Системы
Информационной
Безопасности

Pentest

оценка фактического уровня защищенности
систем, сервисов и инфраструктуры

Pentest

Системы Информационной Безопасности

Pentest - это симуляция атаки на ваши IT-системы, выполняемая внешним экспертом по безопасности или «хакером в белой шляпе».

Исследователь применяет различные типы атак, чтобы идентифицировать ключевые уязвимости в ваших системах безопасности, определить доступные векторы атаки и оценить тип и величину ущерба, который может нанести реальная атака.

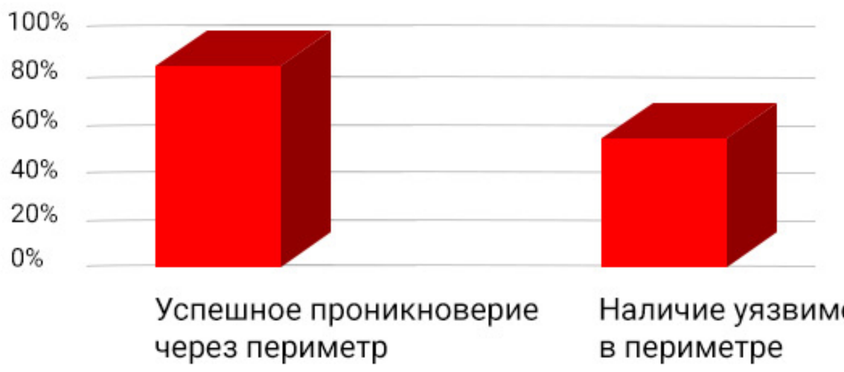
С помощью этого инструмента вы сможете:

- Выявить существующие уязвимости IT-инфраструктуры, сервисов и приложений.
- Определить направления информационной безопасности, требующие особого внимания.
- Получить внешнюю экспертизу по реальному уровню информационной безопасности компании.
- Предотвратить ущерб от кибератак.
- Соответствовать требованиям регуляторов и лучшим мировым практикам в сфере информационной безопасности.

