

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

ПО ЛАБОРАТОРНОЙ РАБОТЕ S'.

(Основы: Техническая Защита Информации,
Информационная безопасность)

by Andrey.

2022г

ВВЕДЕНИЕ.

Техническая защита информации – это комплекс мер и технических средств, направленных на обеспечение *конфиденциальности, целостности и доступности информации*. В рамках ТЗИ используются различные технические средства, такие как антивирусные программы, брандмауэры, криптография, системы контроля доступа и т.д.

Цель ТЗИ – предотвращение несанкционированного доступа к данным, их утраты или повреждения.

Информационная безопасность – это обеспечение сохранности, конфиденциальности и доступности информации, а также защита от различных угроз и рисков, связанных с использованием информационных технологий. ИБ включает в себя технические, организационные и правовые меры, направленные на обеспечение безопасности информационных ресурсов.

Три основных понятия.

КОНФИДЕНЦИАЛЬНОСТЬ	<ul style="list-style-type: none">– информация остаётся в тайне и доступна только тем людям, которым она нужна. <u>Например</u>, личные сообщения на телефоне – они должны быть видны только вам, а не всем.
ЦЕЛОСТНОСТЬ	<ul style="list-style-type: none">– гарантирует, что информация остаётся такой, какой она была, и никто не может её незаметно изменить. Это как сохранение фотографии без потери качества или добавления чужих изменений.
ДОСТУПНОСТЬ	<ul style="list-style-type: none">– нужная информация всегда доступна, когда вам это нужно. Это, например, как быстрый доступ к вашим фотографиям на телефоне без задержек

	или проблем.
--	--------------

Атаки и угрозы в сфере информационной безопасности могут быть разделены на два основных типа: пассивные и активные.

ТИП АТАКИ	РАЗДЕЛЫ
ПАССИВНАЯ	<ol style="list-style-type: none"> 1. Перехват Злоумышленник пытается перехватить передаваемую информацию. Например, когда хакер перехватывает данные, передаваемые через небезопасную сеть. 2. Мониторинг Наблюдение за активностью для сбора информации. Например, следящий за вами в интернете может анализировать, какие сайты вы посещаете. 3. Анализ Изучение собранной информации для выявления шаблонов и связей. Это может использоваться для создания профиля личности или выявления слабостей в системе безопасности.
АКТИВНАЯ	<ol style="list-style-type: none"> 1. Вмешательство Несанкционированное изменение информации или данных. 2. Внедрение Внесение в систему вредоносного кода или данных с целью выполнения злонамеренных действий. Например, SQL-инъекция в веб-приложениях. 3. Отказ в обслуживании

	<p>Атака, при которой злоумышленник перегружает ресурсы системы, делая её недоступной для легальных пользователей. <u>Например</u>, атака на сервер, перегружающая его запросами.</p>
--	---

ВАЖНЫЕ ПОНЯТИЯ.

IP (Internet Protocol) – это набор правил и стандартов, используемых для отправки и получения данных в компьютерных сетях, включая Интернет.

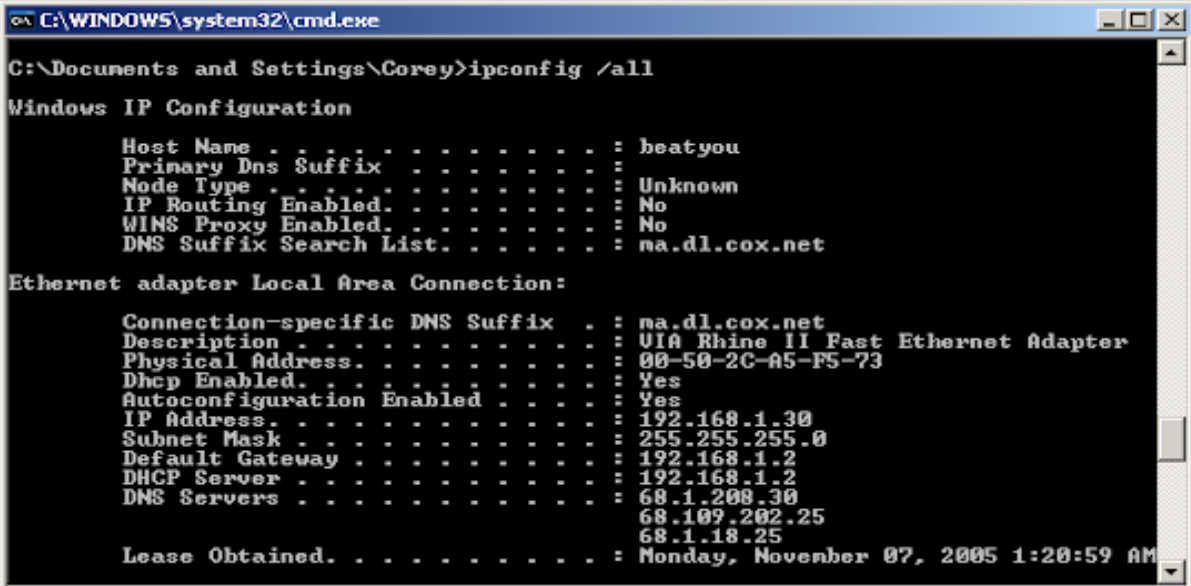
IP-адрес (Internet Protocol address) – это уникальный числовой идентификатор, присвоенный каждому устройству (компьютеру, принтеру, маршрутизатору и т.д.), подключенному к сети, чтобы обеспечить их уникальное определение в сетевой структуре.

