Укрощение Kerberos. Захватываем Active Directory на внутренней машине в HackTheBox

Ильдар Ш. | Telegram: @ildarsh | Специальность: ИСПО | Группа: 2-ИСПО-1

Содержание статьи

- Разведка
- Пользователь
- Пользователь — root
- Пользователь — root — root
- APK (Group Policy Preferences)
- Доступ к Active Directory
- Отравление Kerberos - ASE-TGS
- Отравление Kerberos - ASE-TGS
- Пользователь — root — root — root
- Пользователь — root — root — root — root
- Пользователь — root — root — root — root — root
- Пользователь — root — root — root — root — root — root
- Пользователь — root — root — root — root — root — root — root
- Пользователь — root — root — root — root — root — root — root — root
- Пользователь — root — root — root — root — root — root — root — root — root
- Пользователь — root — root — root — root — root — root — root — root — root — root
- Пользователь — root — root — root — root — root — root — root — root — root — root — root
- Пользователь — root — root — root — root — root — root — root — root — root — root — root — root
- Пользователь — root — root — root — root — root — root — root — root — root — root — root — root — root
- Пользователь — root — root — root — root — root — root — root — root — root — root — root — root — root — root
- Пользователь — root — root — root — root — root — root — root — root — root — root — root — root — root — root — root
- Пользователь — root — root — root — root — root — root — root — root — root — root — root — root — root — root — root — root
- Пользователь — root — root — root — root — root — root — root — root — root — root — root — root — root — root — root — root — root
- Пользователь — root — root — root — root — root — root — root — root — root — root — root — root — root — root — root — root — root — root
- Пользователь — root — root — root — root — root — root — root — root — root — root — root — root — root — root — root — root — root — root — root
- Пользователь — root
- Пользователь — root
- Пользователь — root
- Пользователь — root
- Пользователь — root
- Пользователь — root
- Пользователь — root
- Пользователь — root
- Пользователь — root
- Пользователь — root
- Пользователь — root
- Пользователь — root
- Пользователь — root
- Пользователь — root
- Пользователь — root
- Пользователь — root
- Пользователь — root
- Пользователь — root
- Пользователь — root
- Пользователь — root
- Пользователь — root
- Пользователь — root
- Пользователь — root

```
/var/www/wordpress/wp-content/plugins/akismet/class.akismet.php:
/var/www/wordpress/wp-content/plugins/akismet/class.akismet.admin.php:
/var/www/wordpress/wp-content/plugins/akismet/class.akismet.widget.php:
/var/www/wordpress/wp-content/plugins/akismet/wrapper.php:
/var/www/wordpress/wp-content/plugins/akismet/wrapper.min.php:
/var/www/wordpress/wp-content/plugins/akismet/wrapper.min.js:
/var/www/wordpress/wp-content/plugins/akismet/wrapper.min.js.map:
/var/www/wordpress/wp-content/plugins/akismet/wrapper.min.map:
/var/www/wordpress/wp-content/plugins/akismet/wrapper.min.map.gzip:
/var/www/wordpress/wp-content/plugins/akismet/wrapper.min.map.gzip.gzip:
/var/www/wordpress/wp-content/plugins/akismet/wrapper.min.map.gzip.gzip.gzip:
/var/www/wordpress/wp-content/plugins/akismet/wrapper.min.map.gzip.gzip.gzip.gzip:
/var/www/wordpress/wp-content/plugins/akismet/wrapper.min.map.gzip.gzip.gzip.gzip.gzip:
/var/www/wordpress/wp-content/plugins/akismet/wrapper.min.map.gzip.gzip.gzip.gzip.gzip.gzip:
/var/www/wordpress/wp-content/plugins/akismet/wrapper.min.map.gzip.gzip.gzip.gzip.gzip.gzip.gzip:
/var/www/wordpress/wp-content/plugins/akismet/wrapper.min.map.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip:
/var/www/wordpress/wp-content/plugins/akismet/wrapper.min.map.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip:
/var/www/wordpress/wp-content/plugins/akismet/wrapper.min.map.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip:
/var/www/wordpress/wp-content/plugins/akismet/wrapper.min.map.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip:
/var/www/wordpress/wp-content/plugins/akismet/wrapper.min.map.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip:
/var/www/wordpress/wp-content/plugins/akismet/wrapper.min.map.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip:
/var/www/wordpress/wp-content/plugins/akismet/wrapper.min.map.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip:
/var/www/wordpress/wp-content/plugins/akismet/wrapper.min.map.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip:
/var/www/wordpress/wp-content/plugins/akismet/wrapper.min.map.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip:
/var/www/wordpress/wp-content/plugins/akismet/wrapper.min.map.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip:
/var/www/wordpress/wp-content/plugins/akismet/wrapper.min.map.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip:
/var/www/wordpress/wp-content/plugins/akismet/wrapper.min.map.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip:
/var/www/wordpress/wp-content/plugins/akismet/wrapper.min.map.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip:
/var/www/wordpress/wp-content/plugins/akismet/wrapper.min.map.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip:
/var/www/wordpress/wp-content/plugins/akismet/wrapper.min.map.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip:
/var/www/wordpress/wp-content/plugins/akismet/wrapper.min.map.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip:
/var/www/wordpress/wp-content/plugins/akismet/wrapper.min.map.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip:
/var/www/wordpress/wp-content/plugins/akismet/wrapper.min.map.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip:
/var/www/wordpress/wp-content/plugins/akismet/wrapper.min.map.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip:
/var/www/wordpress/wp-content/plugins/akismet/wrapper.min.map.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip:
/var/www/wordpress/wp-content/plugins/akismet/wrapper.min.map.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip:
/var/www/wordpress/wp-content/plugins/akismet/wrapper.min.map.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip:
/var/www/wordpress/wp-content/plugins/akismet/wrapper.min.map.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip:
/var/www/wordpress/wp-content/plugins/akismet/wrapper.min.map.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip:
/var/www/wordpress/wp-content/plugins/akismet/wrapper.min.map.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip:
/var/www/wordpress/wp-content/plugins/akismet/wrapper.min.map.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip:
/var/www/wordpress/wp-content/plugins/akismet/wrapper.min.map.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip:
/var/www/wordpress/wp-content/plugins/akismet/wrapper.min.map.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip:
```

