Лучшая защита - это нападение

Пентесты, как лучшая профилактика уязвимостей

Михаил Юденков
Бизнес-консультант по информационной безопасности
Группа развития продаж решений ИБ в ЦФО и ЮФО
Отдел территориальной экспертизы Департамента ИБ
Т +7(473) 250-20-23 доб. 6247 | М +7 (920) 210 31 95 |
Mikhail.Yudenkov@softline.com

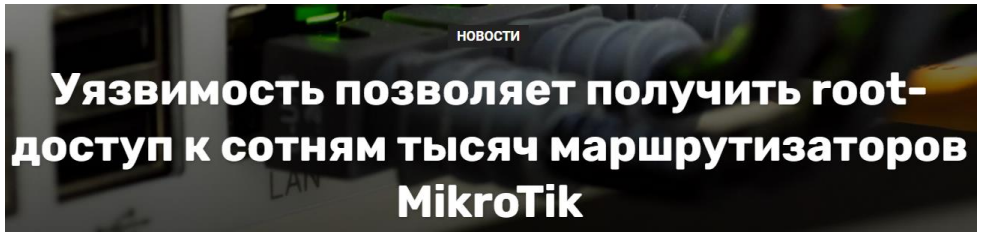
Ситуация на данный момент

Традиционная кибербезопасность сосредотачивается на обнаружении совершаемых атак и устранении их последствий, в то время как Offensive Security реализовывает проактивный подход, где уязвимости выявляются и ликвидируются до реальной атаки. Важно понимать, что обе стратегии имеют ценность: традиционная защищает от известных угроз, а наступательная — от неизвестных.

Заблуждение в неуязвимости

Даже самая
«неприступная»
инфраструктура имеет
«слабые» места.

Сотни тысяч сетевых шлюзов FortiGate сохранили критическую уязвимость, потому что никто не установил на них патчи



Уязвимость Cisco ASA могла позволить злоумышленнику попасть во внутреннюю сеть

Не знание слабых сторон – самая слабая сторона

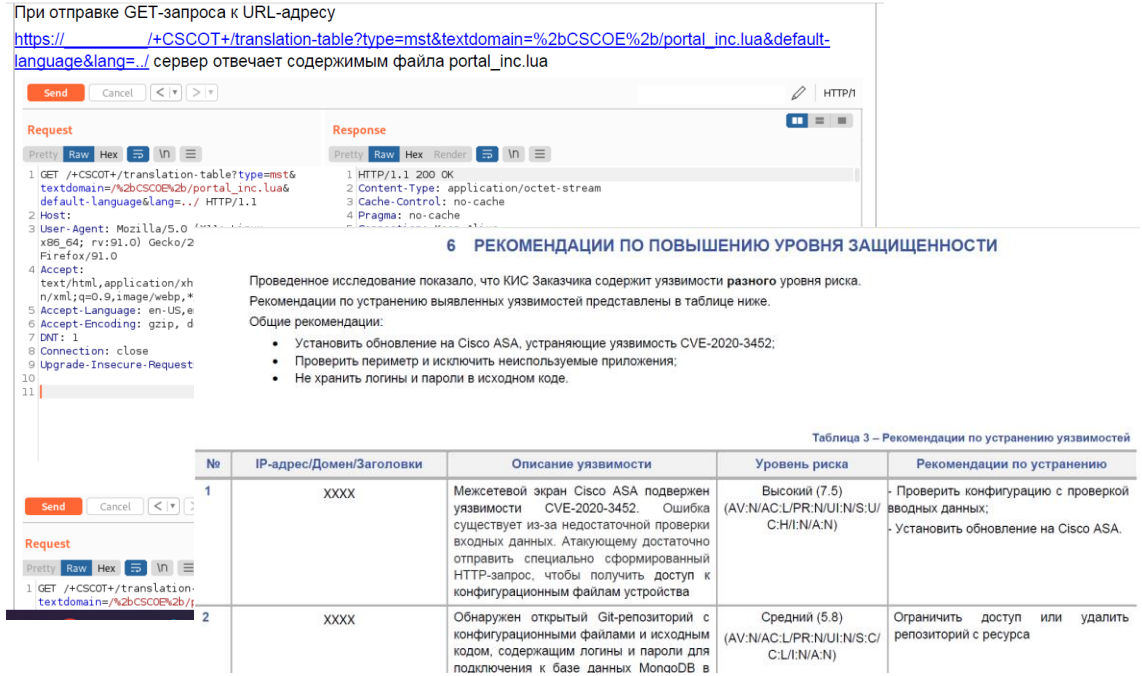
«В Хельмовой Пади есть одно уязвимое место. Наружная стена крепости - сплошной твёрдый камень, но в основании есть небольшой водосток, узкая сточная канавка.»

