Интернет-журнал «Отходы и ресурсы» https://resources.today
Russian Journal of Resources, Conservation and Recycling

2022, Том 9, № 4 / 2022, Vol 9, No 4 https://resources.today/issue-4-2022.html

URL статьи: https://resources.today/PDF/14ITOR422.pdf

DOI: 10.15862/14ITOR422 (https://doi.org/10.15862/14ITOR422)

Ссылка для цитирования этой статьи:
Рудзейт, О. Ю. Оценка пассивных методик тестирования сетей в информационных системах предприятия / О. Ю. Рудзейт, Ю. В. Добржинский, В. Е. Жигульский // Отходы и ресурсы. — 2022. — Т. 9. — № 4. — URL: https://resources.today/PDF/14ITOR422.pdf DOI: 10.15862/14ITOR422

For citation:
Rudzeyt O.U., Dobrzhinskii U.V., Zhigulskiy V.E. Evaluation of passive network testing techniques in enterprise information systems. *Russian Journal of Resources, Conservation and Recycling*. 2022; 9(4): 14ITOR422. Available at: https://resources.today/PDF/14ITOR422.pdf. (In Russ., abstract in Eng.) DOI: 10.15862/14ITOR422

Рудзейт Олег Юрьевич
ФГАОУ ВО «Дальневосточный федеральный университет», Владивосток, Россия
Департамент информационной безопасности
Аспирант группы «Информатика и вычислительная техника»
E-mail: rudzeyt18@mail.ru

Добржинский Юрий Вячеславович
ФГАОУ ВО «Дальневосточный федеральный университет», Владивосток, Россия
Департамент информационной безопасности
Старший преподаватель, профессор
Кандидат технических наук
E-mail: dobrzhinskii.yv@dvfu.ru

Жигульский Владислав Евгеньевич
ФГАОУ ВО «Национальный исследовательский университет ИТМО», Санкт-Петербург, Россия
Аспирант факультета «Программной инженерии и компьютерной техники»
E-mail: upachko@gmail.com

Оценка пассивных методик тестирования сетей в информационных системах предприятия

Аннотация. На данный момент в современных информационных системах широкое распространение получило использование серверных устройств, web-приложений, маршрутизаторов, коммутаторов и т. д. Данные технологии обладают достаточно важными достоинствами в виде простоты использования, простого и удобного интерфейса, даже если их работа осуществляется через использование командной строки, возможности удаленной работы через сеть Интернет, а также технологий быстрого развертывания. Достаточно часто современные технологии имеют и большое число проблем, связанных с обеспечением информационной безопасности, ведь разработка, тестирование и налаживание протоколов передачи данных между устройствами, формирование архитектуры сети предприятия очень часто выполняется в сжатые сроки, а ресурсы компании становятся доступными через Интернет для пользователей как самой компании и клиентов, так и для злоумышленников. Уязвимости различной степени позволяют третьим лицам осуществить похищение корпоративной информации, проводить несанкционированные изменения данных, нарушать доступность приложений предприятия, вызывать проблемы типа «Отказ в обслуживании». В настоящее время проблема обеспечения безопасности инфокоммуникационных технологий весьма актуальна, так, согласно, более 60% от всех обнаруживаемых уязвимостей относятся к

приложениям, использующих доступ во внешнюю сеть. А более чем 70% компаний имеют критически важные риски эксплуатации уязвимостей при вторжении из внешнего периметра сети. Одним из широко распространенных методов обеспечения безопасности сетевых устройств является обнаружение уязвимостей с целью последующего их устранения. В данной работе рассмотрены современные методы и методики пассивного обнаружения уязвимостей в сетевых системах и проведен анализ их возможностей.

Ключевые слова: система; уязвимость; протокол; данные; оценка; злоумышленник; сеть

Методы пассивного анализа

Методы пассивного анализа включают в себя сбор и анализ текущего сетевого трафика или статистики трафика в определенной точке сети — например, в сетевом интерфейсе сервера приложений (рис. 1). Пассивный мониторинг не требует участия или даже осведомленности другого сайта в сети. В простейшем случае пассивный мониторинг может быть ничем иным, как периодическим сбором статистики данных о сетевых портах, например, номеров байт и пакетов при передаче и приеме [1]. Он также включает в себя захват части или всего трафика, проходящего через порты, для подробного анализа протоколов сигнализации, использования приложений или получения информации о максимальной пропускной способности [2].

