Внутренний пентест

написано GlobalTrust.ru | 20.08.2023

В чем особенность внутреннего пентеста?

Тестирование на проникновение внутренней ИТ-инфраструктуры корпоративной сети организации предполагает имитацию сетевых атак со стороны внутреннего нарушителя, имеющего доступ к внутренним сегментам сети. Работы могут выполняться из внутренней сети, либо удаленно, с помощью VPN-подключения.

Цели и задачи внутреннего пентеста

Цели внутреннего пентеста:

- Оценка текущего состояния и уровня защищенности внутренней ИТ-инфраструктуры корпоративной сети организации
- Выработка рекомендаций по устранению выявленных уязвимостей

Решаемые задачи:

- Идентификация и анализ технических уязвимостей информационной безопасности
- Сканирование внутреннего периметра корпоративной сети в автоматическом и ручном режимах
- Имитация действий потенциального внутреннего нарушителя, имеющего физический и/или логический доступ к внутренним сегментам сети, по осуществлению сетевых атак на внутренние ресурсы корпоративной сети
- 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:

- Пассивный сбор информации о ресурсах внутренней сети
- Перехват и анализ сетевого трафика
- Проведение сетевых атак
- Сканирование узлов, доступных из пользовательского сегмента сети, сбор информации об открытых портах, определение типов устройств, анализ сетевой сегментации
- Сканирования и эксплуатация уязвимостей
- Восстановление паролей и хеш-суммы паролей из оперативной памяти и реестра ОС
- Реализация попыток повышение пользовательских привилегий
- Проверка возможности получения доступа к конфиденциальной информации
- Проверка возможности осуществления доступа к внутренним ресурсам с полученными привилегиями

Объекты тестирования:

- Операционные системы и СУБД
- Рабочие станции и серверы
- Сетевые сервисы и бизнес приложения
- Сетевое оборудование
- Средства защиты информации

Как часто следует проводить внутренний пентест?

Рекомендуется проводить внутренние пентесты на ежегодной основе, а также в случае существенного изменения внутренней ИТ-инфраструктуры корпоративной сети: запуска нового бизнес-приложения, замены или изменения конфигурации сетевого оборудования, внедрения нового оборудования, внедрения новых средств защиты информации и т.п.

Заказ услуг

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