- А у вас выстроен процесс управления уязвимостями?
- Классификация и категоризация? Контроль за устранением?
- Патч-менеджмент и контроль соответствия конечных устройств политикам безопасности?
- А работа с персоналом? Осведомлённость?
- Защита веб-сайта? Приложений?
- Анализ кода? Безопасная разработка?

Как увидеть то, что скрыто? Испытание боем

- Задач много, а бюджет не «резиновый»
- С чего начать? Как правильно составить дорожную карту? И надо ли вообще это делать?
- Бизнес хочет понимать – зачем им тратить деньги на WAF и обучение сотрудников азам Инфобеза, если у вас и так «всё закрыто»…
- Нужна ли безопасная разработка, если у нас 2 релиза в год и это наш предел?
- И вообще… Инфобез – это бездонная яма для бюджета… А как понять, что он работает если ничего не происходит?

Пентест или VM?



При отправке GET-запроса к URL-адресу
https://_____/+CSCOT+/translation-table?type=mst&textdomain=%2bCSCOE%2b/portal_inc.lua&default-language&lang=../ сервер отвечает содержимым файла portal_inc.lua

Request

```
GET /+CSCOT+/translation-table?type=mst&
textdomain=/%2bCSCOE%2b/portal_inc.lua&
default-language&lang=../ HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (
x86_64; rv:91.0) Gecko/2
Firefox/91.0
Accept:
text/html,application/xh
n/xml;q=0.9,image/webp,*
Accept-Language: en-US,
Accept-Encoding: gzip, d
DNT: 1
Connection: close
Upgrade-Insecure-Request
```

Response

```
HTTP/1.1 200 OK
Content-Type: application/octet-stream
Cache-Control: no-cache
Pragma: no-cache
```

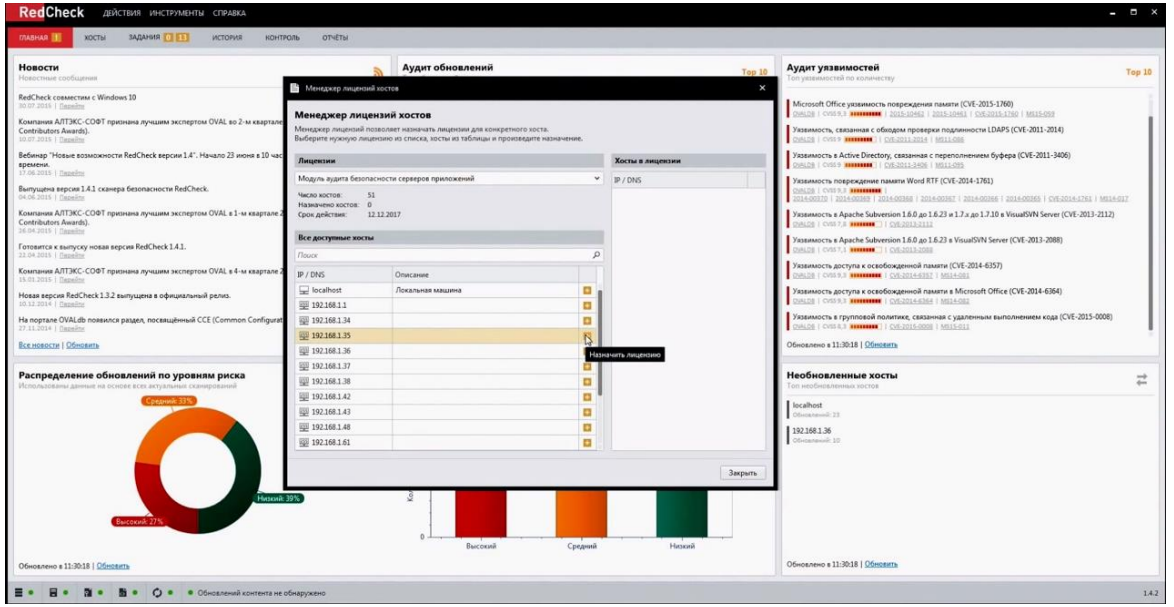
6 РЕКОМЕНДАЦИИ ПО ПОВЫШЕНИЮ УРОВНЯ ЗАЩИЩЕННОСТИ

