Teach Me Skills

Mittre Att&ck

Типы атак II

Teach Me Skills

Вопросы по предыдущим темам или ДЗ

Mini-quize по прошлым темам:

1. **Какие существуют тактики для закрепления ПО в системе?**
2. **Зачем существует матрица Mittre?**
3. **Какие основные пункты к СКС?**
4. **Что такое кейлоггинг?**
5. **Какие виды Reconnaissance (Разведка) существуют?**

Mini-quize по новой теме:

1. **Какие, как вы думаете, еще существуют матрицы Mittre по аналогии с матрицей атакующих?**
2. **Что вредного могут сделать злоумышленники по отношению к инфраструктуре?**
3. **Как можно защититься от атаки?**
4. **Как необходимо реагировать на атаку?**
5. **Где хранятся логи систем Win/Unix?**

Teach Me Skills

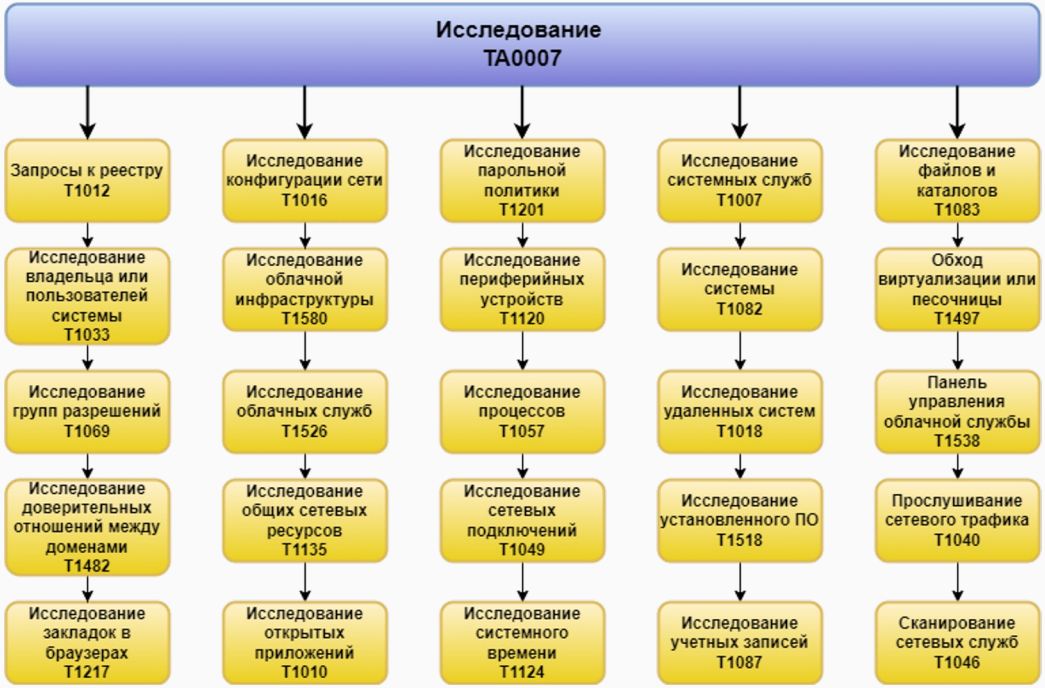
План занятия

1. Разберем остальные матрицы Mittre
2. Изучим оставшиеся тактики и техники злоумышленников
3. Разберем несколько инцидентов при помощи матрицы Mittre Att&ck
4. Придумаем возможные способы защиты от этих атак при помощи матрицы Defend
5. Разработаем план реагирования на инцидент при помощи матрицы Re&ct

Discovery

Teach Me Skills

Discovery(исследование) - состоит из методов, которые злоумышленник может использовать для получения знаний о системе и внутренней сети.

