kaspersky АКТИВИРУЙ БУДУЩЕЕ

Kaspersky Penetration Testing

Надежная защита IT-инфраструктуры от потенциальных кибератак важна для любой организации. Особенно сложной эта задача становится для крупных предприятий, где во многочисленных, географически удаленных подразделениях работают тысячи сотрудников и эксплуатируются сотни информационных систем.

Тестирование на проникновение – это практическая демонстрация возможных сценариев атаки, где злоумышленник пытается обойти средства безопасности в вашей корпоративной сети, чтобы получить привилегированный доступ к важным системам.

Тестирование на проникновение

Выполняемое «Лабораторией Касперского» тестирование на проникновение позволит получить более полное представление о проблемных с точки зрения безопасности местах в инфраструктуре, выявить уязвимости, проанализировать возможные последствия атак различного вида и оценить эффективность уже принятых мер защиты, а также получить рекомендации по устранению уязвимостей и укреплению системы безопасности.

Тестирование на проникновение, проводимое «Лабораторией Касперского», поможет вашей организации:

- **Выявить наиболее уязвимые места в сети,** чтобы сосредоточить на них внимание и снизить риски.
- **Избежать финансовых, операционных и репутационных потерь,** вызванных кибератаками. Заблаговременное обнаружение и устранение уязвимостей позволит предотвратить атаки.
- **Выполнить требования государственных, отраслевых или внутренних корпоративных стандартов,** предусматривающих подобную форму оценки системы безопасности (например, стандарта безопасности данных индустрии платежных карт – PCI DSS).

Варианты предоставления сервиса

Тестирование на проникновение можно проводить в каком-то одном сегменте IT-инфраструктуры, однако мы настоятельно рекомендуем проверять таким образом всю сеть или хотя бы ее крупнейшие сегменты. Ведь результаты тестирования будут более достоверными, если наши специалисты смогут работать в тех же условиях, что и потенциальные злоумышленники.

В зависимости от задач и особенностей IT-инфраструктуры вы можете выбрать любые из следующих вариантов предоставления сервиса:

- **Внешнее тестирование на проникновение.** Оценка системы безопасности, которая проводится через интернет от лица злоумышленника, не обладающего глубокими данными о вашей системе.
- **Внутреннее тестирование на проникновение.** Сценарии с участием злоумышленника, действующего внутри компании. Это может быть посетитель, у которого есть лишь физический доступ в помещения компании, или подрядчик, имеющий ограниченный доступ к системам.
- **Проверка уязвимости к социальной инженерии.** Оценка осведомленности персонала об угрозах безопасности. Моделируется применение методов социальной инженерии: фишинг, псевдовредоносные ссылки в сообщениях электронной почты, подозрительные вложения и т. д.
- **Оценка безопасности беспроводных сетей.** Наши эксперты выезжают к вам и проверяют защищенность сетей Wi-Fi.

Результаты тестирования на проникновение

Сервис выявляет уязвимости в системе безопасности, которыми можно воспользоваться для получения несанкционированного доступа к важным компонентам сети. Такими уязвимостями могут выступать:

- уязвимая архитектура сети, ошибки конфигурации сетевого оборудования;
- уязвимости, делающие возможным перехват и перенаправление сетевого трафика;
- ошибки аутентификации и авторизации в различных службах;
- ненадежные пароли пользователей;
- недостатки конфигурации, в том числе предоставление пользователям
- слишком высоких полномочий;
- уязвимости, вызванные ошибками в коде приложений (внедрение операторов SQL, удаленное выполнение кода, загрузка произвольных файлов, межсайтовое выполнение сценариев и т. д.);
- уязвимости, вызванные использованием устаревших версий
- оборудования и программного обеспечения, для которых не были установлены последние обновления безопасности;
- разглашение информации.

По окончании работ вы получите итоговый отчет с подробной технической информацией о ходе тестирования, его результатах и обнаруженных уязвимостях. В отчете будут также приведены рекомендации по устранению уязвимостей и краткий итог с результатами тестирования и наглядным описанием векторов атак.
В случае необходимости также могут быть подготовлены видеоматериалы и презентации для технического отдела или высшего руководства.

Подход «Лаборатории Касперского»

В рамках тестирования на проникновение имитируются настоящие кибератаки, но ситуация остается под полным контролем. Испытания проводят эксперты «Лаборатории Касперского», которые соблюдают полную конфиденциальность ваших систем и не нарушают их целостность и доступность. Мы строго следуем международным стандартам и принятым в отрасли методикам, среди которых:

- стандарт проведения испытаний на проникновение (PTES);
- специальные публикации института NIST 800-115 (техническое руководство по испытанию и оценке информационной безопасности);
- методическое руководство по испытанию систем безопасности с открытым исходным кодом (OSSTMM)
- платформа оценки безопасности информационных систем (ISSAF)
- классификация угроз, принятая консорциумом безопасности веб-приложений (WASC);
- руководство по испытаниям открытого проекта обеспечения безопасности веб-приложений (OWASP);
- общая система оценки уязвимостей (CVSS).

Специалисты, проводящие работы, – опытные профессионалы, обладающие глубокими и актуальными практическими знаниями. Наши эксперты известны своими исследованиями в области безопасности, в том числе обнаружением новых уязвимостей в крупнейших сервисах и программных продуктах.

Где проводится тестирование

В зависимости от выбранного метода анализа защищенности, особенностей систем и бизнеса клиента тестирование на проникновение может проводиться дистанционно или с выездом на место. Большинство действий можно выполнять дистанционно (даже испытание на проникновение изнутри можно организовать через VPN-доступ), однако для оценки безопасности беспроводных сетей и ряда других задач необходимо присутствие специалистов на вашей территории.

www.kaspersky.ru