Поиск информации и эксфильтрация

Сабина Жигальская
Специалист по комплексной защите информации

Skillbox

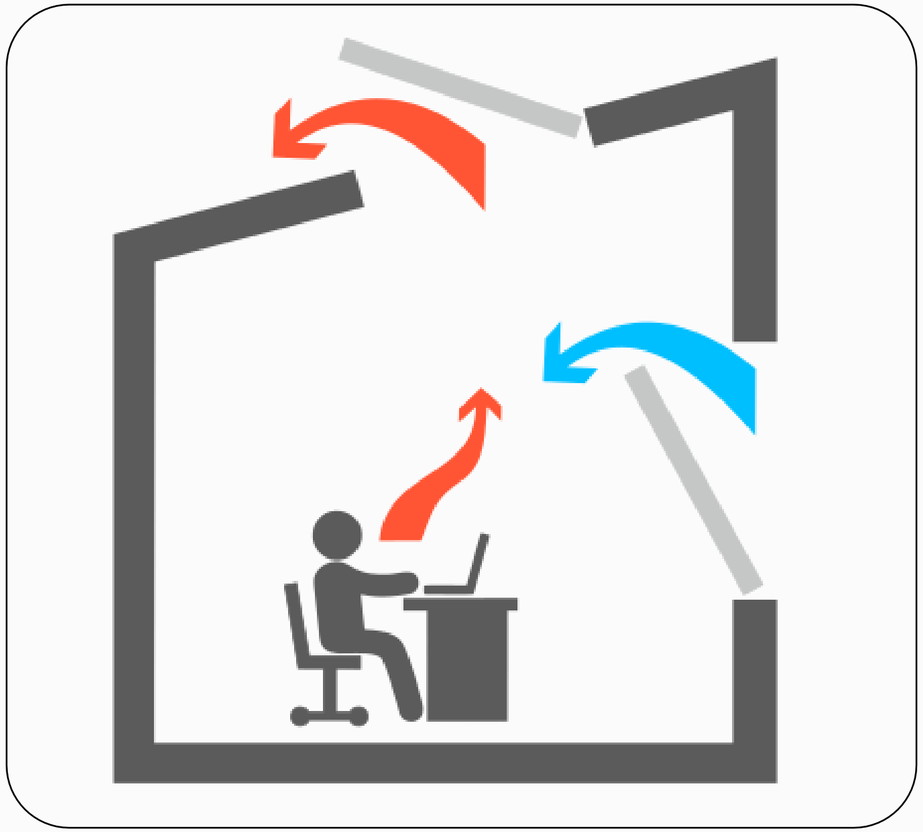
Цели урока

Узнать:

- Что такое эксфильтрация данных?
- Что такое Mitre?
- Как происходит поиск информации?

Сбор и поиск информации

Поиск информации (OSINT) — процесс, в ходе которого производится поиск, выбор, сбор и анализ информации по открытым источникам.



OSINT

Методы сбора информации:

- Автоматизированными средствами
- При помощи сервисов
- Ручным методом

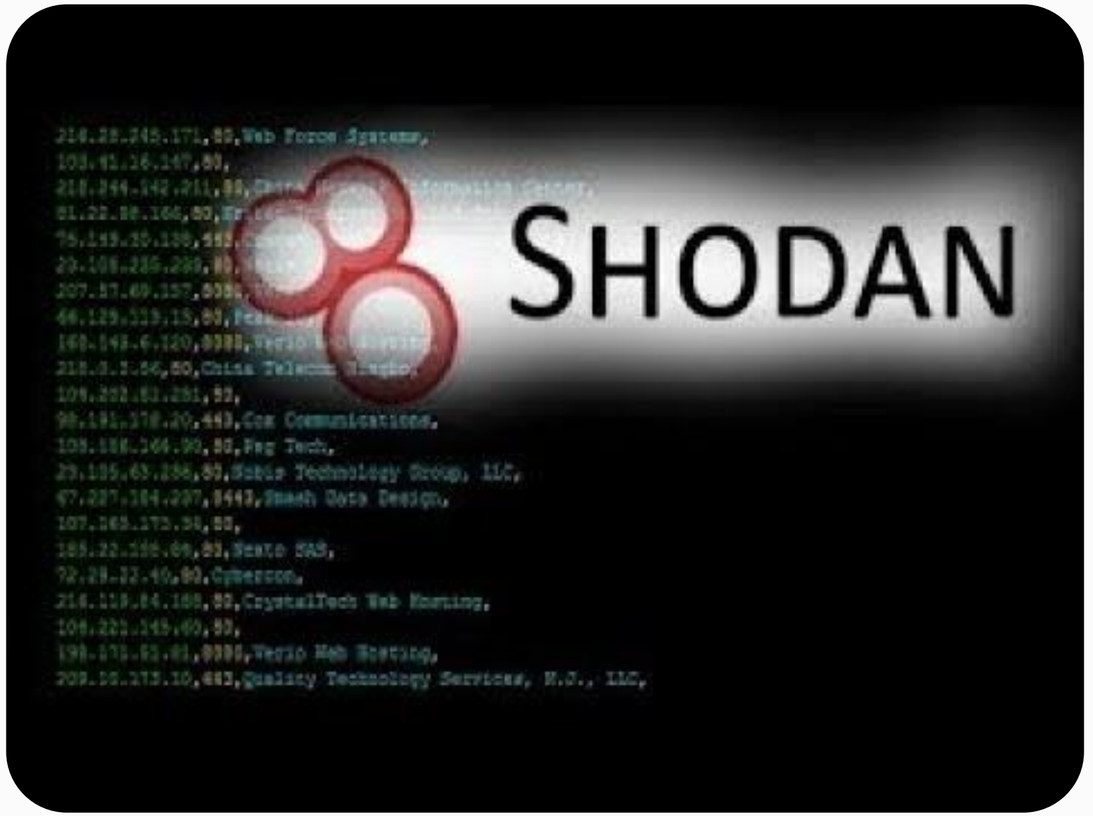
Автоматизированные средства

Собирают следующую техническую информацию по доменному имени:

- перечень активных сетевых узлов и портов
- перечень имён сотрудников
- перечень почтовых адресов
- перечень поддоменов
- аккаунты в социальных сетях
- API-ключи
- поиск по иным внешним базам

Инструменты сбора информации

Shodan — поисковая система, которая позволяет пользователям искать различные типы серверов, подключённых к интернету, с использованием различных фильтров.



Инструменты сбора информации

DNSdumpster — это бесплатный инструмент для изучения доменов, который может находить поддомены, связанные с целевым доменом.

Поиск по открытым источникам

Помогает понять, как выглядит организация
для внешнего потенциального злоумышленника.
Это первый этап эксфильтрации.

Эксфильтрация — кража данных.
Это несанкционированное копирование, передача или получение данных с компьютера или сервера жертвы.

Матрица Mitre

Матрицы Mitre позволяют отслеживать
эволюцию тактик и техник.

В матрице выделены 9 техник:

- автоматизированная эксфильтрация
- сжатие данных
- шифрование данных
- ограничение размера передаваемых данных
- эксфильтрация через альтернативный протокол
- эксфильтрация через командный сервер
- эксфильтрация через альтернативный канал связи
- физическая эксфильтрация
- передача по расписанию

Выводы урока

- Узнали про поиск и сбор данных
- Узнали, что такое эксфильтрация
- Рассмотрели техники атак