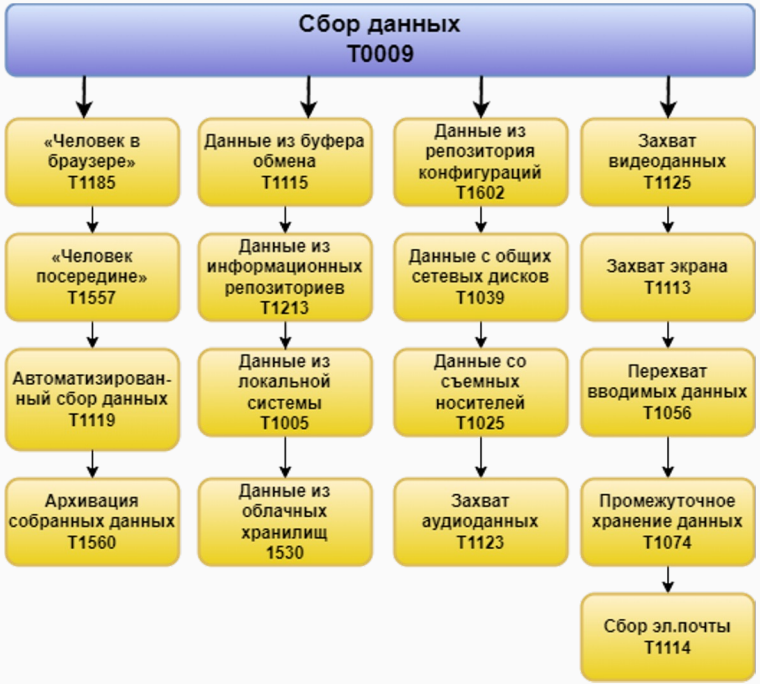


Lateral movement

Lateral movement (премещение внутри периметра) - состоит из методов, которые злоумышленники используют для входа и управления удаленными системами в сети.

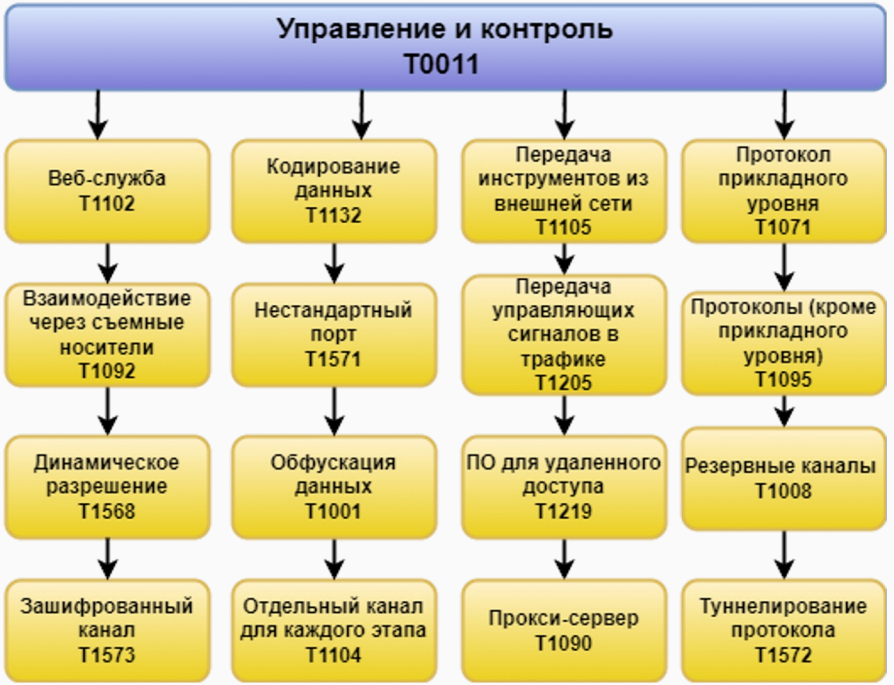
Collection

Collection (сбор данных) - состоит из методов, которые злоумышленники могут использовать для сбора информации, и источников, из которых собирается информация, имеющая отношение к достижению целей.



