КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ
ПРОФИ

DETEACT

ЭФФЕКТИВНЫЙ ПЕНТЕСТ ИЛИ ДУМАЙ КАК ХАКЕР

Как сэкономить время внешних аудиторов и начать пентест своими руками?

Омар Ганиев
DeteAct, основатель

АНАЛИЗ ЗАЩИЩЁННОСТИ

- Какие могут быть цели анализа?
- Как согласовать методологию работ и покрытие?
- Как сэкономить время пентестерам?
- Как провести пентест своими руками?

ЦЕЛИ ТЕСТИРОВАНИЯ

Необходимо понять, чего должны ***добиться*** атакующие.

Помимо перечисленных, могут быть и другие цели, такие как проверка устойчивости к DoS-атакам…

…или прохождение compliance ;)

ПРОБИВ

Тест на *проникновение* подразумевает конечную цель в виде проверки возможности полной компрометации объекта.

ВШИРЬ

Анализ защищённости подразумевает поиск наибольшего количества недостатков в системе без обязательного дальнейшего развития атаки.

РЕДТИМИНГ

В ходе Red Teaming симулируются действия атакующих с минимум ограничений, проверяются процессы реагирования и мониторинга и максимально возможный ущерб.

ОБЛАСТЬ ИССЛЕДОВАНИЯ

Изначально необходимо чётко определить ***скоуп*** работ.

Дать конкретные хосты и IP-адреса или попросить разведку.

White box vs Black box

ПРИЛОЖЕНИЕ
Отдельные приложения: мобильные, веб-, десктопные, API.

СЕРВИС
Инфраструктура, выполняющая некоторую функцию, например, процессинг.

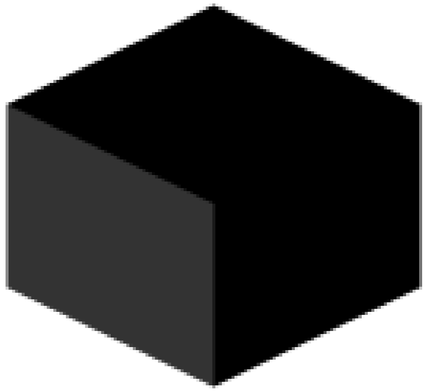
СЕТЬ
Разнородная инфраструктура, такая как офисная сеть.

СОТРУДНИКИ
И их каналы коммуникации: email, CRM, закупочные площадки, мессенджеры.

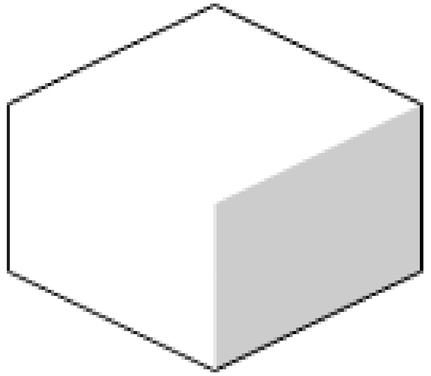
КОМПАНИЯ
IT-системы и бизнес-процессы компании в целом.

ЧТО ДАТЬ НА ВХОД?

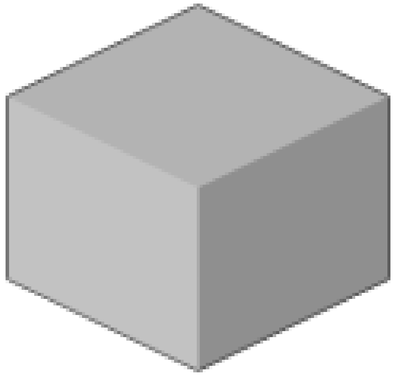
Пентестеры могут потратить много **дорогостоящего** времени на добычу информации, которую вы можете просто выдать



Чёрный ящик:
минимум
вводных данных



Белый ящик:
исходный код,
доступ к
системе



Серый ящик:
на входе
документация,
IP-адреса

МЕТОДОЛОГИЯ

Исполнитель должен понимать цель работ и методику для её достижения.

OWASP Testing Guide, OSSTMM, …

ИНСТРУМЕНТЫ
Количество не столь важно, но важно правильное применение.

ЧЕКЛИСТЫ
Следовать формальным чеклистам без творчества мало, но у исполнителя внутри команды должно быть разделение задач, пусть расскажет.

ВЕХИ
Анализ должен включать как минимум этапы разведки, поиска уязвимостей, демонстрации риска.

ПОКРЫТИЕ

Исполнитель должен максимизировать покрытие системы тестами (с поправкой на цель).

Артефакты: результаты сканирования портов, карта сайта из Burp Suite.

ОБЕЛИТЬ ЯЩИК
Для максимального покрытия нужно дать больше вводных: схема сети, IP-адреса, DNS-зона, OpenAPI-контракты, исходные коды.

ИСКЛЮЧЕНИЯ В IPS
Для облегчения задачи можно добавить IP-адреса исполнителя в исключения WAF, IPS.

МОНИТОРИНГ
Можно предупредить о мониторинге трафика для контроля покрытия со стороны заказчика.

ПОДГОТОВКА

Проведите поверхностный пентест самостоятельно и подсказывайте пентестерам направления для работы.

Этапы разведки и сканирования можно провести без специальных знаний.

ДОСТУПЫ
Подготовьте учётные записи или сетевой доступ с разными ролями, тестовую среду и тестовые сценарии.

ИНВЕНТАРИЗАЦИЯ
Заранее собирайте ассеты, для пентеста выгрузите DNS-зону и хосты из систем ассет-менеджмента.

СКАНИРОВАНИЕ
Пентестерам можно дать доступ к результатам сканирования OpenVAS, Nessus, Nmap, Burp Suite и т. д.

РЕЗЮМИРУЕМ

1

СКОУП И ВВОДНЫЕ
Понять, что тестируем, и чем готовы делиться с исполнителем

2

ЦЕЛИ И МЕТОДОЛОГИЯ
Определяем конечную цель работ, и как к ней идти

3

ПОКРЫТИЕ И ПОДГОТОВКА
Для максимального покрытия проводим предварительный пентест и даём результат пентестерам

#CODEIB

СПАСИБО ЗА ВНИМАНИЕ

beched@deteact.com
+7 905 595 61 32
facebook.com/omar.ganiyev
https://pentest.deteact.ru/