Анализ информационной безопасности сети предприятия

Содержание

- Планирование анализа сетевой безопасности
- Сбор информации об организации
- Тест на проникновение
- Учебный пример: анализ сетевой безопасности компании Northwind Traders

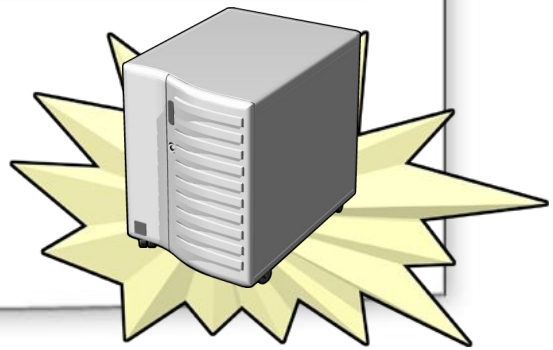
Планирование анализа сетевой безопасности

- Планирование анализа сетевой безопасности
- Сбор информации об организации
- Тест на проникновение
- Учебный пример: анализ сетевой безопасности компании Northwind Traders

Почему взламывают сети?

Сетевая безопасность может подвести по нескольким причинам:

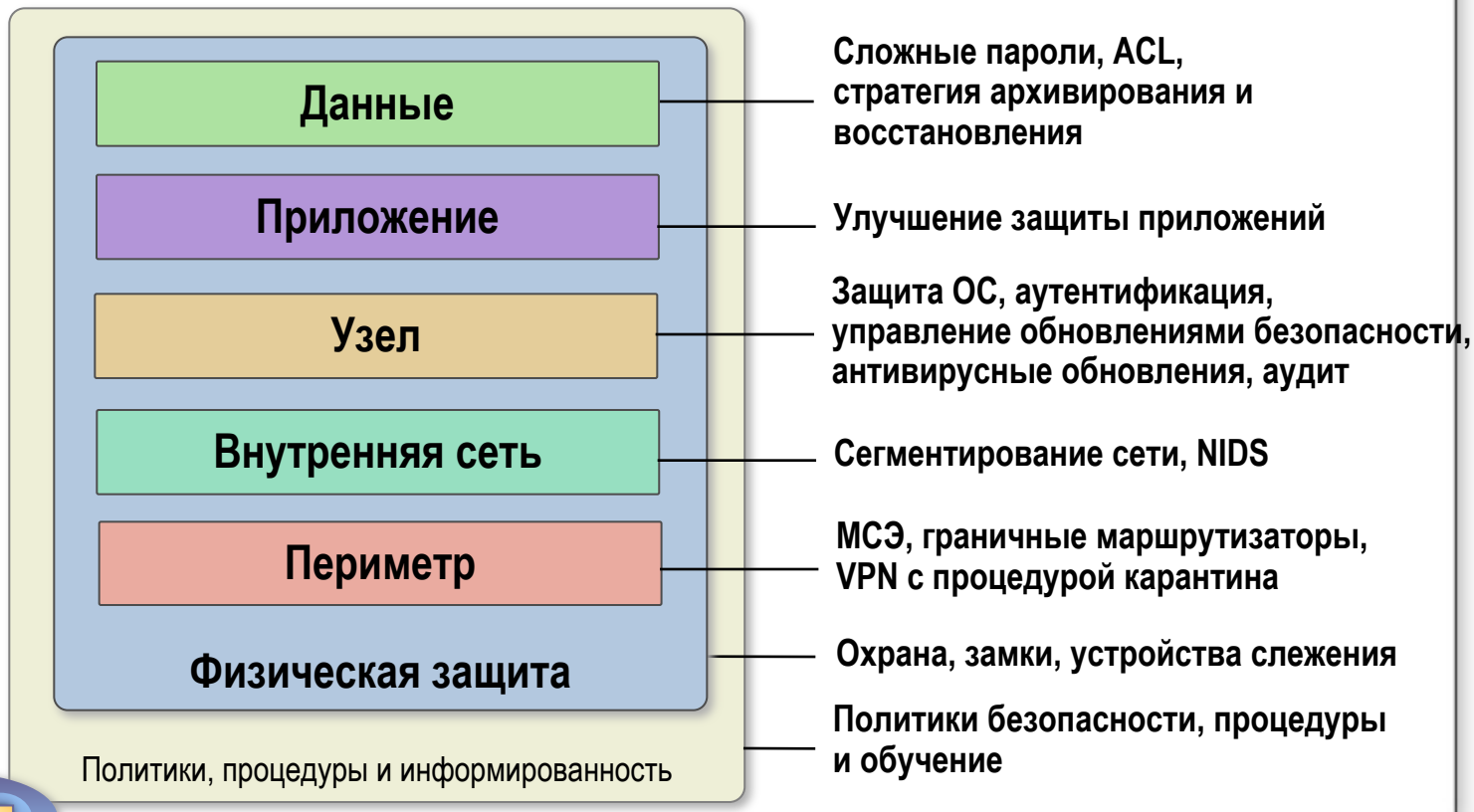
- Человеческий фактор
- Нарушения политик и распоряжений
- Неправильная настройка программного и аппаратного обеспечения
- Незнание собственной сети
- Некомпетентность
- Несвоевременная установка обновлений