Пассивные методы идеально подходят для углубленного анализа трафика и протоколов, особенно в сценариях уже произошедших событий. Данные методы также хорошо подходят для получения более подробной информации о качестве обслуживания клиентов (QoE) [3].

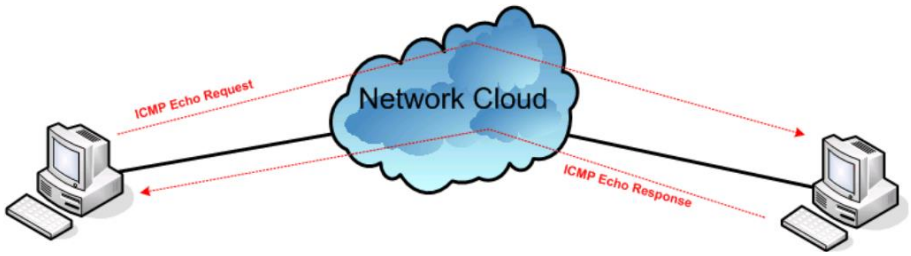

Рисунок 1. *Схема пассивного анализа сети*[1]

Активный мониторинг передает зонды в сеть для сбора измерений между по меньшей мере двумя конечными точками в сети. Активные системы измерения имеют дело с такими показателями, как[2]:

- доступность;
- маршруты;
- задержка пакетов;
- переупорядочение пакетов;
- потеря пакетов;

[1] Обзор методов анализа и мониторинга сетевого трафика [Электронный ресурс] / Режим доступа: http://it-bloknot.ru/?q=content/обзор-методов-анализа-и-мониторинга-сетевого-трафика.

[2] Бройдо, В.Л. Вычислительные системы, сети и телекоммуникации / В.Л. Бройдо. — М.: СПб: Питер, 2017. — 704 с.

- дрожание при поступлении пакетов;
- измерения пропускной способности (пропускная способность, достижимая пропускная способность).

Примерами основных активных инструментов измерения являются часто используемые инструменты, такие как ping, который измеряет задержку и потерю пакетов, и traceroute, который помогает определить топологию сети [4]. Они оба отправляют ICMP-пакеты (зонды) на назначенный хост и ожидают, пока хост ответит отправителю. В сценариях пассивных методов объект отвечает на запросы в результате регулярной работы. В обоих случаях будет получена информация об используемых портах, открытых соединениях и их типах, информация о временных отрезках, к которым создается представление о характеристиках работающей сети [5]. Пассивный методы анализа в отличие от активного мониторинга не увеличивают трафик в сети и не изменяют его. Кроме того, в отличие от активных методов, пассивный мониторинг собирает информацию только об одной точке в сети, а не между двумя конечными точками [6]. Пассивный метод позволяет делать то, что невозможно воссоздать с помощью активного метода: возможность мониторинга за сетью с точки зрения пользователя и изучать поведение приложений во время ежедневных рабочих операций клиента. Пассивные методы не генерируют сообщения от систем опознавания атак и логи записей в узлах и серверах при мониторинге, уменьшая аналитическую нагрузку. В некоторых случаях метод пассивного анализа может обнаружить наличие брандмауэров, маршрутизаторов и коммутаторов и охарактеризовать хосты, стоящие за ними[3].

Несмотря на преимущества пассивных методов анализа трафика, они имеют и недостатки. Для выполнения пассивного анализа необходимо вставить аппаратный или программный датчик в исследуемую область. Датчики должны быть размещены в топологии сети таким образом, чтобы через них проходил полезный трафик. Инструменты для методов пассивного анализа гораздо менее развиты, чем традиционные методы активного анализа, поскольку они требуют значительных усилий от аналитика для размещения датчиков, сбора данных и анализа результата. В некоторых случаях доступны не все области сети, что может ограничить возможность пассивного мониторинга трафика во всей среде ОТ[4].

В настоящее время не существует стандартизированных методов мониторинга сети ИС, поэтому в конкретных ситуациях алгоритмы действий могут значительно различаться.

