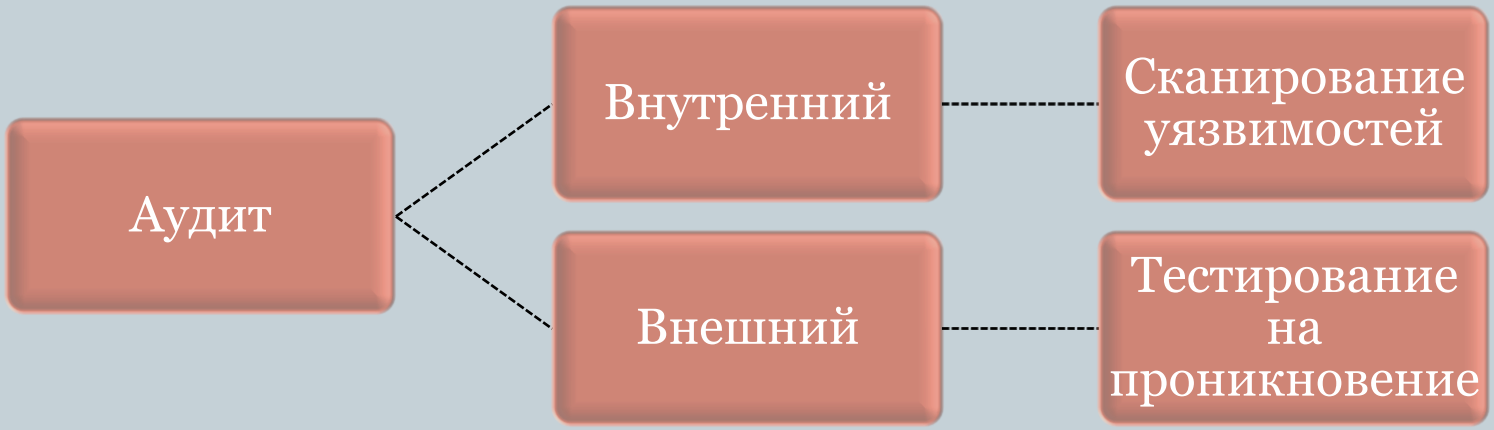
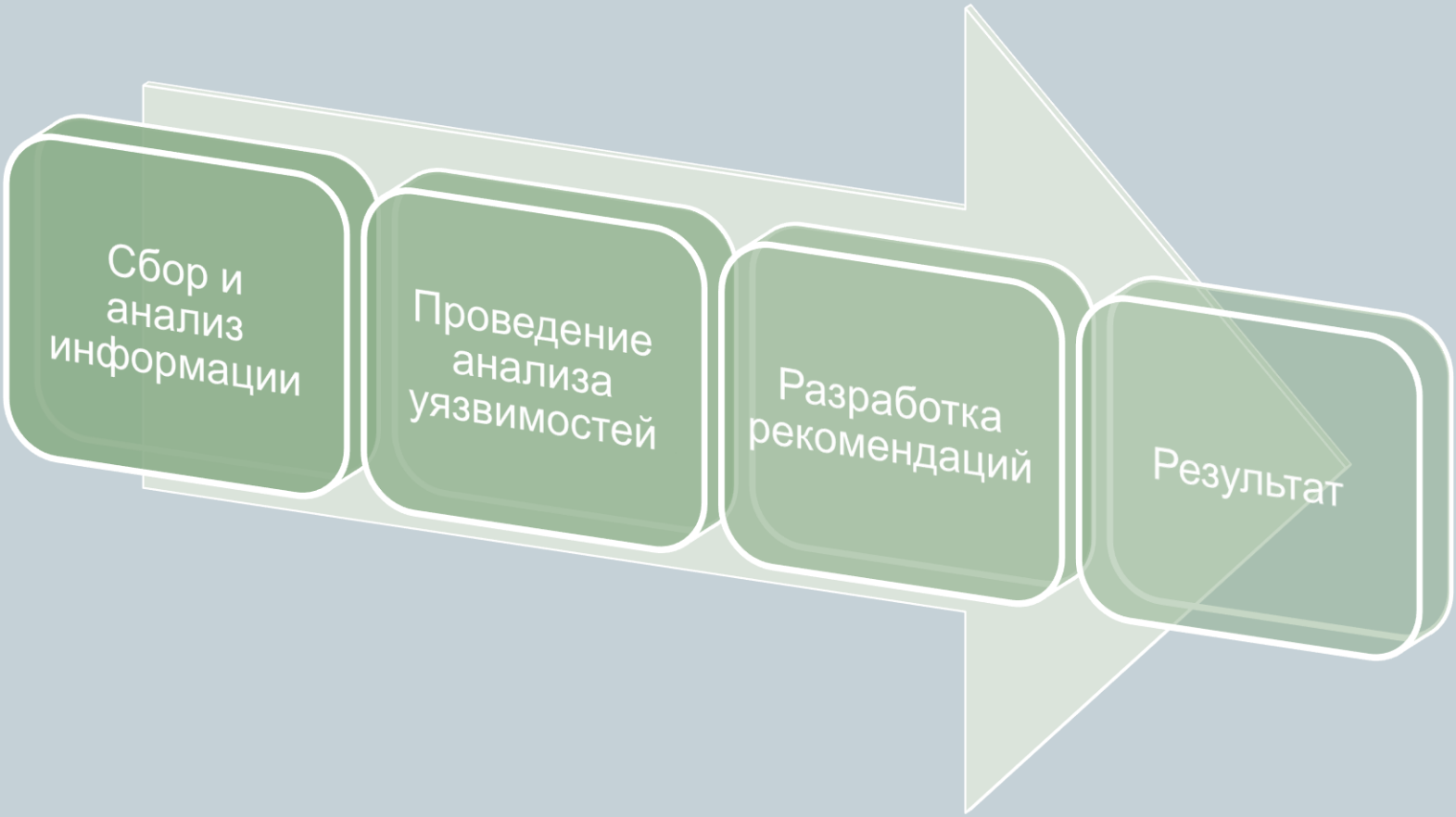
Анализ безопасности автоматизированных систем методом тестирования на проникновение

