«Министерство науки и высшего образования Российской Федерации Федеральное государственное автономное образовательное учреждение высшего образования «Уральский федеральный университет имени первого Президента России Б.Н. Ельцина»

Институт радиоэлектроники и информационных технологий – РТФ

Тема:

Разработка интерактивного обучающего модуля для старшеклассников и студентов младших курсов "Этичный Хакинг"

Куратор проекта: Сергеев Алексей Анатольевич

Студент: РИ-321002 Эльбьяри Мохамед Айман Хассан Эльсайед

Студент: РИ- 411001 Серон Кабрера Алехандро Патрисио

Студент: РИ-321002 Элия Киролос Хайри Фавзи

Студент: РИ-321002 Салем Мохамед Ахмед Элсайед

Екатеринбург

2025

Сегодня перед организациями стоит задача быстро обнаруживать нарушения кибербезопасности и эффективно реагировать на инциденты безопасности. Группы людей в центрах обеспечения безопасности (SOC) внимательно следят за системами безопасности и защищают свои организации, выявляя и реагируя на угрозы кибербезопасности. Курс CCNA Cybersecurity Operations v1.0 (CyberOps) готовит кандидатов к началу карьеры в качестве младшего аналитика по кибербезопасности в центрах безопасности (SOC).

К субъектам угрозы относятся, помимо прочего, любители, хактивисты, организованные преступные группы, спонсируемые государством группы и террористические группы. Субъектами угроз являются отдельные лица или группы лиц, которые осуществляют кибератаки против другого лица или организации. Кибератаки — это преднамеренные вредоносные действия, направленные на то, чтобы нанести ущерб другому человеку или организации.

Любители, которых также называют «сценаристами», не обладают никакими навыками или талантом. Для осуществления атак они часто используют инструменты или инструкции, найденные в Интернете. Некоторые просто любопытны, в то время как другие пытаются блеснуть своими способностями, устраивая пакости. Хотя они используют базовые инструменты,

Активные хакеры

Хакеры-активисты — это хакеры, которые протестуют против различных политических и социальных идей. Активные хакеры публично протестуют против организаций или правительств, публикуя статьи и видео, раскрывая конфиденциальную информацию и нарушая работу веб-сервисов с помощью незаконного трафика в ходе распределенных атак типа «отказ в обслуживании» (DDoS).

финансовая выгода

Значительная часть хакерской активности, которая постоянно угрожает нашей безопасности, имеет финансовую мотивацию. Эти киберпреступники хотят получить доступ к нашим банковским счетам, нашим персональным данным и всему остальному, что они могут использовать для получения денежных средств.

Секреты торговли и мировой политики

За последние несколько лет было зафиксировано множество случаев, когда национальные государства взламывали системы других стран или вмешивались во внутреннюю политику. Национальные государства также заинтересованы в использовании киберпространства для промышленного шпионажа. Кража интеллектуальной собственности может дать стране значительное преимущество в международной торговле. Останется защитой от последствий кибершпионажа

Насколько безопасен Интернет вещей?

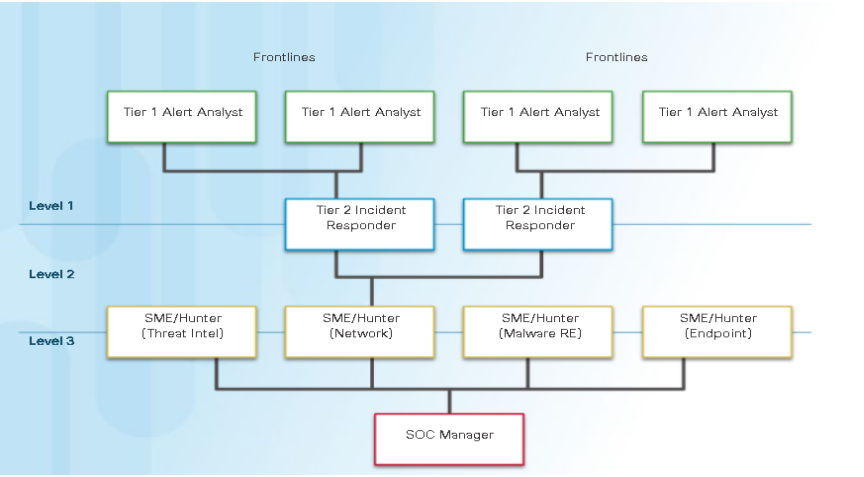
На связи ежедневно. Интернет вещей помогает людям объединять вещи и улучшать качество своей жизни. Например, многие люди теперь используют подключенные носимые устройства для отслеживания своей физической активности. Сколько устройств в настоящее время подключено к вашей домашней сети или Интернету?

Насколько безопасны эти устройства? Например, кто написал прошивку? Заметил ли программист недостатки безопасности? Подвержен ли ваш домашний термостат атакам? А как насчет вашего цифрового видеорегистратора? Если обнаружены уязвимости, можно ли исправить прошивку устройства, чтобы устранить уязвимость? Многие устройства в Интернете не обновлены до последней версии прошивки. Некоторые старые устройства даже не рассчитаны на обновление с помощью патчей. Эти две ситуации создают возможности для злоумышленников и риски безопасности для владельцев этих устройств.

В октябре 2016 года DDoS-атака на провайдера доменных имен Dyn вывела из строя несколько популярных веб-сайтов. Атака осуществлялась с использованием большого количества веб-камер, видеорегистраторов, маршрутизаторов и других устройств Интернета вещей, которые были скомпрометированы вредоносным ПО. Эти устройства образовали «ботнет», контролируемый хакерами. Этот ботнет использовался для создания масштабной DDoS-атаки, которая нарушила работу основных интернет-сервисов. Дин опубликовала здесь запись в блоге, в которой рассказала о нападении и своей реакции на него.

People in the SOC

Tier 1 Alert Analyst – These professionals monitor incoming alerts, verify that a true incident has occurred, and forward tickets to Tier 2, if necessary.
Tier 2 Incident Responder- These professionals are responsible for deep investigation of incidents and advise remediation or action to be taken.
Tier 3 Subject Matter Expert (SME)/Hunter – These professionals have expert-level skill in network, endpoint, threat intelligence, and malware reverse engineering. They are experts at tracing the processes of the malware to determine its impact and how it can be removed. They are also deeply involved in hunting for potential threats and implementing threat detection tools.
SOC Manager – This professional manages all the resources of the SOC and serves as the point of contact for the larger organization or customer



1. Windows NT History and Versions: Since 1993, Microsoft has released over 20 NT-based Windows versions, known for security and enterprise features. It gained traction among individuals and businesses for workstations and servers.

2. Transition to 64-bit: Starting with Windows XP, 64-bit architecture improved memory support and advanced applications while maintaining 32-bit compatibility.

3. Version Evolution: Windows 7, 8, and 10 introduced varied features and pricing. Microsoft shifted to continuous updates with Windows 10.

4. Security: Systems face vulnerabilities, mitigated by antivirus, encryption, firewalls, and access controls.

These are some common Windows OS Security Recommendations:

Virus or malware protection

Unknown or unmanaged services

Encryption

Security policy

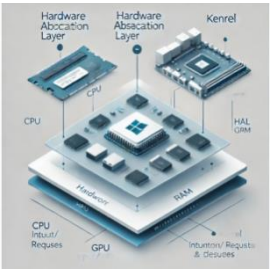
Firewall

File and share permissions

Weak or no password

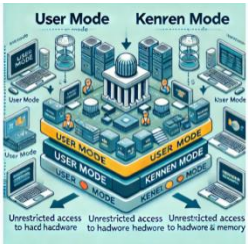
Login as Administrator

5. System Architecture (HAL): The Hardware Abstraction Layer ensures efficient communication between hardware and the kernel.



The Hardware Abstraction Layer (HAL) separates the operating system from hardware variations, allowing the OS to run on different machines. HAL manages communication between the hardware and the kernel, which controls resources like memory and peripherals. While the kernel typically interacts directly with hardware in some cases, HAL handles most communication but depends on the kernel for certain tasks.

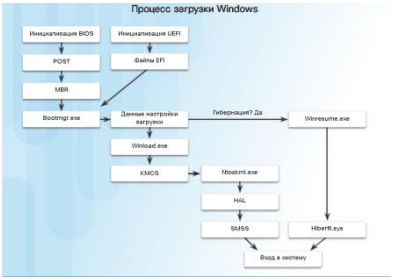
6. User and Kernel Modes: Applications run in user mode for isolation, while kernel mode offers direct hardware access, risking system crashes if errors occur.



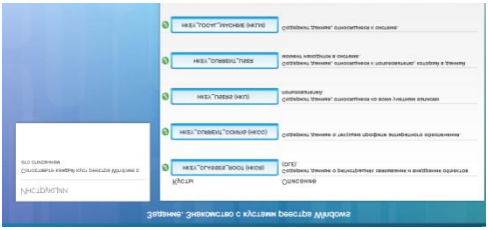
7. File Systems: Includes FAT, exFAT, and NTFS, with NTFS offering advanced security and data recovery. Alternate Data Streams (ADS) may conceal malware.

8. Disk Partitioning and Formatting**: Storage requires partitioning and file systems like NTFS for organized management.

9. Boot Process: Varies between BIOS and UEFI, involving files like Bootmgr.exe and Winload.exe, with Secure Boot enhancing safety.



10. Windows Registry: A database storing system/user information, modifiable via regedit but requires caution to avoid issues.

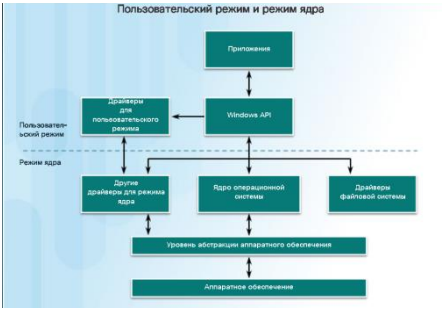


Операционная система Windows (как она работает, ее история и структура(

Windows Operating System Infrastructure:

Hardware and Kernel Abstraction Unit (HAL).

Two operating modes: Kernel mode for running system code, and User mode for running applications.



Windows использует HAL для связи между оборудованием и ядром

Режим ядра: запускает системный код и имеет полный доступ к оборудованию, но ошибки приводят к сбою системы.

Пользовательский режим: приложения запускаются изолированно, ошибки влияют только на приложение.

Драйверы могут работать в любом режиме, а ошибки режима ядра могут привести к сбоям системы.

Файловая система NTFS:
Он состоит из 4 основных структур данных: загрузочный сектор, основная таблица файлов (MFT), системные файлы и файловая область.

Управление процессами и потоками:
Процесс = выполняемая программа.
Поток = исполняемая часть процесса.
Windows поддерживает виртуальное адресное пространство размером до 4 ГБ (32-разрядная версия) и 8 ТБ (64-разрядная версия).

1. BIOS/UEFI: POST и находит операционную систему.

2. Bootmgr.exe: считывает настройки BCD и переводит систему в защищенный режим.

3. Winresume/Winload: выход из спящего режима или загрузка системы с нуля.

4. Ntoskrnl.exe и SMSS: Запустите ядро и настройте пользовательскую среду.

-База данных реестра:

Содержит информацию об устройствах, приложениях и пользователях.