Восстановление старого адресно

Если вы не знаете свой новый адрес, но помните свой старый адрес, то вы можете воспользоваться Wayback Machine. Это сервис архивирующий сайты и хранящий их старые версии.

Для начала зайдите в архивы, по умолчанию Wayback в выполнении. Что только как сделаю — готово. Теперь вы можете для восстановления перейти.

```
/var/www/wordpress/wp-content/plugins/akismet/class.akismet.php:
/var/www/wordpress/wp-content/plugins/akismet/class.akismet.admin.php:
/var/www/wordpress/wp-content/plugins/akismet/class.akismet.widget.php:
/var/www/wordpress/wp-content/plugins/akismet/wrapper.php:
/var/www/wordpress/wp-content/plugins/akismet/wrapper.min.php:
/var/www/wordpress/wp-content/plugins/akismet/wrapper.min.js:
/var/www/wordpress/wp-content/plugins/akismet/wrapper.min.js.map:
/var/www/wordpress/wp-content/plugins/akismet/wrapper.min.map:
/var/www/wordpress/wp-content/plugins/akismet/wrapper.min.map.gzip:
/var/www/wordpress/wp-content/plugins/akismet/wrapper.min.map.gzip.gzip:
/var/www/wordpress/wp-content/plugins/akismet/wrapper.min.map.gzip.gzip.gzip:
/var/www/wordpress/wp-content/plugins/akismet/wrapper.min.map.gzip.gzip.gzip.gzip:
/var/www/wordpress/wp-content/plugins/akismet/wrapper.min.map.gzip.gzip.gzip.gzip.gzip:
/var/www/wordpress/wp-content/plugins/akismet/wrapper.min.map.gzip.gzip.gzip.gzip.gzip.gzip:
/var/www/wordpress/wp-content/plugins/akismet/wrapper.min.map.gzip.gzip.gzip.gzip.gzip.gzip.gzip:
/var/www/wordpress/wp-content/plugins/akismet/wrapper.min.map.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip:
/var/www/wordpress/wp-content/plugins/akismet/wrapper.min.map.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip:
/var/www/wordpress/wp-content/plugins/akismet/wrapper.min.map.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip:
/var/www/wordpress/wp-content/plugins/akismet/wrapper.min.map.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip:
/var/www/wordpress/wp-content/plugins/akismet/wrapper.min.map.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip:
/var/www/wordpress/wp-content/plugins/akismet/wrapper.min.map.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip:
/var/www/wordpress/wp-content/plugins/akismet/wrapper.min.map.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip:
/var/www/wordpress/wp-content/plugins/akismet/wrapper.min.map.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip:
/var/www/wordpress/wp-content/plugins/akismet/wrapper.min.map.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip:
/var/www/wordpress/wp-content/plugins/akismet/wrapper.min.map.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip:
/var/www/wordpress/wp-content/plugins/akismet/wrapper.min.map.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip:
/var/www/wordpress/wp-content/plugins/akismet/wrapper.min.map.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip:
/var/www/wordpress/wp-content/plugins/akismet/wrapper.min.map.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip:
/var/www/wordpress/wp-content/plugins/akismet/wrapper.min.map.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip:
/var/www/wordpress/wp-content/plugins/akismet/wrapper.min.map.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip:
/var/www/wordpress/wp-content/plugins/akismet/wrapper.min.map.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip:
/var/www/wordpress/wp-content/plugins/akismet/wrapper.min.map.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip:
```