Аудит информационной безопасности

Аудит информационной безопасности – независимая оценка текущего состояния системы информационной безопасности, устанавливающая уровень ее соответствия определенным критериям.



Аудит ИБ


Сбор и анализ информации
Проведение анализа уязвимостей
Разработка рекомендаций
Результат

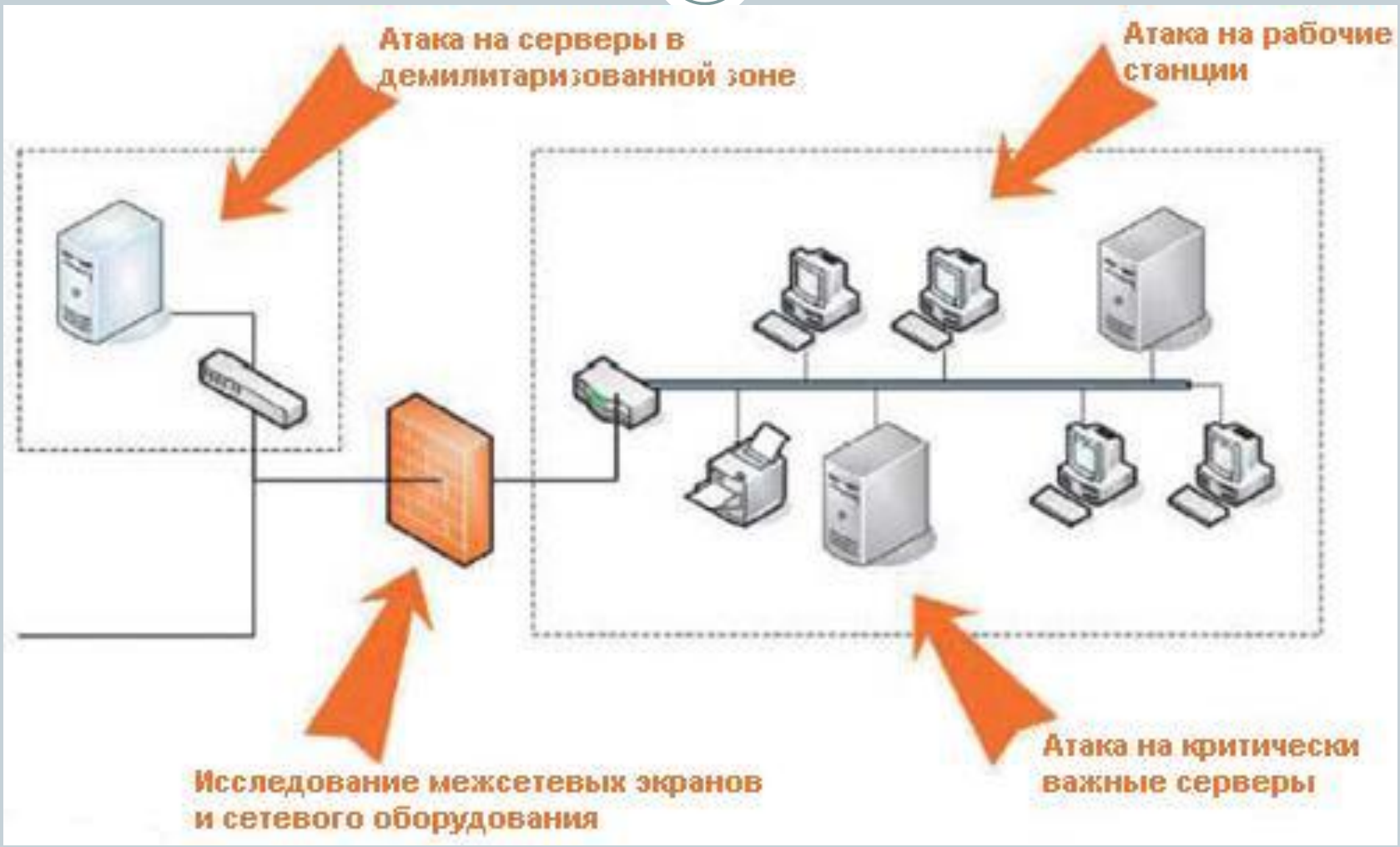
Популярные методологии тестирования на проникновение

