Mittre Att&ck

Часть 1

Teach Me Skills

Вопросы по предыдущим темам или ДЗ

Mini-quize по прошлым темам:

1. **Какими методами можно собрать первичную информацию для атаки?**
2. **Почему наиболее уязвимым звеном является сотрудник?**
3. **Насколько эффективен D-DOS?**
4. **Каким образом можно проникнуть в защищенную сеть?**

Mini-quize по новой теме:

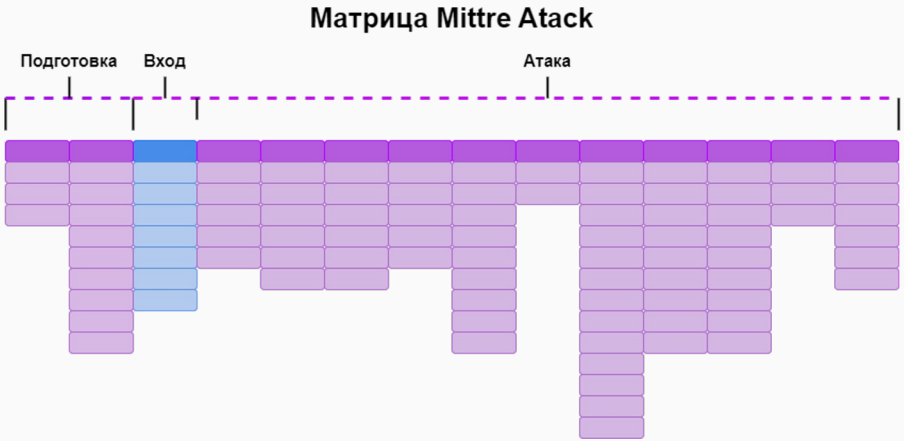
1. **Что такое матрица атак? И зачем она может применяться?**
2. **Что такое killchain?**
3. **В чем суть подписанных файлов?**
4. **Что такое обфускация?** `:(){ :|:& };:`
5. **Зачем нужны токены доступа?**

Teach Me Skills

План занятия

1. Разберем что такое матрица атак
2. Поймем как можно более точно определять и анализировать атаки
3. Разберем понятие убийственной цепочки
4. Изучим методики закрепления в системе
5. Разберем способы проникновения и сокрытия действий в системе.
6. Изучим методики повышения привилегий.

MITRE ATT&CK



Матрица Mittre Attack - инструмент для обеспечения структурированного представления о различных тактиках и техниках,используемых злоумышленниками. Который помогает обнаруживать, предотвращать и реагировать на угрозы более эффективно.

MITRE ATT&CK

MITRE ATT&CK (Adversarial tactics, techniques and common knowledge) – основанная на реальных наблюдениях глобальная база знаний компании MITRE, содержащая описание тактик, приемов и методов, используемых злоумышленниками. Она представлена в виде матриц, постоянно пополняется и широко используется в следующих направлениях:

- Формирование профилей APT-группировок, эмулирование их действий;
- Анализ уязвимостей в системе защиты информации организации;
- Распространение информации об актуальных угрозах;
- Приоритизация наиболее критичных техник и тактик;
- Проведение исследований в области ИБ.

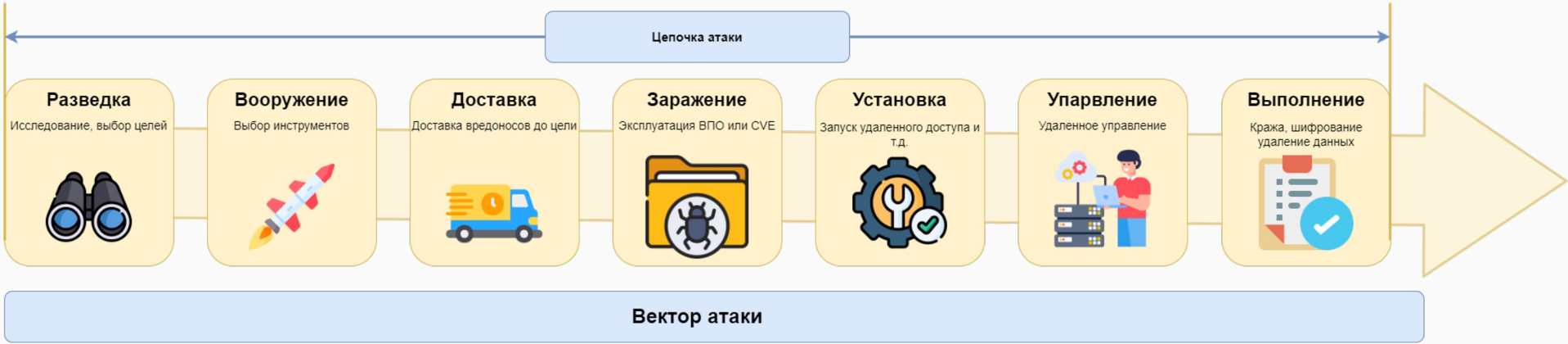
Многие исследователи пытались сделать маппинг MITRE ATT&CK на Cyber Kill Chain, но по ходу процесса возникало очень много споров. Чаще всего при анализе отчетов вы будете встречаться с MITRE ATT&CK.

