Зачем изучать хакерские методы и как исследовательские навыки влияют на усиление защиты

Василий Кравец,
начальник отдела ИИТ,
«Перспективный мониторинг»

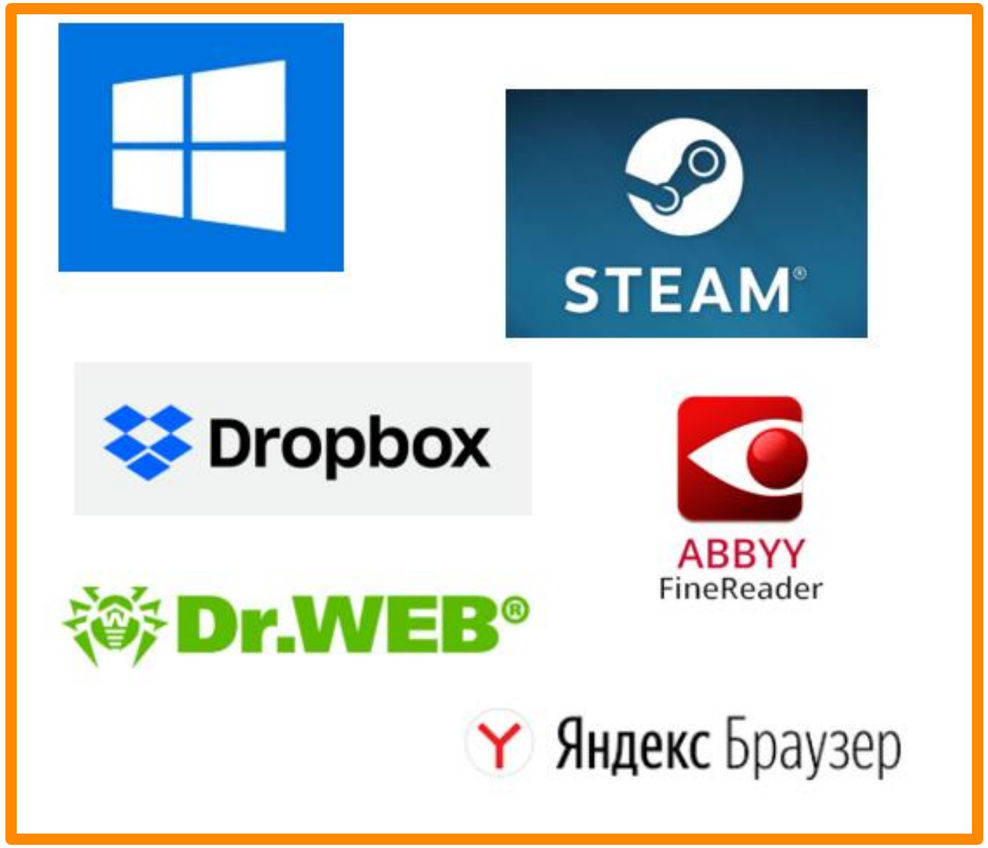
БОЛЬШОЙ МОСКОВСКИЙ ТЕХНО ФЕСТ
infotecs

Отдел ИИТ

О моей команде

Обо мне

- CVE-2019-14743
- CVE-2019-15316
- CVE-2019-17180
- CVE-2019-19247
- CVE-2019-19248
- CVE-2019-20383
- CVE-2020-23967
- CVE-2021-25261
- CVE-2021-25263
- CVE-2022-28226
- CVE-2022-28225
- CVE-2023-5993
- CVE-2023-7016



О команде

6 сертификатов OSCP

3 сертификата OSWE

2 сертификата OSEP

2 сертификата OSWP

Более **45** лет опыта в ИБ

45

Более **200** завершенных проектов

200

Время атаки

Типовое время захвата домена AD:

На основании опыта команды за 2024-2025 год:

При проведении работ «черным ящиком»: **10 часов**

При проведении работ «серым ящиком»: **2 часа**

Роль Ampire RedTeam в обеспечении безопасности

- Узнать типовые сценарии атак
- В «ручном режиме» провести атаки
- Понять, как выглядит «чужая» сеть с точки зрения атакующего
- оценить возможности использования легитимных сервисов для атак
- Успеть все это за 2 часа

Философия

Что такое безопасность?

Безопасность – это…

… не состояние, а процесс!

Нельзя «зафиксировать» безопасность, она постоянно меняется, так как меняется и состояние оцениваемой системы внутри и снаружи.

У безопасности как у процесса есть жизненный цикл.

Внутренний период

Начальные этапы:

- Давайте сделаем побезопаснее

Внутренний период

Начальные этапы:

- Давайте сделаем побезопаснее
- Изучаем Best Practice

Внутренний период

Начальные этапы:

- Давайте сделаем побезопаснее
- Изучаем Best Practice
- Проводим аудит

Внешний период

Существенные мероприятия:

- Исследование возможностей

Внешний период

Существенные мероприятия:

- Исследование возможностей
- Анализ защищенности

Внешний период

Существенные мероприятия:

- Исследование возможностей
- Анализ защищенности
- Точечные исследования

Внешний период

Существенные мероприятия:

- Исследование возможностей
- Анализ защищенности
- Точечные исследования
- Пентест

Пост-защита

Что еще можно сделать:

- RedTeaming
- Учения Blue Team
- Purple Teaming
- Bug Bounty

ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

Спасибо
за внимание!

Кравец Василий

Начальник отдела ИИТ

Vasily.Kravets@amonitoring.ru

t.me/pm_public

amonitoring.ru

ТЕХНО infotecs ФЕСТ

Подписывайтесь
на наши соцсети,
там много интересного

CYBER MEDIA

NBJ НАЦИОНАЛЬНЫЙ БАНКОВСКИЙ ЖУРНАЛ

GLOBAL DIGITAL SPACE

CISOCLUB

РУТОКЕН КОМПАНИЯ АКТИВ

ПЕРСПЕКТИВНЫЙ МОНИТОРИНГ

АВАНГАРД

ARinteg

АТБ ЭЛЕКТРОНИКА

infotecs {/-cademy}

merlion

УЧЕБНЫЙ ЦЕНТР ИНФОТЕКС