Command & Control

Command & Control (управление и контроль) – состоят из методов, которые злоумышленники могут использовать для связи с системами, находящимися под их контролем в сети жертвы.



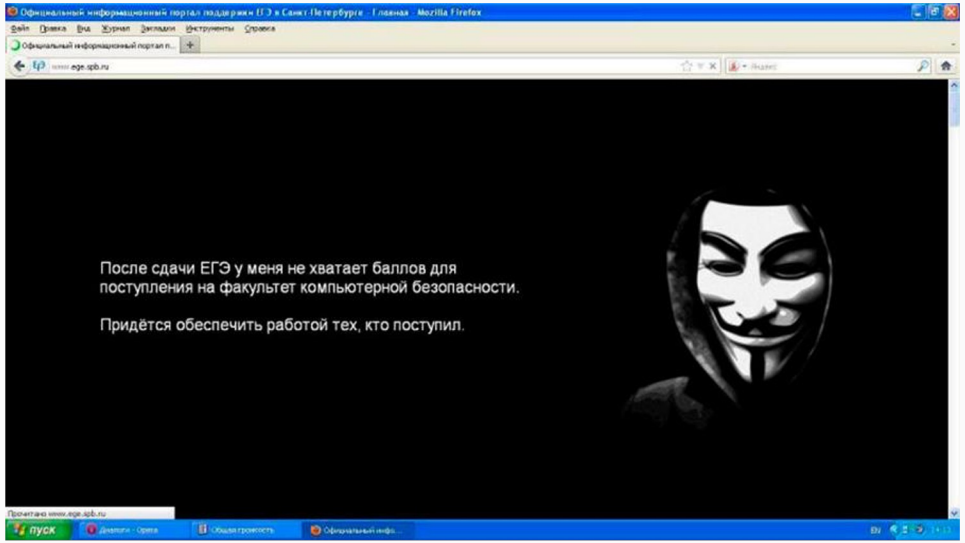
Exfiltration

Exfiltration (Эксфильтрация данных) - состоит из методов, которые злоумышленники могут использовать для кражи данных из вашей сети.

Эксфильтрация, или экстракция — тактика перемещения персонала с территории, находящейся под контролем противника, и доставки в безопасную зону.

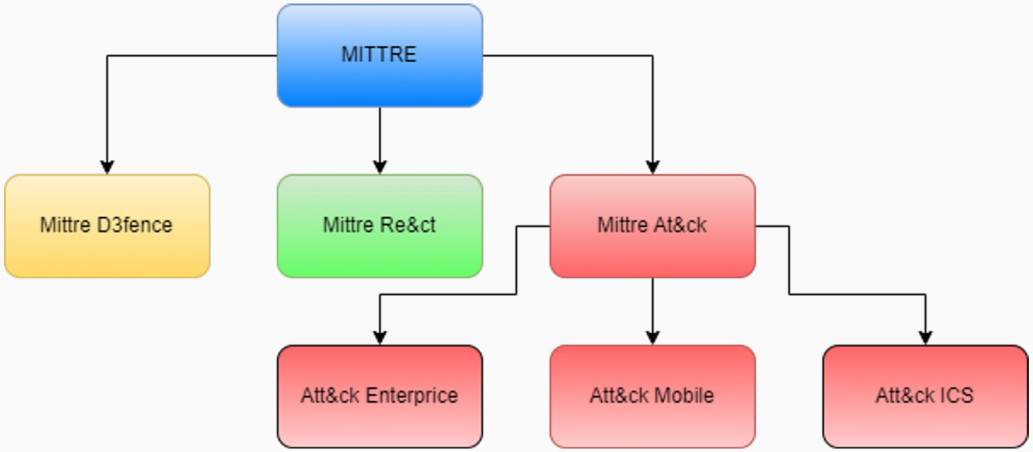
Impact

Impact (воздействие) - состоит из методов, которые злоумышленники используют для нарушения доступности или нарушения целостности путем манипулирования бизнес-процессами и операционными процессами.



