УДК 004.7
2.3.1. Системный анализ, управление и обработка информации




Д.И. Воронин, Д.В. Кочкин
Вологодский государственный университет

ОБНАРУЖЕНИЕ КОМПЬЮТЕРНЫХ АТАК НА ПРЕДПРИЯТИИ И ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В настоящее время в сфере информационной безопасности наблюдается значительный дефицит высококвалифицированных специалистов. Связано это, с одной стороны, с быстрыми темпами развития информационных технологий и искусственного интеллекта, с другой – с усовершенствованием и появлением новых методов проведения компьютерных атак. В статье предложен практико-ориентированный метод для подготовки специалистов по информационной безопасности. Метод позволяет использовать современные инструменты для анализа трафика при проведении компьютерных атак, а также имеет потенциал для дальнейшего применения при подготовке профильных специалистов.

Информационная безопасность, компьютерные сети, кибератаки, пентест, анализ трафика.

Задача обнаружения и устранения угроз безопасности информационной системы не является тривиальной. Современные корпоративные сети предприятий состоят из множества различных устройств и приложений, для обнаружения угроз необходимо иметь четкое представление о принципах работы данных систем, используемых протоколах, средствах защиты и многом другом [1, 2].

Информационную безопасность можно разделить на два основных направления: административная информационная безопасность; техническая информационная безопасность. Если для специалистов административной информационной безопасности знания технических деталей не являются основополагающими, то для технических специалистов понимание принципов работы компьютерных сетей, основных сетевых узлов и способов проведения компьютерных атак являются критически значимыми. Для получения и закрепления таких знаний целесообразно применять практико-ориентированный подход.

При проведении компьютерных атак существуют возможности удаления следов компрометации на целевой машине, сетевом оборудовании, серверах, а также в системах и оборудовании по защите информации. При использовании данного метода будет проводиться захват и анализ сетевого трафика, что позволяет увидеть все то, что происходит в компьютерной сети.

Для понимания принципов обмена сетевым трафиком не обойтись без изучения эталонной модели OSI (Open Systems Interconnection – модель взаимодействия открытых систем), которая описывает передачу данных в компьютерных сетях. Модель OSI состоит из семи уровней: физический, канальный, сетевой, транспортный, сеансовый, представления, прикладной [3, 4].

Многие разработчики считают модель OSI излишне сложной в плане классификации протоколов, так как современные устройства зачастую работают сразу на нескольких уровнях иерархической модели. В противовес модели OSI была разработана модель DoD (Department of Defense – модель сетевого взаимодействия, разработанная Министерством обороны США), состоящая из четырех уровней: сетевого доступа, межсетевого, транспортного, приложений.

В предложенном методе подготовки специалистов используется виртуальная лаборатория для изучения компьютерных атак. Данная виртуальная лаборатория состоит из следующих инструментов:

- персональный компьютер с установленной операционной системой (ОС) Linux/Windows;
- программное обеспечение Oracle VirtualBox;
- образ виртуальной машины Kali Linux;
- образы целевых виртуальных машин;
- программное обеспечение Wireshark.

На рисунке 1 изображена структурная схема виртуальной лаборатории для изучения компьютерных атак.

Виртуальная лаборатория состоит из 4 элементов:

- межсетевой экран для организации передачи трафика и настройки ACL (Access Control List – «список управления доступом»);
- коммутатор со span-портом для организации передачи трафика в компьютерной сети и зеркалирования сетевого трафика;
- ноутбук с ОС Kali Linux для пентестера;
- ноутбук с ОС Windows и Oracle VirtualBox для системного администратора (создание и администрирование целевых машин, настройка коммутатора);
- сервер с ОС Linux и Wireshark для администратора ИБ (захват и анализ зеркалированного сетевого трафика с коммутатора).

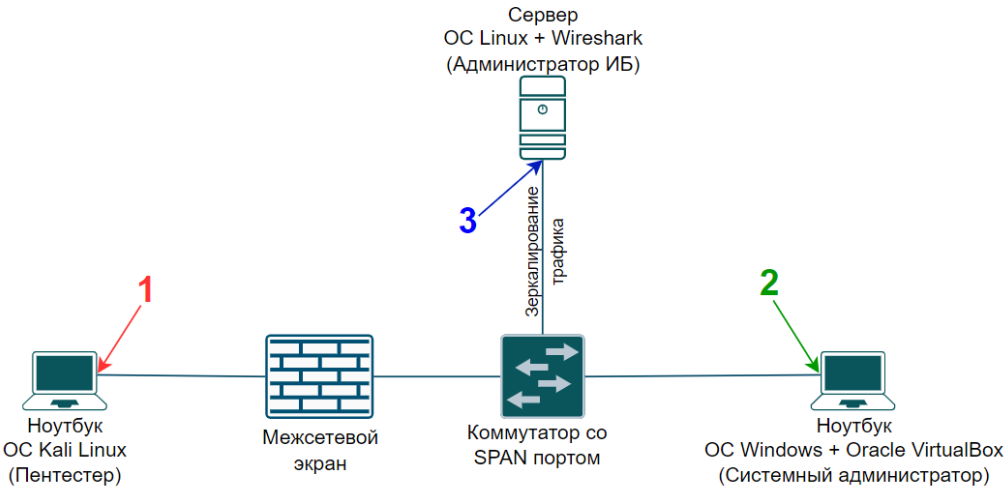


Рис. 1. Структурная схема виртуальной лаборатории

Определение точки захвата сетевого трафика является одним из определяющих факторов для его эффективного анализа, который даст полное понимание происходящего в компьютерной сети. Для сравнения в виртуальной лаборатории предложено осуществлять захват трафика в трех точках, как показано на рисунке 1: с ноутбука пентестера, с ноутбука системного администратора, с сервера администратора ИБ для зеркалированного трафика с коммутатора.