Стандартная методология включает в себя:

- изучение первоначальных данных относительно изучаемой системы;
- оценка рисков, связанных с проведением тестов сети предприятия на уязвимости;
- исследование средств и политик безопасности, изучение документации для обеспечения безопасной деятельности внутри системы предприятия и оценка соответствия документации требованиям нормативно — правовых норм;
- анализ файлов конфигурации маршрутизаторов, коммутаторов и прокси-серверов, осуществляющих взаимодействия между различными частями корпоративной сети, DNS-серверов и других критически важных элементов коммуникационной структуры предприятия;

[3] Смирнова Е.В. Технологии современных сетей Ethernet. Методы коммутации и управления потоками данных / Е.В. Смирнова. — М.: БХВ-Петербург, 2017. — 480 с.

[4] Чипига, А.Ф. Информационная безопасность автоматизированных систем / А.Ф. Чипига. — М.: Гелиос АРВ, 2017. — 336 с. Учебное пособие.

- сканирование адресов внешней локальной сети из вне;
- сканирование ресурсов локальной сети изнутри предприятия;
- анализ конфигурации серверов и рабочих станций с помощью специализированного ПО [7].

Данная методология исследования сети предполагает использование активного, пассивного и комбинированного подходов тестирования системы защиты.

Пассивное тестирование содержит анализ конфигурации ОС и приложений по шаблонам, используя списки проверки [8].

Во время проведения анализа и оценки средств защиты внешнего периметра ЛВС компании и управления взаимосвязью между различными частями сети особое внимание уделяется следующим аспектам:

- настройка правил разграничения и экранирования доступа на маршрутизаторах;
- создание настроек аутентификации пользователей;
- конфигурирование параметров журнала регистрации событий;
- использование методов сокрытия топологии защищаемой сети, включающих в себя NAT и маскарадинг;
- настройка методов оповещения о вторжении в сеть и реагирования на внештатные события;
- работоспособность инструментов контроля целостности;
- поддержка актуальных версий используемого ПО и проверка наличия установленных пакетов программных коррекций.

Традиционно используются два основных метода тестирования:

1. Тестирование по методу «черного ящика».
2. Тестирование по методу «белого ящика».

Метод «черного ящика» — это **метод тестирования** программного обеспечения, при котором функциональные возможности программных приложений тестируются без знания внутренней структуры кода, деталей реализации и внутренних путей. Метод "черного ящика" в основном фокусируется на вводе и выводе программных приложений и полностью основано на требованиях и спецификациях к программному обеспечению. Это также известно как поведенческое тестирование. Основными средствами проверки в данном случае являются сетевые сканеры, располагающие базами данных уязвимостей, которые дополняются различными компаниями.

Метод «белого ящика» — это **метод тестирования**, при котором внутренняя структура, дизайн и код программного обеспечения не скрыт от тестировщика [9].

Сетевые сканеры — это наиболее доступные и широко используемые средствами анализа защищенности. Основной принцип их работы заключается в эмуляции действий потенциального злоумышленника по осуществлению сетевого вторжения в систему.

Смысл сканирования IP-сети заключается в том, чтобы получить представление о следующих ее элементах:

- типах сообщений ICMP, генерирующих ответы от целевых хостов;

- доступных сетевых службах протоколов передачи данных TCP и UDP, работающих на предполагаемых целевых хостах;
- операционных платформах целевых хостов и их конфигурации;
- определении поверхности атак и области уязвимости в реализациях стека IP-адресов целевого хоста (включая предсказуемость порядкового номера для подмены TCP и перехвата сеанса);
- настройки систем фильтрации трафика и политик безопасности (включая брандмауэры, пограничные маршрутизаторы, коммутаторы и механизмы IDS/IPS) [10].

Выполнение как задач сканирования сети, так и задач разведки позволяет получить четкое представление о топологии сети и ее функциях безопасности.

Возможности сканера по анализу уязвимостей ограничены информацией, которую могут предоставить ему доступные сетевые сервисы [11].

Принцип работы сканера заключен в моделировании действий злоумышленника, производящего анализ сети при помощи стандартных сетевых утилит. При этом используется база данных известных уязвимостей сетевых сервисов и протоколов и ОС для осуществления удаленных атак на системные ресурсы, а также осуществляется документирование удачных попыток.

Существует два основных механизма, при помощи которых сканер безопасности проверяет наличие уязвимости — сканирование и зондирование [12].