Проведенное исследование показало, что КИС Заказчика содержит уязвимости **разного** уровня риска.
Рекомендации по устранению выявленных уязвимостей представлены в таблице ниже.
Общие рекомендации:

- Установить обновление на Cisco ASA, устраняющие уязвимость CVE-2020-3452;
- Проверить периметр и исключить неиспользуемые приложения;
- Не хранить логины и пароли в исходном коде.

Таблица 3 – Рекомендации по устранению уязвимостей

№	IP-адрес/Домен/Заголовки	Описание уязвимости	Уровень риска	Рекомендации по устранению
1	XXXX	Межсетевой экран Cisco ASA подвержен уязвимости CVE-2020-3452. Ошибка существует из-за недостаточной проверки входных данных. Атакующему достаточно отправить специально сформированный HTTP-запрос, чтобы получить доступ к конфигурационным файлам устройства	Высокий (7.5) (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)	- Проверить конфигурацию с проверкой вводных данных; - Установить обновление на Cisco ASA.
2	XXXX	Обнаружен открытый Git-репозиторий с конфигурационными файлами и исходным кодом, содержащим логины и пароли для подключения к базе данных MongoDB в	Средний (5.8) (AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:N/A:N)	Ограничить доступ или удалить репозиторий с ресурса



- Практичный и комплексный подход
- Эксплуатация уязвимостей(при необходимости)
- Гибкость и кастомизация предложения под задачи заказчика
- Операционные расходы
- Контроль результата
- Сезонность
- Результат сильно зависит от исполнителя и его компетенций
- Не заменяет VM, а является скорее назависимой оценкой работы с уязвимостями

- Необходимо иметь в штате человека, который бы постоянно обрабатывал отчёты и контролировал результат
- Капитальные(в классическом случае) затраты
- Отсутствие возможности корреляции данных об уязвимостях для формирования потенциального вектора атаки(в классическом варианте)
- Возможность в любой момент получить полную картину о текущем состоянии инфраструктуры
- Автоматизированные сценарии пентестирования и анализа кода

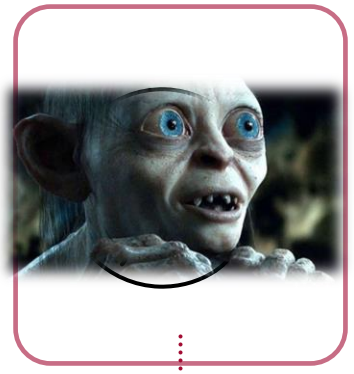
Пентесты от Софтлайн

Пентест
web-приложений

Пентест
внешнего периметра

Пентест
внутреннего периметра

Анализ Кода



Социотехнический пентест

Пентест
Wi-Fi сетей

Итоговые документы

ТЕХНИЧЕСКИЙ ОТЧЕТ

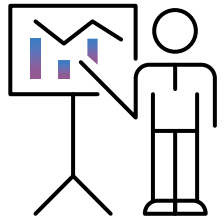
- структурированное описание полученных данных о целевой инфраструктуре (видение целевой инфраструктуры с позиции потенциального злоумышленника)
- описание выявленных уязвимостей
- описание предпринятых попыток проникновения и результатов их выполнения
- аналитические выводы о текущем уровне защищенности целевой информационной инфраструктуры
- перечень разработанных рекомендаций по повышению уровня защищенности

