????? 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. C

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.

Revision #8
Created 1 October 2025 17:16:42 by Admin
Updated 20 November 2025 16:23:26 by Admin