ПРОВЕДЕНИЕ ТЕСТИРОВАНИЙ НА ПРОНИКНОВЕНИЕ И АНАЛИЗА УЯЗВИМОСТЕЙ

Сергей Леонтьев
Заместитель руководителя отдела консалтинга
АО «ДиалогНаука»

ДиалогНаука

Введение

Виды услуг по тестированию

Главная — Услуги — Тестирование на проникновение и анализ защищенности

ТЕСТИРОВАНИЕ НА ПРОНИКНОВЕНИЕ И АНАЛИЗ ЗАЩИЩЕННОСТИ

Тестирование на проникновение в рамках выполнения требования Положений Банка России по защите информации, требований SWIFT CSP, требований PCI DSS

Аудит Интернет-порталов и web-приложений

Анализ безопасности мобильных приложений

Аудит безопасности беспроводных сетей

Внутреннее тестирование на проникновение

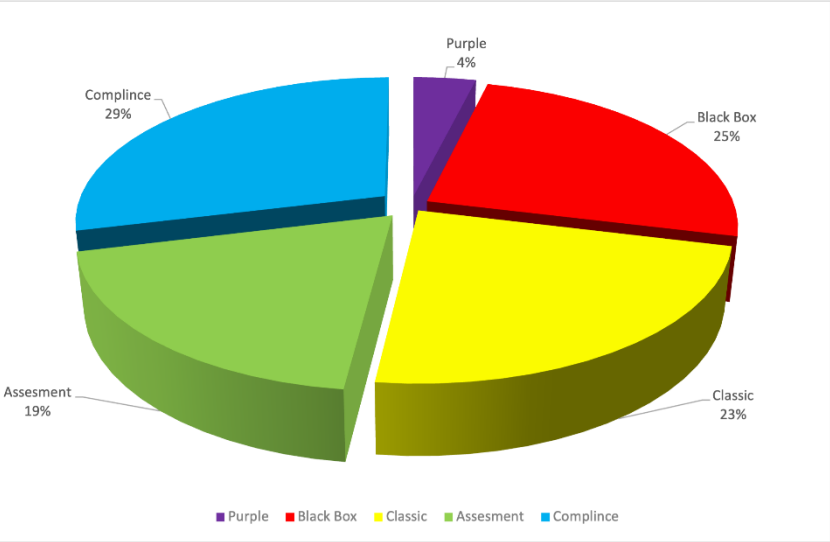
Проведение тестирования на проникновение с целью оценки защищенности от внешних угроз

Виды услуг по тестированию

Услуга	Стандарт	Периодичность
Тестирование на проникновение в рамках выполнения требования Положений Банка России по защите информации, требований SWIFT CSP, требований PCI DSS и т.д.	757-П ГОСТ 57580 PCI DSS SWIFT МинЦифры	ежегодно или чаще
Проведение тестирования на проникновение с целью оценки защищенности от внешних угроз		разово или регулярно (обычно ежегодно)
Внутреннее тестирование на проникновение		разово или регулярно (обычно ежегодно)
Аудит Интернет-порталов и web-приложений		разово или постоянно (например при каждом релизе)
Анализ безопасности мобильных приложений		разово или постоянно (например при каждом релизе)
Аудит безопасности беспроводных сетей	PCI DSS	разово или регулярно
Внешние ежеквартальные сканирования ASV	PCI DSS	ежеквартально
Внутреннее ежеквартальные сканирования	PCI DSS	ежеквартально и после серьезных изменений инфраструктуры