Сканирование — средство пассивного анализа, при помощи которого утилиты пытаются определить наличие уязвимости по косвенным признакам. Сканер уязвимостей запускается с конечной точки пользователя, проверяющего рассматриваемую поверхность атаки. Процедура сканирования портов на примере протокола TCP изображена на рисунке 2, составленный автором данной статьи. Программное обеспечение сравнивает сведения о целевой поверхности атаки с базой данных информации об известных слабых местах в безопасности, в службах и портах, аномалиях в построении пакетов и возможных путях к уязвимым программам или сценариям эксплуатаций уязвимости. Программное обеспечение сканера пытается использовать каждую обнаруженную уязвимость [13].

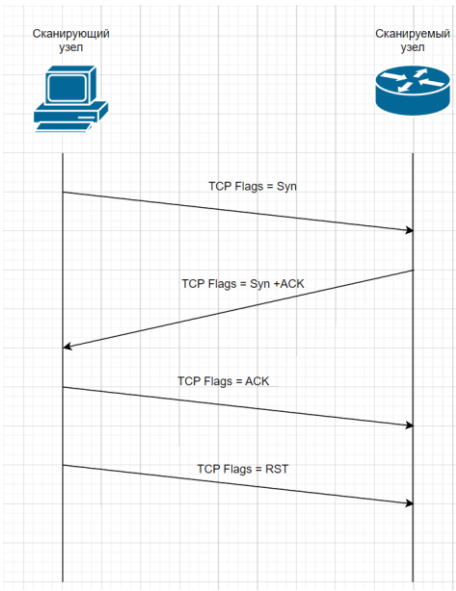

Рисунок 2. *Схема осуществления сканирования портов*

Запуск сканирования уязвимостей может представлять свои собственные риски, поскольку данные утилиты могут повлиять на исполнение запущенного кода целевой машины. В результате сканирование может вызвать такие проблемы, как ошибки и перезагрузки, что снижает производительность.

Зондирование является механизмом активного анализа сети, который позволяет убедиться в фактическом наличии уязвимости на анализируемом узле сетевой инфраструктуры. Зондирование выполняется путем имитации атаки, эксплуатирующей проверяемую уязвимость. Этот метод более медленный, чем сканирование сети, но более точный. Согласно данным компании Cisco этот процесс использует информацию, предоставляемую в процессе сканирования, чтобы совершить детальный анализ каждого сетевого узла. Этот процесс также использует известные методы реализации атак для того, чтобы полностью подтвердить предполагаемые уязвимости, совершить сопоставление с имеющимися базами данных уязвимостей и потенциально обнаружить другие, которые не могут быть обнаружены пассивными методами [14].

Методы и исследования

Для лучшего понимания пассивных методов анализа представлен пример захвата с использованием программного обеспечения Ethereal. Ethereal предлагает множество инструментов, включая улучшенные возможности фильтрации и быструю сортировку собранных пакетов относительно любых заданных полей данных (рис. 3). Поскольку большинство используемых служб в инфраструктуре служб связаны с определенными портами, то данные порты назначаются службой IANA (Internet Assigned Numbers Authority) и описаны в RFC (Request for Comments) для стандартных TCP/IP служб и протоколов [15; 16]. Для предотвращения сокрытия трафика в сети во время вторжения могут быть исследованы малоизвестные или используемые злоумышленниками порты могут с использованием Internet Storm Center, предоставленного SANS Institute.