Что такое многоуровневая защита?

Использование многоуровневого подхода:

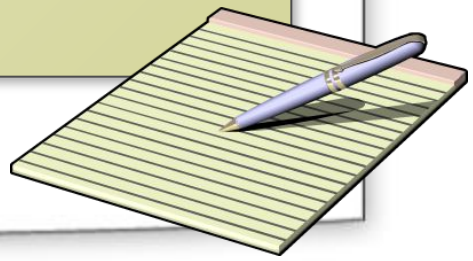
- Повышает риск обнаружения для взломщика
- Снижает шансы взломщика на успех



Для чего выполнять анализ безопасности?

Анализ безопасности может:

- Ответить на вопросы “Защищена ли наша сеть?” и “Как нам узнать, защищена ли наша сеть?”
- Обеспечить рекомендациями, которые помогут улучшить защиту
- Обнаружить ошибки в настройке или отсутствующие обновления безопасности
- Обнаружить неожиданные уязвимости в защите организации
- Удостоверить в соответствии государственным предписаниям



Планирование анализа безопасности

Фаза проекта	Планируемые этапы
Подготовка к анализу	• Диапазон • Цели • Временные рамки • Основные правила
Анализ	• Выбор технологий • Проведение оценки • Объединение результатов
Обработка результатов	• Оценка рисков, привносимых обнаруженными уязвимостями • Создание плана устранения • Определение уязвимостей, которые не могут быть устранены • Определение временного графика устранения уязвимостей
Отчет об исследовании	• Создание итогового отчета • Представление исследования • Планирование следующих исследований

Определение диапазона анализа безопасности

Компоненты	Пример
Цели	Все сервера, использующие: • Windows 2000 Server • Windows Server 2003
Диапазон целевых систем	Все сервера в подсетях: • 192.168.0.0/24 • 192.168.1.0/24
Временные рамки	Сканирование будет выполняться с 3 по 10 июня в нерабочее время
Сканируемые уязвимости	• Уязвимость RPC-over-DCOM (MS 03-026) • Анонимная инвентаризация SAM • Незаблокированные учетные записи Гостя • Более 10 учетных записей в локальной группе Администраторы

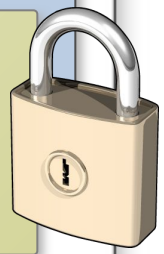
Определение целей анализа безопасности

Цель проекта	
Все компьютеры, использующие Windows Server 2000 и Windows Server 2003 в подсетях 192.168.0.0/24 и 192.168.1.0/24 будут просканированы и исправлены в соответствии со стандартами	
Уязвимость	**Исправление**
Уязвимость RPC-over-DCOM (MS 03-026)	Установить обновление Microsoft 03-026 и 03-39
Анонимная инвентаризация учетных записей SAM	Сконфигурировать RestrictAnonymous в: 2 на Windows Server 2000 1 на Windows Server 2003
Разрешена учетная запись Гость	Запретить учетную запись Гость
Более 10 учетных записей в локальной группе Администраторы	Уменьшить количество учетных записей в локальной группе Администраторы

Типы анализа безопасности

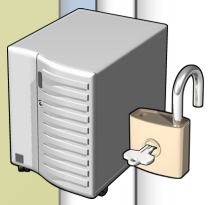
Сканирование уязвимостей:

- Нацелено на известные недостатки
- Может быть автоматизировано
- Требует минимальной обработки экспертами



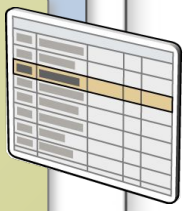
Тестовое проникновение:

- Нацелено на известные и неизвестные недостатки
- Требует высококвалифицированных экспертов
- Несет угрозу нарушения законов в некоторых странах или внутренних распоряжений организаций



Аудит IT- безопасности:

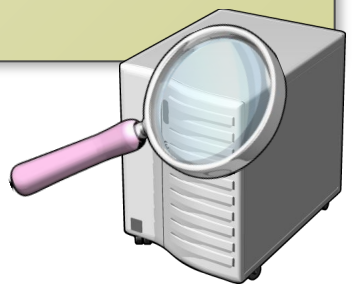
- Нацелен на политики и процедуры в области безопасности
- Используется для обеспечения обоснований внутренних распоряжений



Использование сканирования уязвимостей для анализа сетевой безопасности

Разработка процесса сканирования:

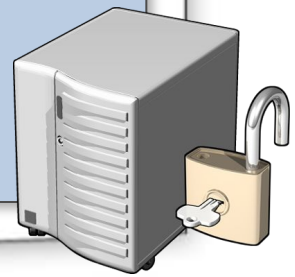
- Определение уязвимостей
- Присвоение уровня риска обнаруженным уязвимостям
- Определение уязвимостей, которые не были устранены
- Определение временного графика улучшения защищенности



Использование тестового проникновения для анализа сетевой защищенности

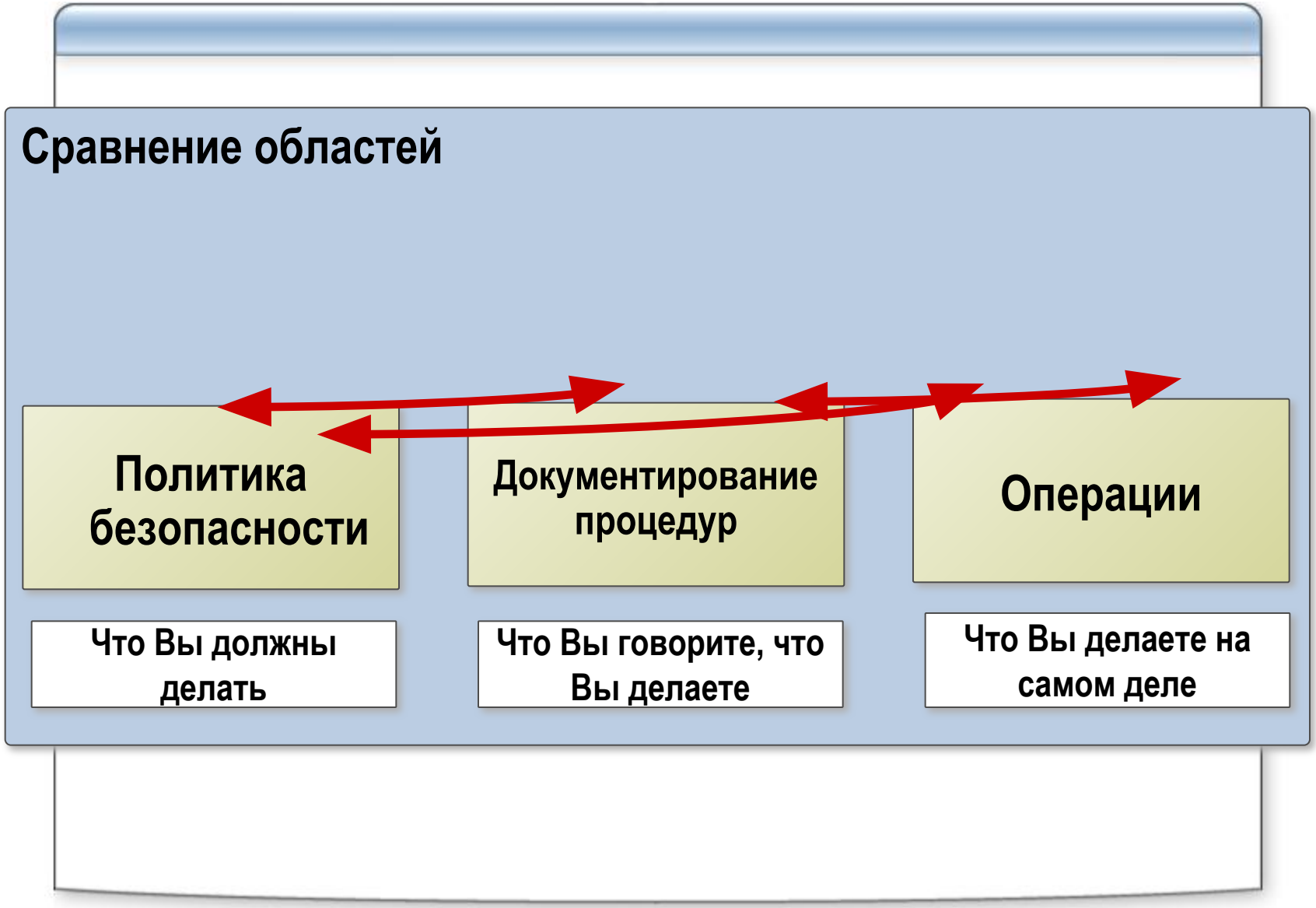
Шаги для успешного тестового проникновения:

1. Определите наиболее вероятные действия взломщика сети или приложения
2. Найдите недостатки в защите сети или приложения
3. Определите, как атакующий может использовать уязвимость
4. Найдите ресурсы, к которым есть доступ на чтение, модификацию или удаление
5. Определите, была ли обнаружена атака
6. Определите сигнатуры и характеристики атаки
7. Дайте рекомендации



Понимание компонентов аудита IT-безопасности

Реализация аудита IT-безопасности



Отчет об анализе безопасности

Объедините информацию в отчете по следующему шаблону:

- Определите уязвимости
- Документируйте планы исправлений
- Определите, где должны произойти изменения
- Назначьте ответственных за реализацию принятых рекомендаций
- Порекомендуйте время следующего анализа безопасности

Сбор информации об организации

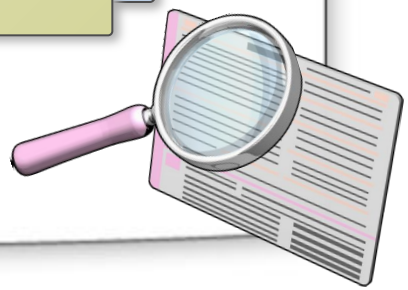
- Планирование анализа сетевой безопасности
- Сбор информации об организации
- Тестовое проникновение
- Учебный пример: анализ сетевой безопасности компании Northwind Traders

Что такое неагрессивная атака?

Неагрессивная атака: сбор информации о сети предприятия из открытых источников, для подготовки к последующей проникающей атаке

Примеры неагрессивных атак:

- Информационная разведка
- Сканирование портов
- Получение информации об узле на основе сигнатур
- Обнаружение сетей и узлов



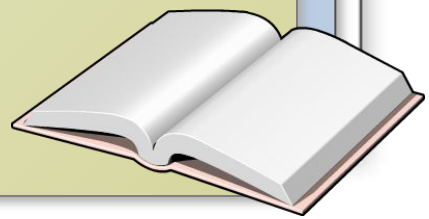
Техника информационной разведки

Основные типы информации, разыскиваемой атакующими:

- Конфигурация системы
- Действующие учетные записи пользователей
- Контактная информация
- Ресурсы экстранет и сервера удаленного доступа
- Бизнес-партнеры, слияния и поглощения

Информация о вашей сети может быть получена из:

- Запросов в каталоги
- Выяснения выделенных IP-адресов
- Корпоративного веб-сайта
- Поисковых машин
- Открытых форумов



Противодействие информационной разведке

- Предоставляйте для регистрации в Интернет только безусловно необходимую информацию
- Регулярно просматривайте корпоративный веб-сайт в поисках конфиденциальной информации
- Для публикации на веб и регистрации используйте адреса электронной почты, основанные на должностных функциях
- Издайте распоряжение, регламентирующее правила пользования открытыми форумами

Какая информация может быть получена из сканирования портов?

Обычно, результаты сканирования содержат:

- Список «прослушиваемых» («открытых») портов
- Список портов, обрывающих соединения
- Список портов, подключение к которым не было установлено по таймауту

Тонкости в сканировании портов:

- Медленное сканирование
- Сканирование одного и того же порта с разных узлов
- Распределенное сканирование с разных хостов (оптимально из разных сетей)

Противодействие сканированию портов

Меры противодействия сканированию портов:

- ✔ Внедрение многоуровневой фильтрации трафика
- ✔ План на случай компрометации или сбоев
- ✔ Внедрение системы обнаружения вторжений
- ✔ Запуск только необходимых служб
- ✔ Публикация сервисов только через МСЭ

Какая информация может быть собрана об удаленном узле?