- ***Information Systems Security Assessment Framework (ISSAF)***
- ***NIST 800-53 Guideline on Network Security Testing***
- ***Open Source Security Testing Methodology Manual (OSSTMM)***
- ***OWASP Testing Guide***
- ***Wireless Penetration Testing Framework***

Проверки, характерные для типовой корпоративной ЛВС

1. Определение топологии сети.
2. Сканирование портов.
3. Идентификация сервисов.
4. Идентификация системы.
5. Исследование и контроль уязвимостей.
6. Тестирование интернет – приложений.
7. Тестирование маршрутизации.
8. Тестирование межсетевых экранов.
9. Тестирование систем обнаружения вторжений (IDS).
10. Взлом паролей.
11. Тестирование на отказ в обслуживании (DDoS).

Объекты тестирования



Используемые программные средства

Nessus 4

Nikto 2

Nmap 5.0

Metasploit Framework 3

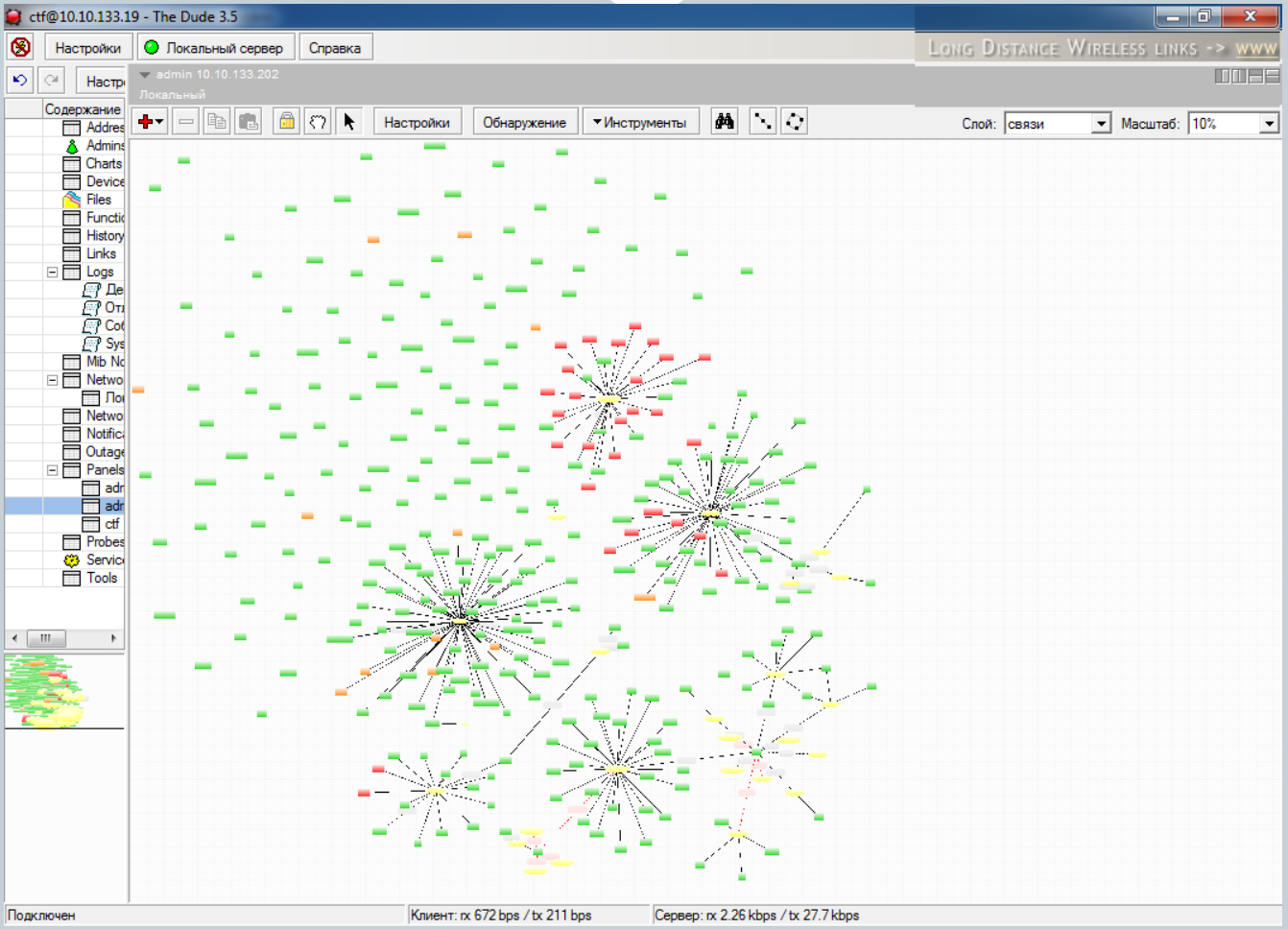
Dude 3.5

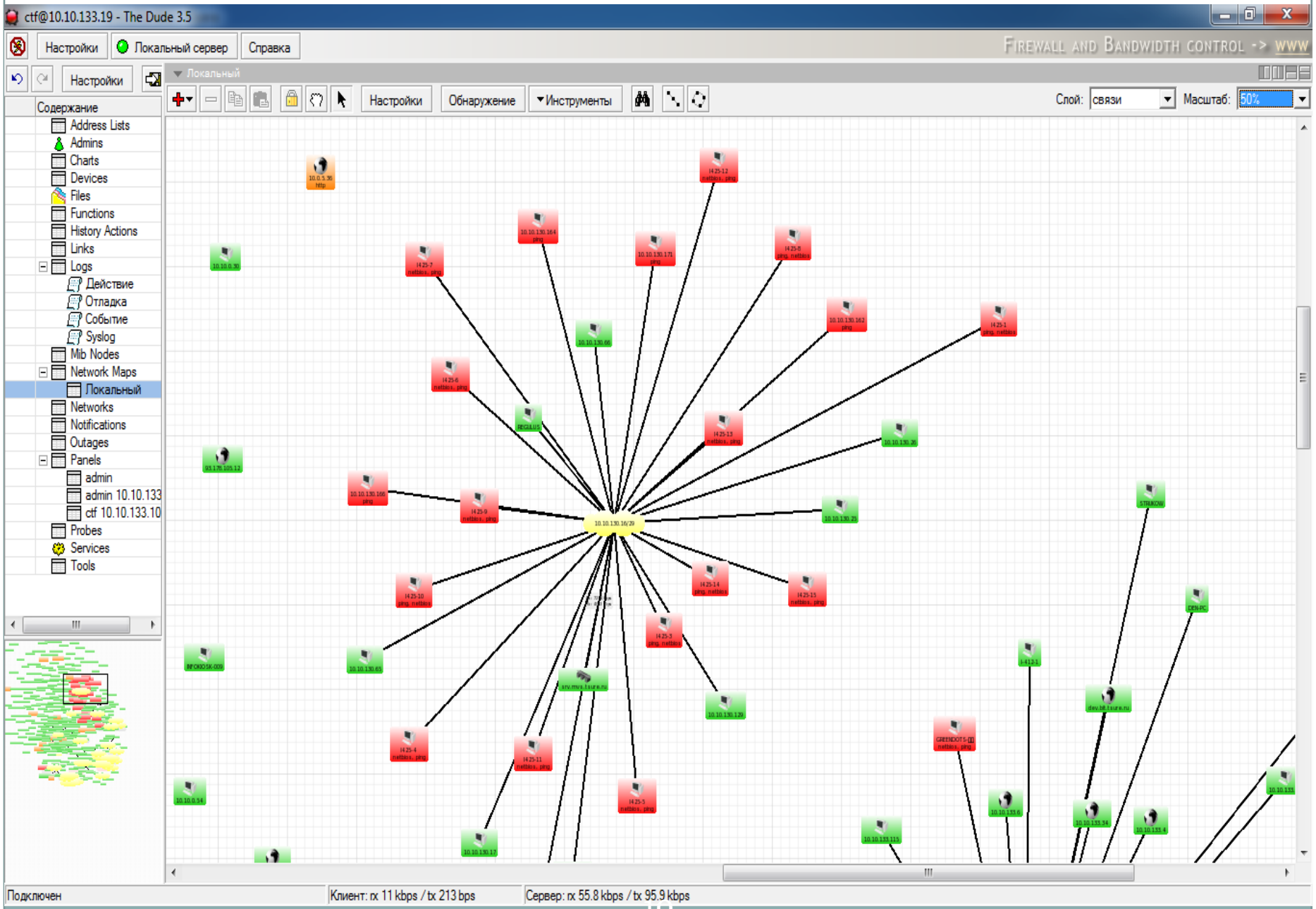
Wireshark 1.0.6

Набор программного обеспечения для оценки основных функций безопасности сети

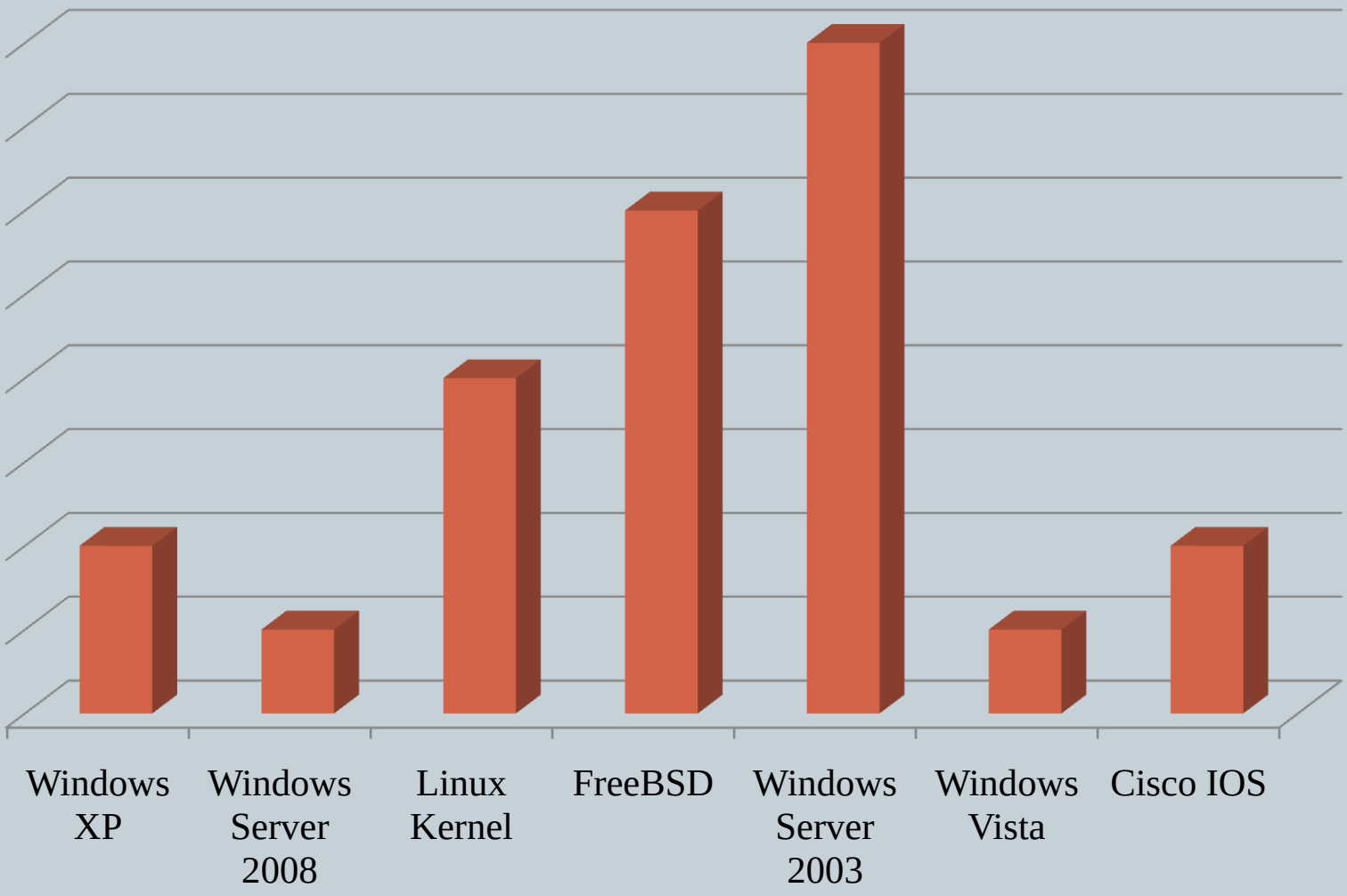
Средство	Функции
Dude	Средство построения карты сети и обзора сети
Nmap	Сканер сетевых портов, средство идентификации операционных систем и сервисов
OpenVAS	Средство поиска уязвимостей в сетевых приложениях (ex-Nessus)
Nikto2, Skipfish	Сканер уязвимостей интернет- приложений
Metasploit Framework 3.4	среда отладки эксплойтов и оценки уязвимостей приложений, в том числе Web-приложений
Wireshark	Средство анализа сетевых протоколов
Aircrack NG	Средство анализа беспроводных сетей
John The Ripper	Средство анализа стойкости паролей.