Наиболее важные клетки: HKCU, HKU, HKCR, HKLM, HKCC.

Запускать:

1. Регистратор: HKEY_LOCAL_MACHINE и HKEY_CURRENT_USER определяют, какие службы и приложения запускаются автоматически.
2. Msconfig: управление настройками загрузки (типы загрузки, службы, приложения).

Неисправность:

1. Регулярно закрывает приложения и службы во избежание повреждения.
2. Способы завершения работы: меню «Пуск», команда завершения работы или сочетание клавиш Ctrl+Alt+Delete.
3. Варианты: Остановить, Перезапустить, Спящий режим.

Отдел системы и безопасности:

Настраивайте пользователей и группы и управляйте ими.

Мониторинг ресурсов с помощью таких инструментов, как PowerShell, WMI и удаленный рабочий стол.

Защитите систему с помощью таких инструментов, как Защитник Windows, Брандмауэр и Просмотр событий.

Операционная система Linux:

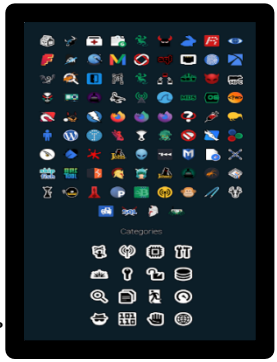
Определение Linux

1. Операционная система с открытым исходным кодом, выпущенная в 1991 году, характеризуется скоростью, гибкостью и высокой производительностью при небольшом потреблении ресурсов.
2. Исходный код можно легко изменить, что делает его пригодным для настройки систем.
3. Он широко используется: от небольших устройств (таких как часы) до суперкомпьютеров.

Linux считается идеальным выбором в области кибербезопасности, поскольку он обеспечивает полный контроль, расширенные инструменты и высокую гибкость настройки. Он широко используется для сетевого анализа, управления журналами и обнаружения вторжений, что делает его основой для специалистов по безопасности SOC.

Важность Linux в центрах управления безопасностью (SOC):

Гибкость в настройке: систему можно настроить и добавить только необходимые инструменты.
Мощный интерфейс командной строки: позволяет эффективно выполнять операции с использованием меньшего количества ресурсов.
Больший контроль: позволяет пользователю root легко изменять каждый аспект системы.
Сетевые инструменты: Обеспечивает идеальную среду для разработки сетевых приложений и аналитических инструментов



Общие инструменты безопасности в Linux:

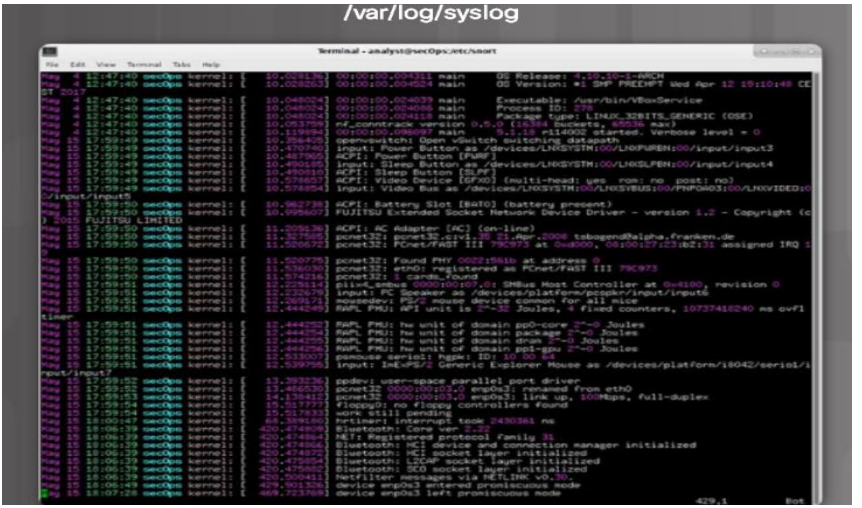
Wireshark: для анализа сетевых пакетов.
Инструменты анализа вредоносного ПО.
Системы обнаружения вторжений (IDS).
Брандмауэры.
Управление журналами: для анализа событий.
Инструменты SIEM: для анализа событий безопасности.

Инструменты каждой версии отличаются от другой, а есть инструменты специально для проникновения или защиты.

Управление журналами:

-Управление журналами означает сбор, анализ и мониторинг файлов журналов для отслеживания производительности системы и выявления ошибок или угроз безопасности

/var/log/messages	-Содержит общие системные сообщения, такие как события запуска службы. -Полезно для отслеживания неопознанных проблем**.**
/var/log/auth.log	-Регистрирует события аутентификации (например, вход/сбой). -Он используется для мониторинга охранной деятельности.
/var/log/boot.log	-Показывает этапы процесса загрузки системы. -Помогает диагностировать ошибки загрузки.
/var/log/dmesg	-Содержит сообщения ядра во время загрузки. -Используется для устранения проблем с оборудованием и драйверами.



Типы файловых систем в Linux:

Локальные системы Linux:

ext2: быстрый, без журналирования, идеально подходит для флэш-памяти.

ext3: поддерживает ведение журнала для защиты данных (размер файла до 32 ТБ).

ext4: быстрее и больше, чем ext3, поддерживает работу без ведения журнала.

Сетевые системы и специализация:

NFS: обмен файлами по сети.

CDFS: для компакт-дисков.

Специальные системы:

Подкачка: используется в качестве памяти, когда ОЗУ заполнено.

Системы Apple:

HFS+: для Apple, поддерживается Linux.

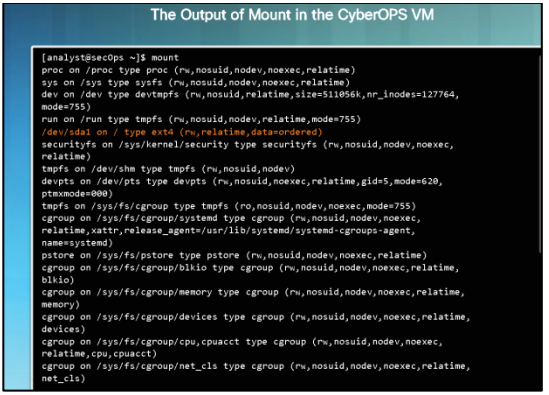
APFS: современный, зашифрованный, для устройств Apple и SSD.

Дополнительная информация:

MBR: хранит информацию о разделах диска.

Монтаж: связывает систему с папкой для доступа

Команда монтирования: отображает смонтированные системы:



Серверы, службы и порты:

Виртуальные порты используются для облегчения связи между клиентом и сервером

Сервер:

Устройство, предоставляющее услуги по сети.

Порт:

Сетевой ресурс, выделенный для определенной службы.

Сервер «прослушивает» порт, связанный со службой.

Порты по умолчанию (хорошо известные порты):

Примеры

Сетевые протоколы и сервисы:

1Роль аналитиков кибербезопасности:

-Анализируйте следы сетевых событий для выявления подозрительных или вредоносных действий.

-Эти трассировки основаны на журналах устройств, таких как адреса подключенных хостов и поведение сети.

Цель: Обнаружение угроз, нацеленных на данные и безопасность организаций**.**

Передача данных:

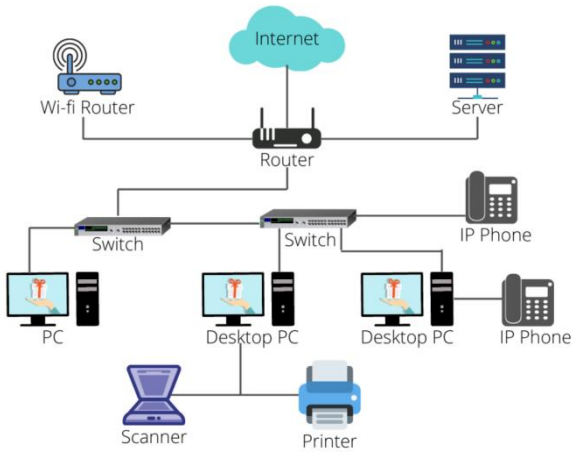
1. **Медные кабели**: используются в локальных сетях, таких как Ethernet.
2. **Оптоволокно**: обеспечивает высокую скорость передачи данных на большие расстояния.
3. **Беспроводная связь**: включает Wi-Fi и мобильные сети.

Уровни сетей:

Первый уровень (Tier 1): глобальные провайдеры соединяют континенты.
Второй уровень (Tier 2): региональные провайдеры подключают города.
Третий уровень (Tier 3): локальные сети для домов и малого бизнеса.

Анализ трафика:

Определение источника и назначения данных помогает обнаруживать подозрительные активности, предотвращая кибератаки.



Протокол TCP/IP обеспечивает коммуникацию между устройствами в интернете.

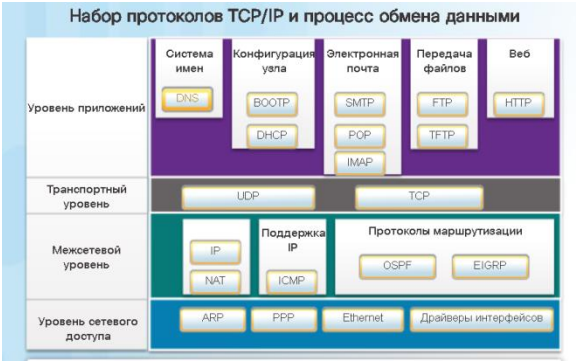
1. Уровень приложений (Application Layer):
Предоставляет интерфейс для приложений:
HTTP/HTTPS: просмотр веб-страниц.
DNS: преобразование доменных имен в IP-адреса.
SMTP: отправка электронной почты.
FTP: передача файлов.

2. Транспортный уровень (Transport Layer):

Отвечает за передачу данных:

TCP: надежная передача с проверкой.

UDP: быстрая передача без проверки.



3. Интернет-уровень (Internet Layer):

Маршрутизация данных:

IP: адресация устройств.

ICMP: диагностика сети

ARP: преобразование IP-адресов в MAC-адреса.

4. Уровень доступа к сети (Network Access Layer):

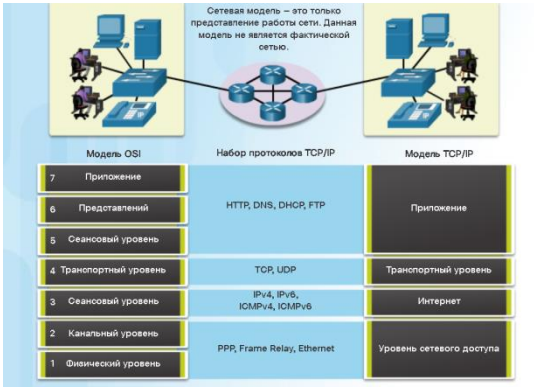
Передача данных через физические носители (кабели, волокно, беспроводная связь).

Роль TCP/IP:

Обеспечивает универсальное соединение.

Используется для анализа трафика и обнаружения угроз

Эти уровни включают в себя: физический уровень, уровень соединения, сетевой, транспортный, сеансовый, презентационный и прикладной.



Сценарий отправки и получения веб-страницы:

1. Отправить данные: Создаётся HTTP-запрос (например, HTML или JSON) браузером. Запрос проходит через уровни протокола TCP/IP.

