

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

МЕТОДИЧЕСКИЕ УКАЗАНИЯ
по выполнению лабораторных работ
по дисциплине «Менеджмент инцидентов кибербезопасности»
для студентов направления подготовки
10.04.01 «Информационная безопасность»
Направленность (профиль)
«Информационная безопасность киберфизических систем»

Ставрополь
2026

Содержание

Лабораторная работа №1-2	3
Лабораторная работа №3-4	12
Лабораторная работа №5-6	37
Лабораторная работа №7-8	44
Лабораторная работа №9-10	56
Лабораторная работа №11-12	62
Лабораторная работа №13-14	69
Лабораторная работа №15-16	78
Лабораторная работа №17-18	83

ВВЕДЕНИЕ

1. Цели и задачи освоения дисциплины:

Целью изучения дисциплины «Менеджмент инцидентов кибербезопасности» является развитие и формирование у студентов профессиональных компетенций, необходимых для решения теоретических и практических задач в сфере управления инцидентами кибербезопасности и обеспечения устойчивого функционирования информационных и киберфизических систем, а также приобретение набора общекультурных и общепрофессиональных компетенций будущего магистра по направлению подготовки 10.04.01 «Информационная безопасность».

Задачи освоения дисциплины «Менеджмент инцидентов кибербезопасности»:

- Сформировать навыки выявления, классификации и оценки инцидентов кибербезопасности;
- Овладеть методологией и инструментами реагирования на инциденты в сфере кибербезопасности;
- совершенствование умений и навыков с учетом специализации профессиональной деятельности;
- повышения профессионального уровня в рамках имеющейся квалификации.

Дисциплина «Менеджмент инцидентов кибербезопасности» (Б1.В.ДВ.02.01) относится к дисциплинам части, формируемой участниками образовательных отношений. Её освоение происходит в 3 семестре.

2. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесённых с планируемыми результатами освоения образовательной программы

Код, формулировка компетенции	Код, формулировка индикатора	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций, индикаторов
ПК-4 Способен оценивать уровень	ИД-1 ПК-4 Демонстрирует способность проводить оценку	Применяет принципы и уровни защищенности

защищенности киберфизических систем и применять решения по обеспечению их информационной безопасности	уровня защищённости киберфизических систем и реализовывать меры по обеспечению их информационной безопасности в соответствии с действующими стандартами и нормативными требованиями	киберфизических систем Оценивает уровень защищенности киберфизических систем и применять решения по обеспечению их информационной безопасности
--	---	---

Лабораторная работа №1-2

Тема: Система управления инцидентами кибербезопасности. Планирование системы управления инцидентами информационной безопасности.

Цель занятия

1. Закрепление теоретических знаний о процессе реагирования на инциденты информационной безопасности.
2. Изучение основных этапов реагирования на инциденты.
3. Изучение методов контроля целостности файлов и использования криптографических контрольных сумм.

Подготовка к занятию

1. Изучить основные понятия реагирования на инциденты информационной безопасности.
2. Повторить принципы: криптографических хеш-функций, контроля целостности файлов, мониторинга событий безопасности.

Учебные вопросы

1. Подготовка инфраструктуры к реагированию на инциденты.
2. Методы обнаружения инцидентов информационной безопасности.
3. Методы сдерживания и локализации инцидентов.
4. Основные теоретические сведения.

Основные теоретические сведения

Основные теоретические сведения изложены в материалах лекций и по данной тематике и рекомендуемой литературе.

Правила работы в лаборатории

К работе в лаборатории допускаются лица, изучившие правила и меры безопасности, сдавшие зачет по ним и усвоившие порядок выполнения практического занятия.

Требования безопасности перед началом работ

- ЗАПРЕЩАЕТСЯ: переодеваться, пользоваться огнем, курить, принимать пищу в лаборатории;

- убедиться в целостности электрических розеток и разъемов. В лаборатории необходимо быть в сменной обуви;
- включение компьютера производить только после получения допуска по выполняемой работе и разрешения преподавателя или лаборанта.

Требования безопасности во время работы

- выполняя практическое занятие, студенты обязаны использовать только вычислительную технику, периферийное оборудование, соединительные кабели, измерительное оборудование и носители информации, непосредственно относящиеся к данному практическому занятию;
- подключение и отключение составляющих вычислительного комплекса производить только при полном снятии напряжения со всех составляющих вычислительного комплекса;
- при обнаружении неисправностей в оборудовании немедленно отключить источники питания и доложить об этом руководителю занятий или лаборанту.

Требования безопасности по окончании работы

- доложить руководителю занятий или лаборанту о завершении работ;
- привести в порядок и сдать рабочее место лаборанту, и доложить руководителю занятий о сдаче.

Аппаратное обеспечение

Класс персональных ЭВМ, электронная доска, проектор.

Программное обеспечение

В комплекте с персональными ЭВМ. Доступ к Интернет. Офисный пакет.

Литература

- 1) Технологии обеспечения безопасности информационных систем: учебное пособие: А. Л. Марухленко, Л. О. Марухленко, М. А. Ефремов [и др.]. – Москва; Берлин: Директ-Медиа, 2021. – 209 с.
- 2) Баланов А. Н. Защита информационных систем. Кибербезопасность: учебное пособие для вузов / А. Н. Баланов. — Санкт-Петербург: Лань, 2024. — 280 с.
- 3) Ховард Рик. Кибербезопасность: главные принципы. — СПб.: Питер, 2024. — 320 с.: ил.
- 4) Kaspersky. Руководство по реагированию на инциденты информационной безопасности [Электронный ресурс]. – Режим доступа: [ссылка](#), свободный. – Дата обращения: 05.04.2026.

Теоретическая часть

Криптографические хеш-функции и контрольные суммы

Контрольная сумма – это результат применения хеш-функции к данным (например, к файлу) и используется для проверки их целостности. Фактически контрольная сумма есть малая репрезентация данных, которую можно быстро пересчитать и сравнить: «значение контрольной суммы – результат применения криптографической хеш-функции к определённому набору данных». Криптографические хеш-функции (MD5, SHA-1, SHA-2 и т.д.) обладают свойствами односторонности и детерминированности, что позволяет надёжно вычислять и затем сверять хеши. При изменении данных контрольная сумма, как правило, меняется, что указывает на нарушение целостности. Например, при передаче файла по сети получатель может сравнить полученный хеш с эталонным.

НМАС и цифровые подписи

НМАС (код аутентификации на основе хеша) сочетает секретный ключ и криптографическую хеш-функцию для обеспечения целостности и аутентичности сообщения. НМАС вычисляет хеш от (секретного ключа + данных), что позволяет обнаружить любые изменения и подтвердить подлинность отправителя, разделяющего секрет с получателем. В отличие от простой контрольной суммы, НМАС защищён ключом и предотвращает подмену сообщения злоумышленником.

Цифровая подпись решает смежную задачу с помощью асимметричной криптографии: она подтверждает и целостность, и авторство документа. В отличие от НМАС (симметричный ключ для отправителя и получателя), в цифровой подписи используются разные ключи: приватный (для создания подписи) и публичный (для проверки). Оба метода используют хеш-функции, но цифровая подпись дополнительно защищает от «отказа от авторства» (non-repudiation). Цифровые подписи применяются для юридически значимых документов, а НМАС – в коммуникациях (протоколы TLS, SSH, SFTP и др.).

Контроль целостности файлов

Для практической проверки неизменности файлов используют специализированные инструменты FIM (File Integrity Monitoring). Например, AIDE (Advanced Intrusion Detection Environment) – открытое ПО, которое сканирует файловую систему по заранее заданным правилам и сохраняет эти сведения в базе данных. AIDE вычисляет хеши (и другие атрибуты) файлов и сравнивает их с предыдущим состоянием: команда `aide --init` создаёт эталонную базу, а `aide --check` выявляет изменения (изменённые файлы, что видно в выводе). К примеру, если `/etc/hosts` будет изменён, AIDE сообщит о расхождении хешей. Аналогичные функции выполняют Tripwire, OSSEC, Samhain и др. По сути, все они используют криптографические хеши файлов и сигнализируют о вмешательстве в файловую систему.

Практическая часть

1. Подготовка системы обнаружения инцидентов

В рамках этапа подготовки к реагированию на инциденты информационной безопасности необходимо обеспечить возможность контроля целостности системных данных. Контроль целостности реализуется путем вычисления и последующего сравнения криптографических контрольных сумм (хеш-значений) файлов.

Ход выполнения:

- 1) Выбрать пять критически важных файлов операционной системы.
 - 2) Определить и применить криптографическую хеш-функцию (например, SHA-256, MD5)
 - 3) Вычислить контрольную сумму файла с использованием стандартных средств операционной системы.
 - 4) Определить назначение файла операционной системы.
- Полученные данные записать в таблицу.

Таблица 1 – Контрольные суммы файлов

Файл	Хэш-функция	Контрольная сумма	Назначение
/etc/shadow	md5	748cdfe653b2b884372ec14d2e094426	Хранение учетных записей пользователей

2. Подготовка системы обнаружения инцидентов

На этапе обнаружения осуществляется выявление признаков возможных инцидентов информационной безопасности на основе анализа событий, происходящих в информационной системе. Обнаружение инцидентов может выполняться с использованием анализа журналов событий, мониторинга сетевой активности, а также специализированных систем обнаружения вторжений.

Ход выполнения:

1) Определить возможные источники событий безопасности в информационной системе (журналы аутентификации, сетевой трафик, системные журналы и др.).

2) Для каждого источника определить тип события, которое может свидетельствовать о потенциальной угрозе безопасности.

3) Указать возможный тип инцидента, который может быть связан с данным событием.

4) Определить метод обнаружения, позволяющий выявить данный инцидент.

Оформление результата, результат представить в виде таблицы.

Таблица 2 – Методы обнаружения инцидентов

Источники события	Тип события	Возможные инциденты	Методы обнаружения
Системные журналы	Изменение системных файлов	Компрометация системы	Контроль целостности файлов

3. Подготовка сдерживания инцидента

После обнаружения инцидента информационной безопасности необходимо принять меры по ограничению его распространения и минимизации возможного ущерба. На данном этапе формируется план действий, направленный на локализацию и сдерживание инцидента.

Ход выполнения

1) Рассмотреть возможные типы инцидентов информационной безопасности.

2) Определить меры реагирования, позволяющие ограничить распространение инцидента.

3) Сформировать план действий по локализации инцидента.

Контрольные вопросы:

1) Что такое реагирование на инциденты информационной безопасности?

2) Какие этапы включает процесс реагирования на инциденты?

3) Для чего используется контроль целостности файлов?

4) Что такое криптографическая хеш-функция?

5) Какие методы используются для обнаружения атак?

6) Какие меры применяются для сдерживания инцидента?

Лабораторная работа №3-4

Тема: Использование системы управления инцидентами информационной безопасности. Анализ обработки инцидентов.

Цель занятия

1. Закрепление теоретических знаний о модели безопасности операционной системы Windows.
2. Изучение механизмов идентификации, аутентификации и разграничения доступа пользователей в ОС Windows.
3. Освоение практических навыков настройки прав доступа, аудита событий безопасности и шифрования данных средствами Windows.

Подготовка к занятию

1. Изучить основные компоненты модели безопасности ОС Windows.
2. Повторить принципы идентификации и аутентификации пользователей, а также механизмов разграничения доступа к объектам.
3. Изучить средства настройки прав доступа, аудита событий безопасности и шифрования данных в Windows.

Учебные вопросы

1. Основные элементы модели безопасности ОС Windows.
2. Идентификация пользователей и использование идентификаторов безопасности (SID).
3. Маркер доступа пользователя и его роль в разграничении доступа к системным объектам.

Основные теоретические сведения

Основные теоретические сведения изложены в материалах лекций и по данной тематике и рекомендуемой литературе.

Правила работы в лаборатории

К работе в лаборатории допускаются лица, изучившие правила и меры безопасности, сдавшие зачет по ним и усвоившие порядок выполнения практического занятия.

Требования безопасности перед началом работ

- ЗАПРЕЩАЕТСЯ: переодеваться, пользоваться огнем, курить, принимать пищу в лаборатории;
- убедиться в целостности электрических розеток и разъемов. В лаборатории необходимо быть в сменной обуви;
- включение компьютера производить только после получения допуска по выполняемой работе и разрешения преподавателя или лаборанта.

Требования безопасности во время работы

- выполняя практическое занятие, студенты обязаны использовать только вычислительную технику, периферийное оборудование, соединительные кабели, измерительное оборудование и носители информации, непосредственно относящиеся к данному практическому занятию;
- подключение и отключение составляющих вычислительного комплекса производить только при полном снятии напряжения со всех составляющих вычислительного комплекса;
- при обнаружении неисправностей в оборудовании немедленно отключить источники питания и доложить об этом руководителю занятий или лаборанту.

Требования безопасности по окончании работы

- доложить руководителю занятий или лаборанту о завершении работ;
- привести в порядок и сдать рабочее место лаборанту, и доложить руководителю занятий о сдаче.

Аппаратное обеспечение

Класс персональных ЭВМ, электронная доска, проектор.

Программное обеспечение

В комплекте с персональными ЭВМ. Доступ к Интернет. Офисный пакет.

Литература

1. Соломон, Русинович. Внутреннее устройство Microsoft Windows: Windows Server 2003, Windows XP и Windows 2000. 4-е издание, СПб.: Питер, 2008., 992 с.
2. А. Чекмарев, А. Вишневский, О. Кокорева Microsoft Windows Server 2003. Русская версия. Наиболее полное руководство. , СПб.: БХВ-Петербург, 2008 г., 1120 с.
3. Лясин Д.Н., Саньков С.Г. Методы и средства защиты компьютерной информации (учебное пособие). – Волгоград, Издательство ВолгГТУ РПК "Политехник", 2005г.
4. У. Р. Станек. Командная строка Microsoft Windows. Справочник администратора. М.: Русская редакция, 2009., 480с.
5. Безопасность Windows Server 2003 в библиотеке Microsoft TechNet. <http://technet.microsoft.com/ru-ru/library/dd548350%28WS.10%29.aspx>

1. Основные сведения

1.1. Классификация защиты семейства ОС Windows

Защита конфиденциальных данных от несанкционированного доступа является важнейшим фактором успешного функционирования любой многопользовательской системы. ОС Windows не является исключением и требования к защите объектов файловой системы, памяти, объектов ядра операционной системы внесли существенный вклад в процесс ее проектирования и реализации.

Современные версии ОС Windows (Windows 10, Windows 11, Windows Server 2019/2022) содержат развитую встроенную подсистему безопасности, включающую механизмы идентификации, аутентификации, разграничения доступа, аудита и защиты данных. Требования к операционной системе, защищенной по классу C2, включают:

- обязательную идентификацию и аутентификацию всех пользователей операционной системы. Под этим понимается способность операционной системы идентифицировать всех пользователей, которые получают санкционированный доступ к системе, и предоставление доступа к ресурсам только этим пользователям;
- разграничительный контроль доступа — предоставление пользователям возможности защиты принадлежащих им данных;
- системный аудит — способность системы вести подробный аудит всех действий, выполняемых пользователями и самой операционной системой;
- защита объектов от повторного использования — способность системы предотвратить доступ пользователя к информации ресурсов, с которыми до этого работал другой пользователь.

Современные версии ОС Windows используются в защищённых информационных системах при условии корректной настройки встроенных механизмов безопасности, таких как разграничение доступа, аудит событий, шифрование данных и управление учетными записями.

1.2. Идентификация пользователей

Для защиты данных Windows использует следующие основные механизмы: аутентификация и авторизация пользователей, аудит событий в системе, шифрование данных, поддержка инфраструктуры открытых ключей, встроенные средства сетевой защиты. Эти механизмы поддерживаются такими подсистемами Windows как LSASS (Local Security Authority Subsystem Service, подсистема локальной аутентификации), SAM (Security Account Manager, диспетчер локальных записей безопасности), SRM (Security reference Monitor, монитор состояния защиты), Active Directory (служба каталогов), EFS (Encrypting File System, шифрующая файловая система) и др.

Защита объектов и аудит действий с ними в ОС Windows организованы на основе избирательного (дискреционного) доступа, когда права доступа (чтение, запись, удаление, изменение атрибутов) субъекта к объекту задается явно в специальной матрице доступа. Для укрупнения матрицы пользователи могут объединяться в группы. При попытке субъекта (одного из потоков процесса, запущенного от его имени) получить доступ к объекту указываются, какие операции пользователь собирается выполнять с объектом. Если подобный тип доступа разрешен, поток получает описатель (дескриптор) объекта и все потоки процесса могут выполнять операции с ним. Подобная схема доступа, очевидно, требует аутентификации каждого пользователя, получающего доступ к ресурсам и его надежную идентификацию в системе, а также механизмов описания прав пользователей и групп пользователей в системе, описания и проверки дискреционных прав доступа пользователей к объектам. Рассмотрим, как в ОС Windows организована аутентификация и авторизация пользователей.

Все действующие в системе объекты (пользователи, группы, локальные компьютеры, домены) идентифицируются в Windows не по именам, уникальность которых не всегда удается достичь, а по **идентификаторам защиты (Security Identifiers, SID)**. SID представляет собой числовое значение

S - R - I - S0 - S1 - ... - Sn - RID

переменной длины:

S - неизменный идентификатор строкового представления SID;

R – уровень ревизии (версия). На сегодня 1.

I - (identifier-authority) идентификатор полномочий . Представляет собой 48-битную строку, идентифицирующую компьютер или сеть, который(ая) выдал SID объекту. Возможные значения:

0 (SECURITY_NULL_SID_AUTHORITY) — используются для сравнений, когда неизвестны полномочия идентификатора;

1 (SECURITY_WORLD_SID_AUTHORITY) — применяются для конструирования идентификаторов SID, которые представляют всех пользователей. Например, идентификатор SID для группы *Everyone* (Все пользователи) — это S-1-1-0;

2 (SECURITY_LOCAL_SID_AUTHORITY) — используются для построения идентификаторов SID, представляющих пользователей, которые входят на локальный терминал;

5 (SECURITY_NT_AUTHORITY) — сама операционная система. То есть, данный идентификатор выпущен компьютером или доменом.

Sn – 32-битные коды (колличеством 0 и более) субагентов, которым было передано право выдать SID. Значение первых подчиненных полномочий общеизвестно. Они могут иметь значение:

5 — идентификаторы SID присваиваются сеансам регистрации для выдачи прав любому приложению, запускаемому во время определенного сеанса регистрации. У таких идентификаторов SID первые подчиненные полномочия установлены как 5 и принимают форму *S-1-5-5-x-y*;

6 — когда процесс регистрируется как служба, он получает специальный идентификатор SID в свой маркер для обозначения данного действия. Этот идентификатор SID имеет подчиненные полномочия 6 и всегда будет *S-1-5-6*;

21 (SECURITY_NT_NON_UNIQUE) — обозначают идентификатор SID пользователя и идентификатор SID компьютера, которые не являются уникальными в глобальном масштабе;

32 (SECURITY_BUILTIN_DOMAIN_RID) — обозначают встроенные идентификаторы SID. Например, известный идентификатор SID для встроенной группы администраторов *S-1-5-32-544*;

80 (SECURITY_SERVICE_ID_BASE_RID) — обозначают идентификатор SID, который принадлежит службе.

Остальные подчиненные полномочия идентификатора совместно обозначают домен или компьютер, который издал идентификатор SID.

RID – 32-битный относительный идентификатор. Он является идентификатором уникального объекта безопасности в области, для которой был определен SID. Например, 500 — обозначает встроенную учетную запись *Administrator*, 501 — обозначает встроенную учетную запись *Guest*, а 502 — RID для билета на получение билетов протокола Kerberos .

При генерации SID Windows использует генератор случайных чисел, чтобы обеспечить уникальность SID для каждого пользователя. Для некоторого произвольного пользователя SID может выглядеть так:

S-1-5-21-789336058-484763869-725345543-1003

Предопределенным пользователям и группам Windows выдает характерные SID, состоящие из SID компьютера или домена и предопределенного RID. В таблице 1 приведен перечень некоторых общеизвестных SID.

Таблица 1. Общеизвестные SID Windows

SID	Название	Описание
S-1-1-0	Все	Группа, в которую входят все пользователи

S-1-5-2	Сеть	Группа, в которую входят все пользователи, зарегистрировавшиеся в системе из сети
S-1-5-7	Анонимный вход	Группа, в которую входят все пользователи, вошедшие в систему анонимно
S-1-5-домен-500	Администратор	Учетная запись администратора системы. По умолчанию только эта запись обеспечивает полный контроль системы
S-1-5-домен-501	Гость	Учетная запись пользователя-гостя

Полный список общеизвестных SID можно посмотреть в документации Platform SDK. Узнать SID конкретного пользователя в системе, а также SID групп, в которые он включен, можно, используя консольную команду **whoami**:

whoami /user /sid

Соответствие имени пользователя и его SID можно отследить также в ключе реестра **HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList**.

После аутентификации пользователя процессом Winlogon, все процессы, запущенные от имени этого пользователя будут идентифицироваться специальным объектом, называемым **маркером доступа (access token)**. Если процесс пользователя запускает дочерний процесс, то его маркер наследуются, поэтому маркер доступа олицетворяет пользователя для системы в каждом запущенном от его имени процессе. Основные элементы маркера представлены на рис. 1.

SID пользователя	SID1 ... SIDn Идентификаторы групп пользователя	DACL по умолчанию	Привилегии	Прочие параметры
-----------------------------	--	------------------------------	-------------------	-----------------------------

Рисунок 1. Обобщенная структура маркера доступа.

Маркер доступа содержит идентификатор доступа самого пользователя и всех групп, в которые он включен. В маркер включен также DACL по умолчанию - первоначальный список прав доступа, который присоединяется к создаваемым пользователем объектам. Еще одна важная для определения прав пользователя в системе часть маркера – список его привилегий. Привилегии - это права доверенного объекта на совершение каких-либо действий по отношению ко всей системе. В таблице 2 перечислены некоторые привилегии, которые могут быть предоставлены пользователю.

Таблица 2. Привилегии, которыми могут быть наделены пользователи

Имя и идентификатор привилегии	Описание привилегии
--------------------------------	---------------------

Увеличение приоритета диспетчирования SeIncreaseBasePriorityPrivilege	Пользователь, обладающий данной привилегией может изменять приоритет диспетчирования процесса с помощью интерфейса Диспетчера задач
Закрепление страниц в памяти SeLockMemoryPrivilege	Процесс получает возможность хранить данные в физической памяти, не прибегая к кэшированию данных в виртуальной памяти на диске.
Управление аудитом и журналом безопасности SeAuditPrivilege	Пользователь получает возможность указывать параметры аудита доступа к объекту для отдельных ресурсов, таких как файлы, объекты Active Directory и разделы реестра.
Овладение файлами или иными объектами SeTakeOwnershipPrivilege	Пользователь получает возможность становиться владельцем любых объектов безопасности системы, включая объекты Active Directory, файлы и папки NTFS, принтеры, разделы реестра, службы, процессы и потоки
Завершение работы системы SeShutdownPrivilege	Пользователь получает возможность завершать работу операционной системы на локальном компьютере
Обход перекрестной проверки SeChangeNotifyPrivilege	Используется для обхода проверки разрешений для промежуточных каталогов при проходе многоуровневых каталогов

Управление привилегиями пользователей осуществляется в оснастке «Групповая политика», раздел **Конфигурация Windows/Локальные политики/Назначение прав пользователя**.