Исследование сети Dude

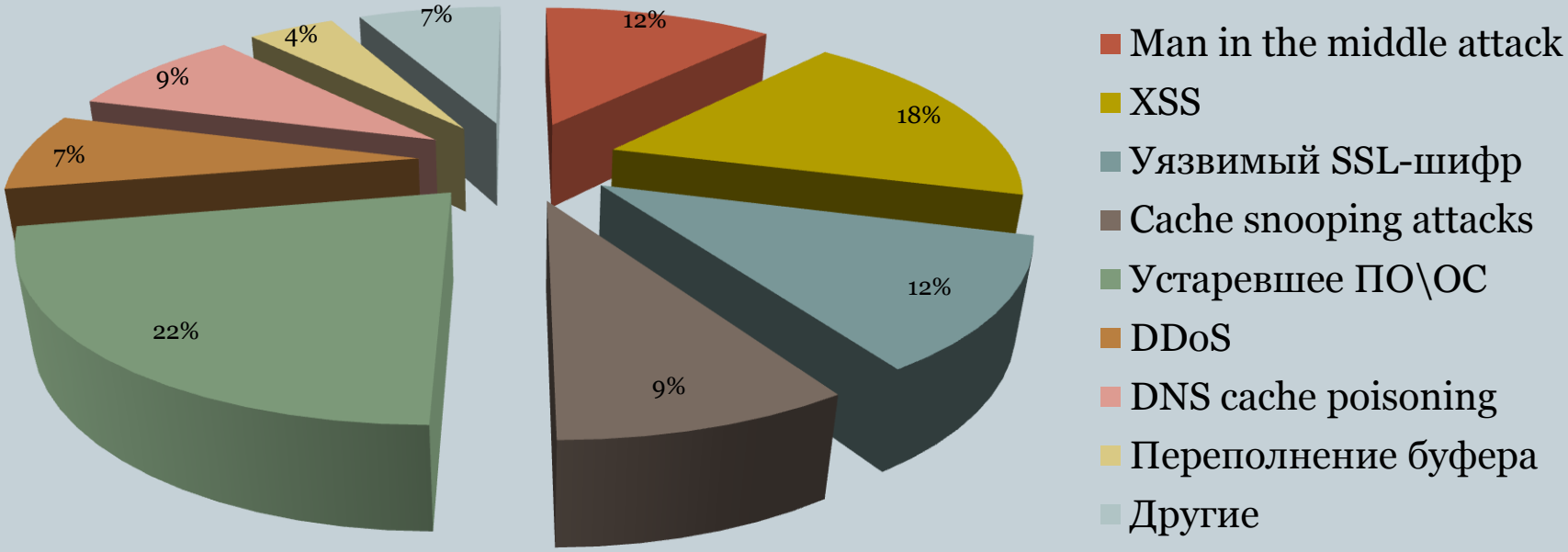



ctf@10.10.133.19 - The Dude 3.5
Настройки
Локальный сервер
Справка
Firewall and Bandwidth control -> www
Настройки
Локальный
Настройки
Обнаружение
Инструменты
Слой:
связи
Масштаб:
50%
Содержание
Address Lists
Admins
Charts
Devices
Files
Functions
History Actions
Links
Logs
Действие
Отладка
Событие
Syslog
Mib Nodes
Network Maps
Локальный
Networks
Notifications
Outages
Panels
admin
admin 10.10.133
ctf 10.10.133.10
Probes
Services
Tools
10.10.130.16/29
Подключен
Клиент: rx 11 kbps / tx 213 bps
Сервер: rx 55.8 kbps / tx 95.9 kbps

Статистика операционных систем



Исследование уязвимостей



Пример тестирования автоматизированной информационной системы на проникновение

Входными данными для тестирования являются:

1. Перечень IP-адресов хостов, образующих внешний периметр информационной системы Заказчика (подсеть 168.192.200.0/28).
2. Перечень адресов корпоративной электронной почты в домене alemneftegaz.ru, представляющий собой репрезентативную выборку по сотрудникам из различных структурных подразделений.

Применялась следующая методика, позволяющая наиболее полно смоделировать действия потенциального нарушителя:

1. Пассивный сбор сведений об информационной системе Заказчика из открытых источников.
2. Активный сбор сведений об информационной системе Заказчика (подключение к хостам внешнего периметра).
3. Проверка возможности проникновения в информационную систему Заказчика при помощи использования уязвимостей сетевых служб, запущенных на хостах внешнего периметра.
4. Проверка возможности проникновения в информационную систему Заказчика.