На уровне TCP данные разбиваются на сегменты

На уровне IP сегменты упаковываются в пакеты с добавлением IP-адресов отправителя и получателя.

На уровне Ethernet пакеты оборачиваются в кадры и отправляются по сети.

2. Передача данных:

Кадры передаются через сеть с использованием маршрутизаторов (Routers) и коммутаторов (Switches) до достижения адресата.

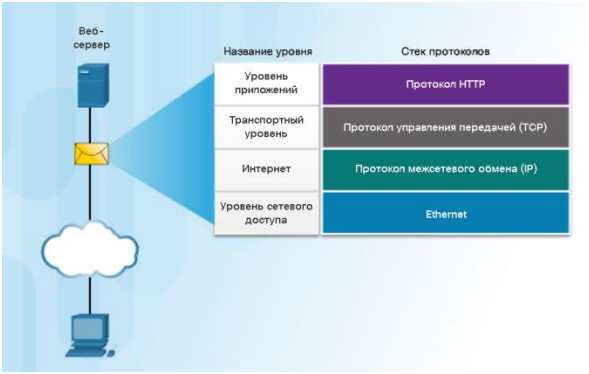
Прием данных:

На стороне получателя оболочки снимаются в обратном порядке:

-Кадры (Ethernet) разбираются на пакеты.

-Пакеты передаются на уровень IP для анализа адресов.

-На уровне TCP сегменты собираются в исходные данные.
В итоге HTTP-контент (HTML) передаётся в браузер и отображается пользователю.

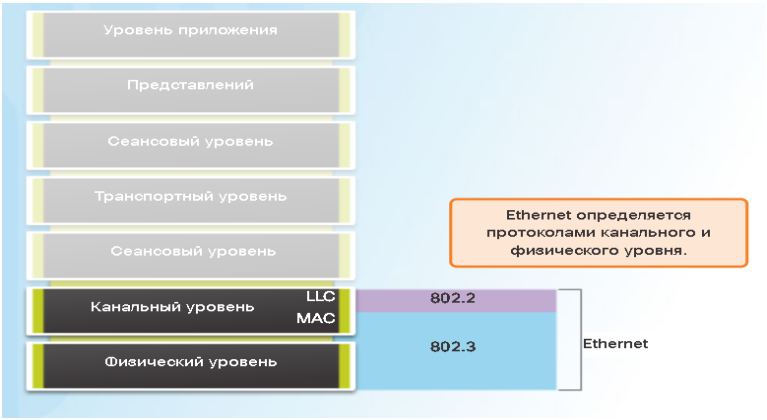


Данные упаковываются и отправляются через сеть, затем распаковываются на стороне получателя.

Протокол Ethernet:

Классы, в которых он работает:Протокол Ethernet работает на двух уровнях модели OSI

Канальный уровень (Data Link): отвечает за упаковку данных в кадры и обеспечение надёжности передачи внутри локальной сети (LAN).
Физический уровень (Physical): отвечает за передачу сигналов по физической среде (кабели, оптоволокно или беспроводная связь).



Упаковка пакетов в рамки:

Ethernet упаковывает данные, поступающие с сетевого уровня (например, пакет IP), в кадр (Frame), который включает:

-MAC-адреса отправителя и получателя.

-Данные пакета.

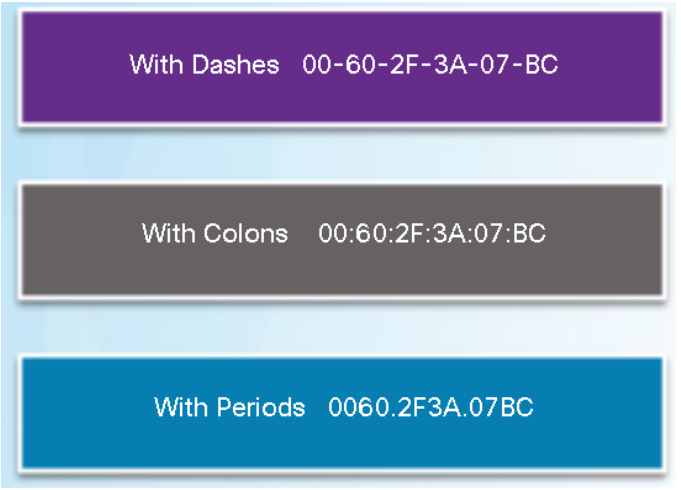
-Код проверки ошибок (CRC) для обеспечения целостности данных

Контроль доступа к медиа:

Ethernet контролирует использование физической среды устройствами:

-Использует методы CSMA/CD (для старых сетей) или CSMA/CA для предотвращения коллизий.

-Определяет время передачи данных каждым устройством для обеспечения их бесперебойного перемещения.



Протокол Ethernet обеспечивает эффективную передачу данных в локальной сети через упаковку и управление доступом к среде.

Класс и IP (IP -инкапсуляция):

1. Инкапсуляция:

-Когда данные отправляются между устройствами, процесс упаковки начинается с верхних слоев формы (например, приложения) до самого низкого уровня (сетевой уровень).

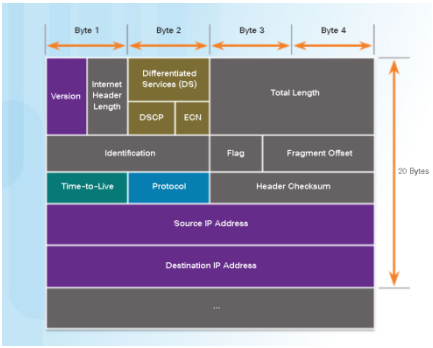
-Данные проходят разные этапы, так как каждый слой добавляет свою информацию (заголовки), прежде чем он будет доставлен на следующий уровень.

2. Транспортный слой:

Такие протоколы, как TCP/UDP, добавляют заголовок, содержащий:

-Номер порта источника и назначения.

-Управляющая информация, такая как порядковые номера пакетов.



3. Сетевой уровень

4. Руководитель:

Заголовок представляет собой структурированные данные, содержащие двоичные настройки (биты).

Эти поля включают в себя:

Версия: выбор версии IP (IPv4 или IPv6).

Общая длина: размер всей упаковки.

Контрольная сумма заголовка: для обеспечения целостности головы.

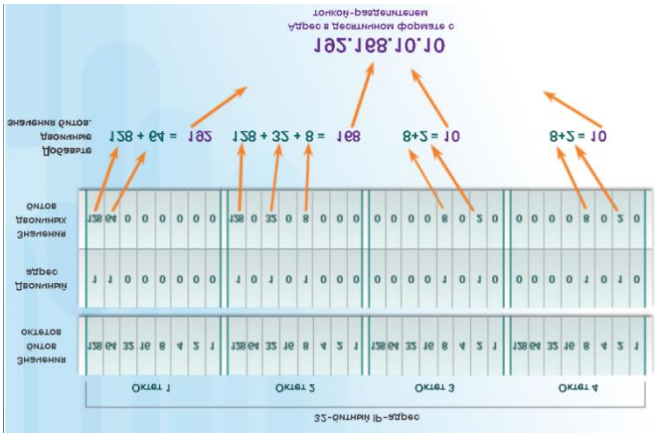
Маршрутизация:

После инкапсуляции пакета он отправляется по сети.

Маршрутизаторы используют информацию в заголовке IP, чтобы определить лучший путь для достижения пункта назначения

Категории IPv4:

В протоколе IPv4 адреса разделены на 5 основных категорий (A, B, C, D, E), но общее использование - A, B и C. Каждая категория имеет свои характеристики, такие как объем адресов и количество хостов.



Класс A:

Домен: от 1,0,0,0 до 126.255.255.255

(Первый заголовок зарезервирован, например, 0,0,0,0, и 127 зарезервирован для Localhost).

Сетевая маска по умолчанию: /8 (255.0.0.0).

Количество сетей: 128 сети (фактически 126).

Количество хостов: около 16,7 миллиона хостов для каждой сети.

Использовать:

Для очень больших сетей, таких как интернет -поставщики (интернет -провайдеры) и крупные учреждения.

Класс B:

Домен: с 128.0.0.0 до 191.255.255.255.

Маска сети по умолчанию: /16 (255.255.0.0).

Количество сетей: 16 384 сети.

Количество хостов: около 65 536 хостов для каждой сети.

Использовать:

Для средних сетей, таких как университеты и крупные компании.

Класс C:

Домен: с 192.0.0.0 до 223.255.255.255.

Маска сети по умолчанию: /24 (255.255.255.0)

Количество сетей: около 2 миллионов сетей.

Количество хостов: 254 хоста для каждой сети.

Использовать:

Для небольших сетей, таких как домашние сети и небольшие компании.

Класс D:

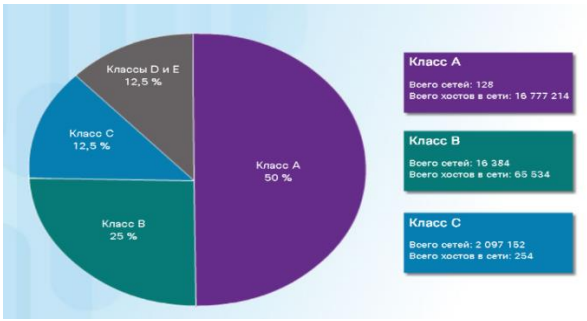
Домен: от 240.0.0.0 до 255.255.255.255

Использование: для многоадресной рассылки (передача данных в определенный набор устройств).

Класс E:

Домен: от 240.0.0.0 до 255.255.255.255

Использование: экспериментальные исследования и разработки.



Классификация определяет названия и количество хостов для каждой сети.

Потребность в IPv6:

1. Проблема с IPv4:
Ограниченные адреса:
IPv4 предоставляет около 4,3 миллиарда титулов (2^32), что является большим, но недостаточным числом из -за:
Увеличение количества устройств (таких как телефоны, компьютеры, интернет IoT).
Представление адресов неэффективно в начале.
Доступные названия начали выходить к 2011 году.
Временные методы:
Такие методы, как NAT (трансляция сетевого адреса), были прибегнуты к адресам, но они не являются постоянным решением.

2. IPv6: устойчивое решение:
Увеличить количество адресов:
IPv6 используется 128 бит вместо 32 бит в IPv4, который предоставляет:
(Нет. Превышает человеческие потребности в этапах).
Расширение использования:
IPv6 может поддерживать быстрое расширение в интернет -подключенных устройствах, особенно в разработке областей, которые необходимо настраивать новые адреса.

Полностью развернутый	2001:0DB8:0000:1111:0000:0000:0000:0200
Без начальных нулей	2001: DB8: 0:1111: 0: 0: 0: 200
Сокращенный	2001:DB8:0:1111::200

3. Функции IPv6:

Огромное распределение:

Каждое устройство может получить уникальный адрес без необходимости в таких технологиях, как NAT.

Лучшая производительность:

Улучшение руководства с меньшими головами и гибкими структурами.

Дополнительные функции:

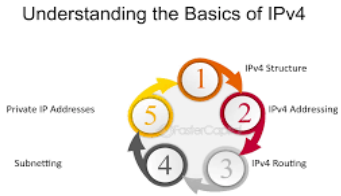
Лучшая поддержка шифрования и безопасного общения.

Механизм автоматической конфигурации для упрощения настройки сети.