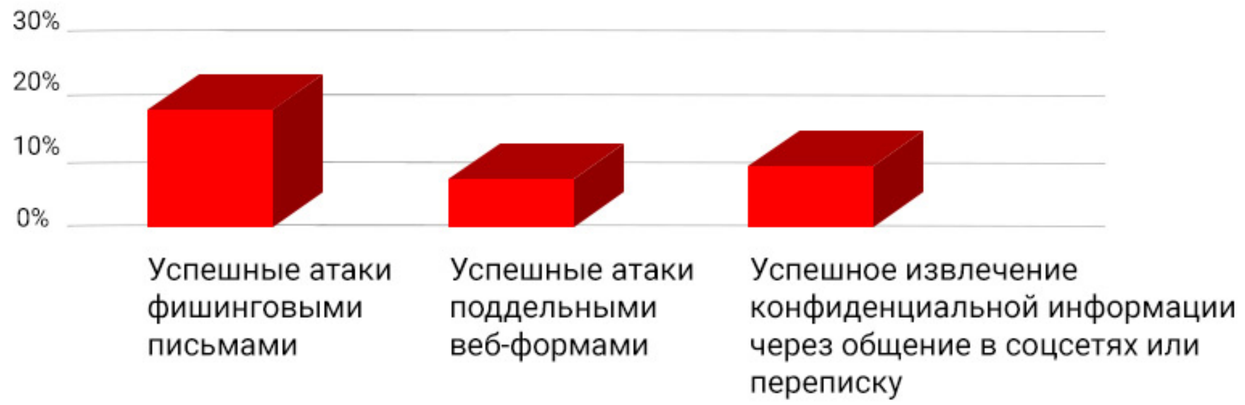
Pentest статистика

Системы Информационной Безопасности

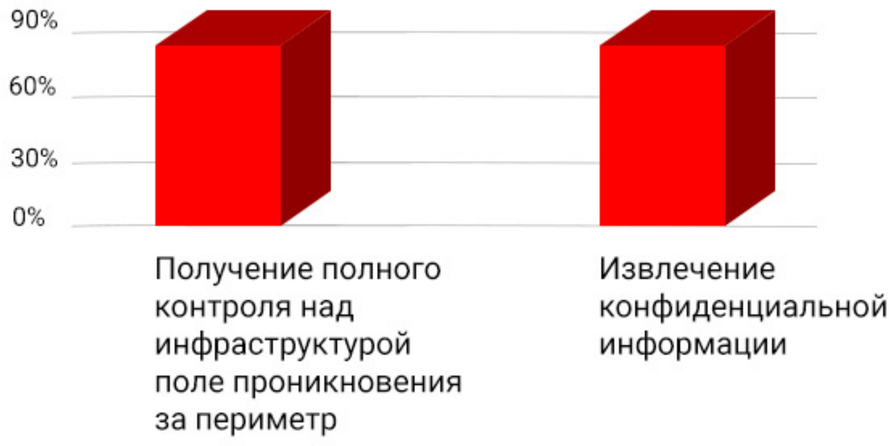
Исследование сетевого периметра



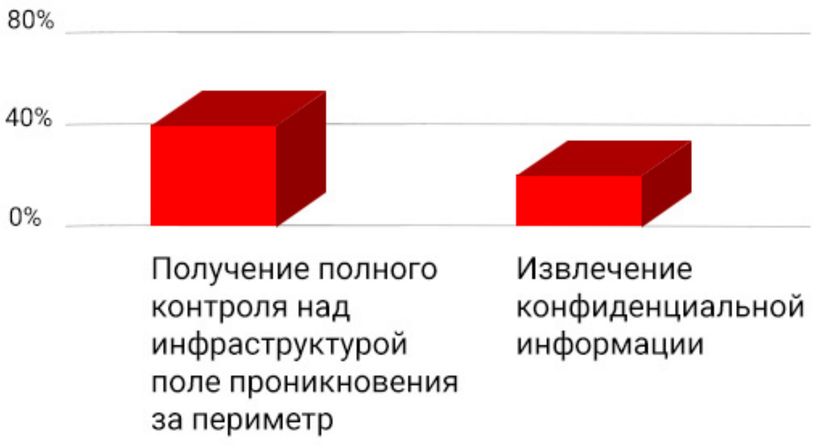
Исследование методам социальной инженерии



Исследование инфраструктуры

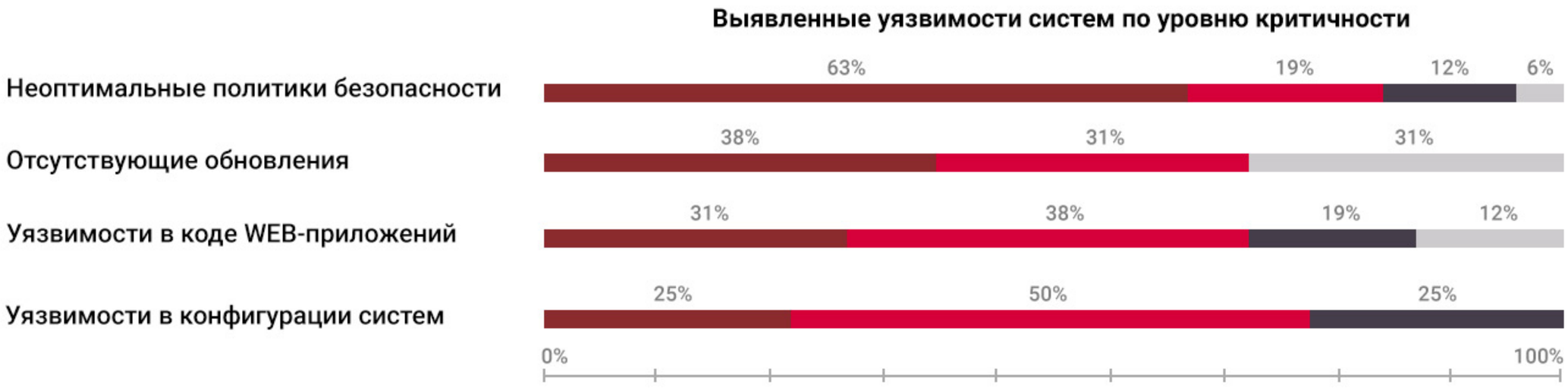


Исследование беспроводных сетей



Pentest статистика

Системы Информационной Безопасности



Мировая статистика по ущербу от киберинцидентов

Средний ущерб от одной атаки	$3.86 млн.
Ежегодное увеличение ущерба	6.4%
Вероятность средней компании подвергнуться кибератаке на двухлетнем горизонте	27.9%