Чтобы посмотреть привилегии пользователя, можно также использовать команду

whoami /all

Остальные параметры маркера носят информационный характер и определяют, например, какая подсистема создала маркер, уникальный идентификатор маркера, время его действия. Необходимо также отметить возможность создания ограниченных маркеров (restricted token), которые отличаются от обычных тем, что из них удаляются некоторые привилегии и его SID-идентификаторы проверяются только на запрещающие правила. Создать ограниченный маркер можно программно, используя API-функцию **CreateRestrictedToken**, а можно запустить процесс с ограниченным маркером, используя пункт контекстного меню Windows «**Запуск от имени...**» и отметив пункт «**Защитить компьютер от несанкционированных действий этой программы**» (рис.2).

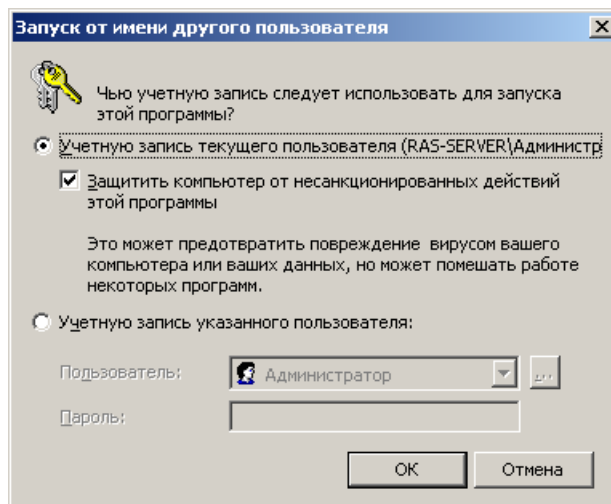


Рисунок 2. Запуск процесса с ограниченным маркером

Ограниченные маркеры используются для процессов, подменяющих клиента и выполняющих небезопасный код.

Маркер доступа может быть создан не только при первоначальном входе пользователя в систему. Windows предоставляет возможность запуска процессов от имени других пользователей, создавая для этих процессов соответствующий маркер. Для этих целей можно использовать:

- API-функции **CreateProcessAsUser**, **CreateProcessWithLogon**;
- оконный интерфейс (рис.2), инициализирующийся при выборе пункта контекстного меню “Запуск от имени...”;
- консольную команду **runas**:

runas /user:имя_пользователя program,

где *имя_пользователя* - имя учетной записи пользователя, которая будет использована для запуска программы в формате *пользователь@домен* или *домен\пользова-тель*;

program – команда или программа, которая будет запущена с помощью учетной записи, указанной в параметре **/user**.

В любом варианте запуска процесса от имени другой учетной записи необходимо задать ее пароль.

1.3. Защита объектов системы.

Маркер доступа идентифицирует субъектов-пользователей системы. С другой стороны, каждый объект системы, требующий защиты, содержит описание прав доступа к нему пользователей. Для этих целей используется **дескриптор безопасности (Security Descriptor, SD)**. Каждому объекту системы, включая файлы, принтеры, сетевые службы, контейнеры Active Directory и другие, присваивается дескриптор безопасности, который определяет права доступа к объекту и содержит следующие основные атрибуты (рис.3):

- SID владельца, идентифицирующий учетную запись пользователя-владельца объекта;
- пользовательский список управления доступом (Discretionary Access Control List, DACL), который позволяет отслеживать права и ограничения,

установленные владельцем данного объекта. DACL может быть изменен пользователем, который указан как текущий владелец объекта.

- системный список управления доступом (System Access Control List, SACL), определяющий перечень действий над объектом, подлежащих аудиту;
- флаги, задающие атрибуты объекта.

Авторизация Windows основана на сопоставлении маркера доступа субъекта с дескриптором безопасности объекта. Управляя свойствами объекта, администраторы могут устанавливать разрешения, назначать право владения и отслеживать доступ пользователей.

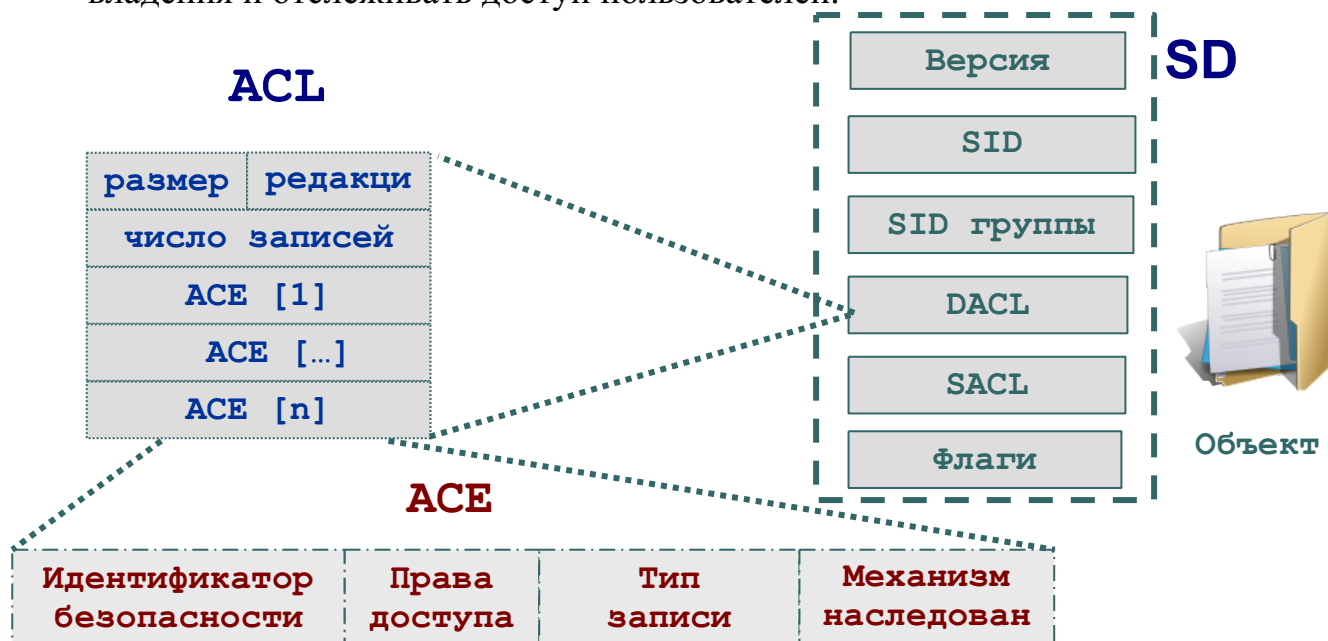


Рисунок 3. Структура дескриптора безопасности объекта

Список управления доступом содержит набор элементов (Access Control Entries, ACE). В DACL каждый ACE состоит из четырех частей: в первой указываются пользователи или группы, к которым относится данная запись, во второй – права доступа, а третья информирует о том, предоставляются эти права или отбираются. Четвертая часть представляет собой набор флагов, определяющих, как данная запись будет наследоваться вложенными объектами (актуально, например, для папок файловой системы, разделов реестра).

Если список ACE в DACL пуст, к нему нет доступа ни у одного пользователя (только у владельца на изменение DACL). Если отсутствует сам DACL в SD объекта – полный доступ к нему имеют все пользователи.

Если какой-либо поток запросил доступ к объекту, подсистема SRM осуществляет проверку прав пользователя, запустившего поток, на данный объект, просматривая его список DACL. Проверка осуществляется до появления разрешающих прав **на все** запрошенные операции. Если встретится запрещающее правило хотя бы **на одну** запрошенную операцию, доступ не будет предоставлен.

Рассмотрим пример на рис.4. Процесс пытается получить доступ к объекту с заданным DACL. В маркере процесса указаны SID запустившего его пользователя, а также SID групп, в которые он входит. В списке DACL объекта присутствуют разрешающие правила на чтение для пользователя с SID=100, и на запись для группы с SID=205. Однако, в доступе пользователю будет отказано, поскольку раньше встречается запрещающее запись правило для группы с SID=201.

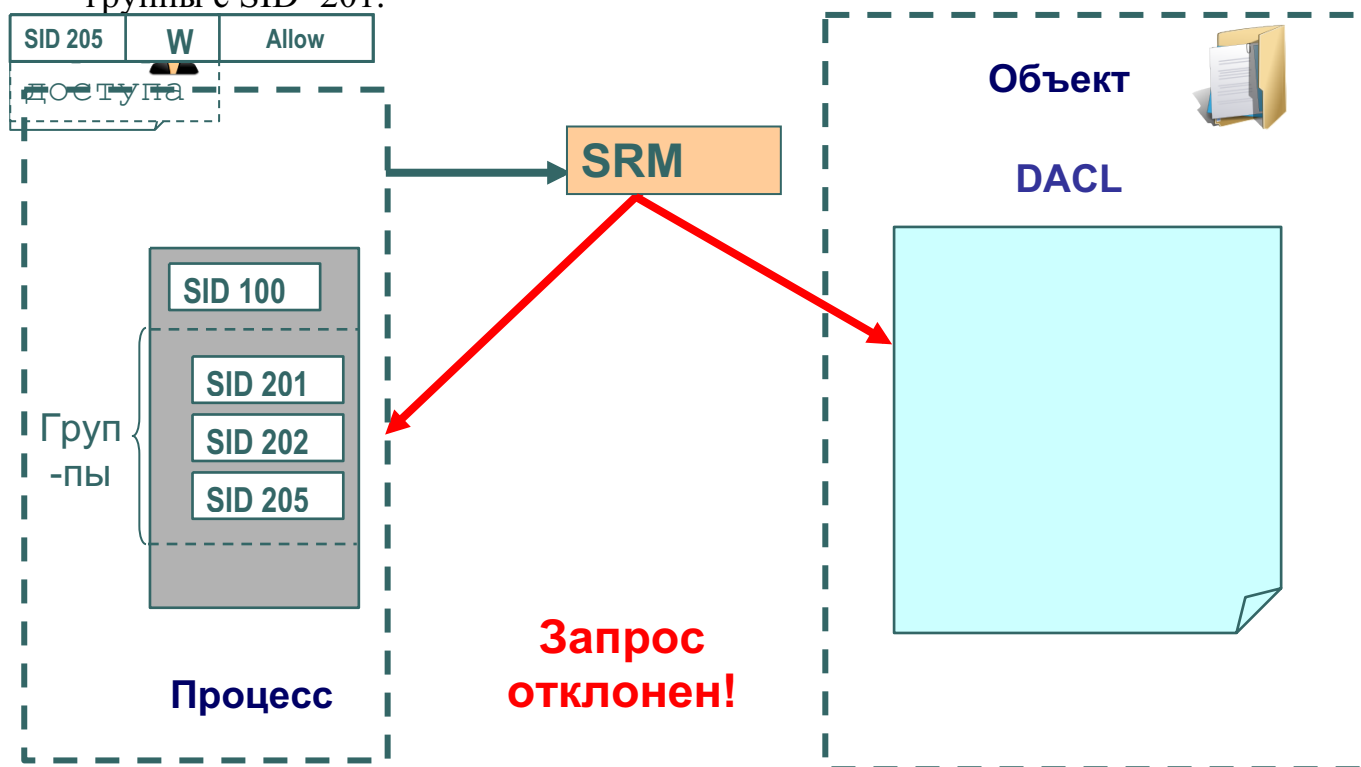


Рисунок 4. Проверка прав доступа пользователя к

Необходимо отметить, что запрещающее правило помещено в списке DACL на рисунке не случайно. Запрещающие правила **всегда** размещаются перед разрешающими, то есть являются доминирующими при проверке прав доступа.

Для определения и просмотра прав доступа пользователей к ресурсам можно использовать как графические средства контроля, так и консольные команды. Стандартное окно свойств объекта файловой системы (диска, папки, файла) на вкладке **Безопасность** (рис. 5) позволяет просмотреть текущие разрешения для пользователей и групп пользователей, редактировать их, создавать новые или удалять существующие.

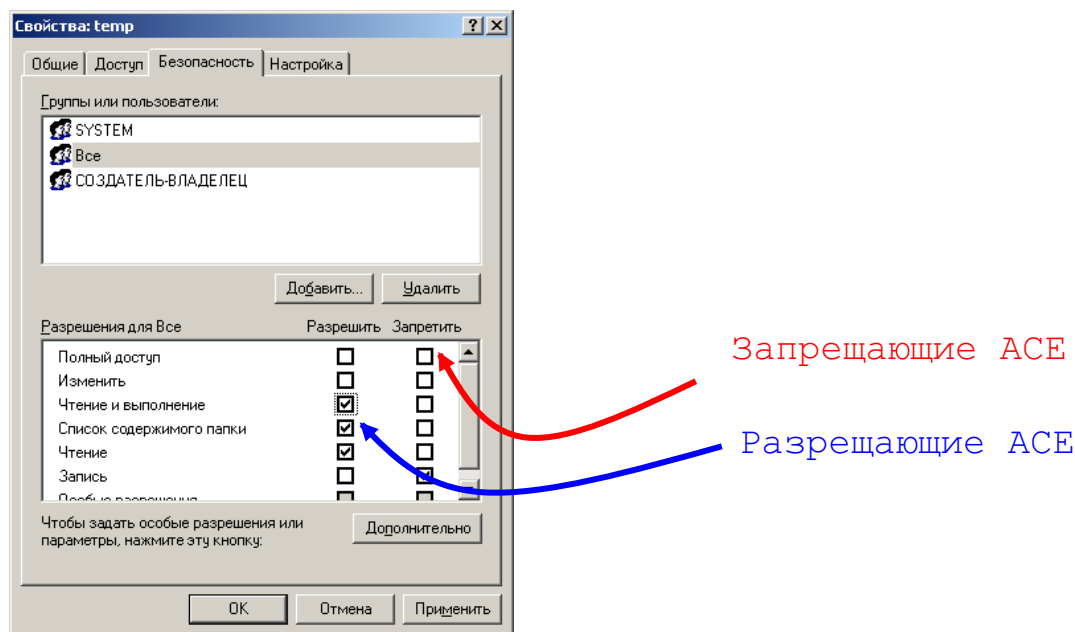


Рисунок 5. GUI-интерфейс Windows для изменения прав

При определении прав доступа к объектам можно задать правила их наследования в дочерних контейнерах. В окне дополнительных параметров безопасности на вкладке **Разрешения** при выборе опции «**Наследовать от родительского объекта применимых к дочерним объектам разрешения, добавляя их к явно заданным в этом окне**» (рис. 6) можно унаследовать разрешения и ограничения, заданные для родительского контейнера, текущему объекту.

При выборе опции «**Заменить разрешения для всех дочерних объектов заданными здесь разрешениями, применимыми к дочерним объектам**» разрешается передача определенных для объекта-контейнера правил доступа его дочерним объектам.

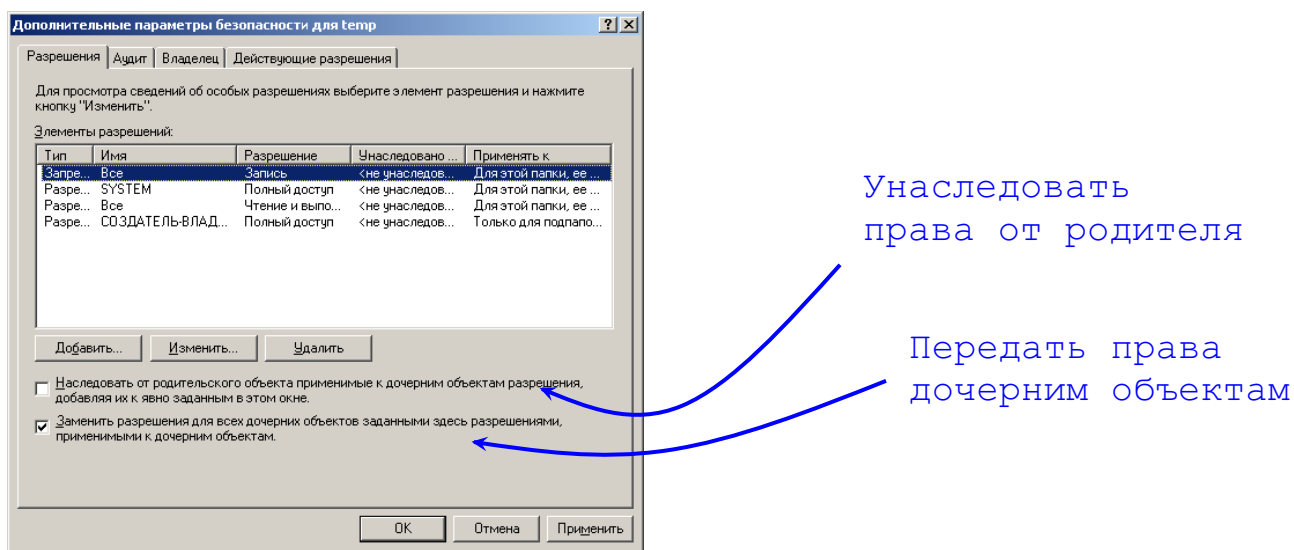
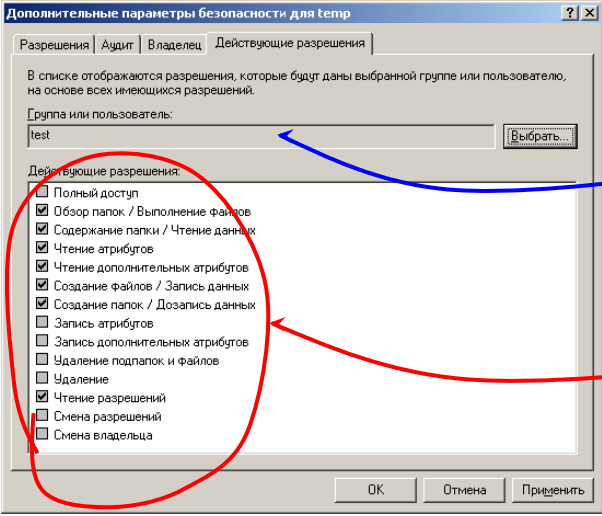


Рисунок 6. Определение параметров наследования прав

В этом же окне на вкладке **Владелец** допустимо узнать владельца объекта и заменить его. Владелец объекта имеет право на изменение списка

его DACL, даже если к нему запрещен любой тип доступа. Администратор имеет право становиться владельцем любого объекта.

С учетом возможности вхождения пользователя в различные группы и независимости определения прав доступа к объектам для групп и пользователей, зачастую бывает сложно определить конечные права пользователя на доступ к объекту: требуется просмотреть запрещающие правила, определенные для самого объекта, для всех групп, в которые он включен, затем то же проделать для разрешающих правил. Автоматизировать процесс определения разрешенных пользователю видов доступа к объекту можно с использованием вкладки «Действующие разрешения» окна дополнительных параметров безопасности объекта (рис. 7).



Имя пользователя или группы

Разрешения на доступ к объекту для выбранного

Рисунок 7. Определение эффективных прав доступа пользователя (группы) к объекту

Для просмотра и изменения прав доступа к объектам в режиме командной строки в современных версиях Windows используется команда **icacls**. Команда **cacls** считается устаревшей, однако может рассматриваться как исторический аналог.

icacls имя_файла [/t] [/e] [/c] [/g пользователь:разрешение] [/r пользователь [...]] [/p пользователь:разрешение [...]] [/d пользователь [...]]

Назначения параметров команды приведены в таблице 3.

Таблица 3. Параметры команды icacls

<имя файла>	Задаёт файл или папку, права доступа к которой необходимо просмотреть/изменить (допустимо использовать шаблоны с символами * и ?).
/t	Изменение избирательных таблиц контроля доступа (DACL) указанных файлов в текущем каталоге и всех подкаталогах
/e	Редктирование избирательной таблицы управления доступом (DACL) вместо ее замены

/c	Заставляет команду продолжить изменение прав доступа при возникновении ошибки, связанной с нарушениями прав доступа
/g <пользователь группа: разрешение>	Предоставление прав доступа указанному пользователю
/r <пользователь группа>	Отнимает права доступа указанного пользователя.
/p <пользователь группа: разрешение>	Заменяет права доступа указанного пользователя
/d <пользователь группа>	Отказывает в праве доступа указанному пользователю или группе

Для указания добавляемых или отнимаемых прав используются следующие значения:

- F - полный доступ;
- C - изменение (запись);
- W - запись;
- R - чтение;
- N - нет доступа.

Рассмотрим несколько примеров.

icacls d:\test

Выдаст список DACL для папки test.

icacls d:\test /d ИмяКомпьютера\ИмяПользователя /e

Запретит доступ к объекту для указанного пользователя.

icacls d:\test /p ИмяКомпьютера\ИмяГруппы:f /e /t

Предоставит полный доступ к папке d:\test и ее подпапкам всем для членов указанной группы.

Для программного просмотра и изменения списков DACL можно использовать API-функции **AddAccessAllowedAce**, **AddAccessDeniedAce**, **SetSecurityInfo**. Подробнее с этими функциями и примерами их использования можно ознакомиться в [пособие].

1.4. Подсистема аудита.

Важный элемент политики безопасности – аудит событий в системе. ОС Windows ведет аудит событий по 9 категориям:

1. Аудит событий входа в систему.
2. Аудит управления учетными записями.
3. Аудит доступа к службе каталогов.
4. Аудит входа в систему.
5. Аудит доступа к объектам.
6. Аудит изменения политики.
7. Аудит использования привилегий.
8. Аудит отслеживания процессов.
9. Аудит системных событий.

Рассмотрим более подробно, какие события отслеживает каждая из категорий.

Аудит событий входа в систему

Аудит попыток пользователя войти в систему с другого компьютера или выйти из нее, при условии, что этот компьютер используется для проверки подлинности учетной записи.

Аудит управления учетными записями

Аудит событий, связанных с управлением учетными записями на компьютере: создание, изменение или удаление учетной записи пользователя или группы; переименование, отключение или включение учетной записи пользователя; задание или изменение пароля.

Аудит доступа к службе каталогов

Аудит событий доступа пользователя к объекту каталога Active Directory, для которого задана собственная системная таблица управления доступом (SACL).

Аудит входа в систему

Аудит попыток пользователя войти в систему с компьютера или выйти из нее.

Аудит доступа к объектам

Аудит событий доступа пользователя к объекту – например, к файлу, папке, разделу реестра, принтеру и т. п., - для которого задана собственная системная таблица управления доступом (SACL).

Аудит изменения политики

Аудит фактов изменения политик назначения прав пользователей, политик аудита или политик доверительных отношений.

Аудит использования привилегий

Аудит попыток пользователя воспользоваться предоставленным ему правом.

Аудит отслеживания процессов

Аудиту таких событий, как активизация программы, завершение процесса, повторение дескрипторов и косвенный доступ к объекту.

Аудит системных событий

Аудит событий перезагрузки или отключения компьютера, а также событий, влияющих на системную безопасность или на журнал безопасности.

Решения об аудите конкретного типа событий безопасности принимаются в соответствии с политикой аудита локальной системы. Политика аудита, также называемая локальной политикой безопасности (local security policy), является частью политики безопасности, поддерживаемой LSASS в локальной системе, и настраивается с помощью редактора локальной политики безопасности (Оснастка **gpedit.msc, Конфигурация компьютера - Конфигурация Windows – Параметры безопасности – Локальные политики – Политика аудита**, рис. 8).

Для каждого объекта в SD содержится список SACL, состоящий из записей ACE, регламентирующих запись в журнал аудита удачных или неудачных попыток доступа к объекту. Эти ACE определяют, какие операции, выполняемые над объектами конкретными пользователями или группами, подлежат аудиту. Информация аудита хранится в системном журнале аудита.

Аудиту могут подлежать как успешные, так и неудачные операции. Подобно записям ACE DACL, правила аудита объектов могут наследоваться дочерними объектами. Процедура наследования определяется набором флагов, являющихся частью структуры ACE.