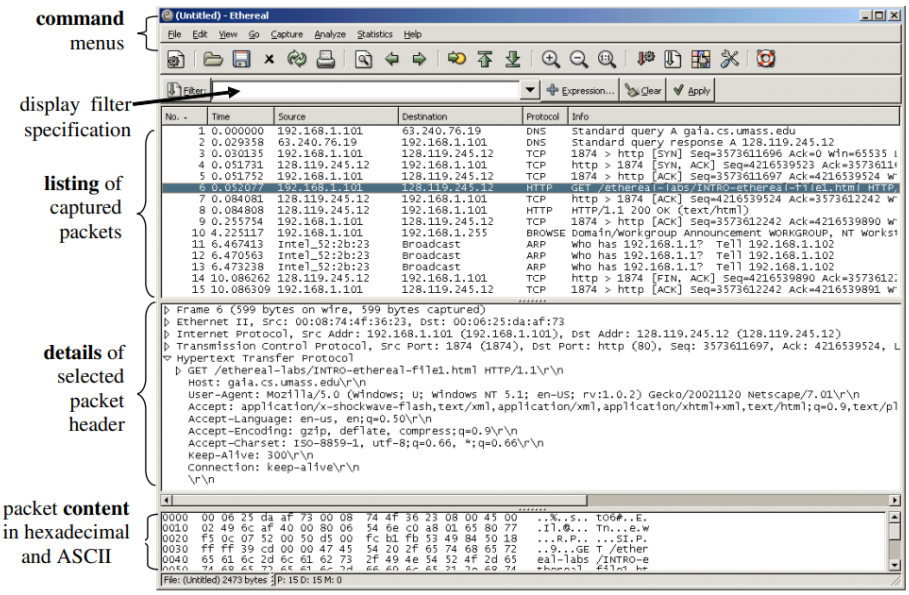

Рисунок 3. *Перехват трафика веб сессии, используя Ethereal*[5]

[5] Ethereal 0.10.14: Сетевые анализаторы и анализаторы протоколов сети. Разработка и внедрение технологических проектов [Электронный ресурс] / Режим доступа: www.ordinarytech.ru http://www.ordinarytech.ru/erdets-278-1.html.

В данной программе можно составить правило разделения трафика клиентов и серверов при пассивном мониторинге. Определяя целевой Web-сервер, может быть определен источник TCP-запроса на 80-ый порт, исходящий из сети, т. к. серверы отправляют пакеты на порт с определенным номером, связанный со соответствующей службой. Для демонстрации работы программного обеспечения Ethereal был проанализирован трафик сети и произведена сортировка трафика по портам TCP-запроса. В данном случае использование ПО не инициировало дополнительного трафика в исследуемой сети.

Работа TCP/IP fingerprinting в пассивном режиме имеет сходство с работой в активном режиме, что представляет возможность выдвинуть некоторые гипотезы об операционных системах целевых узлов, используя системы перехвата трафика. Этот метод основан на том, что различные операционные системы имеют разные реализации стека TCP/IP. Для определения ОС конечного узла требуется сравнивать четыре параметра: TTL, размер окна, DF и TOS. Программа p0f 2.0 представляет возможность получить дополнительные параметры, позволяя проводить более точные тесты для определения операционных систем конечной точки в пассивном режиме. Используя интерфейс eth0 (-i eth0) в неразборчивом режиме (-p), сохраним результат работы программы результаты в файл p0f.log с помощью команды: p0f -i eth0 -p -o /tmp/p0f.log на рисунке 4, составленный автором. Данные действия требуется производить с трафиков, проанализированным через приложение Ethereal.

```
root@WebWare:~# p0f -i eth0 -p -o /tmp/p0f.log
--- p0f 3.07b by Michal Zalewski <lcamtuf@coredump.cx> ---

[+] Closed 1 file descriptor.
[+] Loaded 320 signatures from 'p0f.fp'.
[+] Intercepting traffic on interface 'eth0'.
[+] Default packet filtering configured [+VLAN].
[+] Log file '/tmp/p0f.log' opened for writing.
[+] Entered main event loop.

.-[ 192.168.1.34/63369 -> 211.36.85.142/80 (syn) ]-
|
| client   = 192.168.1.34/63369
| os       = Windows NT kernel 5.x
| dist     = 0
| params   = generic
| raw_sig  = 4:128+0:0:1460:65535,8:mss,nop,ws,nop,nop,sok:df,id+:0
|
`----
```

Рисунок 4. *Отображение информации о тестируемом сервере в интерфейсе p0f*

Данный пример демонстрирует основные принципы пассивного анализа сети. Аналогичные приемы и методы используются для описания различных параметров трафика (процент запросов TCP, UDP, ARP и др.), отслеживания состояния соединений, отслеживания пропускной способности, числа и размера передаваемых пакетов, их заголовков, маршрутов движения и т. д.

Потенциальные возможности использования пассивного анализа

Преимущество пассивного анализа заключается в том, что не требуется использовать каких-либо усилий для сбора данных — данные собираются во время обычной эксплуатации сети. Пассивные методы анализа трафика не увеличивают его объем в сети, что позволяет тестирующему оставаться анонимным при сборе сетевых данных.