Статистика по проектам

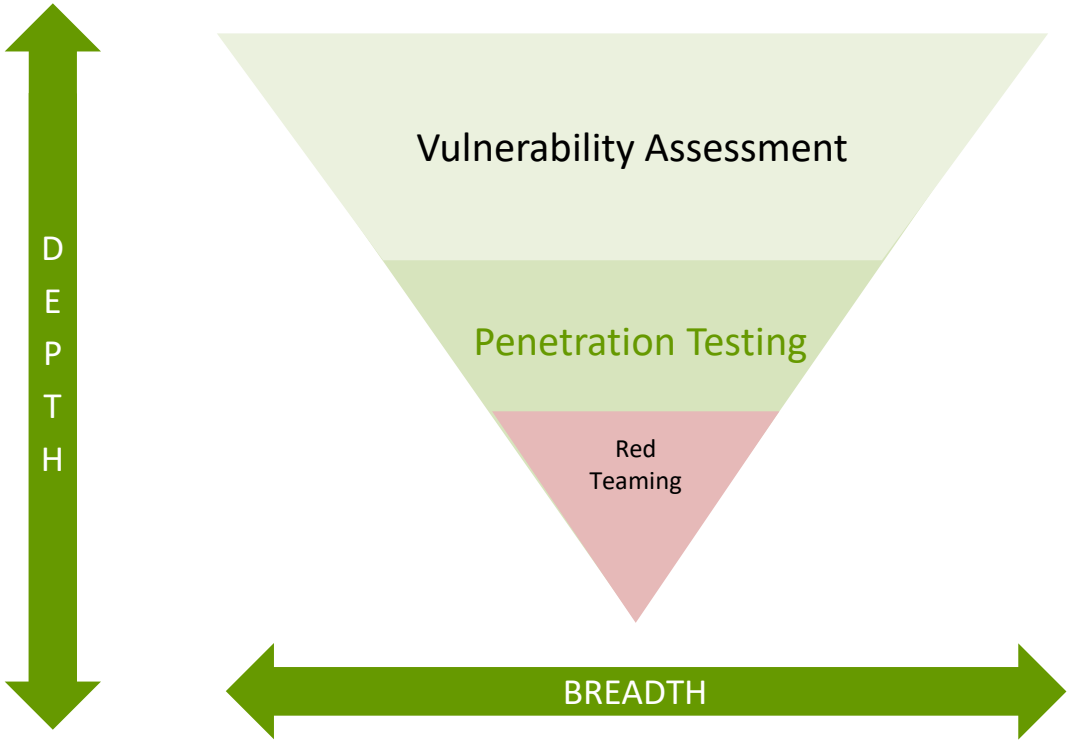
Приблизительная классификация проектов, связанных с тестированием на проникновение и анализом уязвимостей



Топ выполненных проектов за последний год:

- ✓ Compliance (PCI DSS, SWIFT, ЦБ, МинЦифры etc)
- ✓ Black Box (Red Teaming)
- ✓ Classic (внутренние и/или внешние)
- ✓ Assessment (WEB, Mobile etc)
- ✓ Purple Teaming

Подходы к проведению тестирования



Подходы к проведению тестирования

Vulnerability Assessment:

1. Процесс выявления, классификации и определения приоритетности устранения уязвимостей.

2. В первую очередь позволяет понять какие уязвимости и в каком количестве присутствуют в инфраструктуре, а также определить приоритет их устранения.

3. Результаты возможно использовать для базовой оценки рисков ИБ, при этом необходимо понимать контекст в котором находятся данные уязвимости.

4. Обычно является частью процесса Vulnerability/Patch Management и Compliance в организации.

Подходы к проведению тестирования

Penetration Testing:

1. Моделирование реальных атак на контролируемую среду для выявления и эксплуатации уязвимостей.

2. Обычно подразумеваются методы и мотивация реальных злоумышленников.

3. Обычно подразумевается поиск уязвимостей в сетях, системах и приложениях.

4. В некоторых случаях подразумеваются атаки с использованием методов социальной инженерии.

Подходы к проведению тестирования

Red Teaming:

1. Обычно представляет из себя непрерывный процесс симуляции атак с целью оценки всех существующих процессов защиты организации и повышения осведомленности задействованных в этом процессе лиц.

2. При этом имитируется тактика, методы и процедуры (TTP) конкретных субъектов угроз или сценариев.

