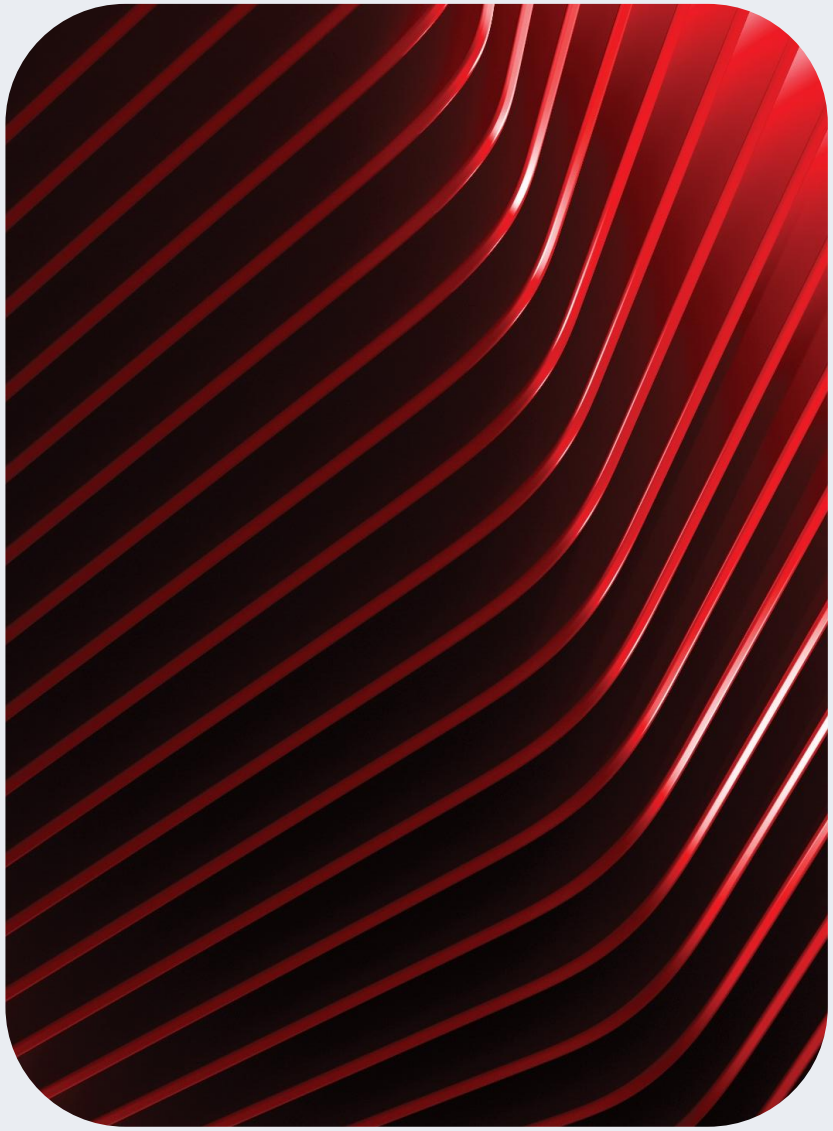
positive technologies

Дубровская Анастасия

Руководитель отдела аналитики
по оценке защищенности,
Positive Technologies



ЗОЛОТОЙ СТАНДАРТ ПЕНТЕСТА:

от методики к практике

МЕТОДИКА ФСТЭК | от 8 сентября 2025 года

Т1. Внешнее тестирование на проникновение

- Имитация атак внешнего нарушителя из сети Интернет
- Анализ периметра: публичные сервисы, веб-приложения, VPN, почта и др.

Цель: получение первоначального доступа к инфраструктуре

Т2. Тестирование беспроводных сетей

- Имитация атак через Wi-Fi внутри и вне контролируемой зоны
- Анализ конфигурации, перехват трафика, атаки на точки доступа

Цель: получение первоначального доступа к инфраструктуре

Т3. Тестирование с применением социальной инженерии

- Имитация атак на пользователей (фишинг, звонки, сообщения и др.)
- Используются служебные почты, телефоны, аккаунты

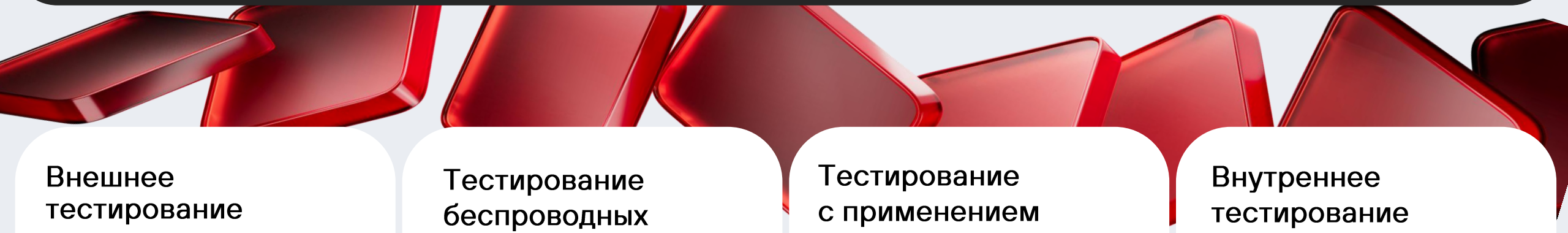
Цель: получение первоначального доступа к инфраструктуре

Т4. Внутреннее тестирование на проникновение

- Имитация действий внутреннего нарушителя или после компрометации
- Повышение привилегий, развитие атаки, доступ к критическим системам