Осведомленность о ситуации.

Пассивные методы мониторинга могут собрать потенциально большое количество информации об инфраструктуре предприятия и о том, как она работает в нормальной ситуации. Без четкого понимания инфраструктуры сети очень сложно разработать эффективную политику в области превентивных мер защиты.

Политика форсирования.

Пассивный анализ позволяет на любом этапе эксплуатации сети выявить неразрешенные службы и другие аномальные поведения пользователей в сети практически мгновенно. Сбор пакетов с помощью различных сканеров будет определять наличие передачи нелигитимных потоков данных в peer-to-peer (P2P) сетях, игровой активности и другие источники несанкционированного использования сети. Самый простой способ отследить нежелательный трафик — использовать сканеры с фильтром пакетов на определенный IP-адрес внутренней сети, а затем воспользоваться сортировкой по определенным портам протоколов TCP или UDP.

Определение утечки информации.

Пассивный анализ помогает выявить уязвимости в системе безопасности, не обнаруженные внутри периметра. Хорошим примером может быть Wualess BackDoor, о котором сообщила компания Symantec. Эта угроза открывала BackDoor и пыталась установить связь с IRC-сервером через TCP-порт 5202 в домене dnz.3322.org, используя канал "# Phantom". Существует три критерия, по которым возможно определить данную угрозу: присутствие TCP 5202, оценка IRC-протокола и исходящего соединения на определенный домен.

Реакция на инцидент.

Пассивный анализ является бесценным и быстрым инструментом для реагирования на инцидент. Мониторинг сети в режиме реального времени позволяет определять зону компрометации, области вторжения в систему и, возможно, отследить как был осуществлен нежелательный доступ в систему.

Сравнение сканеров уязвимостей сети

Российский рынок сканеров огромен, и каждый производитель пытается привлечь на свою сторону все больше потребителей, создавая широкий круг возможностей. В данной части статьи представлены основные утилиты, используемые для обнаружения уязвимостей.

GFI LanGuard.

GFI LanGuard — программное средство, которое осуществляет централизованную проверку на уязвимости всей сети. Преимуществом сканера является обнаружение открытых портов, небезопасных конфигураций сети и ПО, которое не соответствует регламент информационной безопасности предприятия. Средство производит проверку обновлений и патчей не только ОС различного рода (настольных, мобильных, виртуальных), но и установленного ПО.

Сканер сетевой безопасности позволяет настроить проверку на автономный режим работы. В автономном режиме ПО будет осуществлять исправления в системе, которые заранее были одобрены администратором.

Nessus.

Проект Nessus был запущен еще в 1998 году. Согласно статистике данное ПО используют более 17 % компаний. Представленное средство имеет регулярно обновляемую базу уязвимостей. Ключевой особенностью использования приложения является использование плагинов. Аддоны распределяются на 42 различных типа. Например, чтобы провести тест на проникновение, можно активировать как плагины, заданные пользователем отдельно, так и совместно все плагины определенного типа, к примеру, для проведения всех локальных проверок системы под управлением ОС Ubuntu или Unix — подобных систем.

XSpider.

Компания Positive Technologies разработала сканер XSpider, который, может превентивно выявить уязвимости, еще не включенные в базы данных различных компаний, специализирующихся на информационной безопасности. Ключевой особенностью этого сканера является возможность обнаружения максимального количества угроз в сети еще до того, как их обнаружат злоумышленники. При этом сканер работает удаленно, не требуя установки дополнительного ПО.

Стоит отметить, что XSpider сертифицирован Минобороны и ФСТЭК России [17].

QualysGuard.

Многофункциональный сканер уязвимостей. Средство предоставляет обширные отчеты, которые включают:

- оценку уровня уязвимостей;
- анализ времени, которое потребуется для устранения найденных уязвимостей в системе;
- анализ воздействия обнаруженных уязвимостей на осуществление корпоративных дел;

В данном разделе были приведены основные используемые сканеры от различных разработчиков. Для полной оценки на рисунке 6 представлена статистика использования сканеров уязвимостей различных компаний.