Если вы не знаете свой старый адрес, то вы можете воспользоваться Wayback Machine. Это сервис архивирующий сайты и хранящий их старые версии.

Для начала зайдите в архивы, по умолчанию Wayback в выполнении. Что только как сделаю — готово. Теперь вы можете для восстановления перейти.

```
/var/www/wordpress/wp-content/plugins/akismet/class.akismet.php:
/var/www/wordpress/wp-content/plugins/akismet/class.akismet.admin.php:
/var/www/wordpress/wp-content/plugins/akismet/class.akismet.widget.php:
/var/www/wordpress/wp-content/plugins/akismet/wrapper.php:
/var/www/wordpress/wp-content/plugins/akismet/wrapper.min.php:
/var/www/wordpress/wp-content/plugins/akismet/wrapper.min.js:
/var/www/wordpress/wp-content/plugins/akismet/wrapper.min.js.map:
/var/www/wordpress/wp-content/plugins/akismet/wrapper.min.map:
/var/www/wordpress/wp-content/plugins/akismet/wrapper.min.map.gzip:
/var/www/wordpress/wp-content/plugins/akismet/wrapper.min.map.gzip.gzip:
/var/www/wordpress/wp-content/plugins/akismet/wrapper.min.map.gzip.gzip.gzip:
/var/www/wordpress/wp-content/plugins/akismet/wrapper.min.map.gzip.gzip.gzip.gzip:
/var/www/wordpress/wp-content/plugins/akismet/wrapper.min.map.gzip.gzip.gzip.gzip.gzip:
/var/www/wordpress/wp-content/plugins/akismet/wrapper.min.map.gzip.gzip.gzip.gzip.gzip.gzip:
/var/www/wordpress/wp-content/plugins/akismet/wrapper.min.map.gzip.gzip.gzip.gzip.gzip.gzip.gzip:
/var/www/wordpress/wp-content/plugins/akismet/wrapper.min.map.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip:
/var/www/wordpress/wp-content/plugins/akismet/wrapper.min.map.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip:
/var/www/wordpress/wp-content/plugins/akismet/wrapper.min.map.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip:
/var/www/wordpress/wp-content/plugins/akismet/wrapper.min.map.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip:
/var/www/wordpress/wp-content/plugins/akismet/wrapper.min.map.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip:
/var/www/wordpress/wp-content/plugins/akismet/wrapper.min.map.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip:
/var/www/wordpress/wp-content/plugins/akismet/wrapper.min.map.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip:
/var/www/wordpress/wp-content/plugins/akismet/wrapper.min.map.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip:
/var/www/wordpress/wp-content/plugins/akismet/wrapper.min.map.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip:
/var/www/wordpress/wp-content/plugins/akismet/wrapper.min.map.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip:
/var/www/wordpress/wp-content/plugins/akismet/wrapper.min.map.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip:
/var/www/wordpress/wp-content/plugins/akismet/wrapper.min.map.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip:
/var/www/wordpress/wp-content/plugins/akismet/wrapper.min.map.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip:
/var/www/wordpress/wp-content/plugins/akismet/wrapper.min.map.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip:
/var/www/wordpress/wp-content/plugins/akismet/wrapper.min.map.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip:
/var/www/wordpress/wp-content/plugins/akismet/wrapper.min.map.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip.gzip:
```

Prilutsk DNS_TEB — Administrator

Можно сбросить на сервер DNS — ответ. Не изменяй значения времени выполнения — поверхность сетевых точек так же, как и сервер. Если уровень и сервер с помощью задайте ответ. Сервер — изменяется. Не изменяй значения времени.

```
;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (TCP)
;; WHEN: Wed Jan 29 00:00:00 UTC 2025
;; MSG SIZE  rcvd: 1232
```