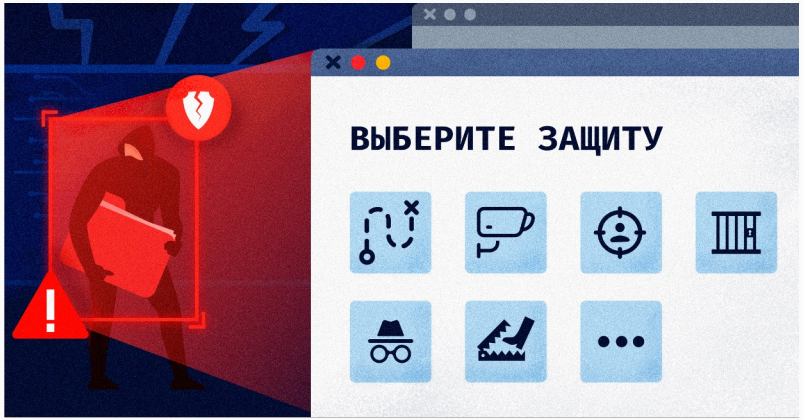
Другие матрицы mittre att&ck

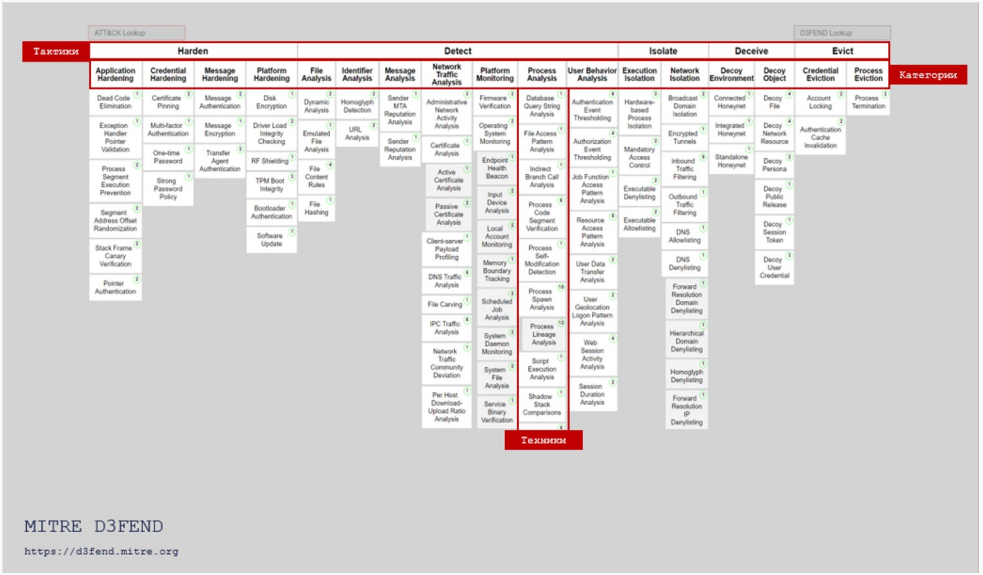
Примерная структура матриц Mittre



Mittre D3fend

D3fend – база, матрица, которая содержит структурированный набор техник для обеспечения контрмер.