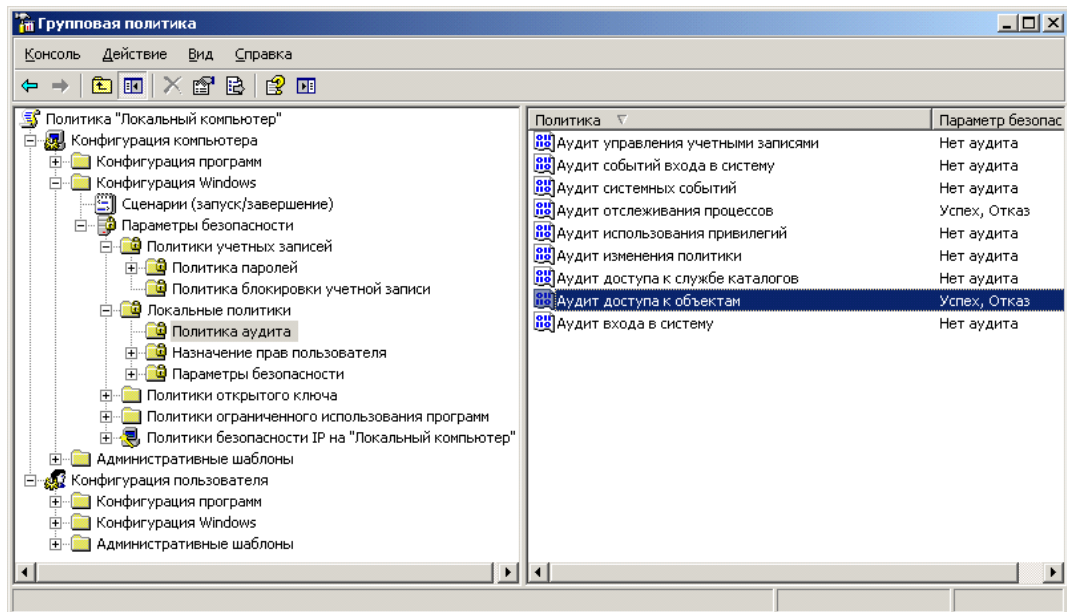
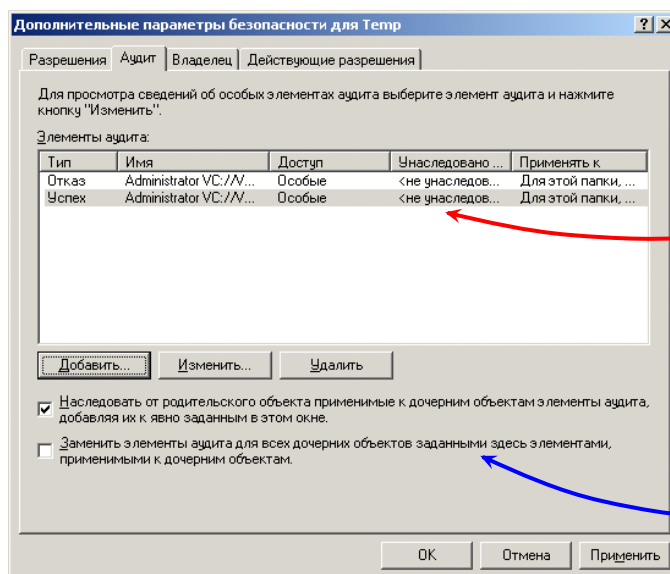


Рисунок 8. Конфигурация политики аудита редактора локальной политики безопасности

Настройка списка SACL может быть осуществлена в окне дополнительных свойств объекта (пункт “Дополнительно”, закладка “Аудит”, рис. 9).

Для программного просмотра и изменения списков SACL можно использовать API-функции **GetSecurityInfo** и **SetSecurityInfo**.



записи ACE списка
SACL объекта

параметры
наследования ACE

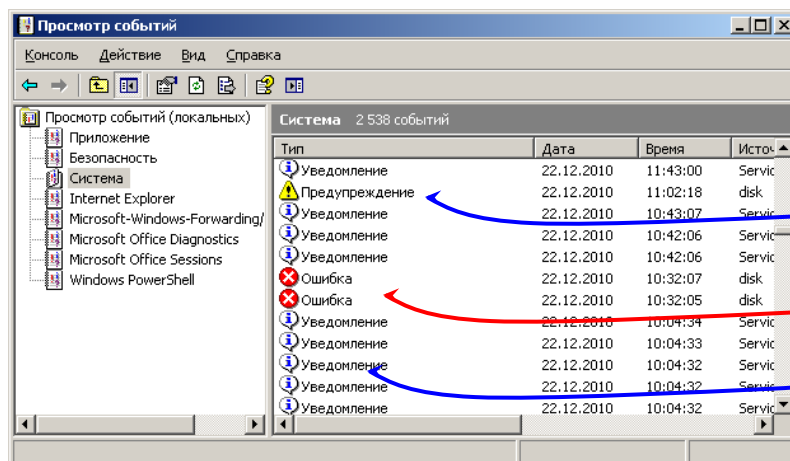
Рисунок 9. Интерфейс редактирования правил аудита для

При инициализации системы и изменении политики LSASS посылает SRM сообщения, информирующие его о текущей политике аудита. LSASS отвечает за прием записей аудита, генерируемых на основе событий аудита от SRM, их редактирование и передачу Event Logger (регистратору событий). SRM посылает записи аудита LSASS через свое LPC-соединение. После этого Event Logger заносит записи в журнал безопасности.

События аудита записываются в журналы следующих типов:

1. **Журнал приложений.** В журнале приложений содержатся данные, относящиеся к работе приложений и программ.
2. **Журнал безопасности.** Журнал безопасности содержит записи о таких событиях, как успешные и безуспешные попытки доступа в систему, а также о событиях, относящихся к использованию ресурсов.
3. **Журнал системы.** В журнале системы содержатся события системных компонентов Windows. Например, в журнале системы регистрируются сбои при загрузке драйвера или других системных компонентов при запуске системы.
4. **Журнал службы каталогов.** В журнале службы каталогов содержатся события, заносимые службой каталогов Windows (на контроллере домена AD).
5. **Журнал службы репликации.** В журнале службы репликации файлов содержатся события, заносимые службой репликации файлов Windows (на контроллере домена AD).

Просмотр журнала безопасности осуществляется в оснастке «Просмотр событий» (eventvwr.msc, рис. 10). Сами журналы хранятся в файлах SysEvent.evt, SecEvent.evt, AppEvent.evt в папке %WinDir%\system32\config.



Предупреждающее сообщение

Сообщение об ошибке

Информационное сообщение

Рисунок 10. Оснастка Windows «Просмотр событий»

В журнал записываются события 3 основных видов:

1. Информационные сообщения о событиях.

Описывают успешное выполнение операций, таких как запуск или некоторое действие системной службы.

2. Предупреждающие сообщения о событиях.

Описывают неожиданные действия, означающие проблему, или указывают на проблему, которая возникнет в будущем, если не будет устранена сейчас .

3. Сообщения о событиях ошибок.

Описывают ошибки, возникшие из-за неудачного выполнения задач.

1.5. Шифрующая файловая система.

В операционных системах семейства Windows с файловой системой NTFS поддерживается механизм шифрования данных EFS (Encrypting File System). Основное ее достоинств во заключается в обеспечении конфиденциальности данных на дисках компьютера за счет использования надежных симметричных алгоритмов для шифрования данных в реальном режиме времени.

В современных версиях Windows шифрующая файловая система EFS (Encrypting File System) использует симметричное шифрование данных с применением стойких криптографических алгоритмов. Для каждого файла генерируется уникальный ключ шифрования файла (FEK, File Encryption Key), с помощью которого шифруется содержимое файла. Для защиты самого FEK используется асимметричное шифрование на основе открытого ключа пользователя. В актуальных версиях Windows для защиты данных применяются современные криптографические механизмы, интегрированные в подсистему безопасности ОС.

При этом для обеспечения секретности самого ключа FEK шифруется асимметричным алгоритмом RSA открытым ключом пользователя, результат шифрации FEK – **Data Decryption Field, DDF** – добавляется в заголовок зашифрованного файла (рис. 11). Такой подход обеспечивает надежное шифрование без потери эффективности процесса шифрования: данные шифруются быстрым симметричным алгоритмом, а для гарантии секретности симметричного ключа используется асимметричный алгоритм шифрования.

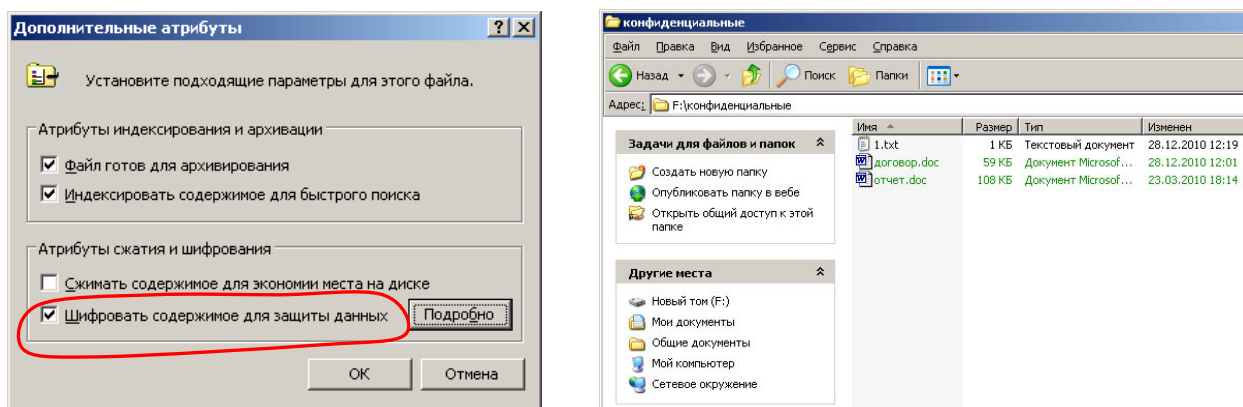


Рисунок 12. Графический интерфейс шифрования файла с

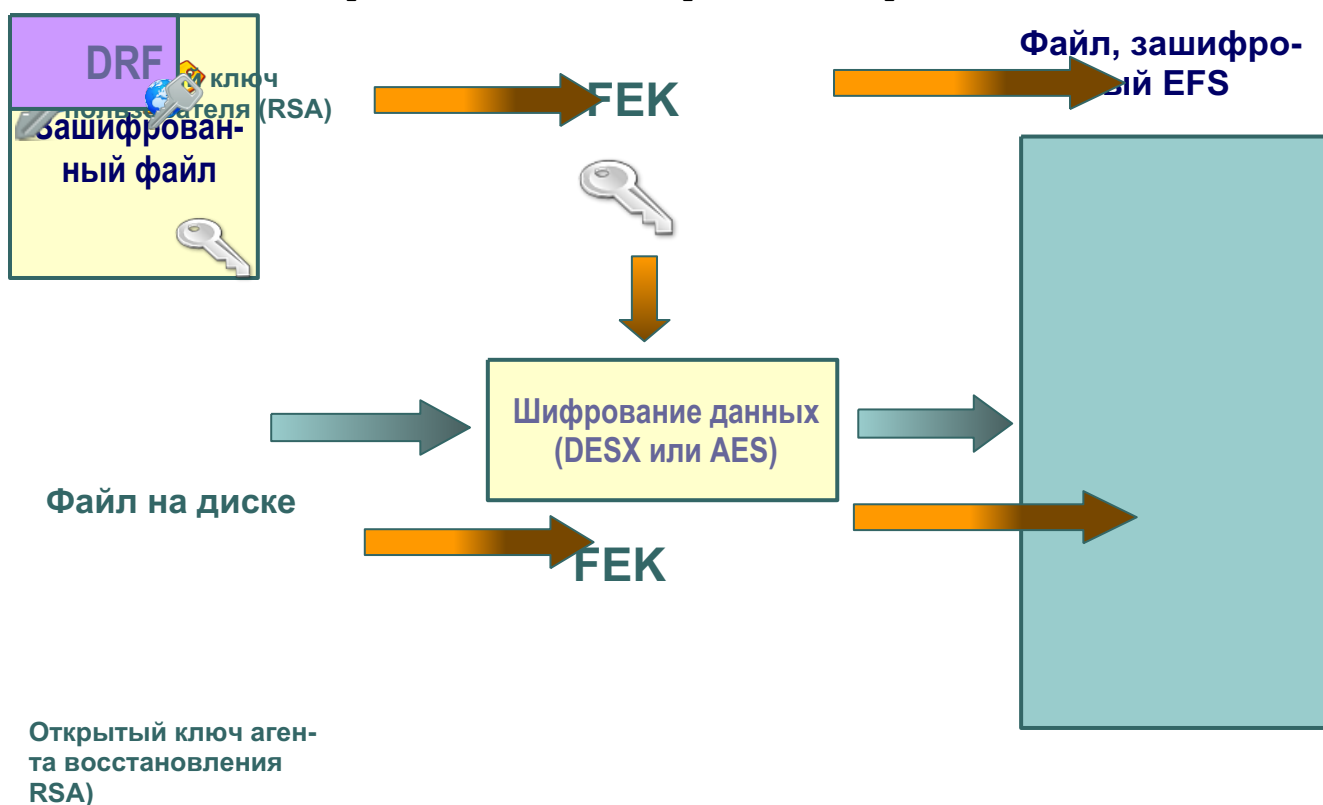


Рисунок 11. Схема шифрации файла в EFS

Для шифрации файлов с использованием EFS можно использовать графический интерфейс или команду **cipher**.

Графический интерфейс доступен в стандартном окне свойств объекта по нажатию кнопки «Дополнительно» (рис. 12). Зашифрованные объекты в стандартном интерфейсе Windows Explorer отображаются зеленым цветом.

Необходимо отметить, что EFS позволяет разделять зашифрованный файл между несколькими пользователями. В этом случае FEK шифруется открытыми ключами всех пользователей, которым разрешен доступ к файлу, и каждый результат шифрации добавляется в DDF.

Шифрование файла с использованием EFS защищает файл комплексно: пользователю, не имеющему права на дешифрацию файла, недопустимы, в том числе, такие операции, как удаление, переименование и копирование файла. Необходимо помнить, что EFS является частью файловой системы NTFS, и в случае копирования защищенного файла авторизованным пользователем на другой том с файловой системой, на поддерживающей EFS (например, FAT32), он будет дешифрован и сохранен на целевом томе в открытом виде.

Консольная команда **cipher** может быть использована для шифрации/дешифрации файлов из командной строки или в bat-сценарии.

cipher [{/e/d}] [/s:каталог] [/a] [/i] [/f] [/q] [/h] [/k] [/u[/n]] [путь [...]] | [/r:имя_файла_без_расширения]

Назначения параметров команды приведены в таблице 4.

Таблица 4. Параметры команды **cipher**

/e	Шифрует указанные папки. Папки помечаются таким образом, чтобы файлы, которые будут добавляться в папку позже, также шифровались.
/d	Расшифровывает указанные папки. Папки помечаются таким образом, чтобы файлы, которые будут добавляться в папку позже, не будут шифроваться
/s: каталог	Выполняет выбранную операцию над указанной папкой и всеми подпапками в ней.
/a	Выполняет операцию над файлами и каталогами
/i	Продолжение выполнения указанной операции даже после возникновения ошибок. По умолчанию выполнение cipher прекращается после возникновения ошибки
/f	Выполнение повторного шифрования или расшифровывания указанных объектов. По умолчанию уже зашифрованные или расшифрованные файлы пропускаются командой cipher
/k	Создание ключа шифрования файла для пользователя, выполнившего команду cipher . Если используется данный параметр, все остальные параметры команды cipher не учитываются.
/u	Обновление ключа шифрования файла пользователя или ключа агента восстановления на текущие ключи во всех зашифрованных файлах на локальном диске (если эти ключи были изменены). Этот параметр используется только вместе с параметром /n.
/n	Запрещение обновления ключей. Данный параметр служит для поиска всех зашифрованных файлов на локальных дисках. Этот параметр используется только вместе с параметром /u.
путь	Указывает шаблон, файл или папку.

/r: имя_файла	Создание нового сертификата агента восстановления и закрытого ключа с последующей их записью в файлах с именем, указанным в параметре <i>имя_файла</i> (без расширения). Если используется данный параметр, все остальные параметры команды cipher не учитываются.
--------------------------------	---

Например, чтобы определить, зашифрована ли какая-либо папка, необходимо использовать команду:

cipher путь\имя_папки

Команда **cipher** без параметров выводит статус (зашифрован или нет) для всех объектов текущей папки.

Для шифрации файла необходимо использовать команду

cipher /e /a путь\имя_файла

Для дешифрации файла, соответственно, используется команда

cipher /d /a путь\имя_файла

Допустима шифрация/дешифрация группы файлов по шаблону:

cipher /e /a d:\work*.doc

Пара открытый и закрытый ключ для шифрации FEK создаются для пользователя автоматически при первой шифрации файла с использованием EFS.

Если некоторый пользователь или группа пользователей зашифровали файл с использованием EFS, то его содержимое доступно только им. Это приводит к рискам утери доступа к данным в зашифрованных файлах в случае утраты пароля данным пользователем (работник забыл пароль, уволился и т.п.). Для предотвращения подобных проблем администратор может определить некоторые учетные записи в качестве агентов восстановления.

Агенты восстановления (Recovery Agents) определяются в политике безопасности **Encrypted Data Recovery Agents (Агенты восстановления шифрованных данных)** на локальном компьютере или в домене. Эта политика доступна через оснастку **Групповая политика (gpedit.msc)** раздел «**Параметры безопасности**»-> «**Политика открытого ключа**»-> «**Файловая система EFS**». Пункт меню «**Действие**»-> «**Добавить агент восстановления данных**» открывает мастер добавления нового агента.

Добавляя агентов восстановления можно указать, какие криптографические пары (обозначенные их сертификатами) могут использовать эти агенты для восстановления шифрованных данных (рис. 13). Сертификаты для агентов восстановления создаются командой **cipher** с ключом **/r** (см. табл. 4). Для пользователя, который будет агентом восстановления, необходимо импортировать закрытый ключ агента восстановления из сертификата, созданного командой **cipher**. Это можно сделать в мастере импорта сертификатов, который автоматически загружается при двойном щелчке по файлу *.pfx.

EFS создает – **DRF (Data Recovery Field)**-элементы ключей для каждого агента восстановления, используя провайдер криптографических сервисов,

зарегистрированный для EFS-восстановления. DRF добавляется в зашифрованный файл и может быть использован как альтернативное средство извлечения FEK для дешифрации содержимого файла.

Windows хранит закрытые ключи в подкаталоге **Application Data\Microsoft\Crypto\RSA** каталога профиля пользователя. Для защиты закрытых ключей Windows шифрует все файлы в папке RSA на основе симметричного ключа, генерируемого случайным образом; такой ключ называется мастер-ключом пользователя. Мастер-ключ имеет длину в 64 байта и создается стойким генератором случайных чисел. Мастер-ключ также хранится в профиле пользователя в каталоге **Application Data\Microsoft\Protect** и зашифровывается по алгоритму 3DES с помощью ключа, который отчасти основан на пароле пользователя. Когда пользователь меняет свой пароль,

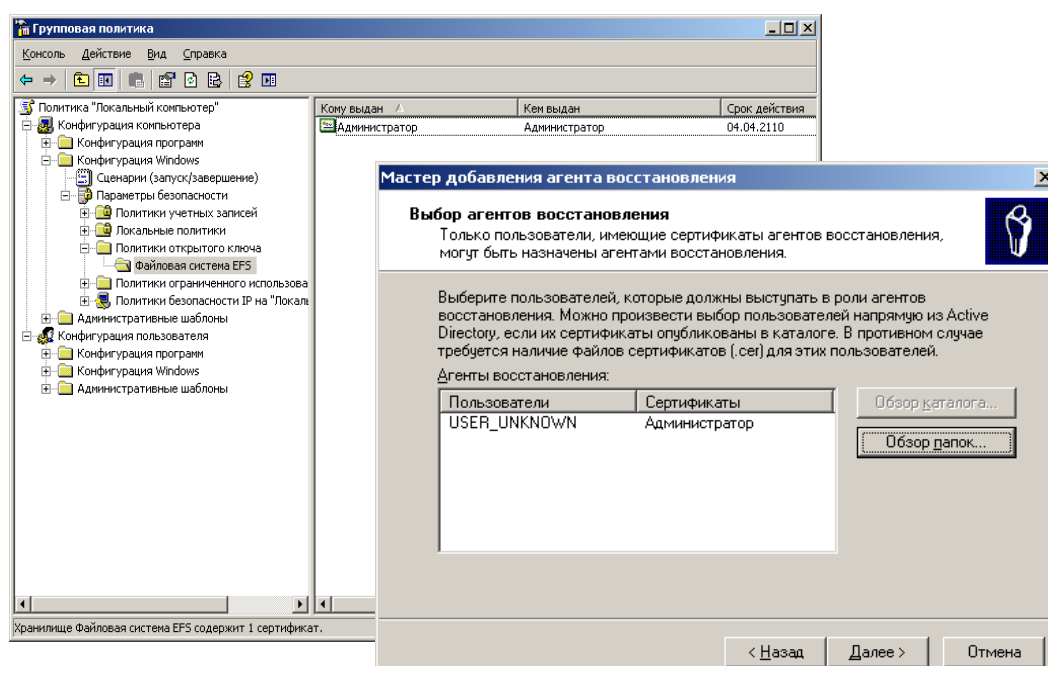


Рисунок 13. Добавление нового агента восстановления EFS

мастер-ключи автоматически расшифровываются, а затем заново зашифровываются с учетом нового пароля.

Для расшифровки FEK EFS использует функции Microsoft CryptoAPI (CAPI). CryptoAPI состоит из DLL провайдеров криптографических сервисов (cryptographic service providers, CSP), которые обеспечивают приложениям доступ к различным криптографическим сервисам (шифрованию, дешифрованию и хэшированию). EFS опирается на алгоритмы шифрования RSA, предоставляемые провайдером **Microsoft Enhanced Cryptographic Provider (\Windows\System32\Rsaenh.dll)**.

Шифрацию и дешифрацию файлов можно осуществлять программно, используя API-функции **EncryptFile** и **DecryptFile**.

2. Порядок выполнения работы.

2.1. Ознакомьтесь с теоретическими основами защиты информации в ОС семейства Windows в настоящих указаниях и конспектах лекций.

2.2. Выполните задания 2.2.1-2.2.8

2.2.1. Запустите в программе **Oracle VM Virtualbox** виртуальную машину Windows 10 или Windows 11. Войдите в систему под учетной записью администратора, пароль узнайте у преподавателя. Все действия в пп 2.2.1-2.2.8 выполняйте в системе, работающей на виртуальной машине.

2.2.2. Создайте учетную запись нового пользователя **testUser** в оснастке «**Управление компьютером**» (**compmgmt.msc**). При создании новой учетной записи запретите пользователю смену пароля и снимите ограничение на срок действия его пароля. Создайте новую группу **"testGroup"** и включите в нее нового пользователя. Удалите пользователя из других групп. Создайте на диске **C:** папку **forTesting**. Создайте или скопируйте в эту папку несколько текстовых файлов (*.txt).

2.2.3. С помощью команды **runas** запустите сеанс командной строки (**cmd.exe**) от имени вновь созданного пользователя. Командой **whoami** посмотрите SID пользователя и всех его групп, а также текущие привилегии пользователя. Строку запуска и результат работы этой и **всех** следующих консольных команд копируйте в файл протокола лабораторной работы.

2.2.4. Убедитесь в соответствии имени пользователя и полученного SID в реестре Windows. Найдите в реестре, какому пользователю в системе присвоен SID **S-1-5-21-1957994488-492894223-170857768-1004** (Используйте ключ реестра **HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList**).