4. Разница между IPv4 и IPv6:

IPv6	IPv4	Особенность
128 бит	32 бита	Длина адреса
340 undecillion	4,3 миллиарда	Количество адресов
Протокол	ограничен	Шифрование
Автоконфигурация	Руководство/Nat	Механизм

IPv6 - это не только решение проблемы посвящения адресов, но и шаг к более эффективному и безопасному будущему, что поддерживает рост современных технологи



ARP (протокол разрешения адреса):

Работа:

Адрес IPv4 переводится в MAC -адрес, чтобы обеспечить связь между устройствами в одной и той же локальной сети (LAN).

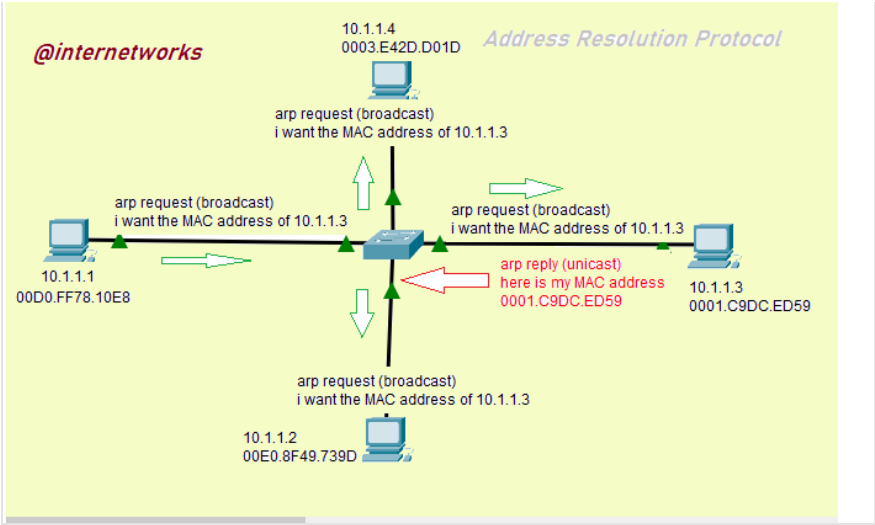
Как работать:

Устройство отправляет запрос ARP в сеть: «У кого есть IP -адрес?»

Желаемый IP -адрес содержится под названием Mac.

Информация хранится в таблице ARP для будущего использования.

-Протокол ARP сопоставляет IP-адрес устройства с его MAC-адресом, отправляя запрос в сеть и получая ответ от устройства-адресата.



TCP/UDP:

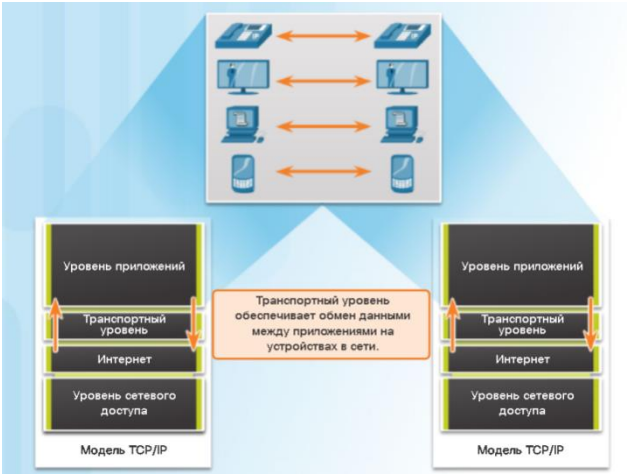
Роль: регулирование потока данных между приложениями.

TCP:

(1Надежное, прибытие данных обеспечивает правильный порядок.

(2Признание и отслеживание деталей.

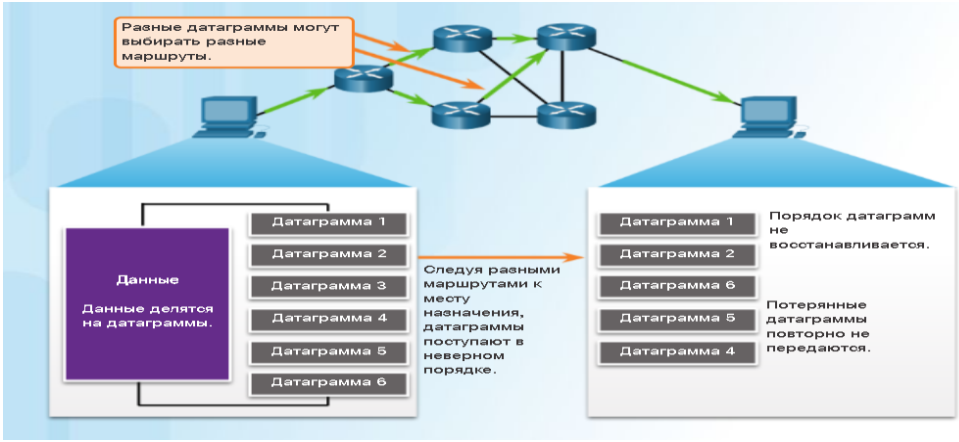
(3Приложения: электронная почта, веб -просмотр.



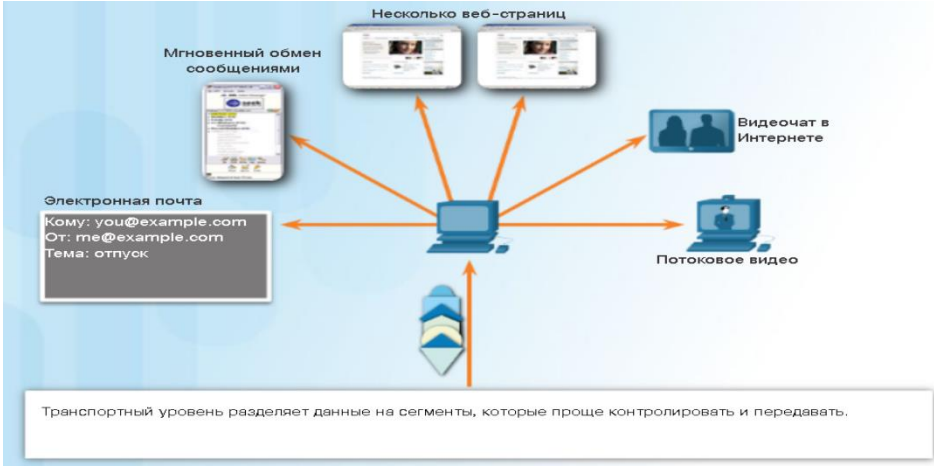
UDP:

Ненадежный (с самыми низкими затратами на лечение

Подходит для приложений, которые несут потерю данных, такие как прямое вещание.



Каждый протокол соответствует различным типам приложений в соответствии с его требованиями.



Адреса TCP/UDP:

Главные компоненты:

Источник и порт назначения для определения приложений.

Серийный номер и номер утверждения для заверения.

Тестовая сумма заключается в обеспечении безопасности данных.

Транспортные протоколы предоставляют механизмы для регулирования данных и подтверждения их прибытия.

DHCP (протокол динамической конфигурации хоста):

Флаг широковещания используется для указания серверу или агенту

Поля ретрансляции отправить ответ в виде широковещательной рассылки.

Поля IP-адреса:

(1IP-адрес клиента: используется при продлении, если адрес действителен, но при запросе нового адреса он равен 0.

(2Ваш IP-адрес: назначается сервером клиенту.

(3IP-адрес сервера: используется для идентификации сервера, отвечающего клиенту.

(4IP-адрес шлюза: используется для маршрутизации через ретрансляционные прокси.

8	16	24	32
Код операции (OP) (1)	Тип аппаратного обеспечения (1)	Длина аппаратного адреса (1)	Переходы (1)
Идентификатор транзакции (XID)			
Секунды – 2 байта		Флаги – 2 байта	
IP-адрес клиента (CIADDR) – 4 байта			
Ваш IP-адрес (YIADDR) – 4 байта			
IP-адрес сервера (SIADDR) – 4 байта			
IP-адрес шлюза (GIADDR) – 4 байта			
Физический адрес клиента (CHADDR) – 16 байт			
Имя сервера (SNAME) – 64 байта			
Имя файла загрузки – 128 байт			
Параметры DHCP – размер не задан			

Имя сервера: Сервер может указать свое текстовое имя или DNS-имя.

Имя загрузочного файла: используется для указания желаемого загрузочного файла.

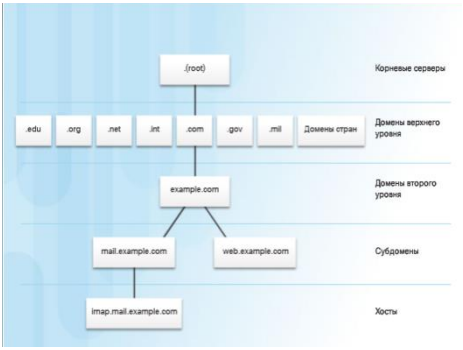
Параметры DHCP: Содержит дополнительные параметры.

Система доменных имен (DNS):

Цель:

Преобразуйте текстовые имена (например, www.cisco.com) в IP-адреса.

Управление иерархией доменов.



Основные ингредиенты:

(1Resolver: клиент, отправляющий DNS-запрос.

(2Авторизованный сервер: отвечает подтвержденной информацией.

(3Рекурсивный сервер: запросы от имени аналитика**.**

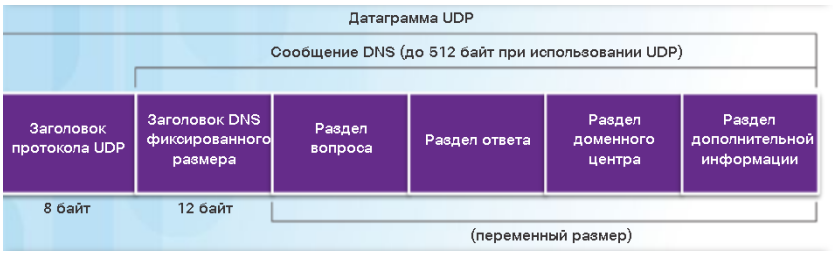
Типы записей:

(1O: IPv4-адрес.

(2AAAA: IPv6-адрес.

(3HC: сервер имен.

(4MX: обмен почтой.



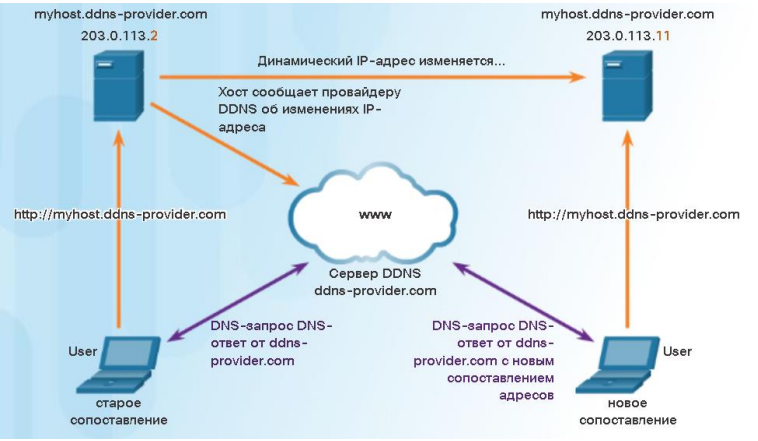
Временное хранение:

Результаты сохраняются локально, чтобы ускорить будущие запросы.

