Пентесты

написано GlobalTrust.ru | 20.08.2023

Что такое пентест?

Тестирование на проникновение (пентест, pentest) — метод оценки защищенности компьютерных систем и сетей путем имитации и моделирования атакующих действий потенциального злоумышленника. Цель теста на проникновение — оценить возможность и трудоемкость осуществления атак, а также спрогнозировать возможный ущерб.

Пентест может входить в состав мероприятий по анализу защищенности информационных систем и сетей, проводимых в рамках комплексного аудита ИБ. Он включает в себя активный поиск и анализ уязвимостей, использование которых злоумышленниками может спровоцировать утечку данных, некорректную работу целевой системы, либо отказ в обслуживании, либо получить контроль над системой. Результатом работы является отчёт, содержащий описание всех обнаруженных уязвимостей, способов их эксплуатации, а также рекомендации по их устранению. Пентест также может включать в себя, при необходимости, демонстрацию заказчику способов использования имеющихся уязвимостей для проникновения в целевую систему и ее компрометации.

Использование современных методик проведения пентеста

Проведение работ по тестированию на проникновения проводится на основе современных методик: OWASP (Open Web Application Security Project) Testing Guide, OSSTMM (The Open Source Security Testing Methodology Manual) и другие.

Наряду с ручными экспертными проверками при тестировании на проникновение используются следующие автоматизированные программные средства: Nmap, Nikto, Nuclei, The Metasploit Framework, Kali linux (THC Hydra, SQLmap и прочие скрипты), OWASP Zed App

Proxy, Сервис https://sitecheck.sucuri.net, Сервис https://www.ssllabs.com/ssltest и прочие.

Использование Банка данных угроз ФСТЭК России

При анализе угроз используется Банк данных угроз безопасности информации Федеральной службы по техническому и экспортному контролю России (БДУ ФСТЭК России), содержащий сведения об основных угрозах безопасности информации и уязвимостях, характерных для государственных информационных систем (ГИС), автоматизированных систем управления производственными и технологическими процессами критически важных объектов ключевой информационной инфраструктуры (АСУ ТП ОКИИ), информационных система персональных данных (ИСПДн), а также различных видов коммерческих систем, обрабатывающих коммерческую тайну (КТ) и прочие виды конфиденциальной и критичной для бизнеса информации.

Сведения, содержащиеся в Банке данных угроз безопасности информации, не являются исчерпывающими и могут быть дополнены по результатам анализа угроз и уязвимостей в конкретной системе с учетом особенностей ее эксплуатации. В качестве дополнения используется База известных уязвимостей Common Vulnerability Enumeration (CVE: http://cve.mitre.org).

Выполнение нормативных требований

Проведение пентеста позволит выполнить требования регуляторов (ФСТЭК, Банк России), экспериментальным путем оценить защищенность ИТ-инфраструктуры и эффективность используемых механизмов защиты, оценить глубину возможного проникновения злоумышленников в системы и сети организации, сформировать представление о вероятных векторах атак, путях и способах проникновения в целевые объекты.

Ежегодное тестирование на проникновение и анализ уязвимостей компьютерных систем и сетей необходимо проводить финансовым организациям (683-П, 719-П, 757-П Банка России, ГОСТ 57580, PCI DSS). Пентест также необходимо проводить до ввода значимого объекта КИИ в эксплуатацию (приказ ФСТЭК России № 239, Указ Президента РФ №250). В

группе повышенного риска находятся все участники электронной коммерции, операторы связи, а также предприятия малого и среднего бизнеса, которые особенно уязвимы к целенаправленным хакерским атакам.

Опытные пентестеры

Эксперты GlobalTrust имеют обширный опыт проведения пентестов в организациях различного масштаба и сферы деятельности. В их арсенале имеются внешние и внутренние пентесты, социальная инженерия, анализ защищенности веб-сайтов, интернет-магазинов, B2B и B2C систем, тестирование на проникновение офисных сетей промышленных предприятий, Wi-Fi сетей, банковских и платежных систем, сложных ИТ-инфраструктур и критичных бизнес-приложений. Высокая квалификация экспертов GlobalTrust подтверждается положительными отзывами клиентов и сертификатами международного образца (OSCP, OSCE, OSWA, OSWP и др.).

Виды пентестов

Мы проводим следующие виды пентестов:

- Внешний пентест
- Внутренний пентест
- Пентест веб-сайта
- Пентест интернет-магазина
- Пентест WiFi-сети
- Социальная инженерия

Заказ услуг

- по телефону: +7 (925) 203-95-11
- по e-mail: info@globaltrust.ru
- через web-форму