KillChain(CKC)

CKC - инструмент нацеленный на понимание, как компании могут усилить обороноспособность своего окружения, ловя и останавливая угрозы на каждой фазе жизненного цикла атаки.

CKC - показывает нам, что в то время как хакеры для достижения успеха должны пройти все этапы процесса, нам, обороняющейся стороне, «всего» лишь необходимо остановить атаку на любом этапе процесса, чтобы, как минимум, не позволить атаке полностью добиться своей цели.

подробное описание



Reconnaissance

Reconnaissance (Разведка) - состоит из методов, в которых противник активно или пассивно собирает информацию, которая может быть использована для поддержки целеуказания.

Что можно применять:

Whois – инфо о домене
Shodan – поиск открытых серверов
TiDos – инфо об уязвимостях
God Eye – поиск информации о людях
TheHarvester – инфо о доменах, почтах
Nmap – сканирование сети
WhatWeb – информация о сайте

Reconnaissance

Разведка делится на **пассивную** (без использования специального ПО) и **активную** (когда используется специальное ПО).

Пассивную разведку обнаружить невозможно, злоумышленник действует, используя возможности, доступные любому пользователю. Единственный способ противодействия ей – максимально ограничить объем общедоступных данных, разграничить доступ к внутренним данным сотрудников организации (только необходимые им данные).

Активную разведку могут обнаружить правильно настроенные средства защиты информации, такие как межсетевые экраны (МЭ), системы обнаружения вторжений (СОВ).
В ходе разведки собирается:
• IP-адреса всех внешних интерфейсов организации;
• DNS и Whois информация;
• Информация о всех доступных извне сервисов организации, портах на которых они подняты;
• Информация об уязвимостях используемых сервисов и сетевого оборудования;
• Почты сотрудников;[SOC]
• Организации, с которыми целевая организация осуществляет взаимодействие;
• Информация о политиках безопасности организации, используемых СЗИ;
• Используемые в организации ОС с указанием их версий.

Resource Development

Resource Development (Подготовка ресурсов) - состоит из методов, в которых злоумышленники создают, покупают или компрометируют/крадут ресурсы, которые могут быть использованы для поддержки таргетинга.

Для выполнения этой цели ему необходимо найти уязвимость (неправильную конфигурацию), которая позволит ему доставить во внутренний периметр организации ВПО, которое, в свою очередь, установит изнутри соединение с хостом злоумышленника.

Что можно применять:

SCA

Initial Access

Initial Access (Первоначальный доступ) - состоит из методов, которые используют различные векторы входа для получения первоначальной точки закрепления в сети.

Что применяется:
Эксплуатация CVE
Различное ВПО
Компроментация цепочки поставок
Социальная инженерия
Drive-by

Persistence

Persistence (закрепление) - состоит из методов, которые злоумышленники используют для сохранения доступа к системам после перезапуска, изменения учетных данных и других прерываний, которые могут прервать их доступ.

Что могут применять:
Службы (демоны)
Автозапуск
Изменение сценариев
Компроментация системных файлов
Загрузка до ОС

Privilege Escalation

Privilege Escalation (Эскалация привелегий) - это методы, которые злоумышленники используют для получения разрешений более высокого уровня в системе или сети.

Что могут применять:

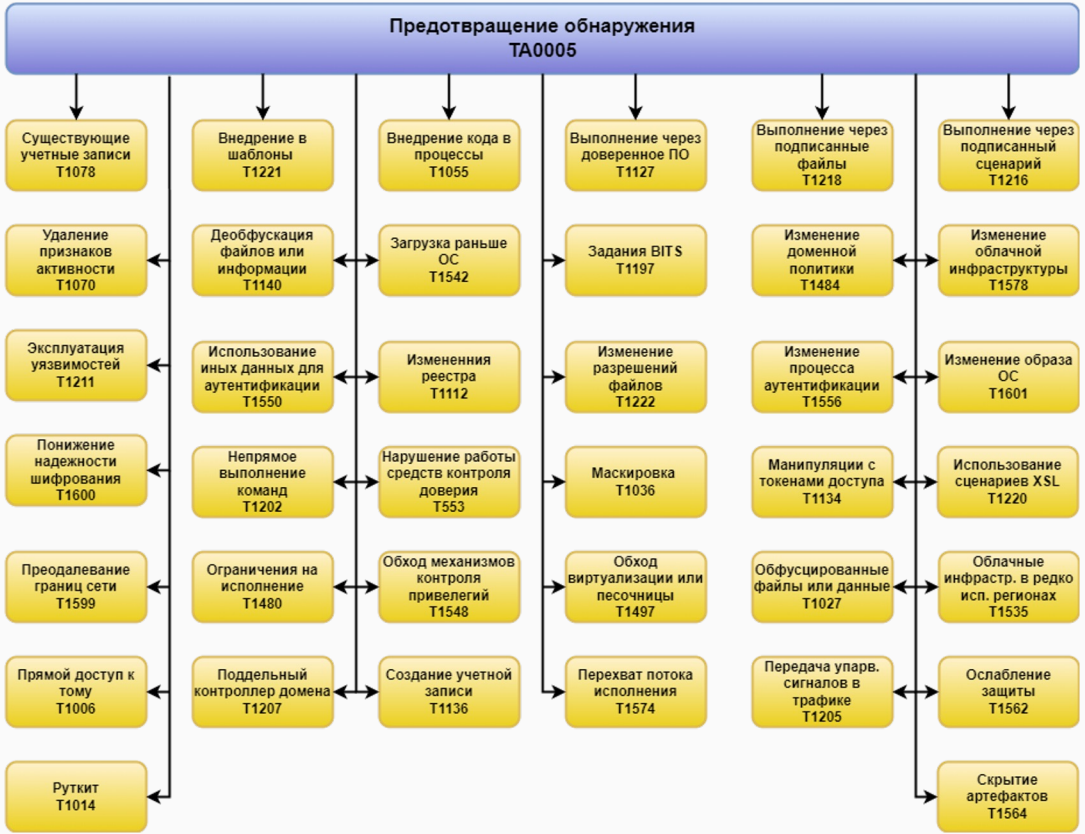
Иньекции кода
Различные CVE
Изменение токенов доступа
Создание процессов
Перехват исполнения
Инструментарий управления

Defence Evasion

Defence Evasion (предотвращение обнаружения) – включает в себя список методик, которые злоумышленники используют, чтобы избежать обнаружения во время компрометации.

Что применяется:

[Обфускация](#)
Маскировка
Внедрение кода
Службы
Изменение реестра
Модификация файлов



Credential Access

Credential Access (Получение учетных данных) - состоит из методов кражи учетных данных, таких как имена учетных записей и пароли. Методы, используемые для получения учетных данных, включают кейлоггер или дамп учетных данных.

Что применяется:

Кейлоггинг

Перехват ключей, токенов

Спуфинг

MITM

Использование CVE

MITRE ATT&CK

На данный момент на официальном сайте MITRE ATT&CK представлено 3 основные матрицы:

- Enterprise (описывает тактики и техники для известных серверных, облачных ОС и ОС для ПК).
- Mobile (тактики и техники для Android и iOS).
- ICS (Industrial Control Systems) содержит тактики и техники, охватывающие SCADA и DSC системы управления тех. процессами предприятий).

Столбцы матриц – это тактики (TA), строки – техники. Они все кликабельны, имеют описание, а также советы по ее нейтрализации (Mitigation) и детектированию (Detection).

MITRE ATT&CK

Также на официальном сайте присутствует информация о самых известных APT-группировках (APT – Advanced Persistence Threat).

Advanced Persistence Threat (APT) — термин кибербезопасности, означающий противника, обладающего современным уровнем специальных знаний и значительными ресурсами, которые позволяют ему создавать угрозу опасных кибератак.

Обобщенная таблица группировок

APT-группировки представляют наибольшую опасность для информационной инфраструктуры организаций. Поэтому в данном курсе мы будем опираться на описание их тактик и техники для организации детектирования их активности в своей системе, а также поиска индикаторов компрометации.

MITRE ATT&CK

Есть ли возможность найти матрицу в переводе на русский?

Да, компания Positive Technologies предоставляет такую возможность

MITRE ATT&CK Navigator

Теперь вы знаете о матрицах MITRE и об основных тактиках и техниках злоумышленников. Но что делать дальше, ведь их так много? Целесообразно ли защищаться от всех них? Матрица Enterprise в хорошем разрешении влезет не каждый экран. Ответ прост – из каждой матрицы нужно убрать лишние, не актуальные для вашей организации тактики и техники. В этом нам поможет онлайн-инструмент под названием MITRE ATT&CK Navigator.