при помощи реверсивной троянской программы. о ходе выполнения работ по тесту на проникновение в информационную систему Заказчика регулярно сообщалось представителям отдела информационной безопасности Заказчика. Сотрудникам отдела информационных технологий, ответственным за администрирование информационной системы, не было сообщено о факте выполнения таких работ.

Анализ защищенности информационных ресурсов

Перед началом работ по проведению теста на проникновения был составлен примерный «профиль информационной системы» – приблизительное описание корпоративных сервисов, предоставляемых информационной системой сотрудникам и пользователям глобальной сети Интернет. Такая предварительная оценка позволяет сразу же выделить основные направления, подлежащие анализу в первую очередь.

Было сделано предположение, что типовые корпоративные сервисы данной информационной системы – это система электронной почты, корпоративный сайт или портал, система доступа удаленных клиентов, а также служебные подсистемы – например, службы DNS, NTP и – ключевой компонент – подсистема средств защиты.

Пассивный сбор сведений

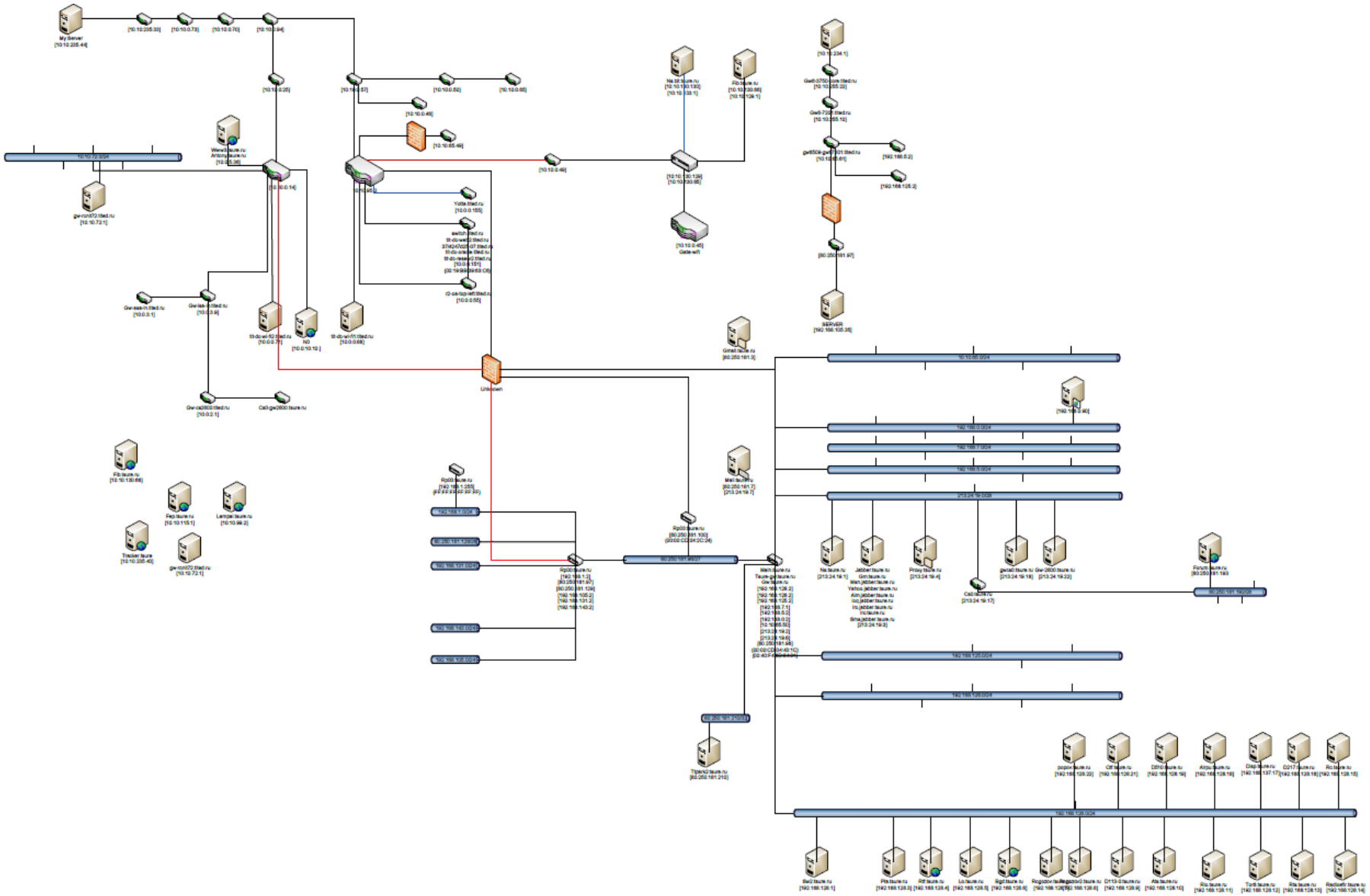
Пассивный сбор сведений об информационной системе проводился при помощи общедоступных сетевых сервисов – службы DNS, службы WHOIS, а также программ traceroute, tracepath и т.п., web-интерфейс к которым предоставляют многие сайты (таким образом, IP-адрес потенциального нарушителя остается неизвестным для атакуемой системы).