2.2.5. Командой **whoami** определите перечень текущих привилегий пользователя **testUser**. В сеансе командной строки пользователя попробуйте изменить системное время командой **time**. Чтобы предоставить пользователю подобную привилегию, запустите оснастку «**Локальные параметры безопасности**» (**secpol.msc**). Добавьте пользователя в список параметров политики «**Изменение системного времени**» раздела **Локальные политики -> Назначение прав пользователя**. После этого перезапустите сеанс командной строки от имени пользователя, убедитесь, что в списке привилегий добавилась **SeSystemtimePrivilege**. Попробуйте изменить системное время командой **time**.

Убедитесь, что привилегия «**Завершение работы системы**» (**SeShutdownPrivilege**) предоставлена пользователю **testUser**. После этого попробуйте завершить работу системы из сеанса командной строки пользователя командой **shutdown -s**. Добавить ему привилегию «**Принудительное удаленное завершение**» (**SeRemoteShutdownPrivilege**). Попробуйте завершить работу консольной командой еще раз (отменить команду завершения до ее непосредственного выполнения можно командой **shutdown -a**).

2.2.6. Ознакомьтесь с справкой по консольной команде **cacls**. Используя эту команду, просмотрите разрешения на папку **c:\forTesting**. Объясните все обозначения в описаниях прав пользователей и групп в выдаче команды.

а) Разрешите пользователю **testUser** запись в папку **forTesting**, но запретите запись для группы **testGroup**. Попробуйте записать файлы или папки в **forTesting** от имени пользователя **testUser**. Объясните результат. Посмотрите эффективные разрешения пользователя **testUser** к папке **forTesting** в окне свойств папки.

б) Используя стандартное окно свойств папки, задайте для пользователя **testUser** такие права доступа к папке, чтобы он мог записывать информацию в папку **forTesting**, но не мог просматривать ее содержимое. Проверьте, что папка **forTesting** является теперь для пользователя **testUser** “слепой”, запустив, например, от его имени файловый менеджер и попробовав записать файлы в папку, просмотреть ее содержимое, удалить файл из папки.

в) Для вложенной папки **forTesting\Docs** отмените наследование ACL от родителя и разрешите пользователю просмотр, чтение и запись в папку. Проверьте, что для пользователя папка **forTesting\Docs** перестала быть “слепой” (например, сделайте ее текущей в сеансе работы файлового менеджера от имени пользователя и создайте в ней новый файл).

г) Снимите запрет на чтение папки **forTesting** для пользователя **testUser**. Используя команду **icacls** запретите этому пользователю доступ к файлам с расширением **txt** в папке **forTesting**. Убедитесь в недоступности файлов для пользователя.

д) Командой **icacls** запретите пользователю все права на доступ к папке **forTesting** и разреште полный доступ к вложенной папке **forTesting\Docs**. Убедитесь в доступности папки **forTesting\Docs** для пользователя. Удалите у пользователя **testUser** привилегию **SeChangeNotifyPrivilege**. Попробуйте получить доступ к папке **forTesting\Docs**. Объясните результат.

е) Запустите файловый менеджер от имени пользователя **testUser** и создайте в нем папку **newFolder** на диске C. Для папки **newFolder** очистите весь список ACL командой **icacls**. Попробуйте теперь получить доступ к папке от имени администратора и от имени пользователя. Кто и как теперь может вернуть доступ к папке? Верните полный доступ к папке для всех пользователей.

ж) Создайте в разделе **HKLM\Software** реестра раздел **testKey**. Запретите пользователю **testUser** создание новых разделов в этом разделе реестра. Создайте для раздела **HKLM\Software\testKey** SACL, позволяющий протоколировать отказы при создании новых подразделов, а также успехи при перечислении подразделов и запросе значений (предварительно проверьте, что в локальной политике безопасности соответствующий тип аудита включен). Попробуйте от имени пользователя **testUser** запустить **regedit.exe** и создать раздел в **HKLM\Software**. Убедитесь, что записи аудита были размещены в журнале безопасности (**eventvwr.msc**).

2.2.7. Шифрование файлов и папок средствами EFS.

а) От имени пользователя **testUser** зашифруйте какой-нибудь файл на диске. Убедитесь, что после этого был создан сертификат пользователя, запустив оснастку **certmgr.msc** от имени пользователя (раздел **Личные**). Просмотрите основные параметры сертификата открытого ключа пользователя **testUser** (срок действия, используемые алгоритмы). Установите доверие к этому сертификату в вашей системе.

б) Создайте в папке **forTesting** новую папку **Encrypt**. В папке **Encrypt** создайте или скопируйте в нее текстовый файл. Зашифруйте папку **Encrypt** и всё её содержимое с использованием свойств NTFS/EFS от имени администратора. Попробуйте просмотреть или скопировать какой-нибудь файл этой папки от имени пользователя **testUser**. Объясните результат. Скопируйте зашифрованный файл в незашифрованную папку (например, **forTesting**). Убедитесь что он остался зашифрованным. Добавьте пользователя **testUser** в список имеющих доступа к файлу пользователей в окне свойств шифрования файла. Повторите попытку получить доступ к файлу от имени пользователя **testUser**.

в) Создайте учетную запись нового пользователя **agentUser**, сделайте его членом группы Администраторы. Определите для пользователя **agentUser** роль агента восстановления EFS. Создайте в папке **forTesting** новый текстовый файл с произвольным содержимым. Зашифруйте этот файл от имени пользователя **testUser**. Убедитесь в окне подробностей шифрования файла, что пользователь **agentUser** является агентом восстановления для данного файла. Попробуйте прочитать содержимое файла от имени администратора и от имени пользователя **agentUser**. Объясните результат.

г) Зашифруйте все текстовые файлы папки **forTesting** с использованием консольной команды шифрования **cipher** от имени пользователя **testUser** (предварительно снимите запрет на доступ к этим файлам, установленный в задании 2.2.6г).

д) Убедитесь, что при копировании зашифрованных файлов на том с файловой системой, не поддерживающей EFS (например, FAT32 на флеш-накопителе), содержимое файла дешифруется.

2.2.8. После демонстрации результатов работы преподавателю восстановите исходное состояние системы: удалите созданные папки и файлы, разделы реестра, удалите учетную запись созданного пользователя и его группы, снимите с пользователя **agentUser** роль агента восстановления.

2.2.9. Представьте отчёт по лабораторной работе преподавателю и отчитайте работу.

2.3. Содержание отчета

Отчет по лабораторной работе должен содержать следующие сведения:

- название и цель работы;
- протокол выполнения лабораторной работы, содержащий список консольных команд, составленных при выполнении работы, и результаты их выполнения.

3. Контрольные вопросы

1. К какому классу безопасности относится ОС Windows по различным критериям оценки?
2. Каким образом пользователи идентифицируются в ОС Windows?
3. Что такое списки DACL и SACL?
4. Перечислите, каким образом можно запустить процесс от имени другого пользователя.
5. Как происходит проверка прав доступа пользователя к ресурсам в ОС Windows?
6. Что такое маркер безопасности, и какова его роль в модели безопасности Windows?
7. Как с использованием команды `icacls` добавить права на запись для всех файлов заданной папки?
8. Какие события подлежат аудиту в ОС Windows?
9. Каким образом шифруются файлы в файловой системе EFS? Что такое FEK, DDF и DRF?
10. Какие алгоритмы шифрования используются в EFS?

Лабораторная работа №5-6

Тема: Улучшение системы управления инцидентами. Управление инцидентами неавторизованного доступа

Цель занятия

1. Закрепление теоретических знаний о методах сетевого наблюдения и мониторинга сетевого трафика.
2. Изучение принципов анализа сетевых пакетов и фильтрации сетевого трафика.
3. Освоение методов обнаружения сетевых инцидентов и способов защиты от сетевых снифферов.

Подготовка к занятию

1. Изучить основные понятия сетевого мониторинга и анализа сетевого трафика.
2. Повторить принципы работы сетевых протоколов и передачи данных в компьютерных сетях.
3. Изучить методы защиты сетевого трафика от перехвата и анализа.

Учебные вопросы

1. Основные принципы сетевого наблюдения и мониторинга сетевого трафика.
2. Использование анализаторов сетевого трафика для обнаружения сетевых инцидентов.
3. Методы фильтрации и анализа сетевых пакетов.
4. Основные методы обнаружения подозрительной активности в сети.

Основные теоретические сведения

Основные теоретические сведения изложены в материалах лекций и по данной тематике и рекомендуемой литературе.

Правила работы в лаборатории

К работе в лаборатории допускаются лица, изучившие правила и меры безопасности, сдавшие зачет по ним и усвоившие порядок выполнения практического занятия.

Требования безопасности перед началом работ

- ЗАПРЕЩАЕТСЯ: переодеваться, пользоваться огнем, курить, принимать пищу в лаборатории;
- убедиться в целостности электрических розеток и разъемов. В лаборатории необходимо быть в сменной обуви;
- включение компьютера производить только после получения допуска по выполняемой работе и разрешения преподавателя или лаборанта.

Требования безопасности во время работы

- выполняя практическое занятие, студенты обязаны использовать только вычислительную технику, периферийное оборудование, соединительные кабели, измерительное оборудование и носители информации, непосредственно относящиеся к данному практическому занятию;
- подключение и отключение составляющих вычислительного комплекса производить только при полном снятии напряжения со всех составляющих вычислительного комплекса;
- при обнаружении неисправностей в оборудовании немедленно отключить источники питания и доложить об этом руководителю занятий или лаборанту.

Требования безопасности по окончании работы

- доложить руководителю занятий или лаборанту о завершении работ;
- привести в порядок и сдать рабочее место лаборанту, и доложить руководителю занятий о сдаче.

Аппаратное обеспечение

Класс персональных ЭВМ, электронная доска, проектор.

Программное обеспечение

В комплекте с персональными ЭВМ. Доступ к Интернет. Офисный пакет.

Литература

- 5) Технологии обеспечения безопасности информационных систем: учебное пособие: А. Л. Марухленко, Л. О. Марухленко, М. А. Ефремов [и др.]. – Москва; Берлин: Директ-Медиа, 2021. – 209 с.
- 6) Баланов А. Н. Защита информационных систем. Кибербезопасность: учебное пособие для вузов / А. Н. Баланов. — Санкт-Петербург: Лань, 2024. — 280 с.

- 7) Ховард Рик. Кибербезопасность: главные принципы. — СПб.: Питер, 2024. — 320 с.: ил.
- 8) Анализ пакетов: практическое руководство по использованию Wireshark и tcpdump для решения реальных проблем в локальных сетях, 3-е изд. : Пер. с англ. — СПб. : ООО “Диалектика”, 2019 — 448с. : ил. — Парал.тит.англ. ISBN 978-5-6040723-01 (рус.)

Теоретическая часть

Современные компьютерные сети являются основой функционирования информационных систем. Передача данных между устройствами осуществляется в виде сетевых пакетов, которые передаются по различным протоколам связи. Для обеспечения безопасности и стабильной работы сети необходимо контролировать и анализировать сетевой трафик. Сетевое наблюдение (network monitoring) представляет собой процесс сбора, анализа и интерпретации данных о сетевом трафике. Основной задачей сетевого наблюдения является выявление аномалий, диагностика сетевых проблем, а также обнаружение возможных инцидентов информационной безопасности. Для анализа сетевого трафика используются специальные программные средства – анализаторы сетевого трафика. Одним из наиболее распространённых инструментов данного типа является программа Wireshark. Она позволяет выполнять захват сетевых пакетов, просматривать их содержимое, анализировать используемые протоколы и исследовать структуру передаваемых данных.

Передача информации в сети осуществляется по определённым сетевым протоколам. Протоколы определяют правила обмена данными между устройствами. К наиболее распространённым протоколам относятся IP, TCP, UDP, DNS, HTTP и HTTPS. Каждый пакет содержит служебную информацию, такую как адрес отправителя и получателя, номер порта, тип протокола и другие параметры, необходимые для корректной передачи данных. Анализ сетевых пакетов позволяет определить источник сетевого соединения, тип передаваемой информации, а также выявить подозрительную активность. Например, большое количество запросов к одному серверу, необычные

сетевые соединения или передача данных по нестандартным портам могут свидетельствовать о возможной атаке или сетевом инциденте.

В процессе анализа сетевого трафика важную роль играет фильтрация пакетов. Фильтрация позволяет выделять из общего потока трафика только те пакеты, которые соответствуют заданным условиям, например определённому протоколу или IP-адресу. Это значительно упрощает поиск необходимой информации и ускоряет анализ сетевых данных.

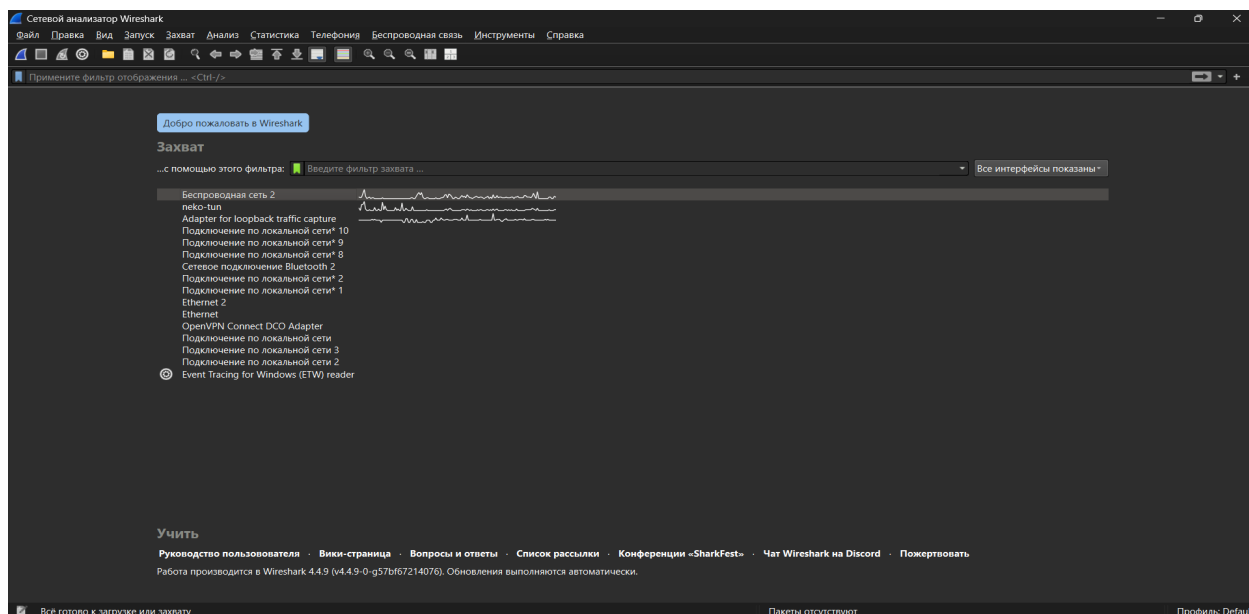
Одной из угроз информационной безопасности является перехват сетевого трафика с помощью специальных программ – сетевых снифферов. Сниффер представляет собой программное средство, которое позволяет перехватывать и анализировать сетевые пакеты, передаваемые по сети. В легальных условиях такие инструменты используются администраторами для диагностики и мониторинга сети. Однако злоумышленники могут применять снифферы для получения конфиденциальной информации, например логинов, паролей или других данных. Для защиты от перехвата сетевого трафика используются различные методы. Одним из основных способов является использование защищённых протоколов передачи данных, таких как HTTPS, которые применяют криптографические методы шифрования информации. Также используются виртуальные частные сети (VPN), позволяющие создавать защищённые каналы связи между устройствами. Дополнительными мерами защиты являются использование систем обнаружения вторжений, сегментация сети и контроль доступа к сетевой инфраструктуре.

Таким образом, анализ сетевого трафика является важным инструментом обеспечения информационной безопасности. Использование средств мониторинга позволяет своевременно обнаруживать сетевые инциденты, выявлять подозрительную активность и принимать меры по защите информационных систем.

Практическая часть

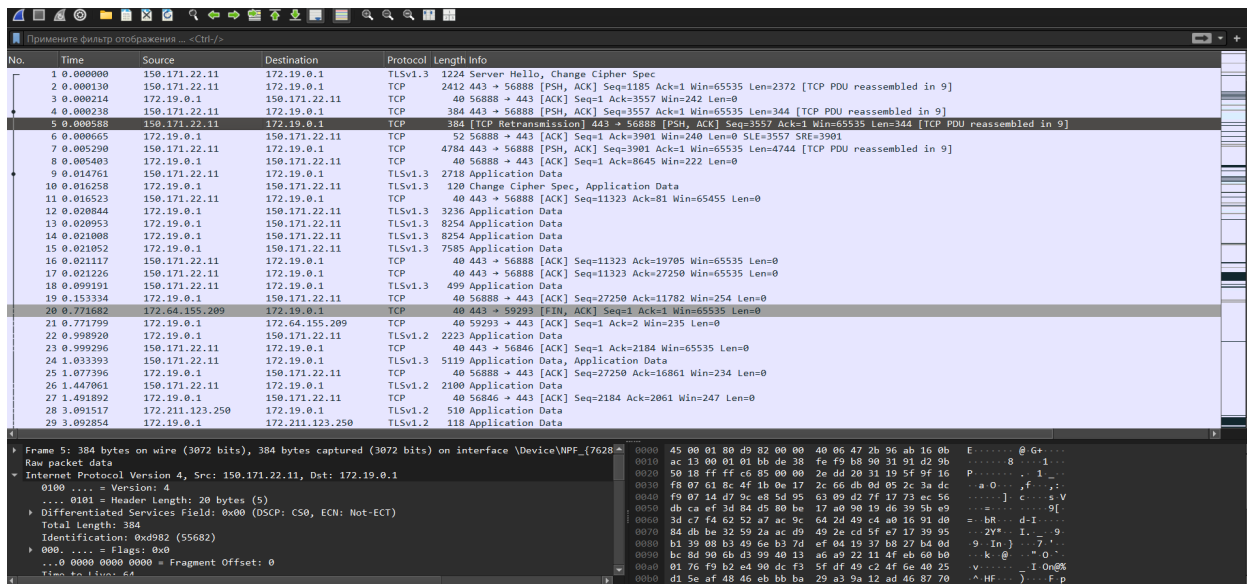
Задание 1. Ознакомление с анализатором трафика

- 1) Установить и запустить программу Wireshark.
- 2) Просмотреть список доступных сетевых интерфейсов.
- 3) Определить, какой интерфейс используется для подключения к интернету. (Выполнить ping 8.8.8.8)



Задание 2. Захват сетевого трафика

- 1) Выбрать активный сетевой интерфейс.
- 2) Запустить захват трафика.
- 3) Открыть любой сайт.
- 4) Остановить захват трафика спустя пару минут.



Задание 3. Фильтрация сетевого трафика

- 1) Использовать фильтр для отображения только DNS-запросов.
- 2) Найти DNS-запрос, связанный с посещенным сайтом.

Полученные данные записать в таблицу 1.

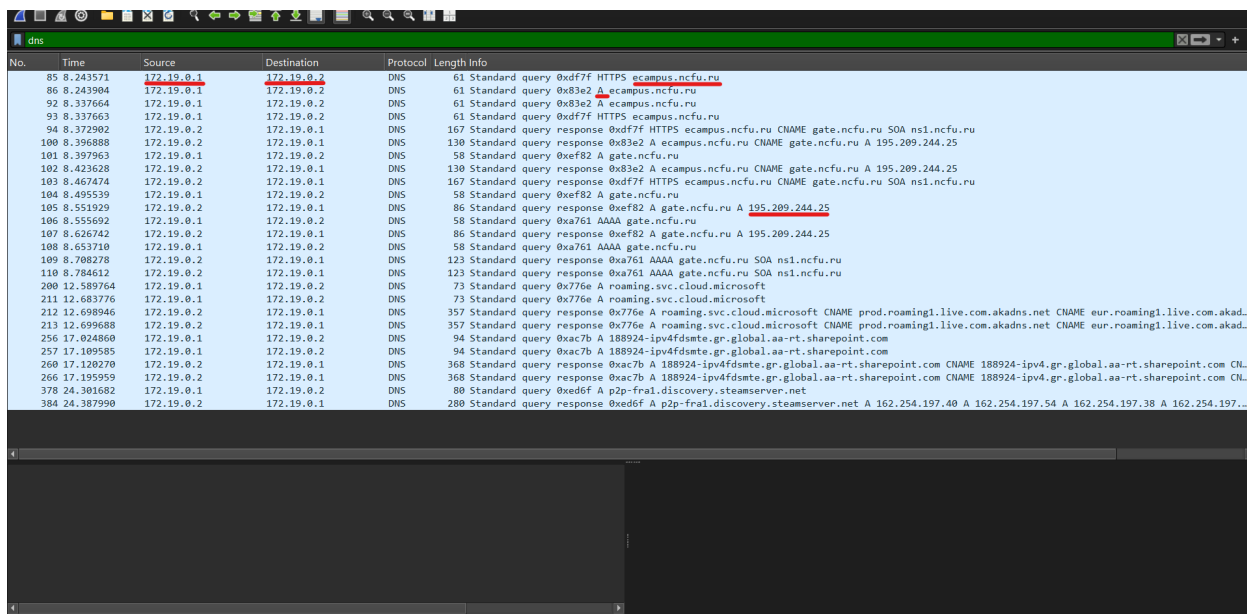


Таблица 1 – DNS фильтрация

IP клиента	IP DNS сервера	Доменное имя	Тип DNS записи	IP адрес ответа
172.19.0.1	172.19.0.2	ecampus.ncfu.ru	A	195.209.244.25

Задание 4. Анализ структуры пакета

- 1) Выбрать любой пакет из списка пакетов

2) Изучить его структуру в Wireshark (IP-адрес отправителя/получателя, используемый протокол)

```
▼ Frame 403: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{1E353D9F-9CB8-4664-93D1-7A792BD42CB2}
  Section number: 1
  ▼ Interface id: 0 (\Device\NPF_{1E353D9F-9CB8-4664-93D1-7A792BD42CB2})
    Interface name: \Device\NPF_{1E353D9F-9CB8-4664-93D1-7A792BD42CB2}
    Interface description: Беспроводная сеть 2
    Encapsulation type: Ethernet (1)
    Arrival Time: Apr  6, 2026 18:31:46.989749000 RTZ 2 (зима)
    UTC Arrival Time: Apr  6, 2026 15:31:46.989749000 UTC
    Epoch Arrival Time: 1775489506.989749000
    [Time shift for this packet: 0.000000000 seconds]
    [Time delta from previous captured frame: 0.002315000 seconds]
    [Time delta from previous displayed frame: 0.002315000 seconds]
    [Time since reference or first frame: 4.968561000 seconds]
    Frame Number: 403
    Frame Length: 66 bytes (528 bits)
    Capture Length: 66 bytes (528 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp]
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80 || http2]
  ▶ Ethernet II, Src: Intel_cb:b2:d1 (e0:c2:64:cb:b2:d1), Dst: Keenetic_8d:fd:db (50:ff:20:8d:fd:db)
  ▶ Internet Protocol Version 4, Src: 192.168.1.114, Dst: 91.108.56.114
  ▶ Transmission Control Protocol, Src Port: 57691, Dst Port: 80, Seq: 0, Len: 0
```

IP отправителя	IP получателя	MAC адрес получателя	Протокол
192.168.1.114	91.108.56.114	ff:ff:ff:ff:ff:ff	TCP

Контрольные вопросы:

- 1) Что такое анализатор сетевого трафика?
- 2) Для каких задач используется Wireshark?
- 3) Что такое сетевой интерфейс?
- 4) Почему для анализа трафика необходимо выбрать активный интерфейс?
- 5) Что называется сетевым пакетом?
- 6) Что такое фильтрация сетевого трафика?
- 7) Что такое DNS-запрос?
- 8) Чем отличается протокол HTTP от HTTPS?