Динамический DNS (DDNS):

Позволяет быстро обновлять сопоставления DNS при изменении IP-адреса.

Субдомен клиента зарегистрирован у провайдера DDNS.



WHOIS:

Цель: Определить владельцев домена.
Ограничения: Хакеры могут скрыть свою личность.

Инструмент для идентификации владельцев потенциально опасных доменов и веб-сайтов.

Протоколы играют жизненно важную роль в мире цифровых сетей и коммуникаций. Это правила и стандарты, которые регулируют обмен данными между различными устройствами по сетям. Каждый протокол имеет определенную функцию, направленную на обеспечение организованной и безопасной передачи данных, обеспечивая эффективную работу Интернета и связанных с ним приложений.

FTP (протокол передачи файлов):

Цель: Передача данных между клиентом и сервером.

Коммуникации:

TCP-порт 21: командное управление.

TCP-порт 20: передача данных.

Особенности: Поддерживает загрузку и загрузку.

Безопасность: Небезопасно по умолчанию; Предпочтительно

использовать SFTP (безопасный FTP) с протоколом SSH.

TFTP (простой протокол передачи файлов):

Назначение: Простая передача файлов.

Коммуникации: UDP-порт 69.

Особенности: Не поддерживает управление файлами (например, удаление/вставку).

Использование: Для некритических сетевых приложений.

Безопасность: Небезопасно, используйте только при необходимости.

SMB (блок сообщений сервера):

Цель: общий доступ к файлам и принтерам по сети.

Связь: протокол запроса/ответа, который поддерживает аутентификацию и контроль доступа.

Использование: необходим в сетях Microsoft.

Возможности: Управление сетевыми ресурсами, такими как файлы и принтеры

SMTP (простой протокол передачи почты):

Цель: Отправка электронной почты.

Коммуникации: TCP-порт 25.

Функции:

Сохранение сообщений, если сервер назначения недоступен.

Повторите попытку отправки недоставленных сообщений.

Безопасность: Небезопасно по умолчанию.

POP3 (протокол почтового отделения версии

Цель: Восстановление электронной почты.

Коммуникации: TCP-порт 110.

Функции:

Загрузите сообщения на клиент и удалите их с сервера.

Он не обеспечивает централизованное место для хранения почты.

Использование: Не идеально подходит для предприятий, которым требуется резервное копирование.

HTTP (протокол передачи гипертекста):

Цель: Перенос веб-страниц и онлайн-ресурсов.

Коммуникации: TCP-порт 80.

Функции:

Методы HTTP: (GET, POST, PUT, DELETE, OPTIONS, CONNECT).

ненадежный; Сообщения отправляются в виде обычного текста.

Использование: Загрузка веб-страниц.

HTTPS (безопасный HTTP):

Цель: Безопасная связь через Интернет.

Связь: TCP-порт 443.

Безопасность:

Шифрование данных с использованием SSL/TLS.

Защитите конфиденциальную информацию (пароли, кредитные карты).

Основное использование	Безопасность	Транспорт	Порты	Протокол
Передача файлов	Небезопасно (безопасно SFTP)	Двунаправленный	TCP 20, 21	FTP
Простая транспортировка	ненадежный	Двунаправленный	UDP 69	TFTP
Обмен файлами	Поддерживает аутентификацию	Двунаправленный	переменная	SMB
Отправить письмо	ненадежный	Только отправлять	TCP 25	SMTP
Восстановить почту	ненадежный	Только скачивание	TCP 110	POP3
Почтовая администрация	Безопаснее	Загрузите и синхронизируйте	TCP 143	IMAP
Веб-страницы	ненадежный	Запрос/ответ	TCP 80	HTTP
Безопасные веб-страницы	Шифрование (SSL/TLS)	Запрос/ответ	TCP 443	HTTPS

В этом документе мы кратко рассмотрим наиболее важные протоколы, используемые в сетях, выделив их основные функции, используемые порты и уровень безопасности, который они обеспечивают. Это понимание помогает лучше управлять сетями и повышать их производительность, одновременно удовлетворяя растущие потребности пользователей.

Сетевая инфраструктура:

В этой главе рассматриваются основы сетевой архитектуры и проектирования, включая проводные и беспроводные сети, сетевая безопасность, а также способы эффективного и безопасного построения сетей.

Routers:

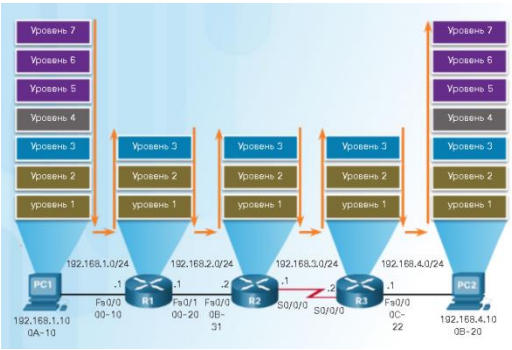
-Он работает на уровне 3 (сети) модели OSI.

Две основные функции:

Определение маршрута: создание и поддержка таблицы маршрутизации для сетей.

Пересылка пакетов: инкапсуляция пакетов данных и их пересылка с использованием соответствующих выходных интерфейсов.

-Они полагаются на таблицы маршрутизации, которые создаются вручную или динамически с использованием протоколов маршрутизации.



Информация о маршрутизации:

Типы треков:

Непосредственно связанные пути.

Удаленные пути (статические или динамические).

Протоколы динамической маршрутизации (такие как OSPF и EIGRP) позволяют адаптироваться к изменениям в сети.

	Interior Gateway Protocols				Exterior Gateway Protocols
	Distance Vector		Link-State		Path Vector
IPv4	RIPv2	EIGRP	OSPFv2	IS-IS	BGP-4
IPv6	RIPng	EIGRP for IPv6	OSPFv3	IS-IS for IPv6	BGP-MP

VLAN:

Сеть разделена на отдельные логические блоки для повышения производительности и безопасности.

Разрешает связь между устройствами только внутри одной VLAN.

Требуется маршрутизатор для связи между различными VLAN.

Протокол связующего дерева (STP):

Он предотвращает образование петель в сетях уровня 2, блокируя дублирующиеся пути.

Обеспечивает резервирование для обеспечения непрерывности сети в случае сбоев.

Многоуровневое переключение

Поддерживает функции коммутации и маршрутизации на уровнях 2, 3 и 4.

Он обеспечивает:

Маршрутизируемые порты: интерфейсы, которые действуют как порты маршрутизатора.

Виртуальные интерфейсы (SVI): для маршрутизации между VLAN.

Протоколы и функции WLAN:

Различия между WLAN и проводной локальной сетью:

В сетях WLAN вместо кабелей используются радиоволны (РЧ).

Для подключения устройств они полагаются на точки беспроводного доступа (AP).

Поддерживает мобильные устройства и использует CSMA/CA для предотвращения коллизий.

Им требуется специальный формат кадра, содержащий дополнительные поля для обеспечения связи.

Характеристика	Беспроводная сеть LAN стандарта 802.11	Сети LAN Ethernet стандарта 802.3
Физический уровень	Радиочастотный диапазон (РЧ)	Кабельное подключение
Доступ к среде передачи данных	Предотвращение конфликтов	Обнаружение конфликтов
Доступность	Все пользователи с сетевыми адаптерами, поддерживающими радиосвязь, в диапазоне действия точки доступа	Требуется подключение кабеля
Влияние помех	Да	Без последствий
Регулирование	Дополнительное регулирование правительством страны	Определяется стандартом IEEE

Формат кадра в 802.11:

Рамка содержит:

1-Контроль кадра.

2-Адреса (MAC).

3-Последовательный контроль.

4-Полезная нагрузка.

5-FCS для проверки ошибок.

Процесс подключения к сетям WLAN:

1-Обнаружение сети.

2-Аутентификация с помощью точки доступа.

3-Ссылка на точку доступа

Настраиваемые параметры:

1-Сетевой режим (802.11).

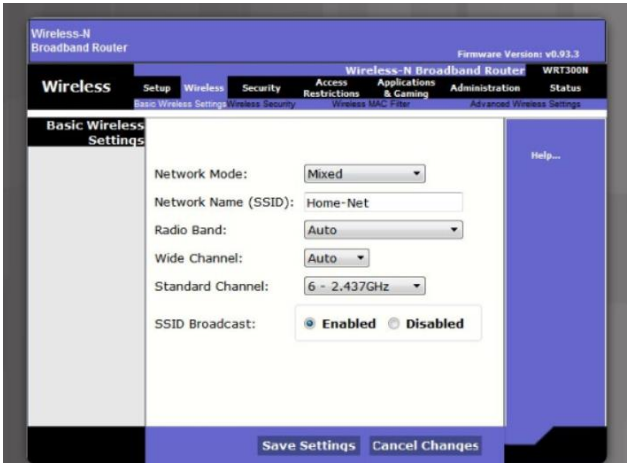
2-SSID для идентификации сети.

3-Настройки канала (ручные или автоматические).

4-Режим безопасности (WEP/WPA/WPA2).

5-Шифрование (AES).

6-пароль.



Методы сканирования:

Пассивный режим: точки доступа периодически передают сигналы.

Активный режим: клиенты ищут SSID с помощью запросов на сканирование.

Типы аутентификации:

Открытая аутентификация: никакой реальной безопасности.

Общий ключ: требуется заранее заданный ключ.

Межсетевые экраны, IDS/IPS и специализированные устройства безопасности:

Брандмауэры:

Функции: соблюдение политики контроля доступа, сопротивление атакам, точка пересечения ключей.

Его виды:

1-Фильтрация пакетов (без сохранения состояния): на основе уровней 3 и 4.

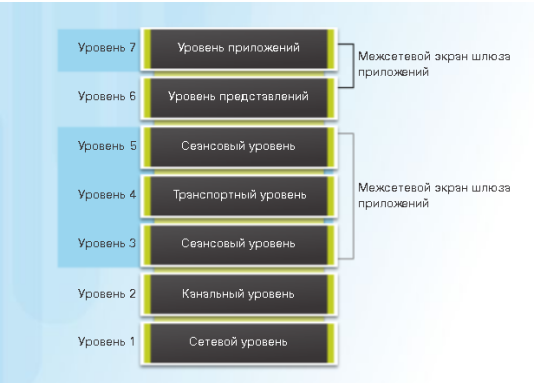
2-Проверка статуса: зависит от контекста и предыдущих сообщений.

3-Портал приложений: основан на нескольких уровнях (3, 4, 5, 7).

4-На основе хоста/прозрачный/гибридный.

Преимущества: Защитите ресурсы, предотвратите эксплуатацию недостатков, уменьшите сложность управления.

Недостатки: медленная сеть, риск неправильной настройки, переполнение пользователями



Системы обнаружения и предотвращения вторжений (IDS/IPS):

Идентификаторы:

Достоинства: Автономный режим, не влияет на производительность, регистрирует угрозы.

Недостатки: Не блокирует атаки напрямую, склонен к уклонению.