Активный сбор сведений

Во время активного сбора информации было проведено сканирование хостов всего диапазона при помощи программы nmap. Для снижения риска обнаружения «нарушителей» средствами предположительно установленной в исследуемой подсети ISS RealSecure сканирование проводилось в течение длительного времени, с большими интервалами между сканированием отдельных портов. Были определены версии программного обеспечения сетевых служб на исследованных хостах. Проведенное сканирование показало корректность исходных предположений о профиле информационной системы.

После этого была выполнена проверка достоверности полученной информации.

С большой долей уверенности можно было утверждать, что сокрытие или изменение версий программного обеспечения сетевых служб администраторами информационной системы не проводилось.



Анализ уязвимостей сетевых служб

Поиск уязвимостей в программном обеспечении сетевых служб не дал положительных результатов, были предприняты лишь контрольные запуски эксплоитов на службы SMTP и WWW для проверки чувствительности сенсора ISS и возможного блокирования IP-адреса, с которого производился запуск эксплоита, средствами маршрутизатора или межсетевого экрана. Подсистема защиты никак не отреагировала на активные попытки атаки, адрес «нарушителя» заблокирован не был.

Запуск реверсивной троянской программы

Следующим этапом выполнения теста на проникновение являлась рассылка троянской программы пользователям информационной системы согласно согласованному перечню адресов электронной почты. Необходимо отметить, что при помощи популярных поисковых систем (www.yandex.ru, www.google.com) потенциальный нарушитель может получить адреса электронной почты сотрудников, которые по тем или иным причинам оказались опубликованы в сети Интернет, и использовать эту информацию для более эффективной атаки при помощи троянской программы. Была использована троянская программа, позволяющая в случае ее запуска на компьютере пользователя получить удаленный (через Интернет) доступ к ресурсам данного компьютера и корпоративной сети с правами пользователя, запустившего программу.

Троянская программа является реверсивной – то есть, самостоятельно инициирующей запросы к своему управляющему серверу (установленному в сети атакующего), который сообщает ей последовательность команд для выполнения на компьютере пользователя, а в ответ получает результат выполнения этих команд. Это позволяет использовать троянскую программу в сетях с трансляцией сетевых адресов (NAT).

Выводы

1. Внешний периметр информационной системы Заказчика защищен достаточно надежно: регулярно выполняется установка обновлений программного обеспечения сетевых служб, конфигурация служб соответствует требованиям информационной безопасности. Тем не менее, сетевые службы предоставляют потенциальному нарушителю достоверную служебную информацию, что может быть использовано при организации атак на внешний периметр.

2. Система обнаружения вторжений установлена в конфигурации по умолчанию, её настройка неэффективна и не обеспечивает адекватный уровень реакции на явно выраженную сетевую активность нарушителя.

3. Общая архитектура информационной системы Заказчика, конкретные технические решения по обеспечению информационной безопасности и низкая квалификация пользователей информационной системы не обеспечивают требуемый уровень защиты, что позволило осуществить успешный запуск троянской программы.

4. Уровень защищенности серверов и рабочих станций информационной системы Заказчика – низкий. Отдельно необходимо отметить низкий уровень защиты критически важных серверов: контроллера домена и сервера СУБД, в которой хранится важная для бизнеса информация.

5. Анализ скомпрометированной базы паролей пользователей показал низкую стойкость паролей как обычных пользователей, так и администраторов системы.

Рекомендации

1. Включить скрытие служебной информации, предоставляемой сетевыми службами пользователям.

2. Выполнить тонкую настройку системы обнаружения вторжений.

3. Развернуть в информационной системе сервер обновлений Windows Update, включить автоматическое обновление на всех серверах и рабочих станциях.

4. Развернуть в информационной системе сетевую систему обнаружения вторжений, которая позволила бы протоколировать подозрительную сетевую активность и оперативно реагировать на подобные инциденты.

5. Разработать парольную политику, включающую в себя требования по стойкости паролей, правила хранения и периодической замены ключевых фраз. Недопустимо использование единого пароля для администрирования всех ресурсов информационной системы. К паролям административных учетных записей должны предъявляться особые требования по стойкости.

6. Разработать и реализовать на практике программу обучения пользователей вопросам информационной безопасности.