Внешний пентест

написано GlobalTrust.ru | 20.08.2023

В чем особенность внешнего пентеста?

Тестирование на проникновение внешнего периметра корпоративной сети проводится по методу черного ящика (Black-box). Данный метод тестирования направлен на поиск уязвимостей в приложениях и сетевых ресурсах, а также путей проникновения внешнего нарушителя во внутреннюю сеть организации без предоставления заказчиком какой-либо дополнительной информации о сетевой инфраструктуре и объектах тестирования.

Цели и задачи внешнего пентеста

Цели внешнего пентеста:

- Оценка текущего состояния и уровня защищенности внешнего периметра корпоративной сети организации
- Выработка рекомендаций по устранению выявленных уязвимостей

Задачи внешнего пентеста:

- Идентификация и анализ технических уязвимостей информационной безопасности
- Сканирование внешнего периметра корпоративной сети в автоматическом и ручном режимах
- Имитация действий потенциального внешнего злоумышленника по осуществлению сетевых атак на корпоративную сеть из сети Интернет методом «Black-box»
- Подготовка отчета по результатам тестирования, включая рекомендации по ликвидации выявленных уязвимостей

Методики, этапы и объекты тестирования

Методики тестирования:

- OWASP testing guide
- OSSTMM: The Open Source Security Testing Methodology Manual
- NIST Special Publication 800-115: Technical Guide to Information Security Testing and Assessment

Этапы тестирования:

- OSINT (Open-Source Intelligence) — получение предварительной информации о сетевом периметре на основе источников информации, доступных потенциальному нарушителю (поисковые системы, новости, конференции и т.п.)
- Изучение исходных данных по составу внешнего периметра корпоративной сети
- Сканирование сетевого периметра, определение типов устройств, операционных систем и приложений
- Анализ элементов сетевой инфраструктуры
- Сканирования на наличие уязвимостей
- Проведение брутфорс-атак
- Идентификация, анализ и оценка уязвимостей сетевых служб и приложений
- Эксплуатация критичных уязвимостей с целью преодоления сетевого периметра
- Анализ возможностей распространения атаки на внутреннюю сеть

Объекты тестирования:

- Сетевое оборудование
- Операционные системы
- Средства защиты внешнего периметра сети
- Сетевые сервисы и приложения

Как часто следует проводить внешний пентест?

Рекомендуется проводить внешние пентесты на ежегодной основе, а также в случае существенного изменения ИТ-инфраструктуры внешнего периметра корпоративной сети: запуска нового веб-приложения, замены или изменения конфигурации сетевого оборудования, внедрения нового оборудования, внедрения средств удаленного доступа, внедрения новых средств защиты периметра сети и т.п.

Заказ услуг

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