ОТЧЕТ ДЛЯ РУКОВОДСТВА (EXECUTIVE SUMMARY)

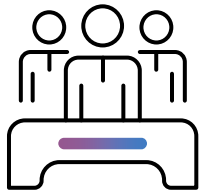
- краткий отчет для руководства, написанный не техническим языком
- основные выводы/рекомендации

Отчёт для руководства разрабатывается вместе с Техническим отчётом и содержит описание наиболее критичных уязвимостей и оценку уровня защищённости тестируемых объектов

ОПЦИОНАЛЬНО:

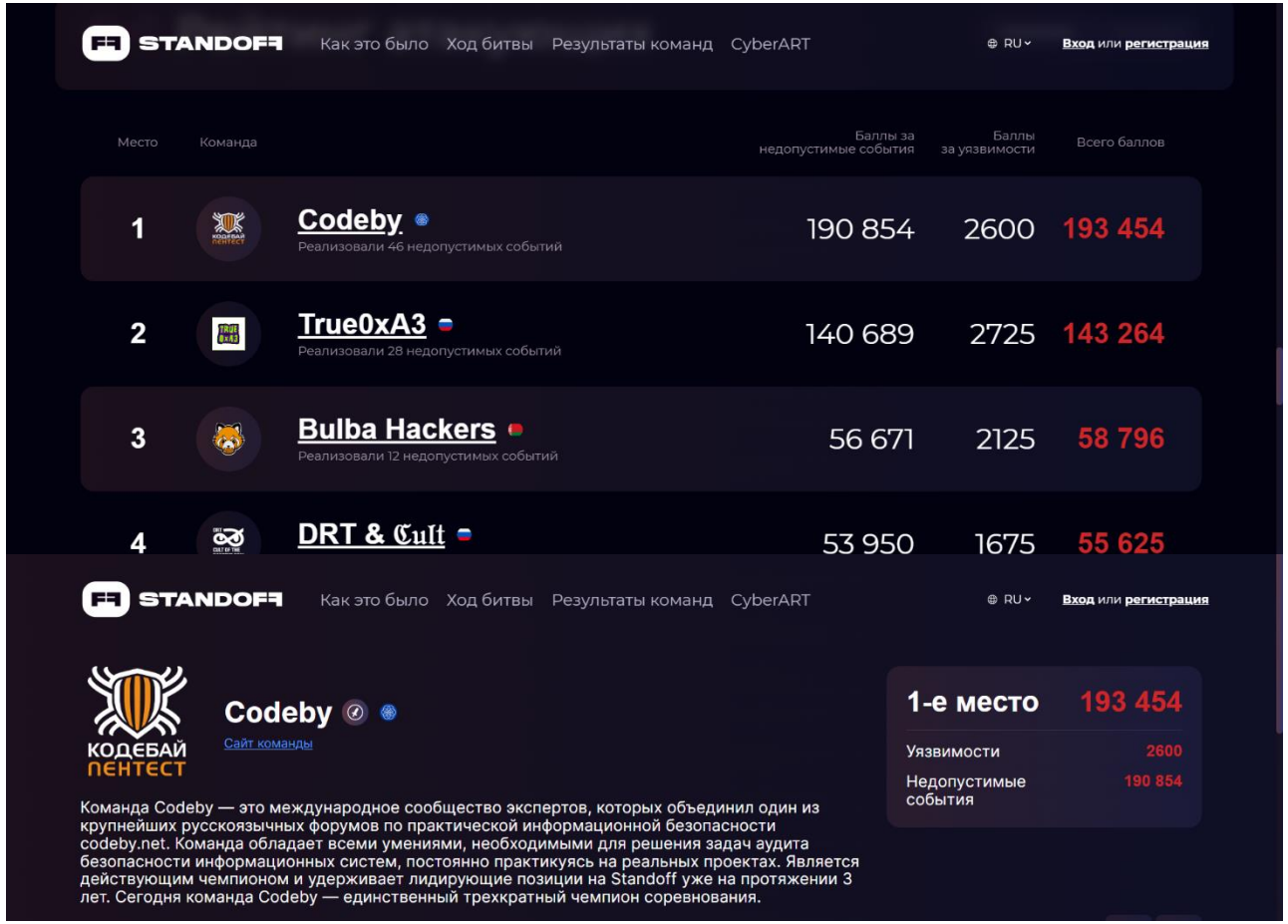


ИТОГОВАЯ ПРЕЗЕНТАЦИЯ



ОБУЧАЮЩИЙ СЕМИНАР ПО ИТОГАМ ПЕНТЕСТА

Команда и компетенции



ОПЫТ В СФЕРЕ ИБ

- Эксперт по анализу защищенности (пентестер) – 8 лет
- Входит в команду Codeby

КОМПЕТЕНЦИИ

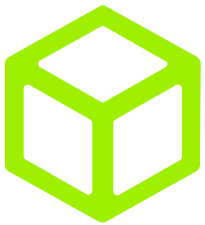
- Аудит информационной безопасности
- Анализ защищённости беспроводной и сетевой инфраструктуры
- Продвинутые навыки работы с операционными системами семейства Linux и Windows
- Опыт работы с инструментами и средствами для проведения анализа защищённости и аудита информационной безопасности (Nessus, OpenVAS, Metasploit, Cobalt Strike, Intercepter-NG, Scapy, Burp Suite, etc.)
- Разработка инструментов для тестирования на Python,Golang

КУРСЫ И СЕРТИФИКАТЫ

- Red Team operation
- eCPTX_v2
- Cybernetics HackTheBox lab
- APT HackTheBox lab

Награды и достижения

Сертификаты, которые выдает организация **Offensive Security** являются свидетельствами достаточных навыков в проведении тестирования на проникновение (OSCP) и проведения аудита и обеспечения защиты беспроводных устройств (OSWP)