Лабораторная работа №7-8

Тема: Планирование системы управления инцидентами неавторизованного доступа. Использование системы управления инцидентами неавторизованного доступа

Цель занятия

1. Закрепление материала, полученного на лекционных занятиях.
2. Приобретение практических навыков по установке, настройке и использованию системы обнаружения вторжений **Snort**.
3. Формирование навыков выявления, анализа и интерпретации событий и инцидентов информационной безопасности на основе сетевого трафика.
4. Освоение методов создания и применения правил обнаружения подозрительной и потенциально вредоносной сетевой активности.

Подготовка к занятию

1. Изучить (повторить) теоретический материал лекций и рекомендованную литературу по теме систем обнаружения вторжений (IDS/IPS).
2. Изучить принципы работы системы Snort, ее архитектуру, режимы функционирования и область применения.
3. Ознакомиться с методическими рекомендациями по выполнению практического задания.
4. Подготовить виртуальную или физическую лабораторную среду для установки и тестирования Snort.

Учебные вопросы

1. Установка и базовая настройка системы обнаружения вторжений **Snort**.
2. Настройка и редактирование правил обнаружения сетевых атак и подозрительных событий.
3. Исследование и анализ результатов работы Snort при мониторинге сетевого трафика.

4. Выявление признаков события и инцидента информационной безопасности на основе сработавших правил.

Основные теоретические сведения

Основные теоретические сведения изложены в материалах лекций и по данной тематике и рекомендуемой литературе.

Правила работы в лаборатории

К работе в лаборатории допускаются лица, изучившие правила и меры безопасности, сдавшие зачет по ним и усвоившие порядок выполнения практического занятия.

Требования безопасности перед началом работ

- ЗАПРЕЩАЕТСЯ: переодеваться, пользоваться огнем, курить, принимать пищу в лаборатории;
- убедиться в целостности электрических розеток и разъемов. В лаборатории необходимо быть в сменной обуви;
- включение компьютера производить только после получения допуска по выполняемой работе и разрешения преподавателя или лаборанта.

Требования безопасности во время работы

- выполняя практическое занятие, студенты обязаны использовать только вычислительную технику, периферийное оборудование, соединительные кабели, измерительное оборудование и носители информации, непосредственно относящиеся к данному практическому занятию;
- подключение и отключение составляющих вычислительного комплекса производить только при полном снятии напряжения со всех составляющих вычислительного комплекса;
- при обнаружении неисправностей в оборудовании немедленно отключить источники питания и доложить об этом руководителю занятий или лаборанту.

Требования безопасности по окончании работы

- доложить руководителю занятий или лаборанту о завершении работ;
- привести в порядок и сдать рабочее место лаборанту, и доложить руководителю занятий о сдаче.

Аппаратное обеспечение

Класс персональных ЭВМ, электронная доска, проектор.

Программное обеспечение

В комплекте с персональными ЭВМ. Доступ к Интернет. Офисный пакет.

Литература

- 9) Технологии обеспечения безопасности информационных систем: учебное пособие: А. Л. Марухленко, Л. О. Марухленко, М. А. Ефремов [и др.]. – Москва; Берлин: Директ-Медиа, 2021. – 209 с.
- 10) Баланов А. Н. Защита информационных систем. Кибербезопасность: учебное пособие для вузов / А. Н. Баланов. — Санкт-Петербург: Лань, 2024. — 280 с.
- 11) Ховард Рик. Кибербезопасность: главные принципы. — СПб.: Питер, 2024. — 320 с.: ил.

Теоретическая часть

Система обнаружения вторжений (Intrusion Detection System, IDS) – это программно-аппаратный комплекс, предназначенный для выявления признаков несанкционированной, подозрительной или вредоносной активности в информационной системе или сети.

IDS позволяет:

1. анализировать сетевой трафик;
2. выявлять известные атаки;
3. обнаруживать аномалии;
4. регистрировать события безопасности;
5. оповещать администратора о потенциальных угрозах.

Snort – это одна из наиболее распространенных открытых систем обнаружения вторжений, предназначенная для анализа сетевого трафика в режиме реального времени.

Snort может использоваться:

1. как сниффер сетевого трафика;
2. как логгер пакетов;
3. как система обнаружения вторжений на основе сигнатур.



Рисунок 1 – Архитектура Snort

Алгоритм работы Snort следующий:

1. Встроенная в Snort библиотека libpcap перехватывает сетевой пакет, поступающий на устройство.
2. Декодер преобразовывает полученный пакет в данные.
3. Препроцессор получает данные от декодера и готовит их к дальнейшей отправке детектору.
4. Детектор принимает данные от препроцессора и анализирует их, сопоставляя с правилами, в которых описаны необходимые действия для работы с пакетами, и сигнатурами из базы данных.

Среди достоинств Snort можно выделить:

Обширную поддержку протоколов и сервисов. Snort выявляет атаки на протоколы TCP, UDP, ICMP, ARP, IGRP, GRE, OSPF, RIP, IPX, SMTP, IMAP, POP3, Telnet, DNS, FTP, работает с сервисами Apache, Nginx, IIS, серверами баз данных – Microsoft SQL Server, Oracle Database и другими.

1. Поддержку более 200 плагинов для расширения работы Snort.
2. Функционал для работы с правилами. Можно использовать готовые правила и писать свои.

3. Кросс-платформенность. Установить и использовать Snort можно на любой ОС — Windows, macOS, Linux/Unix.

4. Открытый исходный код.

Практическая часть

Установим Snort (рис. 2), откроем терминал и перейдем в папку, где Snort установлен, вызовем команду `snort -w`, тем самым отобразив доступные интерфейсы (рис. 3).

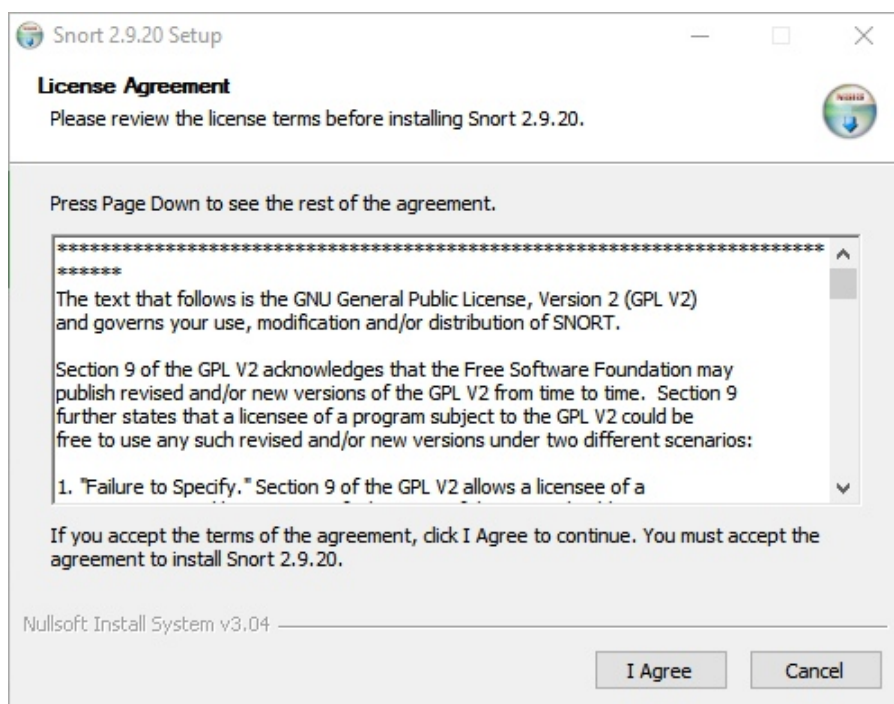


Рисунок 2 – Установка Snort

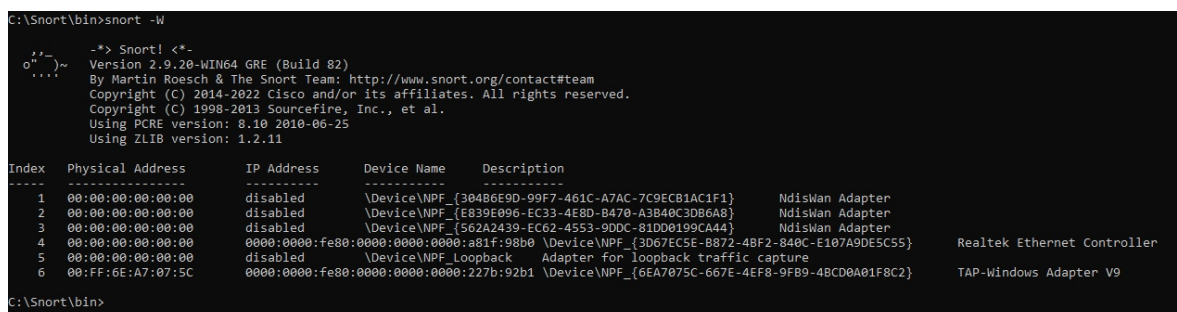


Рисунок 3 – Доступные интерфейсы

```
C:\Snort\bin>snort -v -i 4 -n 3
Exiting after 3 packets
Running in packet dump mode

    --- Initializing Snort ---
Initializing Output Plugins!
pcap DAQ configured to passive.
The DAQ version does not support reload.
Acquiring network traffic from "\Device\NPF_{3D67EC5E-B872-4BF2-840C-E107A9DE5C55}".
Decoding Ethernet

    --- Initialization Complete ---

    ,,_      -*> Snort! <*-
    o"_)~    Version 2.9.20-WIN64 GRE (Build 82)
    '...'    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
            Copyright (C) 2014-2022 Cisco and/or its affiliates. All rights reserved.
            Copyright (C) 1998-2013 Sourcefire, Inc., et al.
            Using PCRE version: 8.10 2010-06-25
            Using ZLIB version: 1.2.11

Commencing packet processing (pid=19364)
WARNING: No preprocessors configured for policy 0.
12/04-16:29:08.305041 192.168.1.5:57249 -> 87.240.129.180:443
TCP TTL:222 TOS:0x0 ID:64667 IpLen:20 DgmLen:91 DF
***AP*** Seq: 0xD5B63D3D Ack: 0xBB04FCCC Win: 0x201 TcpLen: 32
TCP Options (3) => NOP NOP TS: 680323221 1123387035
+++++

WARNING: No preprocessors configured for policy 0.
12/04-16:29:08.305144 192.168.1.5:57255 -> 87.240.185.169:443
TCP TTL:222 TOS:0x0 ID:34643 IpLen:20 DgmLen:91 DF
***AP*** Seq: 0x3EC9D33E Ack: 0xB5EC2A5B Win: 0x1FF TcpLen: 32
TCP Options (3) => NOP NOP TS: 680323221 456310117
+++++

WARNING: No preprocessors configured for policy 0.
12/04-16:29:08.315184 87.240.185.169:443 -> 192.168.1.5:57255
TCP TTL:58 TOS:0x0 ID:14898 IpLen:20 DgmLen:52 DF
***A*** Seq: 0xB5EC2A5B Ack: 0x3EC9D365 Win: 0x15 TcpLen: 32
TCP Options (3) => NOP NOP TS: 456368130 680323221
+++++

=====
Run time for packet processing was 4.60000 seconds
Snort processed 3 packets.
Snort ran for 0 days 0 hours 0 minutes 4 seconds
Pkts/sec:      0
=====
Packet I/O Totals:
  Received:      8
  Analyzed:      3 ( 37.500%)
  Dropped:       0 (  0.000%)
  Filtered:      0 (  0.000%)
  Outstanding:   5 ( 62.500%)
  Injected:      0
=====
Breakdown by protocol (includes rebuilt packets):
  Eth:           3 (100.000%)
  VLAN:          0 (  0.000%)
  IP4:           3 (100.000%)
  Frag:          0 (  0.000%)
  ICMP:          0 (  0.000%)
```

Отправим командой `ping` несколько пакетов на любой узел сети (рис. 5). Убедимся, что Snort перехватывает пакеты и отображает их (рис. 6).

```

C:\Users>ping ya.ru

Обмен пакетами с ya.ru [87.250.250.242] с 32 байтами данных:
Ответ от 87.250.250.242: число байт=32 время=6мс TTL=248
Ответ от 87.250.250.242: число байт=32 время=5мс TTL=248
Ответ от 87.250.250.242: число байт=32 время=6мс TTL=248
Ответ от 87.250.250.242: число байт=32 время=5мс TTL=248

Статистика Ping для 87.250.250.242:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 5мсек, Максимальное = 6 мсек, Среднее = 5 мсек

C:\Users>

```

Рисунок 5 – ping удаленного узла сети

```

+++++
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
12/04-16:27:04.429248 192.168.1.5 -> 87.250.250.242
ICMP TTL:222 TOS:0x0 ID:20344 IpLen:20 DgmLen:60
Type:8 Code:0 ID:1 Seq:5 ECHO
+++++

WARNING: No preprocessors configured for policy 0.
12/04-16:27:04.435476 87.250.250.242 -> 192.168.1.5
ICMP TTL:248 TOS:0x0 ID:24269 IpLen:20 DgmLen:60
Type:0 Code:0 ID:1 Seq:5 ECHO REPLY
+++++

WARNING: No preprocessors configured for policy 0.
12/04-16:27:05.444573 192.168.1.5 -> 87.250.250.242
ICMP TTL:222 TOS:0x0 ID:20345 IpLen:20 DgmLen:60
Type:8 Code:0 ID:1 Seq:6 ECHO
+++++

WARNING: No preprocessors configured for policy 0.
12/04-16:27:05.450261 87.250.250.242 -> 192.168.1.5
ICMP TTL:248 TOS:0x0 ID:24485 IpLen:20 DgmLen:60
Type:0 Code:0 ID:1 Seq:6 ECHO REPLY
+++++

WARNING: No preprocessors configured for policy 0.
12/04-16:27:06.457105 192.168.1.5 -> 87.250.250.242
ICMP TTL:222 TOS:0x0 ID:20346 IpLen:20 DgmLen:60
Type:8 Code:0 ID:1 Seq:7 ECHO
+++++

WARNING: No preprocessors configured for policy 0.
12/04-16:27:06.462860 87.250.250.242 -> 192.168.1.5
ICMP TTL:248 TOS:0x0 ID:24719 IpLen:20 DgmLen:60
Type:0 Code:0 ID:1 Seq:7 ECHO REPLY
+++++

```

Рисунок 6 – Перехват и вывод пакетов, отправленных при помощи ping

Добавим свой конфигурационный файл `my.conf`, и запишем правило для обнаружения входящих ECHO запросов (рис. 7).

```

my.conf – Блокнот
Файл Правка Формат Вид Справка
var HOME_NET 192.168.1.5
var EXTERNAL_NET !$HOME_NET

alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg: "Incoming ECHO request"; sid: 1; itype: 8;)

```

Рисунок 7 – Конфигурационный файл

Запустим Snort с необходимыми параметрами и укажем вывод в лог-файл (рис. 8).

```

C:\Snort\bin>snort -i 4 -c ../etc/my.conf -l ../log
Running in IDS mode

==== Initializing Snort ====
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "../etc/my.conf"
Tagged Packet Limit: 256
Log directory = ../log

+++++
Initializing rule chains...
1 Snort rules read
  1 detection rules
  0 decoder rules
  0 preprocessor rules
1 Option Chains linked into 1 Chain Headers
+++++

+-----[Rule Port Counts]-----+
|      tcp      udp      icmp      ip      |
|  src      0      0      0      0      |
|  dst      0      0      0      0      |
|  any      0      0      1      0      |
|  nc       0      0      1      0      |
|  s+d      0      0      0      0      |
+-----+

+-----[detection-filter-config]-----+
| memory-cap : 1048576 bytes
+-----[detection-filter-rules]-----+
| none
+-----+

+-----[rate-filter-config]-----+
| memory-cap : 1048576 bytes
+-----[rate-filter-rules]-----+
| none
+-----+

+-----[event-filter-config]-----+
| memory-cap : 1048576 bytes
+-----[event-filter-global]-----+
+-----[event-filter-local]-----+
| none
+-----[suppression]-----+
| none
+-----+

Rule application order: pass->drop->sdrop->reject->alert->log
Verifying Preprocessor Configurations!

[ Port Based Pattern Matching Memory ]
pcap DAQ configured to passive.
The DAQ version does not support reload.
Acquiring network traffic from "\\Device\\NPF_{3D67EC5E-B872-4BF2-840C-E107A9DE5C55}".
Decoding Ethernet

```

Рисунок 8 – Запуск Snort с конфигурационным файлом и лог-файлом

С другого компьютера в сети выполним ЕСНО запрос на наш компьютер. Убедимся, что в логе выводится нужная информация (рис. 9).

```
C:\Snort\bin>snort -r ../log/snort.log.1670161555
Running in packet dump mode

==== Initializing Snort ====
Initializing Output Plugins!
pcap DAQ configured to read-file.
The DAQ version does not support reload.
Acquiring network traffic from "../log/snort.log.1670161555".

==== Initialization Complete ====

o" )~
'...'
-*)> Snort! <*-
Version 2.9.20-WIN64 GRE (Build 82)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014-2022 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using PCRE version: 8.10 2010-06-25
Using ZLIB version: 1.2.11

Commencing packet processing (pid=15664)
WARNING: No preprocessors configured for policy 0.
12/04-16:45:57.840132 192.168.1.7 -> 192.168.1.5
ICMP TTL:64 TOS:0x0 ID:53546 IpLen:20 DgmLen:84
Type:8 Code:0 ID:54537 Seq:0 ECHO
=====
WARNING: No preprocessors configured for policy 0.
12/04-16:45:58.835950 192.168.1.7 -> 192.168.1.5
ICMP TTL:64 TOS:0x0 ID:28599 IpLen:20 DgmLen:84
Type:8 Code:0 ID:54537 Seq:1 ECHO
=====
WARNING: No preprocessors configured for policy 0.
12/04-16:45:59.844472 192.168.1.7 -> 192.168.1.5
ICMP TTL:64 TOS:0x0 ID:8481 IpLen:20 DgmLen:84
Type:8 Code:0 ID:54537 Seq:2 ECHO
=====
WARNING: No preprocessors configured for policy 0.
12/04-16:46:00.836524 192.168.1.7 -> 192.168.1.5
ICMP TTL:64 TOS:0x0 ID:5544 IpLen:20 DgmLen:84
Type:8 Code:0 ID:54537 Seq:3 ECHO
=====
WARNING: No preprocessors configured for policy 0.
12/04-16:46:01.839754 192.168.1.7 -> 192.168.1.5
ICMP TTL:64 TOS:0x0 ID:42356 IpLen:20 DgmLen:84
Type:8 Code:0 ID:54537 Seq:4 ECHO
=====

=====
Run time for packet processing was 0.39000 seconds
Snort processed 5 packets.
Snort ran for 0 days 0 hours 0 minutes 0 seconds
Pkts/sec: 5
=====
Packet I/O Totals:
Received: 5
Analyzed: 5 (100.000%)
Dropped: 0 ( 0.000%)
Filtered: 0 ( 0.000%)
Outstanding: 0 ( 0.000%)
```

Рисунок 9 – Вывод лог-файла

Дополним конфигурационный файл несколькими правилами (рис. 10)

```

my.conf - Блокнот
Файл Правка Формат Вид Справка
var HOME_NET 192.168.1.5
var EXTERNAL_NET !$HOME_NET

alert icmp $EXTERNAL_NET any -> $HOME_NET any (msg: "Incoming ECHO request"; sid: 1; itype: 8;)

preprocessor flow: stats_interval 0 hash 2
preprocessor sfportscan: proto { all } scan_type { all } sense_level { medium } logfile { portscan.log }

```

Рисунок 10 - Обновленный файл конфигурации

Установим утилиту nmap (рис. 11) и сделаем с помощью неё 4 сканирования.

```

C:\Program Files (x86)\Nmap>nmap
Nmap 7.93 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
  -sY/sZ: SCTP INIT/COOKIE-ECHO scans
  -sO: IP protocol scan
  -b <FTP relay host>: FTP bounce scan
PORT SPECIFICATION AND SCAN ORDER:
  -p <port ranges>: Only scan specified ports
  Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
  --exclude-ports <port ranges>: Exclude the specified ports from scanning
  -F: Fast mode - Scan fewer ports than the default scan
  -r: Scan ports sequentially - don't randomize
  --top-ports <number>: Scan <number> most common ports
  --port-ratio <ratio>: Scan ports more common than <ratio>
SERVICE/VERSION DETECTION:
  -sV: Probe open ports to determine service/version info
  --version-intensity <level>: Set from 0 (light) to 9 (try all probes)
  --version-light: Limit to most likely probes (intensity 2)
  --version-all: Try every single probe (intensity 9)
  --version-trace: Show detailed version scan activity (for debugging)
SCRIPT SCAN:
  -sC: equivalent to --script=default
  --script=<Lua scripts>: <Lua scripts> is a comma separated list of
    directories, script-files or script-categories
  --script-args=<n1=v1,[n2=v2,...]>: provide arguments to scripts
  --script-args-file=filename: provide NSE script args in a file
  --script-trace: Show all data sent and received
  --script-updatedb: Update the script database.
  --script-help=<Lua scripts>: Show help about scripts.
    <Lua scripts> is a comma-separated list of script-files or
    script-categories.

