Kerberoasting** на контролер домена.

5. Подобрать пароль учетных записей по полученным билетам.

Для повышения уровня защищенности ресурсов рекомендуется:

• устранить обнаруженные уязвимости;
• пересмотреть процесс мониторинга событий информационной безопасности;
• пересмотреть парольную политику: составить требования для всех паролей по длине и сложности, а также запретить использование стандартных или предсказуемых паролей;
• регулярно проводить различными методами анализ защищенности;
• использовать на всех серверах и рабочих местах активированную, лицензионную версию операционной системы;
• своевременно устанавливать обновления операционной системы;
• использовать актуальные версии программного обеспечения;
• сегментировать сети, жестко разделять сетевой доступ между сегментами;
• пересмотреть правила межсетевого экранирования;
• корректно настраивать безопасность веб-серверов, использовать права ограниченного доступа;
• использовать средства расширенного аудита событий операционных систем.

Не бойтесь проводить тестирование своих ресурсов и инфраструктуры – это один из наиболее эффективных и безопасных способ выявить проблемы в защищенности вашей корпоративной информационной системы. И помните, защищенность всей информационной системы определяется защищённостью самого слабого звена.



Благодарю за внимание!