Типы информации, которая может быть собрана с использованием технологии сигнатур:

- Реализация IP и ICMP
- Ответы TCP
- Открытые порты
- Баннеры
- Поведение служб
- Запросы удаленной операционной системы

Защита информации о конфигурации сетевого узла

Источник	Противодействие
IP, ICMP, и TCP	• Будьте консерватором в плане определения типа пакетов, которые могут попасть в вашу сеть • Используйте МСЭ или IDS для управления трафиком • Предположим, что атакующий знает версию операционной системы на Ваших компьютерах. Убедитесь, что она защищена!
Баннеры	• Поменяйте баннеры, выдающие версию операционной системы • Предположим, что атакующий знает версию операционной системы на Ваших компьютерах. Убедитесь, что она защищена!
Сканирование портов, поведение служб, удаленные запросы	• Запретите неиспользуемые службы • Фильтруйте трафик, приходящий на определенные порты узла • Внедрите IPSec на всех узлах в сети

Тестовое проникновение

- Планирование анализа сетевой безопасности
- Сбор информации об организации
- Тестовое проникновение
- Учебный пример: анализ сетевой безопасности компании Northwind Traders

Что такое тестовое проникновение?

Взлом (атака, проникновение): Выполнение определенных действий, которые приводят к компрометации информации, снижению устойчивости или доступности системы

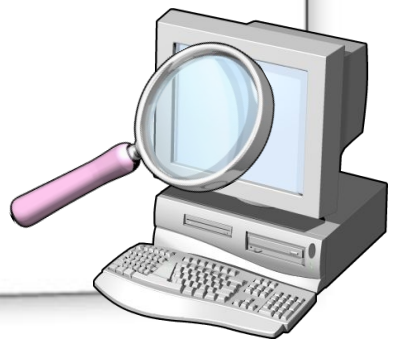
Примеры методов тестового проникновения:

- Автоматическое сканирование уязвимостей
- Атаки на пароли
- Атаки на отказ в обслуживании
- Атаки на приложения и базы данных
- Сетевой анализ («вынюхивание», sniffing)

Что такое автоматическое сканирование уязвимостей?

Сканирование уязвимостей производится с помощью утилит, автоматизирующих следующие задачи:

- Сбор баннеров и сигнатур
- Реализация уязвимости
- Тестирование на основе косвенных данных
- Определение установленных обновлений



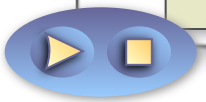
Что такое атаки на пароли?

Два основных типа атак на пароли:

- Атаки «грубой силы» (прямой перебор)
- Обнаружение сохраненных паролей

Противодействие для защиты от атак на пароли:

- Потребуйте использовать сложные пароли
- Обучите пользователей
- Внедрите смарт-карты
- Издайте распоряжение, запрещающее сохранять пароли в командных файлах, сценариях, веб-страницах



Что такое атаки по типу «отказ в обслуживании»?

Атаки «отказ в обслуживании» (DoS): Любая попытка действий, которые могут привести к выходу из строя системы, и нарушению ее нормального функционирования

Атаки на отказ в обслуживании могут быть разделены на 3 категории:

- Флуд
- Атаки на истощение ресурсов
- Сбой службы

Примечание: Атаки на отказ в обслуживании не должны запускаться против Вашей собственной работающей сети

Противодействие атакам на отказ в обслуживании

Атака	Противодействие
Флуд	• Убедитесь, что на Ваших маршрутизаторах есть правила, запрещающие подмену адреса и блокирующие широковещательные запросы • Ограничение скорости трафика для смягчения последствий атаки • Обдумайте возможность запрещения пакетов ICMP
Истощение ресурсов	• Установите последние обновления операционной системы и приложений • Установите дисковые квоты
Сбой службы	• Установите последние обновления операционной системы и приложений • Тестируйте обновления, прежде чем применять их в работающей системе • Запретите неиспользуемые службы

Понимание атак на приложения и базы данных

Основные атаки на приложения и базы данных включают в себя:

Переполнения буфера:

- Пишите приложения с управляемым кодом

Атаки внедрения SQL:

- Проверяйте ввод на корректность размера и типа

Что такое анализ сетевого трафика?