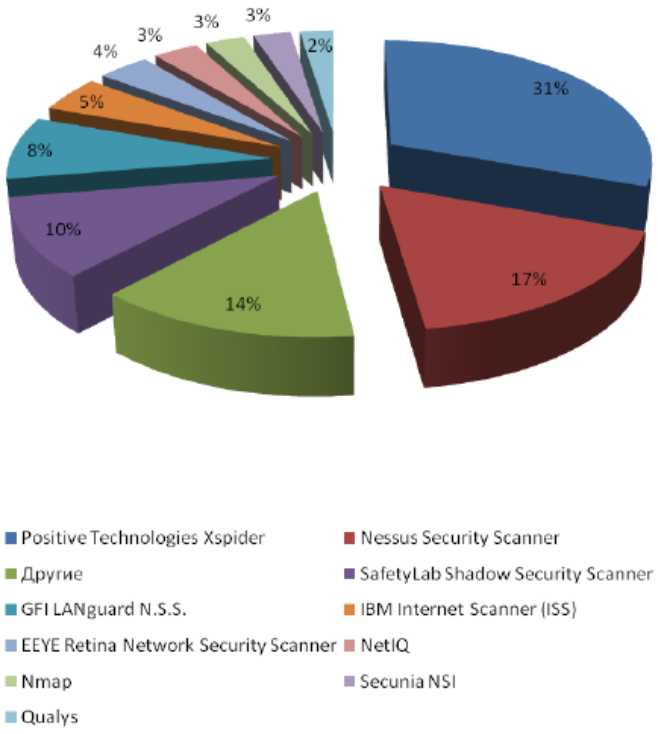

Рисунок 5. *Статистика использования сканеров уязвимостей*[6]

[6] Сравнительный анализ сканеров безопасности. Часть 1: тест на проникновение [Электронный ресурс] / Режим доступа: https://www.securitylab.ru/analytics/365241.php.

Заключение

В статье, представлены результаты работы по оценке инфраструктуры предприятия на основе методов пассивного анализа сети, их особенностей, достоинств, недостатков и рамок применимости.

Основным результатом работы является разработка подхода к анализу защищенности компьютерных сетей, предназначенного для использования как на этапах их проектирования, так и эксплуатации. Подход базируется на сканировании поверхности атак предприятия и определения уязвимых узлов для дальнейшего сокрытия топологии сети и устранения угроз путем получения полной информации о сети предприятия. Сценарии сканирования отражают возможные распределенные сценарии атак, которые учитывают конфигурацию сети, реализуемые политики безопасности, а также местоположения, целей, уровня знаний и стратегий злоумышленника. Основными компонентами методик пассивного анализа защищенности периметра сети является формирование внутреннего представления анализируемой сети и политики безопасности.

Рекомендации, полученные в результате сканирования инфраструктуры позволяют выработать стратегию по устранению выявленных узких мест и усилению защищенности системы. На имеющихся рекомендаций пользователь вносит изменения в конфигурацию реальной сети или в ее модель, а затем, если необходимо, повторяет процесс анализа уязвимостей и оценки уровня защищенности. Таким образом, обеспечивается требуемый уровень защищенности компьютерной сети на всех этапах ее жизненного цикла.

ЛИТЕРАТУРА

1. P. Manzanares-Lopez, J. P. Muñoz-Gea and J. Malgosa-Sanahuja, "Passive In-Band Network Telemetry Systems: The Potential of Programmable Data Plane on Network-Wide Telemetry", in IEEE Access, vol. 9, pp. 20391-20409, 2021, doi: 10.1109/ACCESS.2021.3055462.
2. Скотт, Хогдал Дж. Анализ и диагностика компьютерных сетей / Скотт Хогдал Дж. — М.: ЛОРИ, 2019. — 180 с.
3. Таненбаум, Э. Компьютерные сети / Э. Таненбаум. — СПб.: Питер, 2019. — 960 с.
4. McLaughlin S., Konstantinou C., Wang X., Davi L., Sadeghi A.R., Maniatakos M., Karri R. The Cybersecurity Landscape in Industrial Control Systems. Proc. IEEE, 2016, no. 104, pp. 1039–1057. doi: 10.1109/JPROC.2015.2512235.
5. Малыгин И.В. Широкополосные системы связи / И.В. Малыгин- М.: LAP Lambert Academic Publishing, 2018. — 200 с.
6. S. Samtani, S. Yu, H. Zhu, M. Patton, and H. Chen. Identifying SCADA vulnerabilities using passive and active vulnerability assessment techniques. In Proceedings of the 14th IEEE International Conference on Intelligence and Security Informatics, ISI 2015, pp. 25–30, USA, September 2016.
7. Бузов, Г.А. Защита информации ограниченного доступа от утечки по техническим каналам / Г.А. Бузов. — М.: ГЛТ, 2016. — 586 с.
8. C. Wu, T. Wen and Y. Zhang, "A revised CVSS-based system to improve the dispersion of vulnerability risk scores", Sci. China Inf. Sci., vol. 62, pp. 39102.