Площадка Hack The Box предоставляет инструменты, необходимые для постоянного улучшения практических навыков в тестировании на проникновение.

Сертификат Burp Suite Certified Practitioner (BSCP) является официальным подтверждением уровня экспертизы от создателей одного из самых популярных продуктов для тестирования безопасности web-приложений **Burp Suite**.

Red Team Ops — сертификат, который подтверждает уровень владения основными принципами, инструментами и методами, используемыми участниками Red Team.

Сертификаты **eLearnSecurity** это на 100% практические и весьма уважаемые профессиональные сертификаты по различным направлениям тестирования на проникновение.

Члены команды являются Победителями соревнований the standoff в составе Codeby: в 2020, 2021, 2022, 2023 году.

Корпоративные лаборатории **Pentestit**
Уникальная в России и СНГ программа подготовки в области информационной безопасности.
В основе курса – сильнейшая практическая подготовка в лабораториях, разработанных на основе сетей реальных компаний.

А что дальше?

«Ждите меня с первым лучом солнца, я приду на пятый день, с востока»

- Провести оценку текущего состояния внешнего периметра
- Провести оценку текущих регламентов и настроек защиты внутреннего периметра
- Работа с персоналом. Повышение осведомлённости
- Работа с уязвимостями. Определить приоритеты согласно тем недопустимым событиям, которые согласует бизнес
- Провести работу над ошибками и проверить результат
- Контроль состояния на ежегодной основе

softline®

Цифровая Трансформация.
Успешная. Эффективная.