Анализ сетевого трафика (sniffing): возможность атакующего прослушать коммуникации между сетевыми узлами

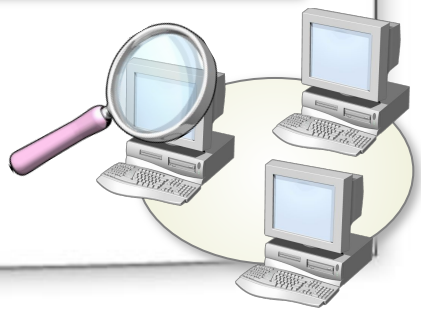
Атакующий выполняет следующие действия:

1. Компрометация узла
2. Установка сетевого монитора
3. Использование сетевого анализатора для захвата передаваемой по сети конфиденциальной информации (н-р, сетевые учетные данные)
4. Использование полученных учетных данных для компрометации других узлов

Противодействие атакам сетевого анализа

Чтобы снизить угрозу атак сетевого анализа, убедитесь в следующем:

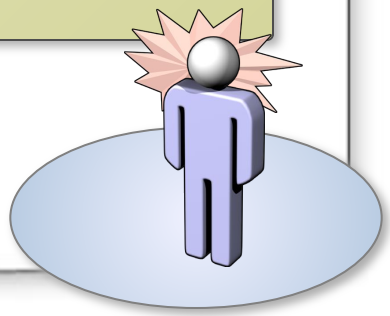
- Используйте шифрование для защиты данных
- Используйте коммутаторы вместо концентраторов
- Защитите основные сетевые устройства
- Используйте crossover-кабели
- Запретите использование сетевых анализаторов
- Выполняйте регулярное сканирование



Как атакующие избегают обнаружения во время атаки

Основные способы избежать обнаружения во время атаки:

- Переполнение или замусоривание файлов журналов
- Нарушение работоспособности служб записи событий
- Атаки на систему обнаружения вторжений
- Атаки со сменой представления
- Отправка фальшивых пакетов



Как атакующие избегают обнаружения после атаки

Основные способы избежать обнаружения после осуществления атаки:

- Подмена системных файлов (установка руткитов)
- Подчистка журналов

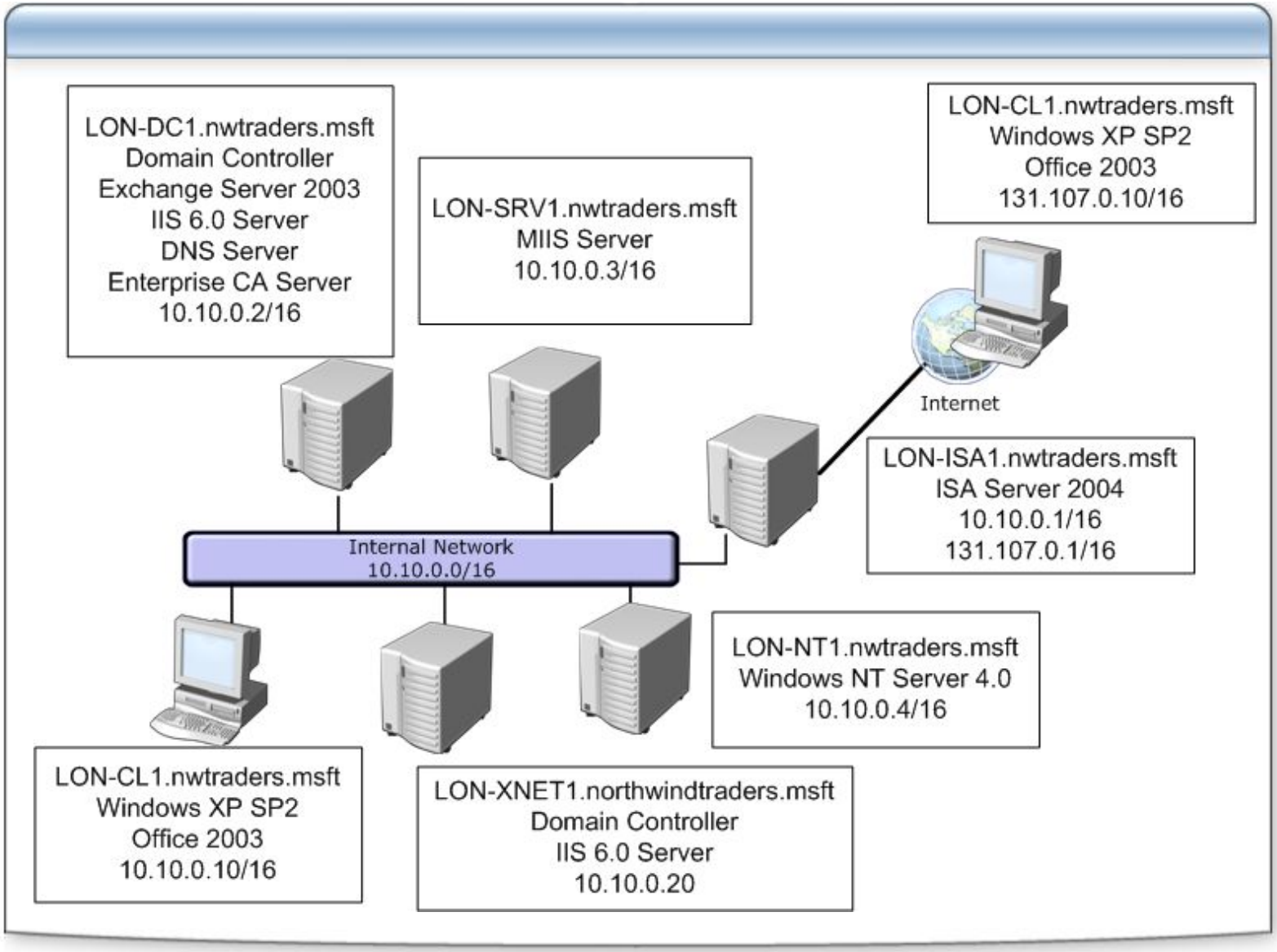
Противодействие технологиям сокрытия от обнаружения