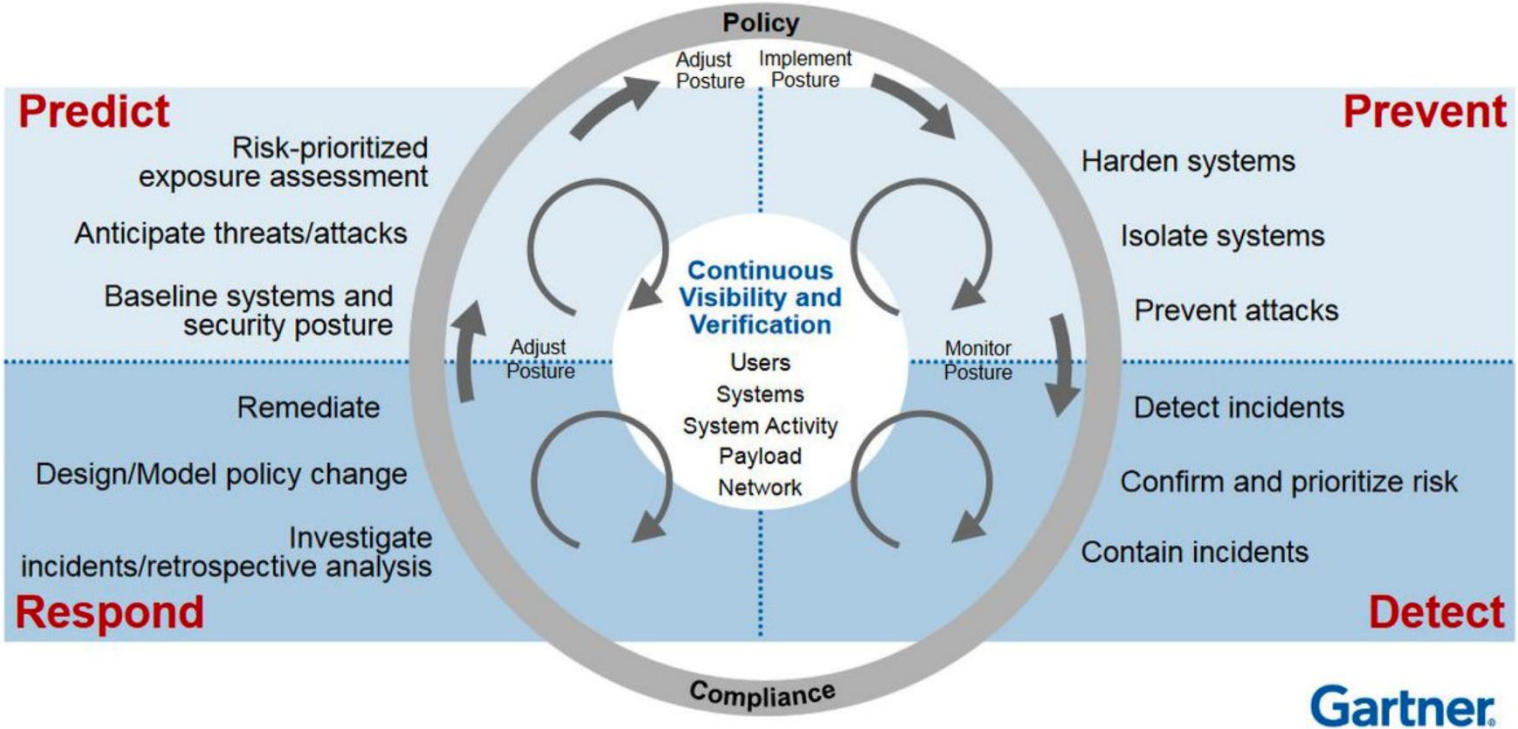
3. Считается что Red Teaming выходит за рамки классического тестирования на проникновение.

4. Обычно подразумевается использование значительно большей поверхности атаки, чем при Vulnerability Assessment и Penetration Testing.

Концепция адаптивной безопасности

Адаптивная безопасность — подход, который позволяет контролировать, обнаруживать и реагировать в реальном режиме времени на известные риски безопасности а также прогнозировать появления новых.