```

Рисунок 11 – Утилита nmap

```

C:\Program Files (x86)\Nmap>nmap 192.168.1.5 -v -sN -p 0-65535
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-04 17:12 RTZ 2 (чшър)
Initiating NULL Scan at 17:12
Scanning host.docker.internal (192.168.1.5) [65536 ports]
Completed NULL Scan at 17:12, 5.20s elapsed (65536 total ports)
Nmap scan report for host.docker.internal (192.168.1.5)
Host is up (0.00046s latency).
Not shown: 65535 closed tcp ports (reset)
PORT      STATE      SERVICE
137/tcp   open|filtered netbios-ns

Read data files from: C:\Program Files (x86)\Nmap
Nmap done: 1 IP address (1 host up) scanned in 5.41 seconds
Raw packets sent: 65537 (2.621MB) | Rcvd: 131072 (5.243MB)

C:\Program Files (x86)\Nmap>nmap 192.168.1.5 -v -sS -p 0-65535
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-04 17:30 RTZ 2 (чшър)
Initiating SYN Stealth Scan at 17:30
Scanning host.docker.internal (192.168.1.5) [65536 ports]
Discovered open port 445/tcp on 192.168.1.5
Discovered open port 139/tcp on 192.168.1.5
Discovered open port 80/tcp on 192.168.1.5
Discovered open port 443/tcp on 192.168.1.5
Discovered open port 135/tcp on 192.168.1.5
Discovered open port 49664/tcp on 192.168.1.5
Discovered open port 49690/tcp on 192.168.1.5
Discovered open port 912/tcp on 192.168.1.5
Discovered open port 61983/tcp on 192.168.1.5
Discovered open port 20008/tcp on 192.168.1.5
Discovered open port 5357/tcp on 192.168.1.5
Discovered open port 102/tcp on 192.168.1.5
Discovered open port 27036/tcp on 192.168.1.5
Discovered open port 49667/tcp on 192.168.1.5
Discovered open port 49666/tcp on 192.168.1.5
Discovered open port 5040/tcp on 192.168.1.5
Discovered open port 902/tcp on 192.168.1.5
Discovered open port 49665/tcp on 192.168.1.5
Completed SYN Stealth Scan at 17:30, 5.32s elapsed (65536 total ports)
Nmap scan report for host.docker.internal (192.168.1.5)
Host is up (0.00059s latency).
Not shown: 65517 closed tcp ports (reset)
PORT      STATE      SERVICE
80/tcp    open       http
102/tcp   open       iso-tsap
135/tcp   open       msrpc
137/tcp   filtered  netbios-ns
139/tcp   open       netbios-ssn
443/tcp   open       https
445/tcp   open       microsoft-ds
902/tcp   open       iss-realscure
912/tcp   open       apex-mesh
5040/tcp  open       unknown
5357/tcp  open       wsdapi
20008/tcp open       unknown
27036/tcp open       unknown
49664/tcp open       unknown
49665/tcp open       unknown
49666/tcp open       unknown
49667/tcp open       unknown
49690/tcp open       unknown
61983/tcp open       unknown

Read data files from: C:\Program Files (x86)\Nmap

```

Рисунок 12 – Сканирование пакета при помощи ТСР пакета со сброшенными флагами и сканирование с неполным циклом подключения

```

C:\Program Files (x86)\Nmap>nmap 192.168.1.5 -v -sX -p 0-65535
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-04 17:30 RTZ 2 (чшьр)
Initiating XMAS Scan at 17:30
Scanning host.docker.internal (192.168.1.5) [65536 ports]
Completed XMAS Scan at 17:31, 5.30s elapsed (65536 total ports)
Nmap scan report for host.docker.internal (192.168.1.5)
Host is up (0.0011s latency).
Not shown: 65535 closed tcp ports (reset)
PORT      STATE      SERVICE
137/tcp   open|filtered netbios-ns

Read data files from: C:\Program Files (x86)\Nmap
Nmap done: 1 IP address (1 host up) scanned in 5.52 seconds
Raw packets sent: 65537 (2.621MB) | Rcvd: 131072 (5.243MB)

C:\Program Files (x86)\Nmap>nmap 192.168.1.5 -v -sT -p 0-65535
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-04 17:31 RTZ 2 (чшьр)
Initiating Connect Scan at 17:31
Scanning host.docker.internal (192.168.1.5) [65536 ports]
Discovered open port 80/tcp on 192.168.1.5
Discovered open port 139/tcp on 192.168.1.5
Discovered open port 443/tcp on 192.168.1.5
Discovered open port 135/tcp on 192.168.1.5
Discovered open port 445/tcp on 192.168.1.5
Connect Scan Timing: About 1.06% done; ETC: 18:19 (0:48:12 remaining)
Discovered open port 49667/tcp on 192.168.1.5
Connect Scan Timing: About 4.53% done; ETC: 18:19 (0:45:42 remaining)
Discovered open port 49690/tcp on 192.168.1.5

```

Рисунок 13 – Сканирование при помощи TCP пакета со всеми установленными флагами и сканирование с полным циклом подключения

Просмотрим лог-файл, он обновился при сканировании с полным циклом подключения (рис. 14). Соответственно, этот метод позволяет практически выявить наличие открытых портов.

```

portscan.log – Блокнот
Файл  Правка  Формат  Вид  Справка
Time: 12/04-17:32:04.484349
event_ref: 0
192.168.1.5 -> 95.163.52.67 (portscan) TCP Filtered Portsweep
Priority Count: 0
Connection Count: 30
IP Count: 29
Scanned IP Range: 87.240.132.72:217.20.155.57
Port/Proto Count: 2
Port/Proto Range: 80:443

```

Рисунок 14 – Лог-файл portscan

Лабораторная работа №9-10

Тема: Управление инцидентами отказа в обслуживании. Планирование системы управления инцидентами отказа в обслуживании.

Цель занятия

1. Закрепление теоретических знаний о принципах применения обманных систем (deception technologies) для выявления и анализа инцидентов информационной безопасности.
2. Изучение методов обнаружения подозрительной и вредоносной активности с использованием систем типа Honeypot и Padded Cell.
3. Освоение практических навыков по анализу действий потенциального нарушителя, выявлению признаков атаки и регистрации событий информационной безопасности в контролируемой среде.

Подготовка к занятию

1. Изучить (повторить) теоретические сведения о назначении, архитектуре и принципах работы обманных систем в области информационной безопасности.
2. Ознакомиться с основными типами honeypot-систем, уровнями взаимодействия и особенностями применения технологии Padded Cell.
3. Изучить методы обнаружения инцидентов на основе анализа поведения, атакующего в изолированной или эмулированной среде.
4. Ознакомиться с программными средствами, используемыми для развёртывания и анализа работы honeypot-систем.

Учебные вопросы

1. Изучить основные принципы функционирования обманных систем типа Honeypot и Padded Cell.
2. Рассмотреть особенности применения honeypot-систем для выявления несанкционированного доступа, сканирования и попыток эксплуатации уязвимостей.

3. Изучить возможности использования технологии Padded Cell для перенаправления злоумышленника в контролируемую среду.

Основные теоретические сведения изложены в материалах лекций и по данной тематике и рекомендуемой литературе.

Правила работы в лаборатории

К работе в лаборатории допускаются лица, изучившие правила и меры безопасности, сдавшие зачет по ним и усвоившие порядок выполнения практического занятия.

Требования безопасности перед началом работ

- ЗАПРЕЩАЕТСЯ: переодеваться, пользоваться огнем, курить, принимать пищу в лаборатории;
- убедиться в целостности электрических розеток и разъемов. В лаборатории необходимо быть в сменной обуви;
- включение компьютера производить только после получения допуска по выполняемой работе и разрешения преподавателя или лаборанта.

Требования безопасности во время работы

- выполняя практическое занятие, студенты обязаны использовать только вычислительную технику, периферийное оборудование, соединительные кабели, измерительное оборудование и носители информации, непосредственно относящиеся к данному практическому занятию;
- подключение и отключение составляющих вычислительного комплекса производить только при полном снятии напряжения со всех составляющих вычислительного комплекса;
- при обнаружении неисправностей в оборудовании немедленно отключить источники питания и доложить об этом руководителю занятий или лаборанту.

Требования безопасности по окончании работы

- доложить руководителю занятий или лаборанту о завершении работ;
- привести в порядок и сдать рабочее место лаборанту, и доложить руководителю занятий о сдаче.

Аппаратное обеспечение

Класс персональных ЭВМ, электронная доска, проектор.

Программное обеспечение

В комплекте с персональными ЭВМ. Доступ к Интернет. Офисный пакет.

Литература

- 12) Технологии обеспечения безопасности информационных систем: учебное пособие: А. Л. Марухленко, Л. О. Марухленко, М. А. Ефремов [и др.]. – Москва; Берлин: Директ-Медиа, 2021. – 209 с.
- 13) Баланов А. Н. Защита информационных систем. Кибербезопасность: учебное пособие для вузов / А. Н. Баланов. — Санкт-Петербург: Лань, 2024. — 280 с.
- 14) Ховард Рик. Кибербезопасность: главные принципы. — СПб.: Питер, 2024. — 320 с.:

Теоретическая часть:

Honey Pot и Padded Cell

Honey Pot (Система-ловушка) – это специализированная система, предназначенная для привлечения потенциальных злоумышленников и их отвлечения от реально уязвимых критических систем организации.

Основные цели использования Honey Pot:

- Отвлечение: перенаправление внимания атакующего от ценных ресурсов.
- Сбор информации: изучение методов и инструментов, используемых хакером.
- Фиксация следов: создание условий, при которых злоумышленник оставляет достаточно доказательств своей деятельности.

Системы Honey Pot наполняются ложной информацией, которая выглядит ценной для атакующего. Важной особенностью является то, что легитимные пользователи не должны иметь доступа к этой системе, поэтому любое обращение к Honey Pot априори считается подозрительным. Внутри ловушки устанавливаются мониторы уязвимостей и логгеры событий для детальной фиксации действий.

Padded Cell (Изолированная ячейка) – это развитие концепции ловушек, работающее в тесном взаимодействии с традиционной системой обнаружения вторжений (IDS).

- Механизм работы: когда IDS обнаруживает атаку, она не просто блокирует её, а незаметно перенаправляет злоумышленника в специальную эмулированную среду (Padded Cell).

- Безопасность: внутри такой «ячейки» атакующий находится в контролируемом окружении, где он не может причинить вред реальной сети.

- Иллюзия успеха: среда наполнена интересными данными, чтобы убедить взломщика, что его атака проходит успешно и он находится в реальной системе.

Преимущества и недостатки:

- Плюсы: администраторы получают дополнительное время для принятия решений, а действия атакующего можно детально проанализировать для улучшения общей системы защиты. Honey Pot также эффективны для выявления внутренних нарушителей, сканирующих сеть.

- Минусы: использование таких систем требует высокой квалификации администратора. Существует риск, что опытный хакер, поняв, что он в ловушке, станет более агрессивным. Кроме того, законодательные аспекты использования подобных систем не всегда четко определены.

Практическая часть

Прочитайте приведённый ниже материал. Представьте, как настраивается honeypot, какие действия он фиксирует, и как анализируются результаты. Выполнение команд в Linux не требуется.

1) Установка Honeyd

sudo apt-get install honeyd

2) Настройка Honeyd

- Настройка происходит через файл конфигурации honeyd.conf (обычно находится в /etc/honeypot/honeyd.conf).

- Можно использовать стандартный файл или создать свой.

```
create default
set default default tcp action block
set default default udp action block
set default default icmp action block
create windows
set windows personality "Microsoft Windows XP Professional SP1"
set windows default tcp action reset
add windows tcp port 135 open
add windows tcp port 139 open
add windows tcp port 445 open
set windows ethernet "00:00:24:ab:8c:12"
bind 192.168.1.117 windows
```

Рисунок 1 – Пример настройки

3) Работа honeypot

После настройки honeypot он запускается и начинает «ждать» входящие подключения. При этом фиксируются действия атакующего, включая IP атакующего, сканируемые порты, попытки определить сервисы и операционную систему. Логи, которые собирает honeypot, позволяют анализировать разведывательные действия злоумышленников ещё до реальной атаки.

Контрольные вопросы

- 1) Каково определение систем Honey Pot и для чего они предназначены?
- 2) Какие три основные задачи решаются с помощью создания Honey Pot?
- 3) Какого типа информация используется для наполнения систем-ловушек и какой она должна казаться атакующему?
- 4) На каком основании любой вход в систему Honey Pot априори считается подозрительным?
- 5) В чем заключается основной принцип функционирования системы Padded Cell?
- 6) Как именно взаимодействуют между собой традиционная IDS и хост Padded Cell при обнаружении атаки?
- 7) Какие основные преимущества дает использование систем Honey Pot и Padded Cell для обеспечения безопасности организации?

8) Каким образом Honey Pot помогают в выявлении внутренних нарушителей, просматривающих ресурсы сети?

9) Перечислите ключевые недостатки и риски, связанные с эксплуатацией систем-ловушек и изолированных ячеек.

10) Какие требования предъявляются к квалификации администратора и знанию законодательства для работы с данными системами?

Лабораторная работа №11-12

Тема: Использование системы управления инцидентами отказа в обслуживании. Управление инцидентами внедрения вредоносного кода

Цель занятия

1. Закрепление теоретических знаний о принципах обеспечения безопасности беспроводных сетей Wi-Fi.
2. Изучение методов контроля безопасности беспроводной сети с использованием аппаратных и программных средств анализа.
3. Освоение практических навыков обнаружения неавторизованных беспроводных точек доступа и анализа режимов работы Wi-Fi сети.

Подготовка к занятию

1. Закрепление теоретических знаний о принципах сканирования сетевых портов и выявления сетевых сервисов.
2. Изучение методов контроля состояния хостов и сервисов с использованием программного средства Nmap.
3. Освоение практических навыков обнаружения открытых, закрытых и фильтруемых портов, а также базового анализа сетевых служб.

Учебные вопросы

1. Изучить основные принципы работы сетевых протоколов TCP и UDP.
2. Повторить назначение портов и особенности их состояния: открытый, закрытый, фильтруемый.
3. Изучить базовые возможности сканера Nmap и методы проведения безопасного сканирования в локальной сети. Основные теоретические сведения

Основные теоретические сведения изложены в материалах лекций и по данной тематике и рекомендуемой литературе.

Правила работы в лаборатории

К работе в лаборатории допускаются лица, изучившие правила и меры

безопасности, сдавшие зачет по ним и усвоившие порядок выполнения практического занятия.

Требования безопасности перед началом работ

- ЗАПРЕЩАЕТСЯ: переодеваться, пользоваться огнем, курить, принимать пищу в лаборатории;
- убедиться в целостности электрических розеток и разъемов. В лаборатории необходимо быть в сменной обуви;
- включение компьютера производить только после получения допуска по выполняемой работе и разрешения преподавателя или лаборанта.

Требования безопасности во время работы

- выполняя практическое занятие, студенты обязаны использовать только вычислительную технику, периферийное оборудование, соединительные кабели, измерительное оборудование и носители информации, непосредственно относящиеся к данному практическому занятию;
- подключение и отключение составляющих вычислительного комплекса производить только при полном снятии напряжения со всех составляющих вычислительного комплекса;
- при обнаружении неисправностей в оборудовании немедленно отключить источники питания и доложить об этом руководителю занятий или лаборанту.

Требования безопасности по окончании работы

- доложить руководителю занятий или лаборанту о завершении работ;
- привести в порядок и сдать рабочее место лаборанту, и доложить руководителю занятий о сдаче.

Аппаратное обеспечение

Класс персональных ЭВМ, электронная доска, проектор.

Программное обеспечение

В комплекте с персональными ЭВМ. Доступ к Интернет. Офисный пакет.

Литература

- 15) Технологии обеспечения безопасности информационных систем: учебное пособие: А. Л. Марухленко, Л. О. Марухленко, М. А. Ефремов [и др.]. – Москва; Берлин: Директ-Медиа, 2021. – 209 с.
- 16) Баланов А. Н. Защита информационных систем. Кибербезопасность: учебное пособие для вузов / А. Н. Баланов. — Санкт-Петербург: Лань, 2024. — 280 с.
- 17) Ховард Рик. Кибербезопасность: главные принципы. — СПб.: Питер, 2024. — 320 с.: ил.

- 18) Парасрам Ш., Замм А., Хериянто Т., Али Ш., Буду Д., Йохансен Д., Аллен Л. Kali Linux. Тестирование на проникновение и безопасность. -- СПб.: Питер, 2020. – 448 с.
- 19) Аудит безопасности информационных систем. – СПб.: Питер, 2018. – 272 с.: ил – (Серия “Библиотека программиста”)

Теоретическая часть

Активная разведка и аудит сетевых сервисов

1. Переход к активному сбору информации

Аудит информационной системы (ИС) начинается со сбора данных. Если на этапе пассивного сбора аудитор не взаимодействует с системой напрямую (используя Google, DNS или социальные сети), то активная разведка подразумевает непосредственное обращение к сервисам целевой организации.

- **Особенность:** Действия на этом этапе легко заметить с помощью систем обнаружения вторжений (IDS) и журналов аудита, так как сканер портов инициирует сетевые соединения.
- **Цель:** Выявление активных хостов, открытых портов, версий запущенного ПО (баннеров) и операционных систем.

2. Механизмы сканирования портов

Сканирование является фундаментом активного аудита. Оно опирается на принципы работы сетевых протоколов:

- **TCP-сканирование и «трехстороннее рукопожатие»:** Стандартное соединение TCP включает три этапа: клиент шлет SYN, сервер отвечает SYN-ACK, клиент подтверждает ACK.
- **SYN-сканирование (-sS):** Называется «полуоткрытым». Сканер шлет SYN, получает SYN-ACK (порт открыт), но вместо подтверждения обрывает связь пакетом RST. Это позволяет оставаться менее заметным для приложений, так как сессия не считается полностью установленной.
- **ACK-сканирование (-sA):** Используется не для поиска открытых портов, а для определения правил брандмауэра и фильтрации пакетов.

- UDP-сканирование (-sU): Протокол UDP не гарантирует доставку и не использует рукопожатий. Если порт закрыт, система может вернуть сообщение «порт недоступен» (ICMP), но отсутствие ответа часто интерпретируется как «открыто», что делает этот метод менее надежным, особенно при наличии брандмауэра.

3. Сбор данных через специфические протоколы

Сетевые сервисы часто выдают избыточную информацию, которая помогает злоумышленнику спланировать атаку:

- DNS (Domain Name System): через запросы типов MX (почтовые серверы) и NS (серверы имен) можно восстановить структуру сети. Самая критичная операция – передача зоны (AXFR): если DNS-сервер настроен неверно, он может выдать список всех внутренних и внешних хостов организации.

- SNMP (Simple Network Management Protocol): Протокол для управления роутерами и серверами. Если не изменена стандартная строка сообщества (Community String) «public», аудитор может удаленно получить списки запущенных программ, открытых портов и учетных записей пользователей.

- NetBIOS и Null Session: В Windows-системах (и Linux с Samba) существует возможность установления неавторизованного сеанса – Null session. Это позволяет узнать политики паролей, имена пользователей, названия групп и общие ресурсы без знания пароля.

4. Анализ баннеров и поиск уязвимостей

Баннер – это текстовый ответ сервиса, содержащий его название и версию (например, Apache 2.2.16). Знание точной версии ПО позволяет найти соответствующие эксплойты в публичных базах данных. Для автоматизации этого процесса используются сканеры уязвимостей (например, OpenVAS или Nessus), которые сопоставляют найденные версии сервисов с базой известных

брешей и формируют отчет о критических точках защиты.

5. Контрмеры и скрытность

Чтобы избежать обнаружения администраторами, аудиторы используют:

- Тайминги (-T): Режимы от Paranoid (паузы по 5 минут между пакетами) до Insane. Медленное сканирование помогает обойти системы IDS, которые ищут всплески трафика.
- Фрагментацию пакетов: Разбиение запроса на мелкие части может помешать системе защиты собрать их воедино для анализа сигнатуры атаки.
- Анонимность: Использование прокси-серверов или сети Tor для скрытия реального IP-адреса атакующего

Практическая часть

Задание 1. Распределение пользователей

Предположим, что по результатам сканирования узла были обнаружены следующие открытые порты:

22/tcp -- SSH

80/tcp -- HTTP

443/tcp -- HTTPS

3389/tcp -- RDP

445/tcp -- SMB

В системе предусмотрены три категории пользователей:

1. Системный администратор
2. Обычный пользователь
3. Удалённый пользователь

Необходимо ответить на вопросы

1. Какие из перечисленных сервисов могут быть необходимы:

- системному администратору;
- обычному пользователю;

- удалённому пользователю?

2. Какие порты потенциально не должны быть доступны всем пользователям одновременно?

3. Какие из перечисленных сервисов следует ограничить:

- по IP-адресу;
- по роли пользователя;
- по способу подключения?

4. Какие риски возникают, если:

- SSH открыт для всех пользователей;
- RDP доступен без ограничений;
- SMB доступен извне?

5. Можно ли по результатам сканирования сделать вывод о том, что система настроена небезопасно? Обоснуйте ответ.

Задание 2. Установка и конфигурирование сканера портов

Сканер портов Nmap используется для анализа сетевой доступности узлов и служб.

С его помощью можно определить:

- доступность хоста;
- открытые TCP- и UDP-порты;
- доступные сетевые сервисы;
- предполагаемые версии служб;
- возможные признаки небезопасной конфигурации.

При работе с Nmap важно не только уметь запускать команды, но и понимать, какую задачу решает каждая из них.

Для выполнения задания необходимо занести в Таблицу 1 основные команды сканера портов Nmap, используемые для анализа сети.

Таблица 1 – Анализ результатов сканирования

Принцип действия команды	Команда
Определение доступных стандартных портов	nmap 192.168.1.0

на удаленном узле	
Сканирование только заданного диапазона портов (20 – 1024)	
Проверка одного конкретного порта	
Сканирование нескольких конкретных портов	
Определение версии сетевого сервиса	
Сканирование UDP-портов	
Определение операционной системы удалённого узла	
Получение подробной информации о работе команды	
Выполнение анализа узла с определением сервисов и ОС	

Лабораторная работа №13-14

Тема: Планирование системы управления инцидентами внедрения вредоносного кода. Использование системы управления инцидентами внедрения вредоносного кода.

Цель занятия

1. Закрепление материала, полученного на лекционных занятиях, по вопросам применения систем защиты информации для выявления, регистрации и анализа событий и инцидентов кибербезопасности.

2. Приобретение практических навыков по изучению возможностей системы защиты информации Secret Net в части контроля действий пользователей, регистрации событий безопасности и обнаружения признаков нарушений политики безопасности.

3. Формирование навыков анализа событий и инцидентов кибербезопасности на основе журналов регистрации, предупреждений системы защиты, признаков несанкционированного доступа, попыток нарушения правил разграничения доступа и иных артефактов, зафиксированных средствами Secret Net.

4. Освоение порядка интерпретации результатов мониторинга, выявления подозрительных действий пользователей и анализа зарегистрированных системой событий, которые могут свидетельствовать о возникновении инцидента кибербезопасности.

Подготовка к занятию

1. Изучить (повторить) теоретический материал лекций и рекомендованную литературу по вопросам применения систем защиты информации, обнаружения событий и инцидентов информационной безопасности, а также анализа журналов безопасности и результатов контроля доступа.

2. Изучить основные понятия, связанные с событиями и инцидентами информационной безопасности, нарушениями политики безопасности,

разграничением доступа, регистрацией действий пользователей и администраторов, а также механизмами защиты, реализуемыми в системе Secret Net.

3. Ознакомиться с основными функциональными возможностями системы Secret Net, связанными с контролем доступа, регистрацией событий безопасности, выявлением нарушений и формированием отчетной информации.

4. Подготовить лабораторную среду, содержащую установленную систему Secret Net, учетные записи пользователей, тестовые защищаемые объекты, журналы регистрации событий, а также исходные данные, необходимые для моделирования и анализа инцидентов информационной безопасности.

Учебные вопросы

1. Назначение и основные функции системы защиты информации Secret Net в обеспечении информационной безопасности автоматизированных систем.

2. Основные виды событий информационной безопасности, регистрируемых системой Secret Net.

3. Признаки и критерии отнесения зарегистрированных событий к инцидентам информационной безопасности.

4. Возможности системы Secret Net по обнаружению нарушений политики безопасности, несанкционированного доступа и подозрительных действий пользователей.

5. Особенности анализа журналов регистрации, сообщений и уведомлений системы Secret Net при исследовании инцидентов информационной безопасности.

6. Порядок интерпретации событий безопасности и оценки их влияния на состояние защищенности информационной системы.

7. Практические аспекты документирования результатов анализа событий и инцидентов информационной безопасности, выявленных средствами системы Secret Net.

Основные теоретические сведения

Основные теоретические сведения изложены в материалах лекций и по данной тематике и рекомендуемой литературе.

Правила работы в лаборатории

К работе в лаборатории допускаются лица, изучившие правила и меры безопасности, сдавшие зачет по ним и усвоившие порядок выполнения практического занятия.

Требования безопасности перед началом работ

- ЗАПРЕЩАЕТСЯ: переодеваться, пользоваться огнем, курить, принимать пищу в лаборатории;
- убедиться в целостности электрических розеток и разъемов. В лаборатории необходимо быть в сменной обуви;
- включение компьютера производить только после получения допуска по выполняемой работе и разрешения преподавателя или лаборанта.

Требования безопасности во время работы

- выполняя практическое занятие, студенты обязаны использовать только вычислительную технику, периферийное оборудование, соединительные кабели, измерительное оборудование и носители информации, непосредственно относящиеся к данному практическому занятию;
- подключение и отключение составляющих вычислительного комплекса производить только при полном снятии напряжения со всех составляющих вычислительного комплекса;
- при обнаружении неисправностей в оборудовании немедленно отключить источники питания и доложить об этом руководителю занятий или лаборанту.

Требования безопасности по окончании работы

- доложить руководителю занятий или лаборанту о завершении работ;
- привести в порядок и сдать рабочее место лаборанту, и доложить руководителю занятий о сдаче.