ИПС:

Преимущества: Блокирует вредоносные пакеты, восстанавливает поток данных.

Недостатки: Влияет на производительность, требует тонкой настройки.

Типы ИПС:

На базе хоста: защищает критически важные системные процессы.

На основе сети: обнаруживает вредоносную активность в режиме реального времени.

=

	Преимущества	Недостатки
IDS	• Не оказывает влияния на сеть (задержки, джиттер). • Не оказывает влияния на сеть в случае сбоя сенсора. • Не оказывает влияния на сеть в случае перегрузки сенсора.	• Ответное действие не может остановить отправку пакетов, которые вызвали тревогу. • Для ответных действий требуется правильная настройка. • Более уязвима к методам обхода системы сетевой безопасности.
IPS	• Останавливает отправку пакетов, которые вызвали тревогу. • Может использовать методы нормализации потока.	• Неполадки сенсоров могут влиять на сетевой трафик. • Перегрузка сенсора оказывает влияние на сеть. • Оказывает определенное влияние на сеть (задержки, джиттер).

Специализированные охранные устройства:

1-Cisco AMP: защита от вредоносного ПО до, во время и после атаки.

2-Cisco WSA: безопасный веб-трафик.

3-Cisco CWS: защитите пользователей за пределами сети.

4-Cisco ESA: безопасность электронной почты с такими функциями, как защита от спама и AMP.

=

Списки управления доступом (Acl):

1-Типы:

Стандартные: разрешают или блокируют трафик только по исходному адресу.

2-Расширенные: **фильтруют по:**

1-Типу протокола.

2-Исходным и целевым адресам.

3-Портам TCP/UDP.

4-Другим параметрам.

Идентификация ACL:

1-Использование номера или имени (имена более понятны).

3-Дополнительные функции:

1-Логирование ACL.

2-Разрешение только существующих TCP-сессий.

Протокол простого управления сетью (SNMP):

Позволяет управлять устройствами и мониторить их производительность.

Состоит из:

1-Менеджера SNMP.

2-Агента SNMP.

3-Базы данных управления (MIB).

NetFlow:

1-Технология для сбора статистики о пакетах.
2-Используется для мониторинга, планирования и анализа трафика.
3-Определяет потоки по 7 полям, включая:
IP-адреса и порты.
Тип протокола 3 уровня.

Дублирование порта (Port Mirroring):

Копирует трафик на мониторинговый порт.

Используется с анализаторами пакетов.

Серверы Syslog:

Блокируют системные сообщения о событиях. Основные функции:

1-Сбор информации.

2-Определение типа записей.

3-Указание места хранения сообщений

Протокол NTP:

Синхронизирует время между устройствами.
Основан на иерархии (уровни от 0 до 16).

Серверы A:
Архитектура безопасности включает:
Аутентификацию: проверка личности.
Авторизацию: определение прав доступа.

Учет: запись действий.

Протоколы: TACACS+ (более безопасный) и RADIUS.

Виртуальная частная сеть (VPN):

Обеспечивает безопасное соединение через интернет.

Типы:

1-Уровень 2: GRE.

2-Уровень 3: IPsec, MPLS.

3-Использует шифрование для обеспечения конфиденциальности.

Топологии и проектирование сетей:

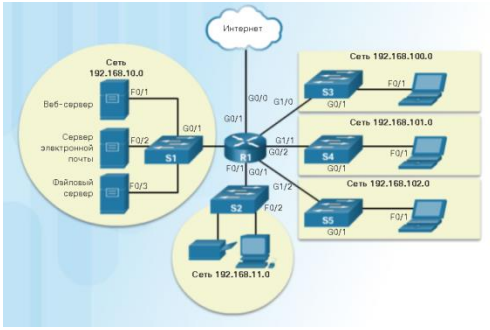
Типы топологий:

1- Физическая топология:

Определяет способ физического подключения устройств, например соединения между маршрутизаторами и коммутаторами.

2- Логическая топология:

Он описывает, как данные передаются между узлами, и определяется протоколами канального уровня.



Топологии WAN:

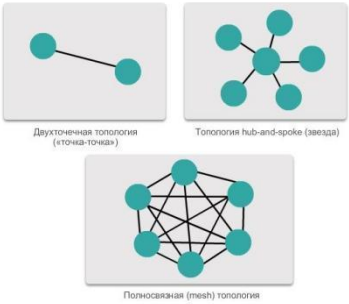
Архитектурные шаблоны, определяющие способ подключения сайтов и устройств в глобальной сети (WAN). Помогает организовать коммуникации и определить эффективность и гибкость.

1-Точка-точка: прямое соединение между двумя точками.

2-Ступица и спица: центральное соединение, соединяющее ветви.

3-Ячеистая сеть: соединение каждой точки со всеми другими точками (высокая стоимость).

4-Гибридная сеть: комбинация предыдущих топологий.



Топологии локальной сети:

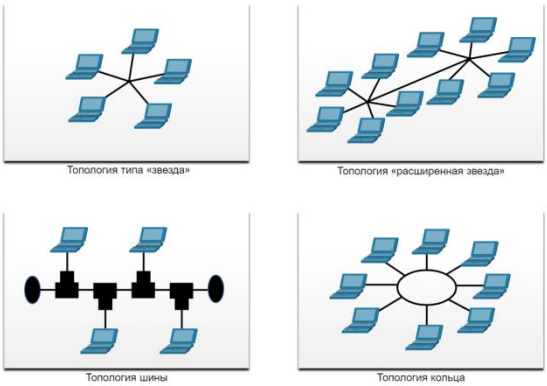
Шаблоны, определяющие способ подключения устройств в локальной сети (LAN). Включать:

1-Asterisk: устройства, подключенные к центральному устройству.

2-Расширенная звезда: свяжите несколько звезд с дополнительными ключами.

3-Шина: линейное соединение между устройствами.

4-Кольцо: Соединение устройств по кругу.

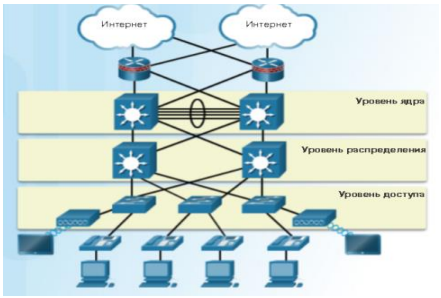


Модель проектирования трехуровневой сети:

Уровень доступа: обеспечивает подключение устройств к сети.

Уровень распространения: соединяет уровни доступа и предоставляет услуги.

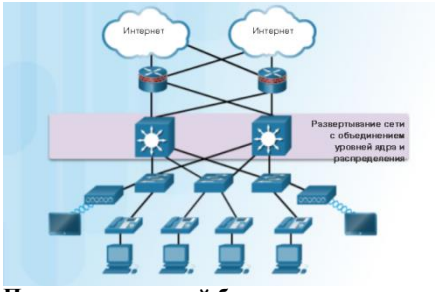
Базовый уровень: обеспечивает связь между уровнями распределения.



Малые сети: уровни распределения и ядра можно объединить для снижения затрат.

Плоские сети. Изменения затрагивают большое количество систем.

Иерархический дизайн: облегчает управление и изоляцию, а также повышает гибкость



Принципы сетевой безопасности:

Важность сетевой безопасности и угроз:

Мотивы: включают финансовую выгоду, шпионаж, злонамеренные действия и злые намерения.

Целевые активы: данные, устройства, серверы и другое ценное имущество.

Основные условия:

Угроза: потенциальная угроза активам.

Уязвимости и поверхность атаки: Слабые места в системе, которые можно использовать.

Эксплуатация: метод, используемый для проникновения в уязвимости.

Риск: Возможность того, что угроза воспользуется слабостью.

Управление рисками:

Принятие: оставить риск в покое, если его стоимость ниже.

Избегание: снижает подверженность риску, но обходится дороже.

Сокращение: минимизируйте воздействие, используя смешанные стратегии.

Передача: делегирование рисков третьей стороне, например страховым компаниям.

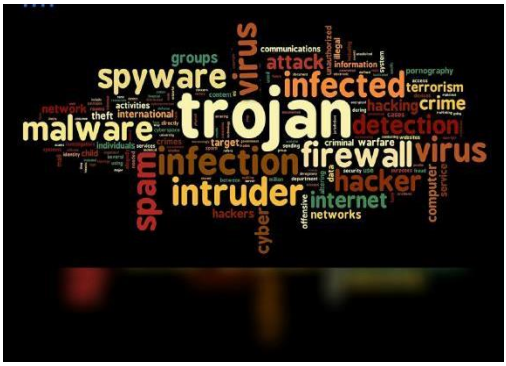
Типы вредоносных программ:

Вирусы: распространяются, внедряясь в другие программы.

Черви: распространяются независимо, не нуждаясь в хозяине.

Трояны: они выглядят как законные программы, но скрывают вредоносные - инструкции.

Программы-вымогатели: блокирует доступ к системе до тех пор, пока не будет выплачен выкуп.



Распространенные инструменты атаки:

Взломщики паролей, инструменты беспроводного взлома, инструменты сетевого сканирования, анализаторы пакетов, инструменты криминалистики, инструменты шифрования.

Категории атак:

Опрос: Несанкционированный сбор информации.

Атаки доступа: взлом учетных записей или баз данных.

Социальная инженерия: обманом заставить людей получить конфиденциальную информацию.

Отказ в обслуживании: наводнение сети огромным количеством запросов с целью ее нарушения.

Переполнение буфера: использование недостатков системной памяти для ее повреждения.

Способы уклонения:

Шифрование и туннелирование: сокрытие контента.

Истощение ресурсов: система настолько загружена, что не может противостоять атакам.

Сегментация трафика: разделение вредоносных данных для обхода систем безопасности.

Руткиты: скрывают атаки путем проникновения в операционные системы.

Непрерывная эволюция атак:

Методы уклонения от кибератак постоянно развиваются, что требует от специалистов по кибербезопасности быть в курсе новейших технологий и инструментов для противодействия этим угрозам. Вот некоторые современные методы уклонения:

Сетевые атаки:

1. Мониторинг трафика:

Его целью является анализ потока данных в сети для выявления аномальных закономерностей.

Для анализа пакетов используются такие инструменты, как Wireshark и Tcpdump.

Реализуется с помощью точек доступа к сети (TAP) или зеркалирования

2. Уязвимости сетевых протоколов:

Включает (**IP, TCP, UDP, ARP, DNS, DHCP, HTTP**) и электронную почту.

Эти уязвимости делают возможным такие атаки, как подделка, взлом и выдача себя за другое лицо.

3. Топология сетевой безопасности:

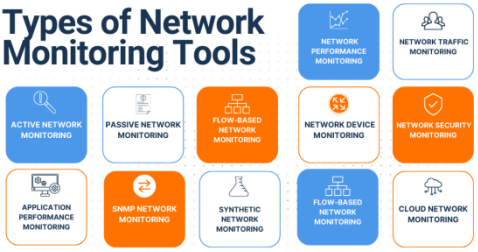
основан на построении защищенной инфраструктуры с использованием межсетевых экранов и систем обнаружения/предотвращения вторжений (IDS/IPS).

Цель состоит в том, чтобы предотвратить угрозы или уменьшить их воздействие.