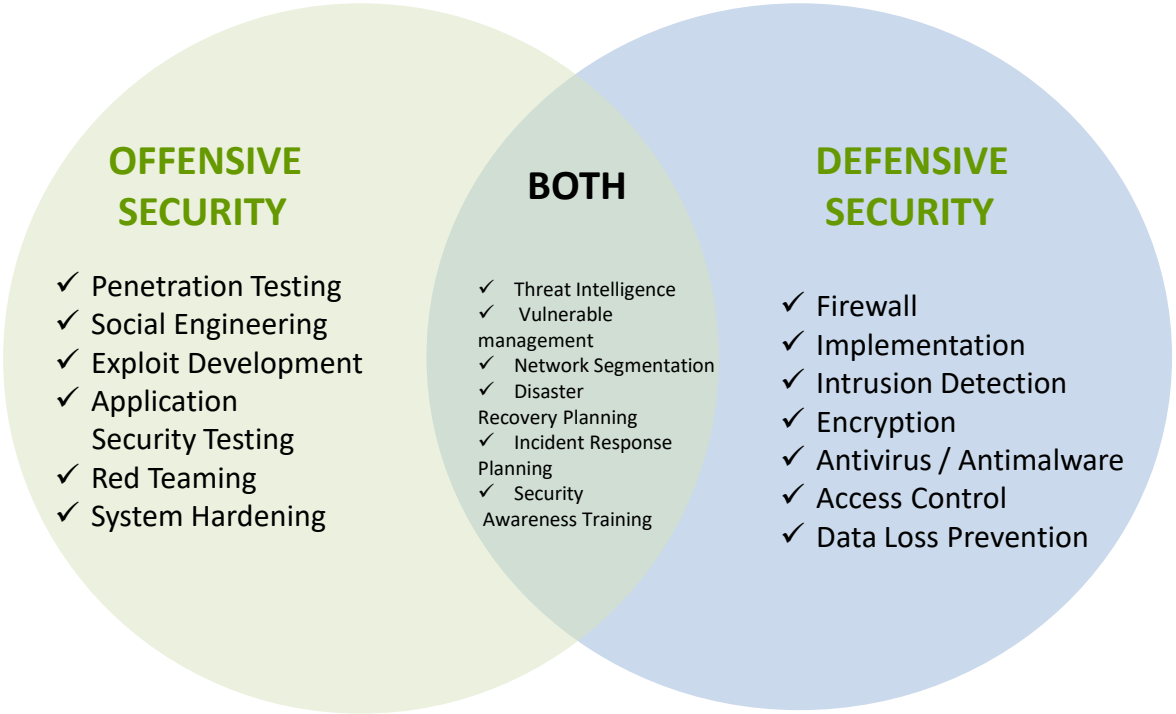
Концепция адаптивной безопасности



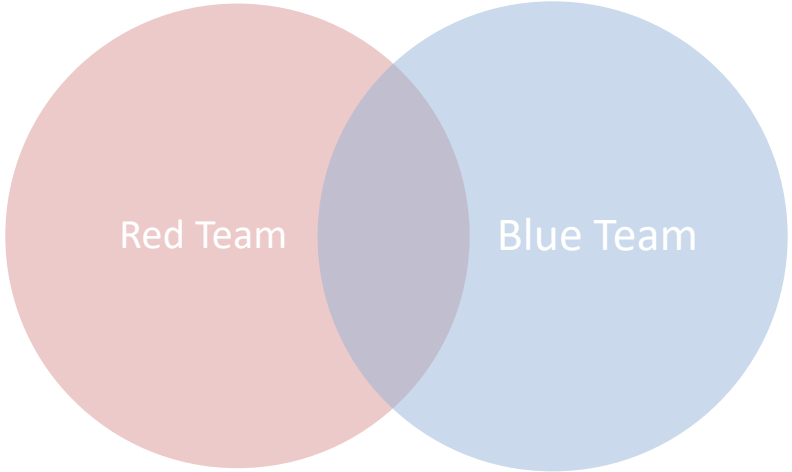
Концепция адаптивной безопасности

Концепция адаптивной безопасности

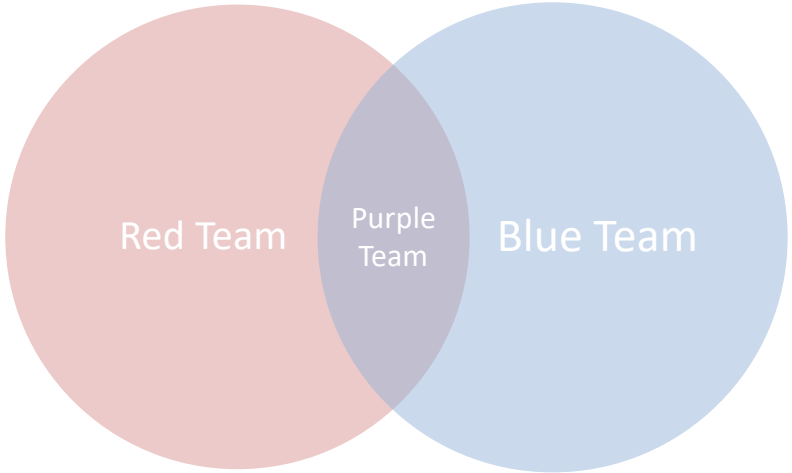
Концепция адаптивной безопасности