Аппаратное обеспечение

Класс персональных ЭВМ, электронная доска, проектор.

Программное обеспечение

В комплекте с персональными ЭВМ. Доступ к Интернет. Офисный пакет.

Литература

- 20) Технологии обеспечения безопасности информационных систем: учебное пособие: А. Л. Марухленко, Л. О. Марухленко, М. А. Ефремов [и др.]. – Москва; Берлин: Директ-Медиа, 2021. – 209 с.
- 21) Баланов А. Н. Защита информационных систем. Кибербезопасность: учебное пособие для вузов / А. Н. Баланов. — Санкт-Петербург: Лань, 2024. — 280 с.
- 22) Ховард Рик. Кибербезопасность: главные принципы. — СПб.: Питер, 2024. — 320 с.: ил.

Теоретическая часть

1. Общие сведения о системе Secret Net

Secret Net – это система защиты информации, предназначенная для обеспечения безопасности автоматизированных рабочих мест и информационных систем от несанкционированного доступа, нарушения политики безопасности, утечки данных и иных угроз информационной безопасности. Данная система применяется для реализации комплекса организационно-технических мер защиты информации, а также для контроля действий пользователей в защищаемой среде.

Основное назначение системы Secret Net заключается в обеспечении разграничения доступа к информационным ресурсам, контроле использования устройств и носителей информации, регистрации действий пользователей, а также в предотвращении и обнаружении событий и инцидентов информационной безопасности. Система может использоваться как в локальных автоматизированных рабочих местах, так и в составе корпоративной защищенной инфраструктуры.

2. Распределение пользователей в защищаемой системе

Одной из важнейших задач при построении защищенной информационной системы является распределение пользователей по ролям,

уровням доступа и полномочиям. От правильного распределения пользователей зависит уровень защищенности системы, возможность предотвращения несанкционированного доступа, а также эффективность контроля действий субъектов доступа.

В системе Secret Net пользователи могут быть разделены в соответствии с их функциональным назначением, служебными обязанностями и необходимым уровнем доступа к защищаемым ресурсам. Как правило, выделяются следующие категории пользователей:

- администратор безопасности, осуществляющий настройку и сопровождение системы защиты;
- системный администратор, отвечающий за функционирование операционной системы и прикладного программного обеспечения;
- обычные пользователи, выполняющие повседневную работу с информацией в пределах предоставленных им полномочий;
- пользователи с ограниченными правами, доступ которых строго ограничен установленной политикой безопасности.

Распределение пользователей необходимо для реализации принципа минимально необходимых привилегий, согласно которому каждому пользователю предоставляется только тот объем прав, который необходим ему для выполнения служебных задач. Это снижает вероятность случайного или преднамеренного нарушения политики безопасности и позволяет повысить уровень защищенности информационной системы.

3. Разграничение доступа в системе Secret Net

Одной из ключевых функций Secret Net является разграничение доступа к объектам информационной системы. Под разграничением доступа понимается установление правил, определяющих, какие пользователи имеют право доступа к тем или иным ресурсам, а также какие действия они могут выполнять.

В качестве объектов доступа могут выступать:

- файлы и каталоги;
- логические диски;
- съемные носители информации;
- устройства ввода-вывода;
- системные и прикладные ресурсы.

Система Secret Net позволяет задавать правила доступа, ограничивать использование устройств, запрещать выполнение определенных действий, а также контролировать обращения пользователей к защищаемым объектам. При этом каждая попытка доступа может быть зафиксирована в журнале регистрации, что позволяет впоследствии анализировать действия пользователей и выявлять признаки инцидентов информационной безопасности.

4. Установка системы Secret Net

Процесс установки Secret Net представляет собой один из важнейших этапов развертывания защищенной среды. Корректная установка системы обеспечивает последующее правильное функционирование механизмов защиты, регистрации событий безопасности и разграничения доступа.

Установка, как правило, включает в себя:

- запуск установочного пакета;
- выбор компонентов системы;
- интеграцию с операционной системой;
- инициализацию защитных механизмов;
- перезагрузку системы;
- проверку работоспособности основных модулей.

После завершения установки система Secret Net начинает функционировать как средство защиты информации и предоставляет

администратору возможность дальнейшего конфигурирования параметров безопасности.

5. Конфигурирование системы Secret Net

После установки системы необходимо выполнить ее конфигурирование, то есть настройку параметров, обеспечивающих реализацию политики безопасности. Конфигурирование позволяет адаптировать систему защиты к требованиям конкретной организации или лабораторной среды.

К числу основных параметров конфигурирования относятся:

- создание и распределение учетных записей пользователей;
- назначение ролей и полномочий;
- настройка правил разграничения доступа;
- включение и настройка журналирования;
- настройка контроля внешних устройств и носителей;
- задание параметров уведомлений и регистрации событий безопасности.

Грамотно выполненное конфигурирование Secret Net позволяет обеспечить устойчивую работу защищаемой системы, предотвратить несанкционированный доступ и повысить эффективность выявления нарушений безопасности.

6. Значение журналов регистрации и контроля действий пользователей

Система Secret Net фиксирует действия пользователей, попытки обращения к защищаемым объектам, изменения параметров безопасности и иные события, имеющие значение для обеспечения информационной безопасности. Эти сведения сохраняются в журналах регистрации, которые

являются важным источником информации для анализа событий и расследования инцидентов.

Журналы регистрации позволяют:

- отслеживать факты входа пользователей в систему;
- выявлять неудачные попытки авторизации;
- фиксировать обращения к защищенным ресурсам;
- контролировать использование внешних носителей;
- анализировать изменение параметров безопасности.

Таким образом, журналы регистрации являются неотъемлемым элементом механизма защиты, так как обеспечивают возможность последующего анализа событий и позволяют своевременно выявлять признаки нарушений информационной безопасности.

Практическая часть

Задание 1:

В ходе выполнения лабораторной работы необходимо изучить принципы распределения пользователей в защищаемой информационной системе, ознакомиться с порядком установки системы Secret Net, ответить на контрольные вопросы.

1. Каково назначение системы защиты информации Secret Net?
2. Для чего необходимо распределение пользователей в защищаемой системе?
3. Какие категории пользователей могут быть выделены в системе Secret Net?
4. В чем заключается принцип минимально необходимых привилегий?
5. Какие объекты могут подлежать защите и разграничению доступа в системе Secret Net?

6. Почему этап установки системы защиты информации является важным для обеспечения безопасности?
7. Какие основные действия выполняются в процессе установки Secret Net?
8. Что понимается под конфигурированием системы защиты информации?
9. Какие параметры безопасности могут быть настроены после установки Secret Net?
10. Для чего в системе Secret Net ведутся журналы регистрации событий?
11. Какие события безопасности могут фиксироваться системой?
12. Почему важно контролировать действия пользователей в защищаемой системе?
13. Как распределение прав доступа влияет на защищенность информационной системы?
14. Какую роль играет администратор безопасности в системе Secret Net?
15. Как можно оценить правильность выполненного конфигурирования системы?

Лабораторная работа №15-16

Тема: Управление инцидентами сбора информации. Планирование системы управления инцидентами сбора информации.

Цель занятия

1. Закрепление теоретических знаний о принципах обеспечения безопасности беспроводных сетей Wi-Fi.
2. Изучение методов контроля безопасности беспроводной сети с использованием аппаратных и программных средств анализа.
3. Освоение практических навыков обнаружения неавторизованных беспроводных точек доступа и анализа режимов работы Wi-Fi сети.

Подготовка к занятию

1. Изучить основные принципы функционирования беспроводных сетей стандарта Wi-Fi.
2. Повторить особенности режимов работы беспроводных сетевых устройств и принципы организации точек доступа.
3. Изучить методы обнаружения неавторизованных точек доступа и средства анализа беспроводного трафика.

Учебные вопросы

1. Основные принципы построения и защиты беспроводных сетей Wi-Fi.
2. Настройка беспроводной сети Wi-Fi в различных режимах работы.
3. Методы контроля состояния и безопасности беспроводной сети.
4. Обнаружение неавторизованных беспроводных точек доступа с использованием встроенного инструментария сетевого оборудования.

Основные теоретические сведения

Основные теоретические сведения изложены в материалах лекций и по данной тематике и рекомендуемой литературе.

Правила работы в лаборатории

К работе в лаборатории допускаются лица, изучившие правила и меры безопасности, сдавшие зачет по ним и усвоившие порядок выполнения практического занятия.

Требования безопасности перед началом работ

- ЗАПРЕЩАЕТСЯ: переодеваться, пользоваться огнем, курить, принимать пищу в лаборатории;
- убедиться в целостности электрических розеток и разъемов. В лаборатории необходимо быть в сменной обуви;
- включение компьютера производить только после получения допуска по выполняемой работе и разрешения преподавателя или лаборанта.

Требования безопасности во время работы

- выполняя практическое занятие, студенты обязаны использовать только вычислительную технику, периферийное оборудование, соединительные кабели, измерительное оборудование и носители информации, непосредственно относящиеся к данному практическому занятию;
- подключение и отключение составляющих вычислительного комплекса производить только при полном снятии напряжения со всех составляющих вычислительного комплекса;
- при обнаружении неисправностей в оборудовании немедленно отключить источники питания и доложить об этом руководителю занятий или лаборанту.

Требования безопасности по окончании работы

- доложить руководителю занятий или лаборанту о завершении работ;
- привести в порядок и сдать рабочее место лаборанту, и доложить руководителю занятий о сдаче.

Аппаратное обеспечение

Класс персональных ЭВМ, электронная доска, проектор.

Программное обеспечение

В комплекте с персональными ЭВМ. Доступ к Интернет. Офисный пакет.

Литература

- 23) Технологии обеспечения безопасности информационных систем: учебное пособие: А. Л. Марухленко, Л. О. Марухленко, М. А. Ефремов [и др.]. – Москва; Берлин: Директ-Медиа, 2021. – 209 с.
- 24) Баланов А. Н. Защита информационных систем. Кибербезопасность: учебное пособие для вузов / А. Н. Баланов. — Санкт-Петербург: Лань, 2024. — 280 с.

- 25) Ховард Рик. Кибербезопасность: главные принципы. — СПб.: Питер, 2024. — 320 с.: ил.
- 26) Парасрам Ш., Замм А., Хериянто Т., Али Ш., Буду Д., Йохансен Д., Аллен Л. Kali Linux. Тестирование на проникновение и безопасность. -- СПб.: Питер, 2020. – 448 с.

Практическая часть

Цель работы: Изучить принципы работы протоколов безопасности Wi-Fi, методы разведки и идентификации несанкционированных точек доступа (Rogue AP) через анализ практических примеров. Ответить на контрольные вопросы.

Часть 1. Теоретические основы и режимы работы

Беспроводные сети регулируются стандартом **IEEE 802.11**. Для захвата трафика и проведения аудита безопасности сетевой адаптер должен поддерживать **режим мониторинга** (Monitor Mode), который позволяет видеть пакеты всех сетей в радиусе действия, а не только те, что адресованы конкретному устройству.

Пример 1. Подготовка интерфейса Для перевода адаптера wlan0 в режим мониторинга используется утилита airmon-ng. Часто процессу мешают системные службы (NetworkManager, dhclient).

- **Команда:** airmon-ng check kill (удаляет конфликтующие процессы).

```
root@kali:~# airmon-ng check kill
Killing these processes:

PID Name
636 dhclient
874 wpa_supplicant
```

- **Команда:** airmon-ng start wlan0.
- **Результат:** интерфейс переименовывается в wlan0mon, а в выводе iwconfig в поле Mode появляется значение **Monitor**.

```

root@kali:~# iwconfig
wlan0mon IEEE 802.11bgn Mode:Monitor Frequency:2.457 GHz Tx-Power=20 dBm
Retry short limit:7 RTS thr:off Fragment thr:off
Power Management:off

lo      no wireless extensions.

eth0    no wireless extensions.

```

Часть 2. Разведка и обнаружение несанкционированных точек

Пример 2. Пассивное сканирование (airodump-ng) Инструмент airodump-ng позволяет увидеть список всех сетей и подключенных к ним клиентов. Рассмотрим типичный фрагмент вывода:

```

CH 6 ][ Elapsed: 18 s ][ 2016-06-14 21:22
BSSID            PWR RXQ Beacons  #Data, #/s CH MB  ENC  CIPHER AUTH ESSID
44:94:FC:37:10:6E -44 100    100      0   0  6  54e WPA2 CCMP  PSK  Aircrack_Wifi
BSSID            STATION          PWR   Rate    Lost    Frames  Probe

```

- **PWR (Power):** чем ближе значение к 0, тем сильнее сигнал. Значение -42 указывает на близкое расположение устройства.
- **BSSID:** физический MAC-адрес точки доступа.
- **ENC:** тип шифрования (WPA2 — современный стандарт, WEP — устаревший и уязвимый).

Пример 3. Выявление атаки «Злой двойник» (Evil Twin) Атака заключается в создании поддельной точки доступа с тем же SSID, что и легитимная, но с более сильным сигналом.

- **Сценарий:** Человек видит в списке две сети с именем Corporate_Guest. Одна имеет BSSID производителя Cisco, а другая — неизвестного производителя с сигналом -20 PWR. Это явный признак Rogue AP.

Часть 3. Инструментарий роутеров и автоматизация

Пример 4. Анализ настроек безопасности в консоли управления Администраторы часто оставляют уязвимые функции включенными.

- **WPS (Wi-Fi Protected Setup):** Позволяет подключаться по PIN-коду, который легко взламывается методом перебора (атака Pixie-Dust).
- **Фильтрация MAC-адресов:** Мера защиты, разрешающая доступ только устройствам из белого списка. Однако злоумышленник может использовать **macchanger**, чтобы подделать свой MAC-адрес под адрес легитимного клиента, найденного при сканировании.

Контрольные вопросы:

1. Зачем перед началом работы рекомендуется выполнять команду `airmon-ng check kill`? К каким последствиям может привести отказ от её выполнения?
2. Какая из двух представленных в таблице сетей является более уязвимой к быстрому взлому и почему? (Подсказка: обратите внимание на тип шифрования).
3. Перечислите два косвенных признака, по которым можно заподозрить наличие в офисе атаки типа «Злой двойник» (Evil Twin).
4. Почему функция WPS считается небезопасной, несмотря на удобство для пользователя?.
5. Если в сети включена фильтрация MAC-адресов, какие шаги предпримет злоумышленник, чтобы обойти это ограничение, используя инструменты Kali Linux?.
6. В чем преимущество использования инструментов типа Wifite перед ручным использованием `aircrack-ng`?.

Лабораторная работа №17-18

Тема: Использование системы управления инцидентами сбора информации.

Устранение инцидента и восстановление после инцидента сбора информации
устранение и восстановление инцидента после сбора информации.

Цель занятия

5. Закрепление материала, полученного на лекционных занятиях по вопросам выявления, анализа и документирования событий и инцидентов кибербезопасности

6. Приобретение практических навыков по разработке сценария события и инцидента кибербезопасности, а также их анализу на основе признаков нарушения информационной безопасности.

7. Формирование навыков выявления, классификации и интерпретации событий и инцидентов кибербезопасности на основе журналов регистрации, сетевой активности, следов нарушения и иных артефактов.

8. Освоение порядка оформления и заполнения форм **«Отчет о событии кибербезопасности»** и **«Отчет об инциденте кибербезопасности»** в соответствии с результатами проведенного анализа.

Подготовка к занятию

1. Изучить (повторить) теоретический материал лекций и рекомендованную литературу по вопросам анализа событий и инцидентов кибербезопасности, а также документирования результатов расследования.

2. Изучить основные понятия, связанные с событиями и инцидентами кибербезопасности, их классификацией, признаками и порядком реагирования.

3. Ознакомиться с методическими рекомендациями по выполнению практического задания и порядком заполнения отчетных форм.

4. Подготовить лабораторную среду, содержащую исходные данные для анализа: журналы событий, описание сценария нарушения, технические признаки инцидента, сетевые и системные артефакты.

Учебные вопросы

5. Анализ признаков события кибербезопасности и определение его характеристик.
6. Выявление признаков инцидента кибербезопасности на основе результатов анализа события и сопутствующих технических данных.
7. Исследование и интерпретация артефактов, подтверждающих наличие нарушения информационной безопасности.
8. Заполнение формы «Отчет о событии кибербезопасности».
9. Заполнение формы «Отчет об инциденте кибербезопасности».

Основные теоретические сведения

Основные теоретические сведения изложены в материалах лекций и по данной тематике и рекомендуемой литературе.

Правила работы в лаборатории

К работе в лаборатории допускаются лица, изучившие правила и меры безопасности, сдавшие зачет по ним и усвоившие порядок выполнения практического занятия.

Требования безопасности перед началом работ

- ЗАПРЕЩАЕТСЯ: переодеваться, пользоваться огнем, курить, принимать пищу в лаборатории;
- убедиться в целостности электрических розеток и разъемов. В лаборатории необходимо быть в сменной обуви;
- включение компьютера производить только после получения допуска по выполняемой работе и разрешения преподавателя или лаборанта.

Требования безопасности во время работы

- выполняя практическое занятие, студенты обязаны использовать только вычислительную технику, периферийное оборудование, соединительные кабели, измерительное оборудование и носители информации, непосредственно относящиеся к данному практическому занятию;
- подключение и отключение составляющих вычислительного комплекса производить только при полном снятии напряжения со всех составляющих вычислительного комплекса;
- при обнаружении неисправностей в оборудовании немедленно

отключить источники питания и доложить об этом руководителю занятий или лаборанту.

Требования безопасности по окончании работы

- доложить руководителю занятий или лаборанту о завершении работ;
- привести в порядок и сдать рабочее место лаборанту, и доложить руководителю занятий о сдаче.

Аппаратное обеспечение

Класс персональных ЭВМ, электронная доска, проектор.

Программное обеспечение

В комплекте с персональными ЭВМ. Доступ к Интернет. Офисный пакет.

Литература

- 27) Технологии обеспечения безопасности информационных систем: учебное пособие: А. Л. Марухленко, Л. О. Марухленко, М. А. Ефремов [и др.]. – Москва; Берлин: Директ-Медиа, 2021. – 209 с.
- 28) Баланов А. Н. Защита информационных систем. Кибербезопасность: учебное пособие для вузов / А. Н. Баланов. — Санкт-Петербург: Лань, 2024. — 280 с.
- 29) Ховард Рик. Кибербезопасность: главные принципы. — СПб.: Питер, 2024. — 320 с.: ил.
- 30) Парасрам Ш., Замм А., Хериянто Т., Али Ш., Буду Д., Йохансен Д., Аллен Л. Kali Linux. Тестирование на проникновение и безопасность. -- СПб.: Питер, 2020. – 448 с.

Теоретическая часть

Разработка и анализ инцидентов кибербезопасности являются важной частью современной практики обеспечения информационной безопасности. В условиях постоянного роста числа сетевых угроз, атак на веб-приложения, серверы, рабочие станции и информационные системы особое значение приобретает не только способность выявлять технические признаки нарушения безопасности, но и умение правильно интерпретировать обнаруженные данные, подтверждать факт нарушения, оценивать последствия и оформлять результаты расследования в виде структурированной отчетности. Поэтому в рамках лабораторной работы по разработке и анализу инцидента кибербезопасности основное внимание уделяется не только техническому анализу, но и процессу документирования, который является обязательной частью профессиональной деятельности специалиста по кибербезопасности.

В процессе функционирования любой информационной системы постоянно возникают различные события, связанные с ее работой. Часть из них является штатной и не представляет угрозы, однако некоторые могут указывать на наличие аномалий, нарушений политики безопасности, попыток несанкционированного доступа или активных атак. Такие события рассматриваются как события кибербезопасности. Под событием кибербезопасности понимается любое зафиксированное действие, изменение состояния системы, сетевой активности, учетной записи или программной среды, которое может быть связано с угрозой безопасности информации. К таким событиям относятся многократные неудачные попытки входа в систему, подозрительные сетевые подключения, обращения к закрытым портам, запуск неизвестных процессов, появление новых учетных записей, изменение конфигурационных файлов, аномальная активность веб-сервера, резкое увеличение сетевого трафика, а также срабатывания средств обнаружения вторжений и антивирусной защиты.

Следует учитывать, что событие кибербезопасности само по себе еще не означает факт нарушения безопасности. Оно представляет собой первичный сигнал, требующий анализа и проверки. На практике многие события могут оказаться ложными срабатываниями, результатом ошибки пользователя, особенностью работы программного обеспечения или допустимой административной активностью. Именно поэтому после обнаружения события требуется анализ, в ходе которого специалист определяет характер зафиксированной активности, устанавливает ее источник, проверяет наличие подтверждающих данных и оценивает потенциальную опасность для информационной системы. Если по результатам анализа устанавливается, что событие действительно связано с нарушением конфиденциальности, целостности или доступности информации либо представляет собой подтвержденную реализацию угрозы, оно квалифицируется как инцидент кибербезопасности.

Инцидент кибербезопасности представляет собой подтвержденное

событие или совокупность событий, которые привели либо могли привести к нарушению нормального функционирования информационной системы, несанкционированному доступу, компрометации учетных данных, утечке информации, нарушению целостности файлов, нарушению доступности сервисов или другим негативным последствиям. В отличие от события, инцидент требует обязательного реагирования, документирования и, как правило, более глубокого расследования. Таким образом, событие и инцидент находятся в причинно-следственной связи: каждый инцидент начинается с одного или нескольких событий, однако не каждое событие перерастает в инцидент.

Процесс разработки и анализа инцидента кибербезопасности включает несколько последовательных этапов. На первом этапе осуществляется обнаружение подозрительной активности. Источниками обнаружения могут быть системные и сетевые журналы, данные антивирусного программного обеспечения, средства IDS/IPS, SIEM-системы, результаты мониторинга, а также сообщения пользователей или администраторов. После обнаружения событие подлежит регистрации. Регистрация необходима для фиксации первичной информации и обеспечения возможности дальнейшего анализа. На этом этапе обычно указываются дата и время обнаружения, источник события, краткое описание признаков, затронутые ресурсы и предварительная оценка потенциальной опасности.

Следующим этапом является анализ. Его задача состоит в том, чтобы установить, является ли зафиксированное событие реальной угрозой или ложным срабатыванием. Для этого исследуются журналы аутентификации, системные логи, сетевой трафик, активные соединения, список процессов, файловая активность, журналы веб-сервера, журналы приложений и иные цифровые следы. На этом этапе важно не ограничиваться одним источником данных, поскольку достоверный вывод может быть сделан только на основе совокупности подтверждающих признаков. Например, многократные неудачные попытки входа в систему могут быть следствием ошибки

пользователя, но если одновременно фиксируются подключения с подозрительного внешнего IP-адреса, сканирование сервисов и последующая успешная авторизация, это уже может свидетельствовать о попытке компрометации учетной записи.

После анализа осуществляется классификация события. В зависимости от полученных результатов оно может быть отнесено к штатной активности, подозрительному событию или подтвержденному инциденту кибербезопасности. Если событие признано инцидентом, запускается этап реагирования. Реагирование включает действия по локализации угрозы, ограничению ее распространения, минимизации ущерба и устранению последствий. К таким действиям относятся изоляция хоста, блокировка учетной записи, завершение вредоносного процесса, отключение подозрительных сетевых соединений, ограничение доступа к сервисам, резервное копирование данных, анализ уязвимостей и восстановление работоспособности системы. После завершения реагирования обязательно выполняется документирование, которое позволяет зафиксировать все существенные сведения об обнаруженном событии, проведенном анализе, подтвержденных признаках инцидента и принятых мерах.