9. M. Parvez, P. Zavarsky and N. Khoury, "Analysis of effectiveness of black-box web application scanners in detection of stored SQL injection and stored XSS vulnerabilities", 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST), London, 2015, pp. 186–191. doi: 10.1109/ICITST.2015.7412085.
10. Ибе, О. Компьютерные сети и службы удаленного доступа / О. Ибе. — М.: ДМК Пресс, 2017. — 334 с.
11. A. Cook, H. Janicke, R. Smith, and L. Maglaras, “The industrial control system cyber defence triage process”, Computers & Security, vol. 70, pp. 467–481, 2017.
12. Шалак В.И. Логический анализ сети Интернет / В.И. Шалак. — Москва: Машиностроение, 2016. — 100 с.
13. Эд. Уилсон. Мониторинг и анализ сетей / Уилсон, Эд. — М.: Лори, 2021. — 350 с.
14. V.R. Kebande, I. Kigwana, H.S. Venter, N.M. Karie and R.D. Wario, "CVSS Metric-Based Analysis, Classification and Assessment of Computer Network Threats and Vulnerabilities", 2018 International Conference on Advances in Big Data, Computing and Data Communication Systems (icABCD), 2018, pp. 1–10, doi: 10.1109/ICABCD.2018.8465420.
15. Шелухин О.И. Обнаружение вторжений в компьютерные сети (сетевые аномалии) / О.И. Шелухин. — М.: ГЛТ, 2013. — 220 с.
16. Баринов А.В. Безопасность сетевой инфраструктуры предприятия / А.В. Баринов. — М.: LAP Lambert Academic Publishing, 2016. — 331 с.
17. М.А. Борисов Основы организационно-правовой защиты информации / М.А. Борисов. — Москва: РГГУ, 2016. — 122 с.

Rudzeyt Oleg Urievich
Far Eastern Federal University, Vladivostok, Russia
Department of Information Security
E-mail: rudzeyt18@mail.ru

Dobrzhinskii Uriy Vyacheslavovich
Far Eastern Federal University, Vladivostok, Russia
Department of Information Security
E-mail: dobrzhinskii.yv@dvfu.ru

Zhigulskiy Vladislav Evgenievich
ITMO University, Saint-Petersburg, Russia
E-mail: upachko@gmail.com

Evaluation of passive network testing techniques in enterprise information systems

Abstract. At the moment, the use of server devices, web applications, routers, switches, etc. has become widespread in modern information systems. These technologies have quite important advantages in the form of ease of use, a simple and convenient interface, even if their work is carried out through the use of the command line, the possibility of remote work via the Internet, as well as technologies for fast deployment. Quite often, modern technologies also have a large number of problems related to information security, because the development, testing and establishment of data transmission protocols between devices, the formation of the enterprise network architecture is very often carried out in a short time, and the company's resources become available via the Internet for users of both the company and customers, and for intruders. Vulnerabilities of varying degrees allow third parties to steal corporate information, carry out unauthorized data changes, disrupt the availability of enterprise applications, and cause Denial-of-Service problems. Currently, the problem of ensuring the security of infocommunication technologies is very relevant, so, according to, more than 60 % of all detected vulnerabilities relate to applications that use access to an external network. And more than 70 % of companies have critical risks of exploiting vulnerabilities in case of intrusion from the external perimeter of the network. One of the widespread methods of ensuring the security of network devices is the detection of vulnerabilities in order to eliminate them later. In this paper, modern methods and techniques of passive vulnerability detection in network systems are considered and their capabilities are analyzed.

Keywords: system; vulnerability; protocol; data; evaluation; attacker; network