4. Системы сетевого мониторинга:

Включает такие инструменты, как SIEM, которые собирают данные и предоставляют комплексную аналитику.

Функции SIEM включают корреляцию, агрегирование и судебно-медицинс



5. Протоколы HTTP/HTTPS:

HTTP уязвим для таких атак, как несанкционированные загрузки и эксплойты.

HTTPS обеспечивает шифрование, что снижает вероятность взлома.

6. Атаки по электронной почте:

Атаки с вложениями: включают вредоносное ПО.

Подмена электронной почты: создание электронных писем, выглядящих как настоящие, с целью обмануть пользователей.

Спам: рассылка сообщений, содержащих вредоносное ПО.

Омофоны: использование похожих символов для обмана пользователей.

7. Инструменты мониторинга сетевой безопасности:

Включать:

Анализаторы протоколов: такие как Wireshark.

SNMP: для запроса данных об оборудовании.

NetFlow: для мониторинга потока д анных

8. Атаки на основе iFrames:

Используется для доставки вредоносного эксплойта.

Профилактика включает обновление браузеров и блокировку вредоносных веб-сайтов с помощью таких инструментов, как Cisco Web Security.

9. Атаки HTTP 302:

Использование перенаправлений HTTP для направления пользователей на вредоносные сайты.

Решения включают в себя инструменты блокировки, такие как Cisco OpenDNS.

10. Штриховка масштаба:

Использование поддоменов скомпрометированных доменов для запуска атак.

Защита включает в себя защиту учетных записей владельцев доменов и использование таких инструментов, как Cisco OpenDNS.

Защита сети:

1. Определить слабые места:

Его цель — понять потенциальные уязвимости в сети и приложениях.

Примеры угроз:

Взлом внутренней системы.

Кража данных клиентов.

Атаки с использованием украденной смарт-карты.

Для понимания важных приложений и их оборудования требуются постоянные исследования.

2. Выявить угрозы:

В рамках глубокоэшелонированной защиты используются:

Граничный маршрутизатор: первая линия защиты.

Брандмауэр: фильтрует соединения и защищает внутреннюю сеть.

Внутренний маршрутизатор: обеспечивает дополнительную фильтрацию.

Включает дополнительное оборудование, такое как системы предотвращения вторжений (IPS) и программное обеспечение для защиты от вредоносных программ (AMP).

3. Подход безопасный лук и безопасный артишок:

Security Onion: требует удаления каждого уровня для доступа к данным.

Артишок безопасности: позволяет злоумышленнику обойти определенные уровни для доступа к конфиденциальным данным.

4. Политика использования собственного устройства (BYOD):

Это обеспечивает такие преимущества, как повышение производительности и снижение затрат.

Требуются политики безопасности для снижения рисков:

Уникальные пароли.

Обновление оборудования.

Антивирусное программное обеспечение.

Программное обеспечение для управления мобильными устройствами (MDM).

5. Модели контроля доступа:

MAC: строгий и используется в чувствительных приложениях.

DAC: дает пользователям контроль над своими данными.

RBAC: на основе ролей пользователей.

ABAC: На основе атрибутов объекта и пользователя.

Принцип минимальных привилегий для уменьшения ненужного доступа

6. Сообщества сетевой разведки:

Предоставляет информацию о недавних угрозах и навыках.

Примеры:

Подпишитесь на новости об угрозах.

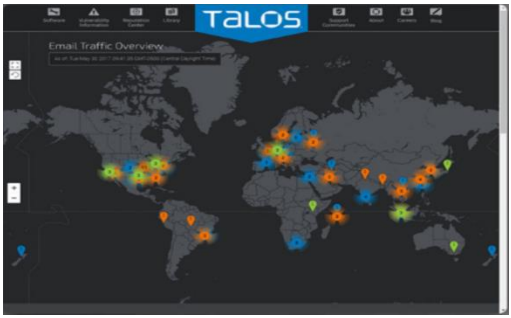
Посещение конференций и семинаров.

7. Циско Талос:

Глобальная команда, предоставляющая информацию об угрозах.

Обеспечивает защиту от атак с помощью обновляемых данных в режиме - реального времени.

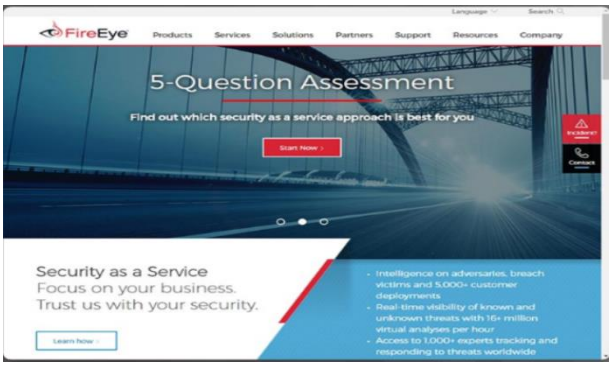
Распространяет правила безопасности на общие устройства



8. Огненный Глаз:

Предоставляет услуги по предотвращению атак через электронную почту, Интернет и вредоносные программы.

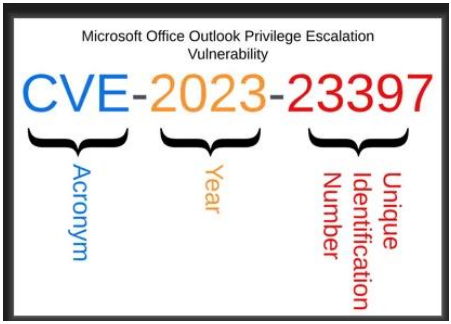
использует передовые методы для обнаружения необнаруженных угроз



9. База данных CVE:

Каталог известных уязвимостей, поддерживаемый MITRE.

Предоставляет уникальные идентификаторы, упрощающие обмен данными об уязвимостях



Криптография и инфраструктура открытых ключей:

1. Защита коммуникаций

Усиление защиты устройства: улучшение настроек безопасности для таких устройств, как маршрутизаторы и коммутаторы.

AAA (аутентификация, авторизация и учет): контроль доступа для пользователей.

Списки контроля доступа (ACL): определяют правила фильтрации трафика.

Брандмауэры: защищают сети от угроз.

Система предотвращения вторжений (IPS): отслеживает и останавливает атаки.

AMP, ESA и WSA: инструменты для повышения безопасности устройств, электронной почты и Интернета.

2. Элементы защищенной связи:

Конфиденциальность данных: предотвращение несанкционированного доступа с помощью шифрования.

Целостность данных: гарантия того, что данные не будут изменены.

Аутентификация источника: проверьте личность отправителя.

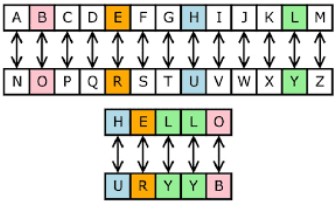
Неотказуемость: гарантирует, что отправитель не отрицает отправку сообщения.

3. Шифр :

Сменное лезвие: то же, что и лезвие Цезаря.

Код перемещения: переставьте символы, например «железнодорожное ограждение».

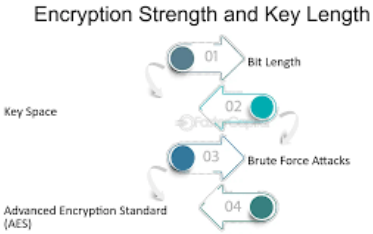
Многоалфавитный шифр: например, шифр Виженье.



4. Ключи:

Надежность шифрования зависит от длины ключа и пространства ключей.

Более длинные ключи более безопасны, но требуют больше ресурсов.



5. Криптографические хеш-функции:

MD5: Устаревший и слабый.

SHA-1: более безопасен, чем MD5, но имеет недостатки.

SHA-2: На данный момент лучший.

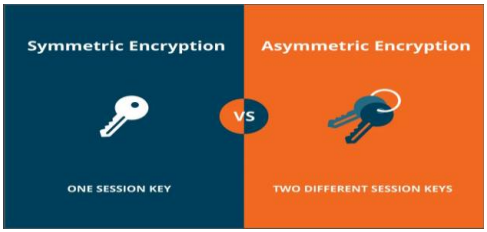
6. HMAC:

Сочетает хэш и секретный ключ для обеспечения целостности и аутентификации.

7. Симметричное и асимметричное шифрование.

Симметричный: один ключ для шифрования и дешифрования.

Асимметричный: разные ключи (открытый и закрытый).



8. Дэви-Хеллман:

Способ безопасного обмена ключами без предварительного обмена ключом.

Если вам нужна более подробная информация по какому-либо товару, я могу уточнить

Безопасность и анализ конечных точек:

1. Угрозы для конечных точек

Определение конечных точек: устройства, которые подключаются к сети, такие как компьютеры, серверы и устройства Интернета вещей (IoT).

Источники угроз: вредоносное ПО, вредоносный спам, нацеленный на системы Android.

Причины опасности вредоносного ПО: быстрая адаптация, широкое распространение и сложность обнаружения.

2. Защита от вредоносного ПО на базе хоста:

Антивирусное программное обеспечение: на основе сигнатур, эвристического анализа и подозрительного поведения.

Брандмауэры на базе хоста: ограничивают соединения и предотвращают распространение.

Пакеты безопасности на базе хоста: обеспечивают многоуровневую защиту и ведение журнала активности.

3. Защита от вредоносного ПО по сети

Передовые технологии:

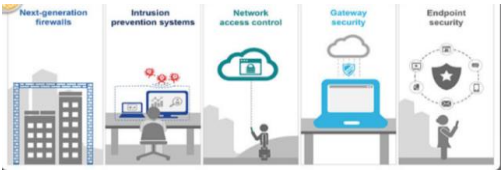
Расширенная защита от вредоносных программ (AMP).

Устройства безопасности электронной почты (ESA).

Устройства веб-безопасности (WSA).

Контроль приемки сети (NAC).

Межтехнологическая интеграция: улучшенная защита по сравнению с решениями, ориентированными только на хост.



4. Поверхность атаки:

Определение: Все уязвимости, которые можно использовать в системе.

Типы поверхностей атаки:

Сеть: использование протоколов.

Программное обеспечение: эксплуатация приложений.

Человек: использование поведения пользователя.

---

5. Профиль сети:

Цель: Определить нормальное поведение сети для обнаружения аномалий.

Инструменты: такие как **NetFlow** и **Wireshark**.

Соображения:

Продолжительность сеанса.

урожай.

Используемые порты.

Адреса важных активов

6. Тестирование уязвимостей сети:

Виды тестов:

Анализ рисков: оценка вероятности и последствий атак.

Оценка уязвимостей: сканирование сетей и серверов с помощью таких инструментов, как Nessus.

Тестирование на проникновение: моделирование атак с целью использования уязвимостей..

Задание	Примеры	Сервис
Анализ рисков	Специалисты проводят всесторонний анализ последствий атак на основные ресурсы и функции компании	внутренние или внешние консультанты, архитектуры управления рисками
Оценка уязвимостей	Управление исправлениями, сканирование хостов, сканирование портов, другое сканирование на наличие уязвимостей и соответствующие службы	OpenVas, Microsoft Baseline Analyzer, Nessus, Qualys, Nmap
Тестирование на проникновение	Использование методов и инструментов хакеров для преодоления защиты сети и определения глубины потенциального проникновения	Metasploit, CORE Impact, «белые» хакеры

7. CVSS (Общая система оценки уязвимостей):

Преимущество: расставьте приоритеты в устранении уязвимостей в зависимости от риска.