Цель: получение контроля над доменом, системами и данными

СТАТИСТИКА УСПЕШНОСТИ АТАК | на основе проведенных проектов



Внешнее тестирование на проникновение

69%

ПРОЕКТОВ

получен доступ во внутреннюю сеть

Тестирование беспроводных сетей

В КАЖДОМ ВТОРОМ

ПРОЕКТЕ

получен доступ во внутреннюю сеть

Тестирование с применением социальной инженерии

В КАЖДОМ

ПРОЕКТЕ

получен доступ во внутреннюю сеть

Внутреннее тестирование на проникновение

94%

ПРОЕКТОВ

получены максимальные привилегии в домене

ВНЕШНЕЕ ТЕСТИРОВАНИЕ на проникновение

Проблемы

Доступность корпоративных сервисов из сети Интернет без достаточной защиты

Прямой доступ к VPN, RDP, почте, веб-порталам без ограничения по источникам

Отсутствие многофакторной аутентификации (2FA)

Использование слабых или скомпрометированных доменных паролей

Уязвимости во внешних сервисах и прикладном ПО

Уязвимости веб-приложений (RCE, SQL Injection, обход аутентификации и др.)

Использование устаревших и/или неподдерживаемых версий ПО

Отсутствие сегментации сети и выделенной ДМЗ-зоны

Внешние сервисы размещены в одной сети с внутренними системами

Отсутствие ограничений на сетевое взаимодействие между сегментами

Рекомендации

Усиление защиты учетных записей и сервисов доступа

Внедрение MFA (OTP, аппаратные токены, push-подтверждение и др.)

Ограничение доступа к сервисам по IP-адресам и через VPN

Проведение регулярного аудита учетных записей и парольной политики

Управление уязвимостями и защита внешнего периметра

Регулярное обновление и патч-менеджмент всех внешних сервисов

Использование WAF для защиты веб-приложений

Минимизация числа доступных из Интернет сервисов

Сегментация сети и изоляция критичных систем

Размещение внешних сервисов в выделенной ДМЗ-зоне

Ограничение доступа из ДМЗ во внутреннюю сеть

Реализация принципа минимально необходимого сетевого доступа



Тестирование БЕСПРОВОДНЫХ СЕТЕЙ

habr.com

Технологии, которые держат мир на связи. Как атакуют современный Wi-Fi

Проблемы

Избыточная зона покрытия беспроводной сети

Сигнал доступен за пределами контролируемой территории (улица, парковка, соседние здания)

Возможность подключения к сети без физического доступа в офис

Использование небезопасных протоколов и методов аутентификации

Использование WPA2-PSK с общим паролем

Отсутствие аутентификации на основе сертификатов

Возможность подбора или компрометации пароля

Недостаточная сегментация и контроль доступа Wi-Fi сети

Отсутствие изоляции беспроводных клиентов от внутренней сети

Гостевая сеть имеет доступ к корпоративным ресурсам

Рекомендации

Ограничение зоны покрытия и защита инфраструктуры

Настройка мощности передатчиков и направления антенн

Использование централизованного управления Wi-Fi (RADIUS, NAC, контроллер)

Регулярное обновление прошивок и ПО точек доступа

Использование защищенных протоколов аутентификации

Использование WPA3-Enterprise с 802.1X и EAP-TLS (аутентификация по сертификатам)

Отключение WPA3-Transition Mode

Использование Protected Management Frames (PMF)

Отказ от использования общего пароля (PSK)

Сегментация и контроль доступа

Сегментация сети (VLAN, выделение ДМЗ и гостевых сегментов)

Ограничение доступа беспроводных клиентов к внутренним ресурсам

Внедрение NAC для контроля и мониторинга подключаемых устройств

СОЦИОТЕХНИЧЕСКИЕ атаки

Проблемы

Возможность подмены корпоративных доменов и отправителей

Отсутствие или некорректная настройка SPF, DKIM, DMARC

Возможность отправки писем от имени сотрудников или доверенных сервисов

Недостаточная фильтрация входящей почты

Недостаточная осведомленность пользователей о современных сценариях атак

Пользователи открывают вложения и переходят по ссылкам из фишинговых писем

Передают учетные данные или выполняют действия по инструкциям злоумышленника

Рекомендации

Усиление защиты корпоративной почтовой инфраструктуры

Настройка SPF, DKIM и DMARC с политикой reject/quarantine

Добавление предупреждений о внешнем отправителе

Использование антиспам / антифишинг решений

Повышение осведомленности пользователей

Регулярное обучение сотрудников с использованием практических сценариев атак

Обучение выявлению фишинга, вишинга и атак через мессенджеры и соцсети

Регламентация передачи учетных данных и обязательное уведомление ИБ при подозрительных событиях

ВНУТРЕННЕЕ ТЕСТИРОВАНИЕ на проникновение

Проблемы

Уязвимости и небезопасная конфигурация Active Directory (AD CS, права доступа)

Небезопасные шаблоны AD CS, позволяющие повысить привилегии

Избыточные права пользователей и сервисных учетных записей

Ошибки разграничения доступа и делегирования прав

Недостатки управления учетными данными и парольной политики

Повторное использование паролей локальных и доменных учетных записей

Отсутствие защиты локальных администраторов

Рекомендации

Усиление защиты Active Directory и AD CS

Безопасная настройка AD CS, контроль шаблонов сертификатов и отключение небезопасных параметров

Разграничение привилегий (AD Tiering), аудит прав доступа и защита критичных учетных записей

Защита учетных записей и учетных данных

Внедрение LAPS / Windows LAPS для защиты локальных администраторов

Исключение повторного использования паролей и аудит привилегированных учетных записей

habr.com

Esплуатация. Повышение привилегий с использованием AD CS

positive technologies

Аналитика проектов, отраслевые тренды и актуальные уязвимости

@PT_CRAB_BOT

pt@ptsecurity.com

ptsecurity.com

СПАСИБО ЗА ВНИМАНИЕ