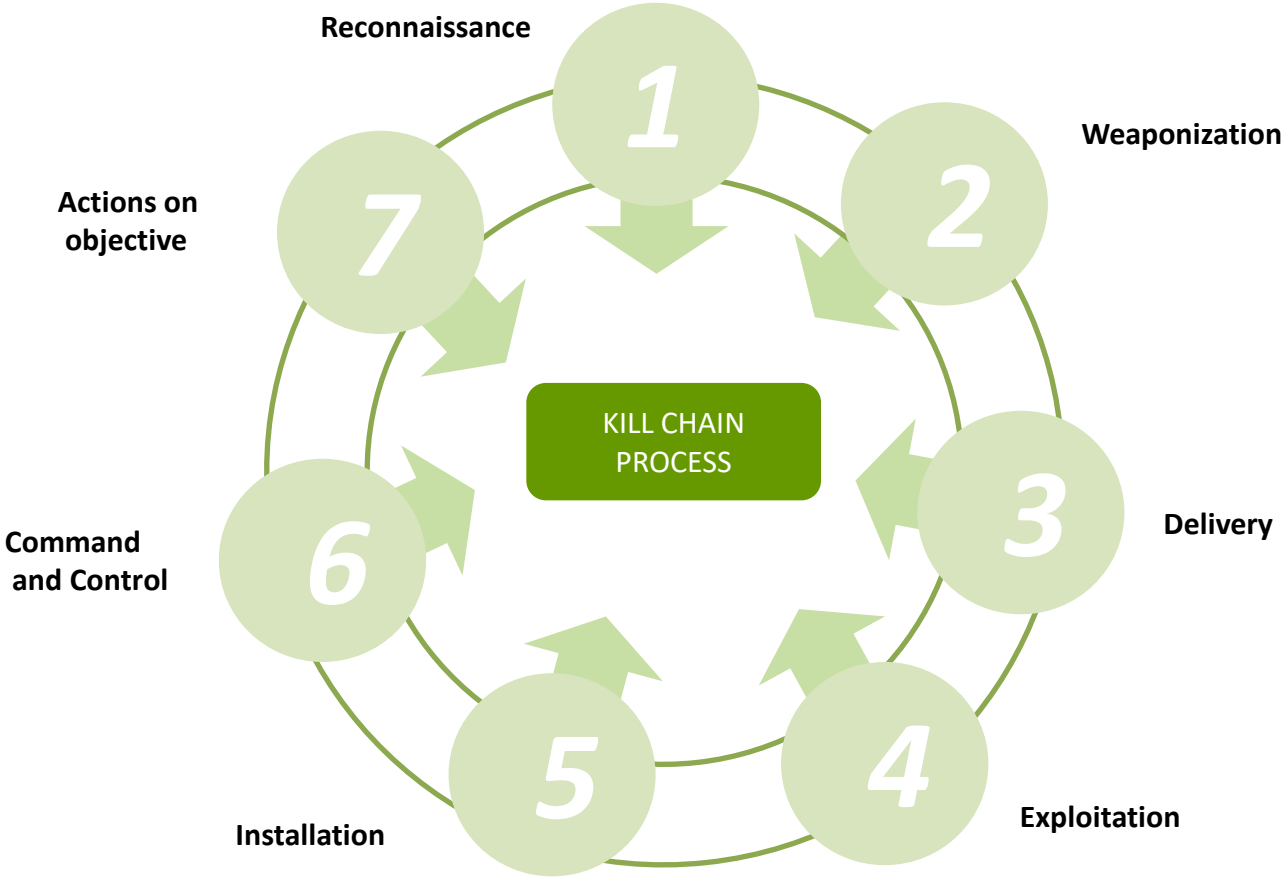
Red Team/Blue Team



Purple Team



Attack/Cyber Kill Chain



MITRE ATT&CK

KILL CHAIN

- Reconnaissance
- Weaponization
- Delivery
- Exploitation
- Installation
- Command & Control
- Actions on objectives