Основные группы:

Фундаментальные: фиксированные характеристики (например, сложность атаки и ее влияние на конфиденциальность).

Временные: свойства, которые меняются со временем.

Окружающая среда: Факторы, связанные с окружающей средой организации.

8. Управление рисками:

Определение: непрерывный процесс определения соответствующих мер безопасности.

Этапы:

оценка риска.

Снижение рисков.

Постоянный мониторинг и улучшение.

Мониторинг безопасности:

Существует большое значение для мониторинга безопасности в сетях и как использовать данные для обнаружения и содержания пробелов в безопасности. Методы безопасности и инструменты сбора записей.

Sylog и NTP:

Sylog является критерием для регистрации сообщений событий с сетевых устройств. Помогает собирать записи с нескольких устройств и отправить их на центральные серверы для их анализа.

NTP гарантирует синхронизацию времени между устройствами, что облегчает расследование инцидентов безопасности.

Сети:

P2P представляет угрозу безопасности из -за простоты распространения вредоносных программ. Приложения P2P должны быть запрещены в институциональных сетях.

TOR позволяет неизвестно просмотреть, делая контроль безопасности.

Скачать бюджет

Бюджет загрузки используется для распространения трафика между ресурсами, чтобы избежать веса в Интернете, но эти операции могут привести к подозрительному трафику.

Хост записи

HIDS используется на хозяевах для обнаружения угроз и предотвращения прорывов. Записи собираются у двух разных хостов и анализируются с помощью инструментов NSM.

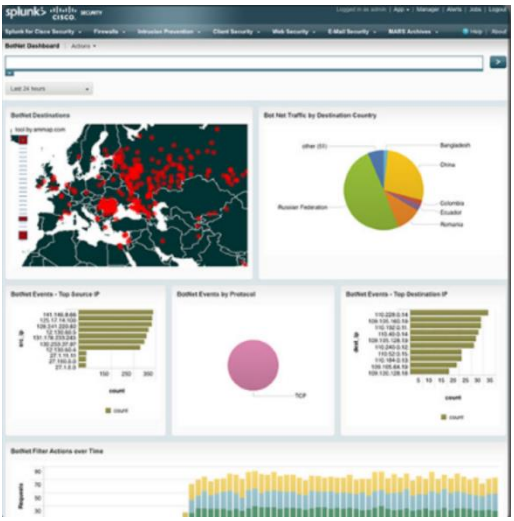
Записи Windows включают в себя прикладные и безопасные записи, которые помогают обнаружить необычные действия, такие как мошенничество с вредоносными программами.

Тип события	Описание
Ошибка	Событие, которое указывает на существенную проблему, такую как потеря данных или функциональных возможностей. Например, если не удается загрузить службу во время запуска, регистрируется ошибка.
Предупреждение	Событие, которое не обязательно является важным, но может означать возможные проблемы в будущем. Например, если недостаточно свободного дискового пространства, регистрируется предупреждение. Если после события возможно восстановление приложения без потери данных или функциональности, событие обычно классифицируется как предупреждение.
Информация	Событие, которое описывает успешную работу приложения, драйвера или службы. Например, после успешной загрузки сетевого драйвера может быть зарегистрировано информационное событие. Обратите внимание, что обычно приложение для ПК не должно регистрировать событие при каждом запуске.
Аудит успешных попыток	Событие, которое записывает успешную проверенную попытку доступа через систему безопасности. Например, успешная попытка входа пользователя в систему записывается как событие успешной попытки.
Аудит неуспешных попыток	Событие, которое записывает неудавшуюся проверенную попытку доступа через систему безопасности. Например, если пользователь пытается получить доступ к сетевому диску и ему это не удается, эта попытка регистрируется как событие неуспешной попытки.

Siem и записи записи:

SIEM собирает и анализирует записи для предоставления отчетов и анализов в фактическое время, и собирает данные из разных источников для их всестороннего анализа.

Splunk и Elk - один из самых известных инструментов, используемых в Siem.



Файл разряда данных:

Инструменты, такие как **TCPDUMP** и **Wireshark**, захватывают пакеты и анализируют сетевые данные в фактическое время.

Netflow:

NetFlow собирает информацию о потоке пакетов и используется для изучения ошибок и анализа несчастных случаев безопасности.

IPFIX - это стандарт, который зависит от NetFlow и используется для мониторинга сетевого потока.

Прокси -записи:

Прокси -журналы - это записи, созданные прокси -серверами, которые действуют как посредники между клиентами сети и другими серверами. Он используется для анализа и достижения безопасности сети.

Примеры прокси -серверов:

1-Кальмар

2-CCProxy

3-Apache Traffic Server

4-Вингейт

1265939281.764	**Time**, время в формате метки времени Unix epoch с миллисекундами
19478	**Duration**, время, прошедшее с момента получения, запроса и ответа от Squid
172.16.167.228	**IP-адрес** клиента
TCP_MISS/200	**Result** Содержит код результата Squid и код состояния HTTP, разделенные косой чертой
864	**Size**, размер/объем данных, доставленных клиенту (в байтах)
GET	**Request** Метод запроса, сделанного клиентом
http://www.example.com//images/home.png	**URI/URL**, адрес запрошенного ресурса
–	**Client identify** - значение RFC 1413 клиента, сделавшего запрос, которое не используется по умолчанию
NONE/-	**Peering code/Peer host** - вычисленный соседний сервер кеша
image/png	**Type**, тип содержимого mime, определенный по

Анализ данных о нарушениях:

Основное внимание уделяется тому, как анализировать, оценивать, распространять и сохранять данные, полученные в результате оповещений о кибербезопасности, с использованием таких инструментов, как Security Onion.

Инструменты обнаружения:

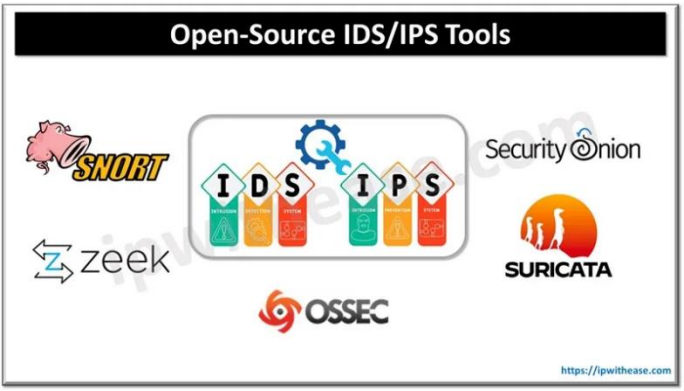
CapME: просмотр полных сеансов уровня 4 и анализ текстов пакетов.

Snort: система обнаружения вторжений (NIDS) на основе правил и сигнатур.

Bro (Zeek): основан на поведении и имеет дополнительные аналитические функции.

OSSEC: обнаружение вторжений на уровне хоста.

Suricata: NIDS с поддержкой многопоточности и улучшенной производительностью.



Инструменты анализа:

Sguil: Центральная консоль для анализа оповещений.

ELSA: Поиск записей из нескольких источников с использованием гибких запросов.

Wireshark: анализ захваченных пакетов.

Создавайте и оценивайте оповещения

Оповещения включают в себя такую информацию, как IP-адрес источника и назначения, порты и протокол.

Классификация оповещений:

Настоящий позитив: реальная угроза.

Ложное срабатывание: Ложная тревога.

Истинно отрицательный: угрозы нет.

Ложный отрицательный результат: необнаруженная угроза.

Управление оповещениями:

Эскалация оповещения: их направляют с уровня 1 на уровень 2 для расширенного расследования.

Ретроспективный анализ безопасности: проверка архивных данных с использованием новых правил.

Важность анализа:

Обеспечьте точное обнаружение угроз.

Повысьте эффективность систем обнаружения и сократите количество ложных срабатываний.

Отслеживайте информацию об угрозах, чтобы избежать ложных срабатываний.

Реагирование на инциденты и их устранение:

В сфере кибербезопасности злоумышленники постоянно внедряют новые методы, что приводит к появлению новых угроз, требующих быстрого обнаружения и эффективного сдерживания. Их методы включают вымогательство, мошенничество и кражу личных данных с целью получения финансовой выгоды, что побудило разработать эффективные модели и процедуры реагирования на инциденты безопасности.

Модели реагирования на инциденты

Кибер-цепочка убийств:

Создание оружия: использование разведывательной информации для разработки оружия, использующего уязвимости целевых систем.

Доставка: Передача оружия цели с помощью таких средств, как электронная почта или USB-носитель.

Эксплуатация: использование оружия для эксплуатации уязвимостей безопасности в системе.

Установка: Создание бэкдора для получения постоянного доступа к системе.

Управление и контроль (C2): установление канала связи между злоумышленником и скомпрометированной системой.

Действия, направленные на достижение цели: достижение конечной цели, например кража данных или проведение DDoS-атаки.

Модель:Бриллиант:

используется для анализа инцидентов кибербезопасности с использованием четырех элементов: субъектов, действий, активов и атрибутов.

Помогает понять, как злоумышленник переходит от одного события к другому.

Схема VERIS (словарь для регистрации событий и обмена информацией об инцидентах):

Набор показателей для структурированного описания инцидентов безопасности.

Используется для регистрации инцидентов безопасности и анонимного распространения информации о них среди сообщества.

состоит из четырех ландшафтов: угрозы, активы, воздействия и контроль.

Рекомендации NIST:

Предоставляет основу для групп реагирования на инциденты компьютерной безопасности (CSIRT) и процессов обработки инцидентов.

включает в себя такие этапы, как подготовка, обнаружение, анализ, сдерживание, ликвидация и восстановление.

Группы реагирования на инциденты компьютерной безопасности (CSIRT)

инцидента безопасности: любое злонамеренное или подозрительное действие, которое нарушает политику безопасности или угрожает безопасности организации.

Типы команд CSIRT:

Внутренние команды: решают проблемы внутри организации.

Национальные команды: решают вопросы, связанные с инцидентами на государственном уровне.

Координационные центры: координируют действия различных групп реагирования.

Команды поставщиков: устраняют уязвимости безопасности в своих продуктах.

Поставщики услуг управляемой безопасности (MSSP): предоставляют услуги реагирования на инциденты другим компаниям.

Фазы реагирования на инциденты:

1-Подготовка:

Создать и обучить команду CSIRT.

Получение необходимых инструментов и активов для расследования несчастных случаев.

Разработать учебные материалы по повышению осведомленности в вопросах безопасности.

2- Обнаружение и анализ:

Выявляйте инциденты с помощью таких инструментов, как системы обнаружения вторжений.

Анализируйте инциденты, чтобы определить их масштабы и последствия.

3- Сдерживание, ликвидация и восстановление:

Остановите инцидент, чтобы не допустить его распространения.

Устраните угрозы и восстановите затронутые системы.

Восстановите нормальное состояние систем.

4- Действия после аварии:

Проводите встречи по извлечению уроков для улучшения операций реагирования.

Собирайте и анализируйте данные об инцидентах для выявления уязвимостей.

Хранение доказательств в течение определенного периода времени в юридических целях.