* Агрегированные данные за 2018 год из собственных исследований и публичных источников

Почему необходим регулярный Pentest

Системы Информационной Безопасности

- Изменяется инфраструктура : исследование предоставляет срез уязвимостей на определенный момент времени, но со временем изменения систем открывают новые уязвимости. Атакующие также не стоят на месте и ежедневно исследуют системы, выявляют и используют новые уязвимости.

- Эволюционируют векторы атак: злоумышленники изобретают всё более изощренные подходы к атакам, улучшая как технические средства, так и применяемые методы проникновения в инфраструктуру и извлечения информации.

- Появляется новый персонал: команда информационной безопасности – Ваш самый ценный актив в деле защиты бизнеса от киберугроз. Необходимо обеспечить высокий уровень готовности новых специалистов к отражению современных угроз.

- Растет трафик приложений: кибератаки не происходят в вакууме. Трафик приложений является динамическим по своей природе - нагрузки могут резко меняться, также как и типы трафика (например, веб-браузеры, загрузки и выгрузки, потоковое видео, коммуникации) - и это может повлиять на эффективность защиты сетевой безопасности. Например, брандмауэр веб-приложения может пропустить атаку , если он испытывает нагрузку близкую к максимальной.

Наше решение
– что исследуем

Системы Информационной Безопасности

- Поиск уязвимостей, способных привести к нарушению конфиденциальности, целостности и доступности информации.

- Общее исследование периметра: ищем все возможные точки входа и проверяем любые гипотезы атак или точечная более тщательная проверка наиболее критичных сервисов и элементов инфраструктуры.

  — Исследование методом «Черного ящика» : тестирование без подробных вводных данных по цели.

  — Исследование методом «Белого ящика» : нам известны детали реализации тестируемой системы или сервиса.

  — Исследование методом «Серого ящика» : комбинация вышеуказанных типов.

- Формирование рекомендации по повышению уровня защищённости.

Наше решение
– как работает

Системы
Информационной
Безопасности

Подготовка и планирование

- Определение модели нарушителя (внутренний или внешний, доступные права и привелегии).
- Определение целей атаки, исходных данных, объема работ и целей тестирования.
- Определение перечня тестируемых систем и сервисов.
- Разработка методологии исследования.

Исследование

- Идентификация точек входа.
- Инструменты сканирования или вторжения разрабатываются при необходимости.
- Обнаружение и сканирование уязвимостей, устранение ложных срабатываний.
- Эксплуатация уязвимостей и получение несанкционированного доступа.
- Использование скомпрометированных систем в качестве плацдарма для дальнейшего вторжения.

Исследование

- Разработка аналитического отчета, рекомендаций по устранению уязвимостей и снижению рисков
- Визуальная демонстрация ущерба, который может быть нанесен системе злоумышленником.

Наше решение
– что дает?

Системы Информационной Безопасности

- Выводы для руководства, содержащие оценку уровня защищённости по результатам анализа.
- Подробное описание всех обнаруженных уязвимостей и их подтверждение.
- Оценку уровня рисков (оценка вероятности эксплуатации уязвимости и степени влияния на бизнес процессы Заказчика).
- Возможные сценарии атаки с учётом различных моделей нарушителя.
- Подробные рекомендации по устранению выявленных уязвимостей.
- Наши специалисты обладают обширным практическим опытом в исследовании и эксплуатации уязвимостей, постоянно расширяют компетенции и кругозор по применяемым методам и векторам атак и являются участниками BugBounty-программ крупнейших международных компаний и ведущих площадках (hackerone, synack, rapid7).

Наше решение
– с чего начать?

Системы
Информационной
Безопасности

- Подписать NDA.
- Подписать авторизационное письмо.
- Выбрать метод демо или полноценного тестирования «Черный ящик», «Белый ящик», «Серый ящик».
- Прислать данные нам на почту.

Системы
Информационной
Безопасности

Как с нами связаться?

+7 495 766-05-38
info@is-systems.org