VS

MITRE ATT&CK

- Initial access
- Execution
- Persistence
- Privilege Escalation
- Defence Evasion
- Credential Access
- Discovery
- Lateral moment
- Collection
- Exfiltration

Жизненный цикл атаки

Жизненный цикл атаки

Жизненный цикл атаки

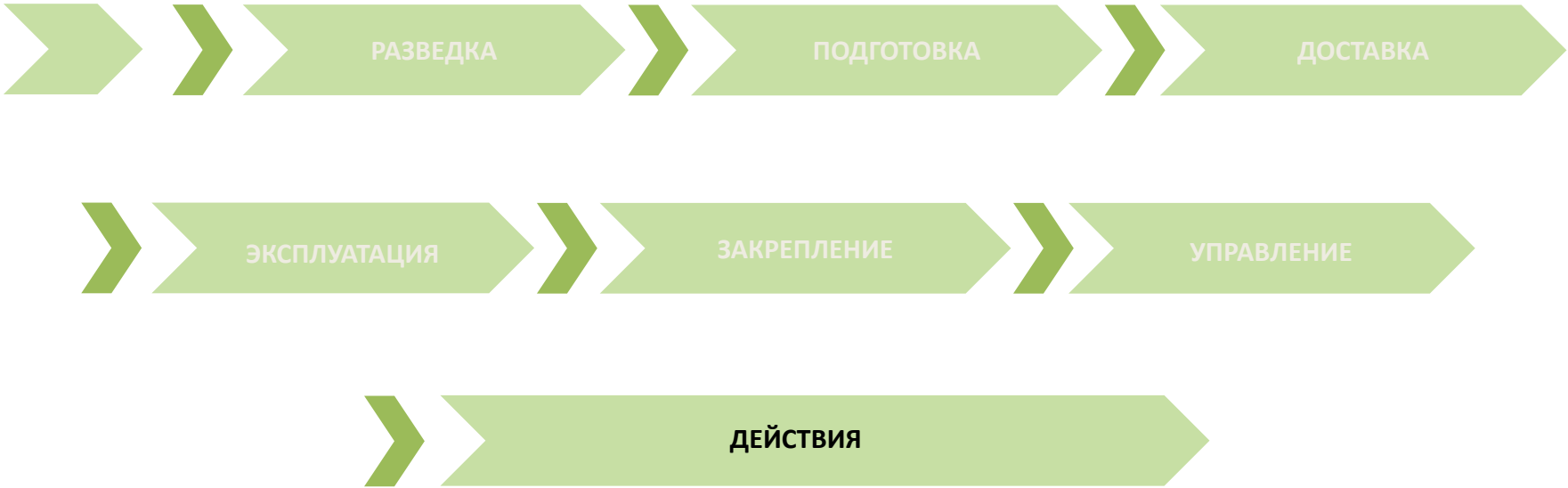
Жизненный цикл атаки

Жизненный цикл атаки

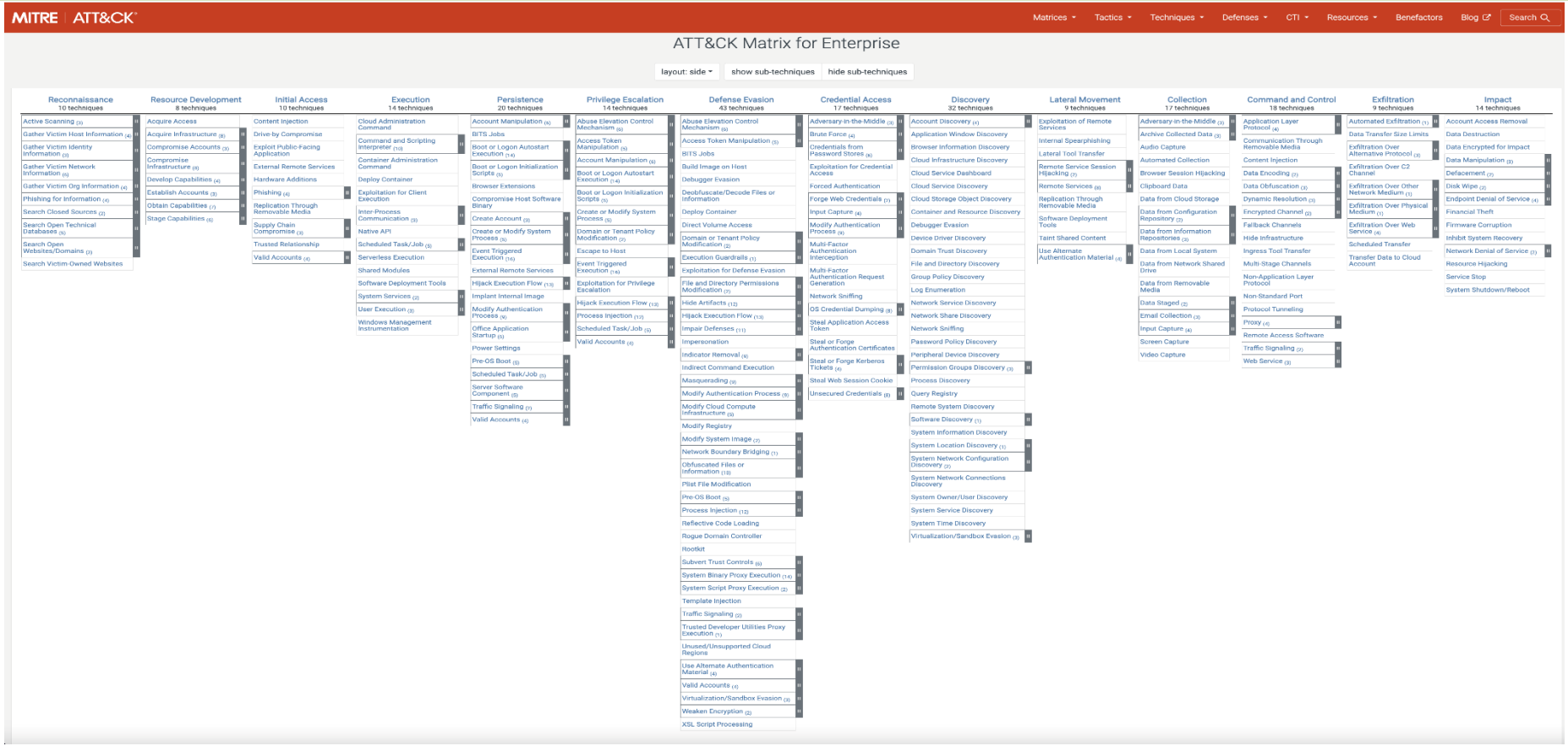
Жизненный цикл атаки

Жизненный цикл атаки

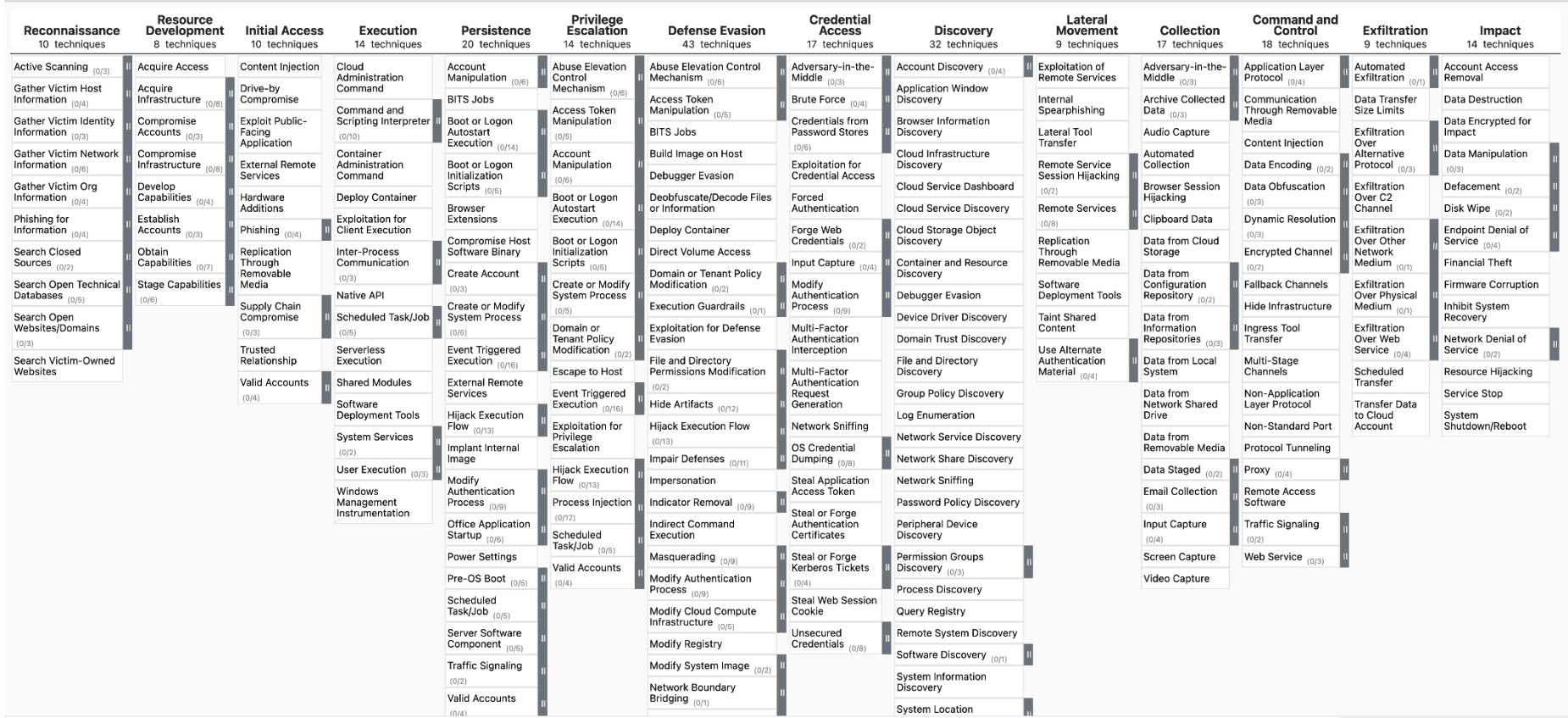
Жизненный цикл атаки



ATT&CK Matrix for Enterprise



ATT&CK Matrix for Enterprise



Методология

Open Source Security Testing Methodology Manual (OSSTMM) – пожалуй, единственная методика, которая акцентирует внимание не только на технических тестах, но и на атаках, связанных с социальной инженерией и направленных на пользователей корпоративной сети.

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Technikal Guide to Information Security Testing and Assessment

NIST SP800-115 – данный документ хотя и не является методикой, но описывает общие аспекты проведения тестов на проникновение.