Документирование занимает центральное место в расследовании инцидентов кибербезопасности. Оно необходимо для обеспечения воспроизводимости анализа, сохранения доказательной базы, стандартизации процесса реагирования, передачи информации другим специалистам и использования результатов расследования для совершенствования политики безопасности. Документирование также имеет учебное и методическое значение, поскольку позволяет обучающимся формировать системный подход к работе с инцидентами, а не ограничиваться только техническим выполнением отдельных команд или использованием инструментов. В профессиональной среде отсутствие корректной документации существенно снижает ценность даже качественно проведенного анализа, поскольку без формализованного описания сложно подтвердить ход расследования,

обосновать выводы и использовать результаты в рамках внутреннего аудита или последующего разбора инцидента.

Для целей лабораторной работы особую роль играют две формы отчетности: «Отчет о событии кибербезопасности» и «Отчет об инциденте кибербезопасности». Эти документы отражают два разных этапа обработки угрозы и позволяют формализовать процесс перехода от первичного наблюдения к подтвержденному расследованию. «Отчет о событии кибербезопасности» предназначен для регистрации выявленного факта, который может иметь отношение к нарушению безопасности. Его основная задача заключается в том, чтобы своевременно зафиксировать признаки подозрительной активности и сохранить исходные данные для последующего анализа. В такой форме обычно отражаются дата и время обнаружения, лицо или средство, выявившее событие, описание наблюдаемой активности, затронутые ресурсы, технические признаки и предварительная оценка значимости. При заполнении этой формы важно придерживаться объективного подхода и фиксировать именно наблюдаемые факты, не подменяя их преждевременными выводами.

«Отчет об инциденте кибербезопасности» составляется в том случае, если по результатам анализа событие признано подтвержденным нарушением или реализацией угрозы. В отличие от первичного отчета, этот документ имеет более высокий уровень детализации и отражает не только признаки события, но и результаты расследования. В нем указываются идентификатор инцидента, дата и время возникновения и обнаружения, описание сценария атаки, вектор проникновения, подтвержденные индикаторы компрометации, затронутые активы, последствия для системы, уровень критичности, действия по локализации, устранению и восстановлению, а также рекомендации по предотвращению повторения аналогичной ситуации.

Одним из важнейших аспектов расследования инцидента является работа с цифровыми следами. Под цифровыми следами понимаются любые технические данные, оставленные в результате работы пользователя,

программы, сетевого соединения или вредоносной активности. К ним относятся системные журналы, логи аутентификации, журналы веб-сервера, дампы трафика, списки активных процессов, сведения о сетевых соединениях, артефакты файловой системы, записи о выполненных командах, временные метки, результаты сканирования, сообщения средств защиты и иные данные, позволяющие восстановить картину произошедшего. Для того чтобы выводы расследования были обоснованными, цифровые следы должны быть достоверными, полными, временно согласованными и пригодными для повторной проверки. Именно поэтому при проведении анализа необходимо не только выявлять подозрительные признаки, но и сохранять подтверждающие материалы: скриншоты, выдержки из логов, журнальные записи, результаты сетевого анализа и иные доказательства.

Особое место в анализе событий и инцидентов кибербезопасности занимает использование специализированных инструментов, в том числе входящих в состав Kali Linux. Kali Linux представляет собой специализированный дистрибутив Linux, предназначенный для тестирования на проникновение, анализа защищенности, цифровой криминалистики и расследования инцидентов. Он содержит широкий набор средств, которые могут использоваться как для моделирования атак, так и для анализа их последствий. В рамках расследования инцидентов такие инструменты позволяют анализировать сетевую активность, проверять доступность сервисов, выявлять открытые порты, исследовать веб-приложения, анализировать трафик, собирать цифровые артефакты и формировать доказательную базу. Практическая ценность Kali Linux в учебной лабораторной среде заключается в возможности смоделировать реальные сценарии компрометации и затем рассмотреть их с точки зрения специалиста по расследованию инцидентов.

Помимо технических средств анализа, важную роль играют инструменты сопровождения и документирования результатов. В современной практике кибербезопасности широко применяются

специализированные платформы, которые позволяют структурировать результаты тестирования, анализа и расследования. Одним из таких инструментов является Dradis. Dradis представляет собой платформу для централизованного ведения информации о ходе анализа безопасности, обнаруженных уязвимостях, признаках компрометации, результатах сканирования и действиях исследователя. Основная функция Dradis заключается в объединении технических данных из различных источников в единую структуру проекта. Это позволяет специалисту систематизировать найденные артефакты, привязывать их к конкретным хостам, сервисам, уязвимостям или этапам атаки, а также формировать итоговую отчетность.

Еще одним важным инструментом является Faraday IDE. Данное приложение ориентировано на сопровождение процесса анализа безопасности и совместную работу с результатами тестирования. В отличие от обычного текстового документирования, Faraday IDE позволяет объединять результаты различных инструментов, автоматически импортировать данные сканирования, классифицировать обнаруженные уязвимости и вести централизованный учет технических находок. В условиях анализа инцидента кибербезопасности такой подход особенно полезен, поскольку позволяет собрать в одном месте сведения о сетевых узлах, сервисах, уязвимостях, следах эксплуатации и подтверждающих данных.

Инструмент MagicTree также относится к средствам организации и структурирования результатов анализа безопасности. Его основное назначение заключается в предоставлении исследователю удобной иерархической модели хранения информации о целях анализа, найденных данных, уязвимостях, хостах, сервисах, учетных записях, доказательствах и промежуточных выводах. По сути, MagicTree позволяет построить логическую структуру расследования, где каждый элемент может быть связан с определенным этапом анализа или конкретным объектом исследования. Для лабораторной работы это особенно полезно с методической точки зрения, поскольку обучающийся получает возможность не просто хранить результаты

хаотично, а оформлять их в виде упорядоченной аналитической модели.

С точки зрения методики обучения важно понимать, что технический анализ и документирование должны рассматриваться как единый процесс. Недостаточно лишь использовать инструмент и получить результат — необходимо интерпретировать этот результат, сопоставить его с другими источниками данных, оценить его достоверность, определить его значимость и зафиксировать в форме, пригодной для последующего использования. Именно такой подход формирует у обучающихся профессиональные компетенции в области реагирования на события и инциденты кибербезопасности. В рамках лабораторной работы студент должен не только обнаружить подозрительную активность, но и продемонстрировать умение классифицировать ее, выделять признаки угрозы, подтверждать факт нарушения, описывать последствия и предлагать меры реагирования. Все это должно быть отражено в отчетных формах в логичной, последовательной и обоснованной форме.

Таким образом, разработка и анализ инцидента кибербезопасности представляют собой комплексную задачу, включающую обнаружение подозрительной активности, регистрацию события, сбор и анализ цифровых следов, подтверждение факта нарушения, классификацию инцидента, реагирование и обязательное документирование результатов. «Отчет о событии кибербезопасности» и «Отчет об инциденте кибербезопасности» выступают не просто формами отчетности, а инструментами структурирования расследования и профессионального осмысления обнаруженных угроз. Использование средств Kali Linux и сопутствующих приложений, таких как Dradis, Faraday IDE и MagicTree, позволяет не только выполнять технический анализ, но и организовывать его результаты в форме, соответствующей требованиям современной практики кибербезопасности. Именно поэтому данная лабораторная работа имеет не только учебное, но и прикладное значение, формируя у обучающихся навыки, непосредственно востребованные в деятельности специалистов по информационной

безопасности.

Практическая часть

- 1) Заполнение формы “Отчет о событии кибербезопасности”

Отчет о событии информационной безопасности

Дата события

Номер события <1>: 12 Соответствующие идентификационные номера событий и (или) инцидентов (если требуется):

Информация о сообщавшем лице

Фамилия	<u>Иванов</u>	Адрес	<u>Ленина 131/2</u>
Организация	<u>Энергомера</u>		
Телефон	<u>+7 (xxx) xxx-xx-xx</u>	Электронная почта	<u>concern@energomera.ru</u>

Описание события ИБ

Описание события:

Что произошло – Несанкционированный доступ к учетной записи сотрудника

Как произошло – Вредоносный скрипт через фишинговое письмо

Почему произошло – Отсутствие двухфакторной аутентификации у сотрудника

Пораженные компоненты – Учетная запись пользователя, а также его файлы

Негативное воздействие на бизнес – Утечка персональных данных

Любые идентифицированные уязвимости – Уязвимости в веб-приложении

Подробности о событии ИБ

Дата и время наступления события 07.04.2026 09:15

Дата и время обнаружения события 07.04.2026 09:45

Дата и время сообщения о событии 07.04.2026 10:00

Закончилось ли событие? (отметить в квадрате) Да ☒ Нет ☐

Если “да”, то уточнить длительность события в днях/часах/минутах

0ч 45 мин

<1> Номера событий назначаются руководителем ГРИИБ организации.

2) Заполнение формы “Отчет об инциденте кибербезопасности”

Изучить работу с фреймворком Dradis и другими инструментами сопровождения расследований (Faraday IDE, MagicTree) для систематизации и документирования инцидентов кибербезопасности.

Задачи:

1. Ознакомиться с интерфейсом **Dradis** и его основными возможностями и ответить на вопрос:

- регистрация и классификация событий кибербезопасности;
- объединение событий в инциденты;
- добавление доказательств и цифровых следов;
- подготовка отчета о событии и отчета об инциденте.

2. Изучить принцип работы **Faraday IDE** и **MagicTree**:

- импорт данных сканирования и логов;
- построение иерархической модели расследования;
- систематизация найденных артефактов.

Вопрос:

Как использование фреймворка Dradis и других инструментов (Faraday IDE, MagicTree) помогает систематизировать данные и подготовить отчет об инциденте кибербезопасности?

Контрольные вопросы:

1. Что такое событие кибербезопасности?
2. Чем событие кибербезопасности отличается от инцидента кибербезопасности?
3. Какие признаки могут указывать на наличие события кибербезопасности?
4. Какие основные этапы включает процесс разработки и анализа инцидента кибербезопасности?

5. Какие источники данных используются для обнаружения и анализа событий кибербезопасности?

6. Что понимается под цифровыми следами и какую роль они играют в расследовании инцидента?

7. Для чего необходимо документирование при расследовании инцидентов кибербезопасности?

8. Чем отличается «Отчет о событии кибербезопасности» от «Отчета об инциденте кибербезопасности»?

9. Какие меры могут применяться при реагировании на подтвержденный инцидент кибербезопасности?

10. Какую роль играют инструменты Kali Linux, Dradis, Faraday IDE и MagicTree в анализе и документировании инцидентов?

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

для обучающихся по организации и проведению самостоятельной работы
по дисциплине «Менеджмент инцидентов кибербезопасности»
для студентов направления подготовки
10.04.01 «Информационная безопасность»
Направленность (профиль):
«Информационная безопасность киберфизических систем»

СОДЕРЖАНИЕ

1. Общая характеристика самостоятельной работы студента.....	99
2. Технологическая карта самостоятельной работы обучающихся дисциплине «Проектирование траектории профессионального роста и личностного развития».....	101
3. Контрольные точки и виды отчетности по ним	102
4. Методические указания по подготовке к лабораторным работам	103
5. Задания, выполняемые по лабораторным работам	104
6. Список рекомендуемой литературы	108

Введение

1. Общая характеристика самостоятельной работы студента

Основными видами учебной работы по достижению результатов освоения дисциплины являются лекции, лабораторные работы и самостоятельная работа студентов (СРС).

На лекциях раскрываются основные положения и понятия курса, формируются знания в области теоретической основы управления. На лабораторных работах формируются умения и навыки, необходимые для решения задач профессиональной деятельности.

Приступая к изучению учебной дисциплины, необходимо ознакомиться с учебной программой, получить в библиотеке рекомендованные учебные пособия, а также получить у ведущего преподавателя в электронном виде конспекты лекций, методические рекомендации к лабораторным занятиям, завести новую тетрадь для конспектирования лекций и выполнения лабораторных заданий.

Для изучения дисциплины предлагается список основной и дополнительной литературы. Основная литература предназначена для обязательного изучения, дополнительная - поможет более глубоко освоить отдельные вопросы, подготовить исследовательские задания и выполнить задания для самостоятельной работы.

В ходе лекционных занятий студент обязан осуществлять конспектирование учебного материала, особое внимание обращая на категории, формулировки, раскрывающие содержание тех или иных понятий, физических явлений, процессов, эффектов. В рабочих конспектах желательно оставлять поля, на которых следует делать пометки из рекомендованной литературы, дополнять материал прослушанной лекции, формулировать научные выводы и практические рекомендации. Студент имеет право задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

Самостоятельная работа студентов над материалом учебной дисциплины является неотъемлемой частью учебного процесса и должна предполагать углубление знания учебного материала, излагаемого на аудиторных занятиях, и приобретение дополнительных знаний по отдельным вопросам самостоятельно.

Основными видами самостоятельной работы студентов по учебной дисциплине являются:

- самостоятельное изучение учебного материала по заданным темам;
- подготовка к лабораторным занятиям, оформление отчета по выполненному практической работе и подготовка к собеседованию по результатам работы.

Основными методами самостоятельной работы студентов являются:

1) для овладения знаниями:

- чтение текста (конспекта лекций, учебника, дополнительной литературы) и конспектирование текста;
- работа с нормативными документами;
- поиск информации в Интернет;

2) для закрепления и систематизации знаний:

- работа с конспектом лекции (обработка текста);
- повторная работа над учебным материалом (учебника, дополнительной литературы, слайдами);
- составление плана и тезисов ответа или графическое изображение структуры ответа;

- составление таблиц для систематизации учебного материала;
- изучение нормативных документов;
- ответы на контрольные вопросы;

3) для формирования умений:

- подготовка к лабораторным занятиям;

- решение задач и лабораторных работ;
- подготовка отчетов по лабораторным занятиям;
- рефлексивный анализ профессиональных умений.

В случае пропуска учебного занятия студент может воспользоваться содержанием различных блоков учебно-методического комплекса (лекции, лабораторные занятия, контрольные вопросы) для самоподготовки и освоения темы. Для самоконтроля необходимо использовать вопросы и задания, предлагаемые к лабораторным занятиям.

2. Технологическая карта самостоятельной работы обучающихся дисциплине «Проектирование траектории профессионального роста и личностного развития»

Коды реализуемых компетенций	Вид деятельности студентов	Средства и технологии оценки	Объём часов, в том числе		
			СРС	Контактная работа с преподавателем	Всего
3 семестр					
ИД-1ПК-2 ИД-2ПК-2 ИД-3ПК-3	Самостоятельное изучение литературы	Собеседование	28.00	8.00	36.00
ИД-1УК-6 ИД-2УК-6 ИД-3УК-6	Подготовка к экзамену	Вопросы к экзамену	28.00	8.00	36.00
Итого за 3 семестр			56.00	16.00	72.00
Итого			56.00	16.00	72.00

3. Контрольные точки и виды отчетности по ним

По дисциплине предусмотрен текущий контроль на каждом учебном занятии и по каждому разделу учебной дисциплины.

Формы текущего контроля:

- устный опрос;
- защита отчетов по лабораторным работам;
- защита отчета по самостоятельному решению разноуровневых задач.

Устный опрос осуществляется на каждом учебном занятии (лекции, лабораторные работы). Все лабораторные работы, выполняемые по разделам дисциплины, подлежат оцениванию по результатам проверки отчета и собеседованию.

Критерии оценки для проверки умений при выполнении лабораторных работ:

- оценка «отлично» выставляется, если студент продемонстрировал высокое умение применять полученные знания на практике через решение конкретной задачи, свободно без затруднений справился с поставленной задачей, показав владение разносторонними приемами и навыками ее выполнения, не допустил ошибок и неточностей;
- оценка «хорошо» выставляется, если студент продемонстрировал умение применять полученные знания на практике через решение конкретной задачи, справился с поставленной задачей, показав владение необходимыми приемами и навыками ее выполнения, при этом допустил не более одной ошибки;
- оценка «удовлетворительно» выставляется, если студент продемонстрировал посредственное умение применять полученные знания на практике через решение конкретной задачи, с трудом справился с поставленной задачей, при этом допустил не более двух ошибок;
- оценка «неудовлетворительно» выставляется, если студент не

продемонстрировал умение применять полученные знания на практике через решение конкретной задачи, не справился с поставленной задачей или допустил при ее решении три и более серьезные ошибки.

4. Методические указания по подготовке к лабораторным работам

При подготовке к практической работе студенту следует:

1. изучить (повторить) теоретический материал, посвящённый теме практической работы;
2. ознакомиться с заданием на лабораторную работу;
3. проверить свой уровень подготовки с помощью вопросов и заданий для самоконтроля.

К работе в лаборатории допускаются лица, изучившие правила и меры безопасности, сдавшие зачет по ним и усвоившие порядок выполнения практической работы.

Требования безопасности перед началом работ:

4. ЗАПРЕЩАЕТСЯ: переодеваться, пользоваться огнем, курить, принимать пищу в лаборатории;
5. убедиться в целостности электрических розеток и разъемов. В лаборатории необходимо быть в сменной обуви;
6. включение компьютера производить только после получения допуска по выполняемой работе и разрешения преподавателя или лаборанта.

Требования безопасности во время работы:

7. выполняя лабораторную работу, студенты обязаны использовать только вычислительную технику, периферийное оборудование, соединительные кабели, измерительное оборудование и носители информации, непосредственно относящиеся к данному практической работе;
8. подключение и отключение составляющих вычислительного комплекса производить только при полном снятии напряжения со всех

составляющих вычислительного комплекса;

9. при обнаружении неисправностей в оборудовании немедленно отключить источники питания и доложить об этом руководителю занятий или лаборанту.

Требования безопасности по окончании работы:

10. доложить руководителю занятий или лаборанту о завершении работ.

11. привести в порядок и сдать рабочее место лаборанту, и доложить руководителю занятий о сдаче.

По результатам выполнения практической работы студенты оформляют и защищают в индивидуальном порядке в форме собеседования результаты выполнения заданий.

При подготовке и выполнении лабораторных работ совместно с оформлением отчетов по лабораторным занятиям позволяет успешно овладеть умениями, необходимыми для дальнейшей учебной и профессиональной деятельности.

Задания, выполняемые по лабораторным работам

Лабораторная работа №1.

Типовые задачи:

Задания базового уровня:

1. Подготовить системы обнаружения инцидентов.
2. Определить возможные источники событий безопасности в информационной системе.

Задания повышенного уровня:

1. Сдержите инцидент с помощью криптографической хеш-функции.

Лабораторная работа №2.

Типовые задачи:

Задания базового уровня:

1. Назовите основные элементы модели безопасности ОС Windows.

2. Дайте определение DACL и SACL.

Задания повышенного уровня:

1. Опишите алгоритмы шифрования в файловой системе EFS.

Лабораторная работа №3.

Типовые задачи:

Задания базового уровня:

1. Назовите основные методы сетевого наблюдения и мониторинга сетевого трафика.
2. Определите принципы работы сетевых протоколов и передачи данных в компьютерных сетях

Задания повышенного уровня:

1. Назовите утилиты и приложения для отслеживания сетевого трафика и цели, для которых они используются

Лабораторная работа №4.

Типовые задачи:

Задания базового уровня:

1. Дайте определение системе обнаружения вторжений (IDS/IPS).
2. Расскажите подробно про систему обнаружения вторжений Snort.

Задания повышенного уровня:

1. Назовите выявление признаков событий на примере работы системы обнаружения вторжений Snort.

Лабораторная работа №5.

Типовые задачи:

Задания базового уровня:

1. Изучите методы обнаружения подозрительной и вредоносной активности с использованием систем типа Honeypot и Padded Cell.
2. Ознакомьтесь с основными типами honeypot-систем, уровнями взаимодействия и особенностями применения технологии Padded Cell.

3. Дайте определение обманным системам (deception technologies).
4. Перечислить ключевые недостатки и риски, связанные с эксплуатацией систем-ловушек и изолированных ячеек.

Задания повышенного уровня:

1. Изучите возможности использования технологии Padded Cell для перенаправления злоумышленника в контролируемую среду.

Лабораторная работа №6.

Типовые задачи:

Задания базового уровня:

1. Изучите основные принципы работы сетевых протоколов TCP и UDP.
2. Изучить базовые возможности сканера Nmap и методы проведения безопасного сканирования в локальной сети.

Задания повышенного уровня:

1. Проведите тестовое сканирование с помощью Nmap и определите риски для каждого найденного узла.

Лабораторная работа №7.

Типовые задачи:

Задания базового уровня:

1. Дайте общие сведения о системе Secret Net.
2. Назовите признаки и критерии отнесения зарегистрированных событий к инцидентам информационной безопасности.
3. Назовите особенности анализа журналов регистрации, сообщений и уведомлений системы Secret Net при исследовании инцидентов информационной безопасности.

Задания повышенного уровня:

1. Подготовьте лабораторную среду, содержащую установленную систему Secret Net, учетные записи пользователей, тестовые защищаемые объекты, журналы регистрации событий, а также исходные данные,

необходимые для моделирования и анализа инцидентов информационной безопасности.

Лабораторная работа №8.

Типовые задачи:

Задания базового уровня:

1. Назовите методы контроля состояния и безопасности беспроводной сети.
2. Дайте определение настройка беспроводной сети Wi-Fi в различных режимах работы.

Задания повышенного уровня:

1. Изучить принципы работы протоколов безопасности Wi-Fi, методы разведки и идентификации несанкционированных точек доступа (Rogue AP) через анализ практических примеров.

Лабораторная работа №9.

Типовые задачи:

Задания базового уровня:

1. Дайте определение основным понятиям, связанные с событиями и инцидентами кибербезопасности, их классификацией, признаками и порядком реагирования.
2. Подготовить лабораторную среду, содержащую исходные данные для анализа: журналы событий, описание сценария нарушения, технические признаки инцидента, сетевые и системные артефакты.
3. Расскажите для чего необходимо документирование при расследовании инцидентов кибербезопасности.

Задания повышенного уровня:

1. Расскажите какую роль играют инструменты Kali Linux, Dradis, Faraday IDE и MagicTree в анализе и документировании инцидентов.

5. Список рекомендуемой литературы

Основная литература:

1. Кибербезопасность цифровой индустрии / Зегжда Д.П. Москва: Горячая линия - Телеком, 2022. — 556, [3] с. ил.; 24. — ISBN 978-5-9912-0827-7.
2. Управление инцидентами кибербезопасности: учеб. пособие / С. Л. Зефирова, А. Ю. Щербакова. – Пенза: Изд-во ПГУ, 2012. – 104 с.
3. Investigation of information security incidents: a manual / I.N. Vasilyeva. – Saint Petersburg: Publishing house of Saint Petersburg State University of Economics, 2019. – 113 p.

Дополнительная литература:

1. Баркалов Ю.М., Гайдин А.И., Потанина И.В. Процессуальные и организационно-тактические особенности фиксации доказательственной информации, обнаруженной в сети Интернет. Метод. рекомендации. – Воронеж: Воронежский институт МВД России, 2016. – 52 с.
2. Баркалов Ю.М., Нестеровский О.И., Лиходедов Д.Ю. Организационно-техническое обеспечение специальных мероприятий. Метод. рекомендации. – Воронеж: Воронежский институт МВД России, 2016. – 82 с.
3. Введенская О.Ю. Расследование преступлений в сфере компьютерной информации: лекции, 2016. – Краснодар: Краснодарский ун-т МВД РФ. Кафедра криминалистики. – 126 с.
4. R.C. Arkin and T. Balch. AuRA: Principles and practice in review. Journal of Experimental and Theoretical Artificial Intelligence, 9(2-3):175–189, 1997.
5. Khalid, A.; Kirisci, P.; Khan, Z.H.; Ghrairi, Z.; Thoben, K.D.; Pannek, J. Security framework for industrial collaborative robotic cyber–physical systems. Comput. Ind. 2018, 97, 132–145.