В процессе подготовки шаг за шагом изучаются множество вариантов использования различных комбинаций целевых машин, проводится захват и анализ сетевого трафика, чтобы получить максимально полное представление о пентесте. Для этого выполняются следующие действия:

- сканирование на обнаружение хоста;
- сканирование портов;
- определение отпечатков (fingerprints) ОС;
- идентификация служб и определение версии;
- выполнение цепочки команд;
- автоматизация с помощью bash-скриптов;
- перечисление служб (HTTP, SNMP, FTP, SMB, SQL);
- получение ценной информации из исходного кода страницы;
- фаззинг (методика тестирования программного обеспечения);
- выполнение локального файла на стороне сервера (local file inclusion);
- обход каталога (Directory traversal);
- внедрение команды ОС;
- обход фильтрации веб-доступа с помощью агента пользователя;
- удаленное выполнение кода;
- обход ограничений на загрузку файлов;
- перечисление и атака на WordPass;
- брутфорс онлайн-форм входа;
- шифрование полезных нагрузок;
- исследование уязвимостей (поисковые системы, использование эксплойтов для веб-сайтов, SearchSploit, Metasploit);
- получение Reverse Shell;
- использование Netcat для обратного подключения и для передачи файлов;
- Reverse Shell на усиленном Netcat с FIFO и перенаправлением ввода/вывода;
- устранение проблем, вызванных ограниченными возможностями обратного подключения (Reverse Shell), и апгрейд до терминала TTY;
- обход локальной системы;
- использование двоичных файлов SUID;
- исследование команд, запускаемых от имени суперпользователя с применением команд sudo;
- эксплуатация ядра;
- эксплуатация неавторизованной службы TFTP;
- эксплуатация с использованием Metasploit;
- обратное подключение с использованием бэкдора на PHP;
- взлом пароля;
- фаззинг входных параметров для проверки уязвимостей;
- повышение привилегий и получение прав суперпользователя (root).

Для изучения перечисленных действий будут применяться инструменты, доступные в Kali Linux. Это позволит получить знания и практические навыки для понимания процесса пентеста.

Для захвата и анализа сетевого трафика будет использоваться программное обеспечение Wireshark, также доступное в Kali Linux.

На рисунке 2 показана упрощенная структура пентеста (алгоритм тестирования на проникновение) [5]. Понимание основ и этапов пентеста позволяет определить эффективные точки для захвата сетевого трафика в компьютерной сети и возможности его дальнейшего анализа [6].



Рис. 2. Структура пентеста

Алгоритм тестирования состоит из следующих этапов:

Этап 1: предварительные действия.

Этап 2: планирование.

Этап 3: сбор информации.

Этап 4: разведка.

Этап 5: составление перечня служб.

Этап 6: исследование уязвимостей.

Этап 7: эксплуатация.

Этап 8: отчетность.

Предложенный в статье метод дает возможность изучения этапов пентеста и анализа сетевого трафика при подготовке специалистов в области информационной безопасности с применением практико-ориентированного подхода. Также метод позволяет извлекать индикаторы компрометации из сетевого трафика – объектов или активности, которые с большой долей вероятности указывают на признаки несанкционированного доступа к системе.

Глубокий анализ сетевого трафика предполагает получение достоверной информации о компьютерных атаках и возможности выявления узких мест в инфраструктуре безопасности. На основании полученной информации принимаются решения для быстрой корректировки настроек безопасности компьютерной сети в целом.

Литература

1. Кузнецов, А. В. Информационная безопасность: анализ и оценка угроз, кибер/криптозащита организаций, разработка безопасного ПО / А. В. Кузнецов – Санкт-Петербург : Издательство Наука и Техника, 2025. – 432 с.

2. Бирюков, А. А. Информационная безопасность: защита и нападение. – 3-е изд., перераб. и доп. / А. А. Бирюков – Москва : ДМК Пресс, 2023. – 440 с.

3. Компьютерные сети. В 2 томах. Том 1. Системы передачи данных / Р. Л. Смелянский. – Москва : Издательский центр «Академия», 2011. – 304 с.

4. Компьютерные сети. Учебник для студентов высших учебных заведений. В 2 томах. Том 2. Сети ЭВМ / Р. Л. Смелянский. – Москва : Издательский центр «Академия», 2011. – 240 с.

5. Тестирование на проникновение с Kali Linux : перевод с английского / П. Джоши, Д. Чанда. – Санкт-Петербург : БХВ-Петербург, 2025. – 256 с.

6. Сандерс, К. Анализ пакетов: практическое руководство по использованию Wireshark и tcpdump для решения реальных проблем в локальных сетях : перевод с английского / К. Сандерс. – 3-е изд. – Санкт-Петербург : ООО «Диалектика», 2019 – 448 с.

D.I. Voronin, D.V. Kochkin
Vologda State University

DETECTING COMPUTER ATTACKS AT ENTERPRISE AND ENSURING INFORMATION SECURITY

There is currently a significant shortage of highly qualified specialists in the fields of information security and cybersecurity. On the one hand, this is due to the rapid development of information technology and artificial

intelligence, and on the other, to the improvement and emergence of new methods of conducting computer attacks. This article proposes a practice-oriented method for training information security specialists. This method enables the use of modern tools for traffic analysis during computer attacks and has potential for further application in the training of specialized specialists.

Information security, computer networks, cyberattacks, pentesting, traffic analysis.