Технология маскировки	Противодействие
Замусоривание журналов	• Архивируйте файлы журналов до того, как они переполнились
Нарушение работоспособности служб записи событий	• Убедитесь, что используемый механизм записи событий использует последнюю обновленную версию программного обеспечения
Атаки на систему обнаружения вторжений	• Обновляйте сигнатуры и программное обеспечение системы обнаружения вторжений
Атаки со сменой представления	• Убедитесь, что приложение нормализует данные к их канонической форме
Использование приманок	• Защитите целевые атакуемые системы и сети
Использование руткитов	• Обеспечьте многоуровневую защиту
Подчистка журналов	• Защитите хранилище журналов • Храните журналы на удаленном узле • Используйте шифрование для защиты файлов журналов • Архивируйте журналы

Учебный пример: анализ сетевой безопасности компании Northwind Traders

- Планирование анализа сетевой безопасности
- Сбор информации об организации
- Тестовое проникновение
- Учебный пример: анализ сетевой безопасности компании Northwind Traders

Описание учебного примера



Определение области оценки безопасности

Компоненты	Scope
Целевая система	LON-SRV1.nwtraders.msft
Временные рамки	Сканирование будет выполнено 5 апреля в нерабочее время
Уязвимости	• Переполнение буфера • Внедрение SQL • Разрешенная учетная запись Гость • Уязвимость RPC-over-DCOM

Определение целей оценки безопасности

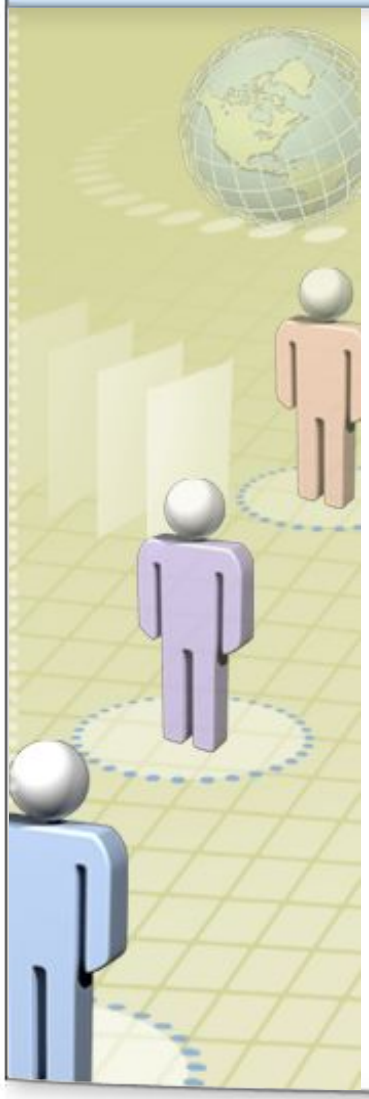
Цель проекта	
LON-SRV1 будет просканирован на наличие следующих уязвимостей, и затем переконфигурирован в соответствии с полученными рекомендациями	
Уязвимость	**Устранение**
Внедрение SQL	Разработчики должны доработать Web-приложения
Переполнение буфера	Разработчики должны обновить приложения
Разрешенная учетная запись Гость	Запретить учетную запись Гость
Уязвимость RPC-over-DCOM	Установить обновление MS04-012