Information Systems Security Assessment Framefork (ISSAF)

The Information Systems Security Assessment Framework (ISSAF) – фреймворк (framework), ориентированный на инструментальный поиск уязвимостей.

Security Standards Council

PCI DSS (раздел 11.3 стандарта) – согласно разделу 11.3 стандарта PCI DSS в организациях, соответствующих стандарту, не реже раза в год должен проводиться тест на проникновение. Для разъяснения данного раздела PCI DSS был выпущен документ Information Supplement Requirement 11.3 Penetration Testing, в очень общих чертах описывающий последовательность проведения инструментальной проверки внешнего периметра сетевой инфраструктуры тестируемой компании (по сути, данная инструментальная проверка не является тестом на проникновение).

The Open Web Application Security Project (OWASP) – руководство по тестированию веб-безопасности, которое является основной методологией тестирования безопасности для разработчиков веб-приложений и специалистов по информационной безопасности и разрабатывается международным консорциумом OWASP.

The Penetration Testing Execution Standard (PTES) – Стандарт по тестированию на проникновение. Стандарт проведения тестирования на проникновение состоит из семи (7) основных разделов. Они охватывают всё, что связано с тестом на проникновение – от первоначального общения и обоснования пентеста до этапов сбора разведданных и моделирования угроз. Тестировщики работают за кулисами, чтобы лучше понять тестируемую организацию, через исследование уязвимостей, эксплуатации и послеэксплуатации, когда технический опыт тестировщиков в области безопасности сочетается с пониманием бизнеса. И, наконец, с отчетностью, которая охватывает весь процесс таким образом, который обеспечивает наибольшую ценность.

PWK – Методология курса «Тестирование на проникновение с Kali Linux». Является основным материалом для получения сертификата по тестированию на проникновение – OSCP и практическим руководством.

Вопросы

Спасибо за внимание