Двухфакторная аутентификация на Windows Server 2012

Открывать RDP для всего мира довольно чревато - какая-нибудь зараза вполне может подобрать пароль. С другой стороны, использовать VPN тоже далеко не всегда удобно (если нужно подключить пользователя быстро или он не хочет/не может устанавливать дополнительное ПО или настраивать всякие PPTP/L2TP/etc).

Одно из решений - двухфакторная аутентификация.

Есть много решений - платных и открытых. Минусы платных (например https://duo.com/) - привязка к сервису, сервер должен иметь доступ к интернету, стоимость как самого сервиса так и звонков/СМС и т.д.

Поэтому данное решение я делаю на основе MultiOTP. Это крайне мощная штука, много чего умеет - Windows, Hyper-V, VMWare, RADIUS и совместима практически со всем. Минус на мой взгляд только один: добавление пользователей не очень удобное.

> **Настройки времени**
>
> Время на сервере и вашем устройстве (телефон, компьютер) должно совпадать, иначе ключи будут генерироваться неверно!

> **Внимание**
>
> При установке необходимо все сделать аккуратно и внимательно, в противном случае придется загружаться в безопасный режим!

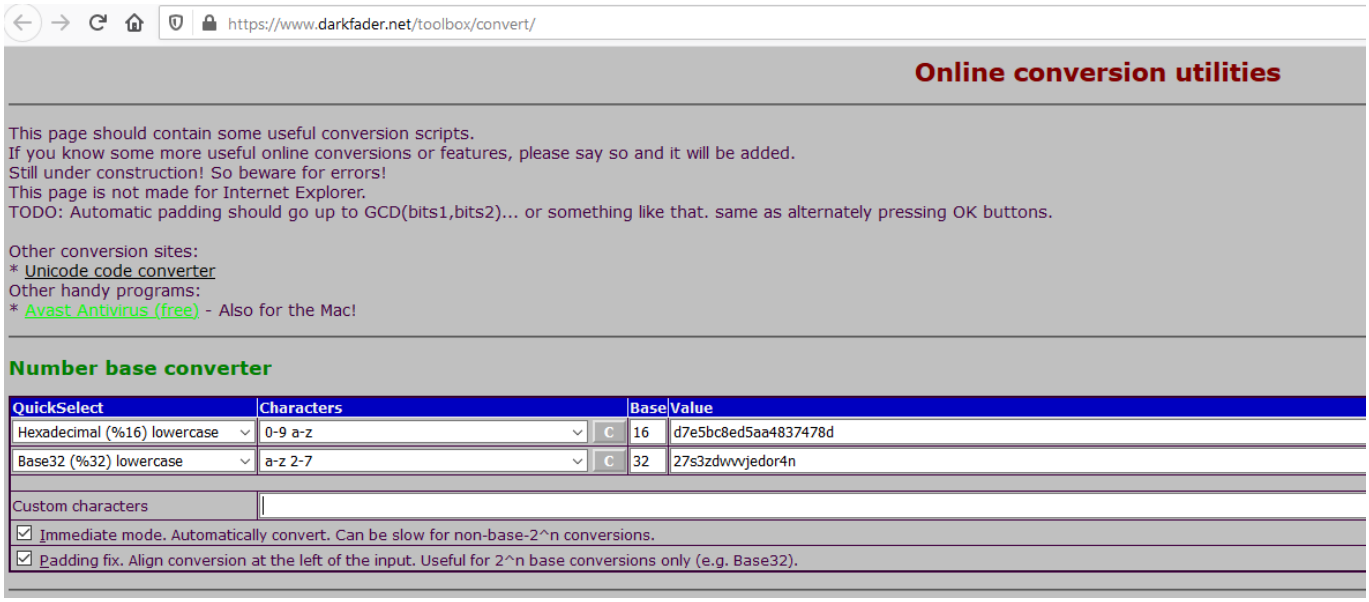
Установка MultiOTP

- Качаем MultiOTP с сайта https://www.multiotp.net
- Распаковываем архив, содержимое папки windows копируем в папку C:\MultiOTP

Создание пользователя MultiOTP

- Создаем пользователя в системе (например tester)
- Открываем командную строку с правами администратора, переходим в папку C:\MultiOTP
- Генерируем 160-битный ключ (20 шестнадцатеричных знаков) - я использую генератор паролей KeePass с шаблоном «h{20}», например он будет «d7e5bc8ed5aa4837478d». Примечание: [a-z 0-9] (маленькие буквы и цифры)
- Добавляем пользователя в MultiOTP. Формат команды: multiotp.exe -debug -create %USERNAME% %TOTP% %KEY% %PIN% %LENGTH% %LIVETIME%

- **multiotp.exe -create tester TOTP d7e5bc8ed5aa4837478d 1234 6 30**
  - %USERNAME% - существующий пользователь системы
  - %KEY% - шестнадцатеричный ключ длиной 160 бит
  - %PIN% - четырехзначный цифровой пин-код. Этот пин не будет использоваться если вы не создаете аккаунт с ключем «-prefix-pin»
  - %LENGTH% - длина пароля OTP (по умолчанию «6»)
  - %LIVETIME% - время жизни пароля OTP (по умолчанию «30» секунд)
- Сбрасываем пин-код, т.к. он нам не нужен:
  - **multiotp.exe -set tester pin=**
- Конвертируем этот ключ при помощи сервиса http://www.darkfader.net/toolbox/convert/ из «Hexadecimal (%16) lowercase» в «Base32 (%32) lowercase», у меня получился код «27s3zdwvvjedor4n»



Включаем двухфакторную аутентификацию в Windows

Качаем нужный пакет отсюда (x32 или x64):
https://github.com/LastSquirrelIT/MultiOneTimePassword-CredentialProvider

Устанавливаем, при установке включаем «Default provider», указываем путь до нашей папки с MultiOTP (в моем случае это C:\MultiOTP), заполняем «Login Text» (например «Введите логин, пароль и одноразовый код»)

Устанавливаем аутентификатор

Для генерации OTP-паролей необходимо установить аутентификатор - это может быть плагин для браузера (Google Chrome: Authenticator) или отдельное приложение на Android (приложение «Google Authenticator») или iOS.

Запускаем аутентикатор, создаем новый аккаунт: вводим понятное название и ранее созданный ключ (у меня это «27s3zdwvvjedor4n»), тип ключа: «По времени» (Time Based)

Тестируем

Подключаемся, вводим логин, пароль и полученный ключ OTP. Если все сделано правильно - попадаем на сервер.

2012, windows server, OTP, multiotp, two-factor authentication, двухфакторная аутентификация, двухфакторная авторизация, MultiOTP