Выбор программ и утилит

Следующие утилиты будут использованы для оценки безопасности в Northwind Traders:

- Microsoft Security Risk Assessment Utility
- Microsoft Baseline Security Analyzer
- KB824146SCAN.exe
- Portqry.exe
- Проверка вручную на уязвимость переполнения буфера
- Проверка вручную на наличие уязвимости внедрения SQL

Демонстрация: Выполнение анализа безопасности



- Выполнение сканирования портов с помощью Portqry.exe
- Использование KB824146Scan.exe для сканирования на уязвимости
- Определение уязвимостей переполнения буфера
- Определение уязвимостей внедрения SQL
- Использование Microsoft Baseline Security Analyzer для сканирования уязвимостей

Отчет о результатах исследования

Ответьте на следующие вопросы, чтобы закончить отчет:

- Какой риск представляют собой уязвимости?
  - В чем причина уязвимости?
  - Каково потенциальное воздействие уязвимости?
  - Какова вероятность того, что уязвимость будет использована для взлома?
- Что нужно сделать, чтобы устранить уязвимость?
  - Если возможно, дайте несколько вариантов
- Как временно устранить уязвимость?
- Кто отвечает за устранение уязвимости?

Итоги

- Планируйте анализ безопасности, определяйте диапазон анализа и его и цели
- Предоставляйте для публикации на сайте и для регистрации в Интернет только безусловно необходимые данные
- Предположите, что атакующий точно знает версию операционной системы, и предпримите все действия для защиты системы
- Потребуйте от пользователей использовать сложные пароли, и обучите их «парольным фразам»
- Устанавливайте последние обновления безопасности и пакеты обновлений

Пример: Microsoft IT

Окружение

- 56000 постоянных сотрудников, 7000 временных, 28000 внешних исполнителей
- 400 офисов по всему миру

Несанкционированный доступ

- 100000 попыток взлома ежемесячно
- 150000 зараженных писем

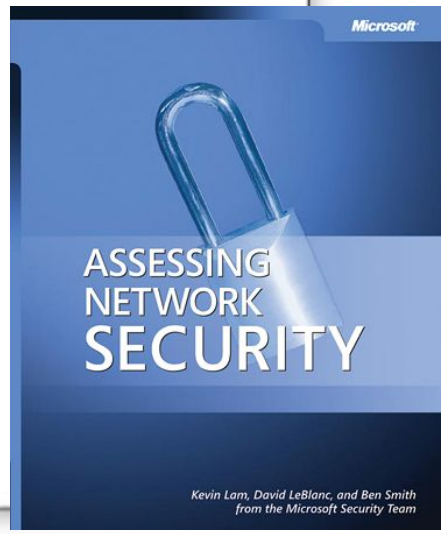
Пример: Microsoft IT

Полезные советы

- Все записывайте
- Создайте сильную команду
- Открывайте новые таланты
- Оценивайте эффективность работы команды и ее участников
- Применяйте отраслевые стандарты и общепринятые методы

Что дальше?

- **Узнайте о семинарах по безопасности:**
  http://www.microsoft.com/seminar/events/security.mspx
- **Подпишитесь на рассылку по безопасности:**
  http://www.microsoft.com/technet/security/signup/default.mspx
- **Security Risk Self-assesment Tool**
  http://www.securityguidance.com
- **Пройдите on-line обучение**
  https://www.microsoftelearning.com/security/
  http://www.microsoft.com/technet/traincert/virtuallab/security.mspx
- **Книга «*Assessing Network Security* by Kevin Lam, David LeBlanc, and Ben Smith»**
  http://www.microsoft.com/mspress/books/6788.asp



Вопросы?