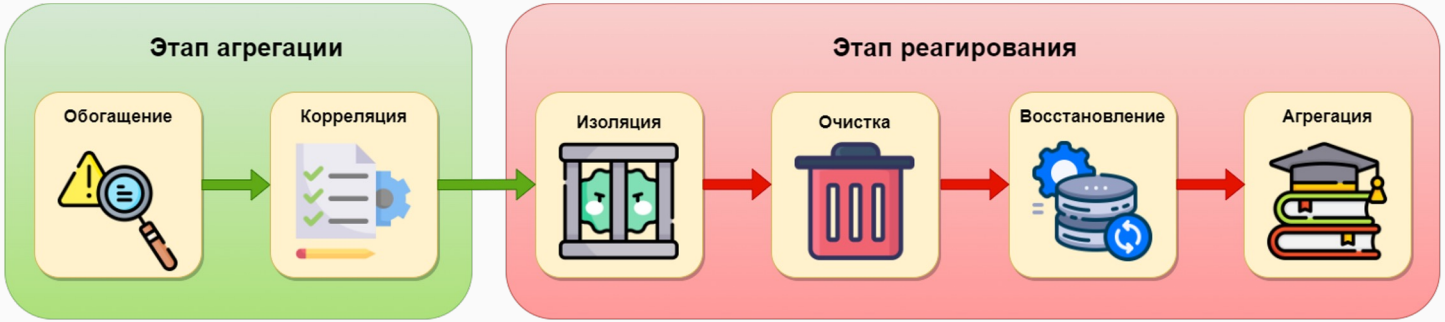
Mittre Re&ct

Реагирование на инциденты (Incident Response, **IR**) — комплекс мероприятий по обнаружению и прекращению кибератаки или утечки данных из инфраструктуры организации. Так же включает в себя действия по устранению последствий.

Схема

Фреймворк создан для сбора, описания и классификации опасных техник реагирования на аварии.

Общее представление о реагировании на компьютерные инциденты



STIX

Структурированное выражение информации об угрозах (STIX™) — это язык и формат сериализации, используемый для обмена информацией о киберугрозах (CTI).

TIP платформы

Kaspersky

Threat Intelligence Portal

ссылка установка MISP

ДЗ

Основное задание:
Вы – хакер находящийся в интернете, вам необходимо проникнуть внутрь инфраструктуры и скопроментировать 2 цели.
1-ая компьютер глав буха компании
2-ая ноутбук системного администратора.
Применяя матрицу Att&ck.

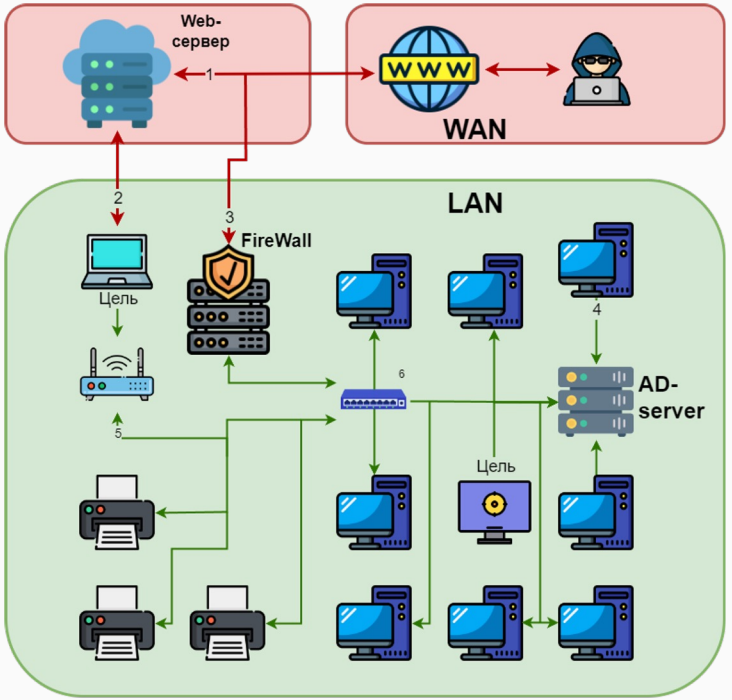


Схема атакуемой инфраструктуры

***Задание:**
Необходимо разработать план защиты и план реагирования на атаку, которую вы провели гипотетически в предыдущем задании.
Используя матрицы D3fence и Re&ct