IP-адреса бывают **IPv4** <standart version> (например, 192.168.0.1) и **IPv6** (например, 2001:0db8:85a3:0000:0000:8a2e:0370:7334), где IPv6 представляет собой расширенную версию IP-адресации для более эффективного использования адресов.

Порт – это числовой идентификатор, который используется для уникальной идентификации приложения или службы в компьютерных сетях. Когда данные направляются к устройству по его IP-адресу, порт определяет, к какому конкретному приложению или службе на этом устройстве нужно направить эти данные. Порт представляет собой 16-битное число, и его диапазон обычно от 0 до 65535. Например, **HTTP-протокол** использует порт **80**, а **HTTPS** – порт **443**.

Как узнать IP адрес устройства? (CMD)

command: `ipconfig`



```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Corey>ipconfig /all

Windows IP Configuration

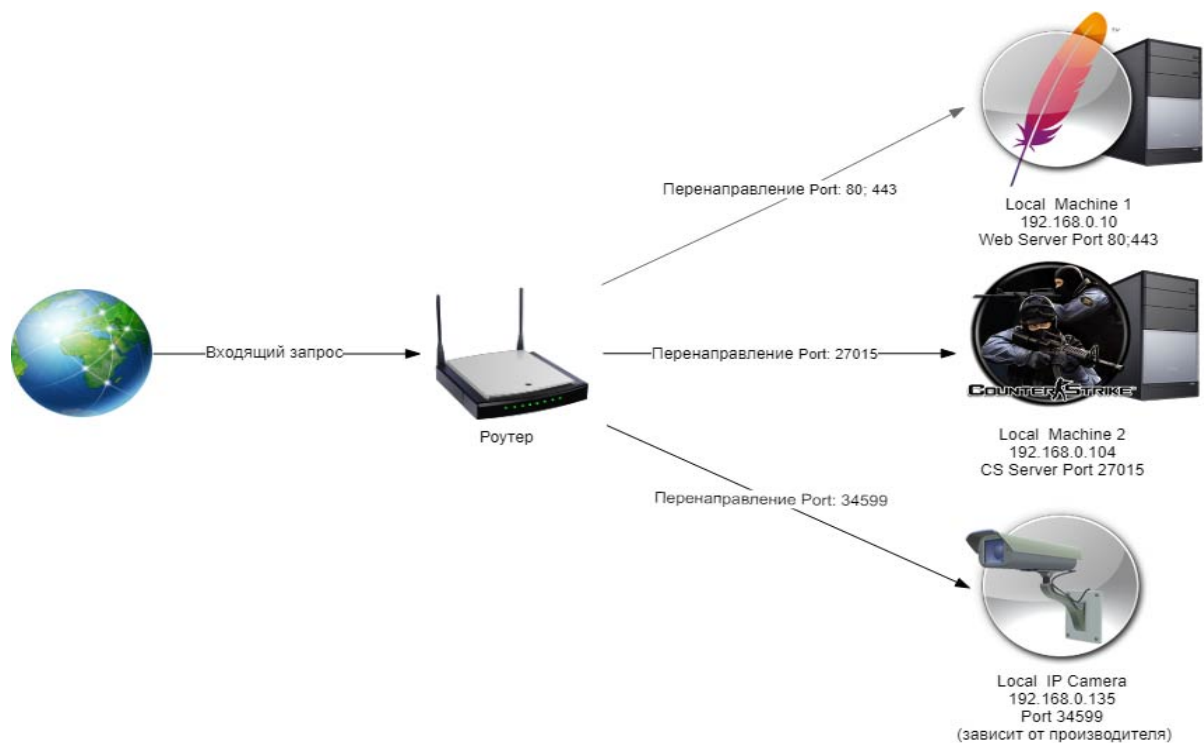
    Host Name . . . . . : beatyou
    Primary Dns Suffix . . . . . : 
    Node Type . . . . . : Unknown
    IP Routing Enabled. . . . . : No
    WINS Proxy Enabled. . . . . : No
    DNS Suffix Search List. . . . . : na.dl.cox.net

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix . : na.dl.cox.net
    Description . . . . . : VIA Rhine II Fast Ethernet Adapter
    Physical Address. . . . . : 00-50-2C-A5-F5-73
    Dhcp Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes
    IP Address. . . . . : 192.168.1.30
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.2
    DHCP Server . . . . . : 192.168.1.2
    DNS Servers . . . . . : 68.1.208.30
                           68.109.202.25
                           68.1.18.25
    Lease Obtained. . . . . : Monday, November 07, 2005 1:20:59 AM
```

В данном примере IPv4: 192.168.1.30

"Подбор порта" или "брутфорс порта" – это метод атаки, при котором злоумышленник пытается найти открытый порт <public port> на **компьютере** или **сетевом устройстве**, пробуя последовательно различные порты. Эта атака использует перебор, чтобы определить, на каком порту работает определенная служба или приложение, а затем может использоваться для попыток несанкционированного доступа или атаки на найденный канал связи.



Для этого примера.

PC1 имеет порт **443** (hTTPS)

PC2 имеет порт **27015**

CAMERA имеет порт **34599**

Технические средства <Устройства> перехвата информации:
например НЧ генераторы и ВЧ-генераторы (высокочастотный генератор) .

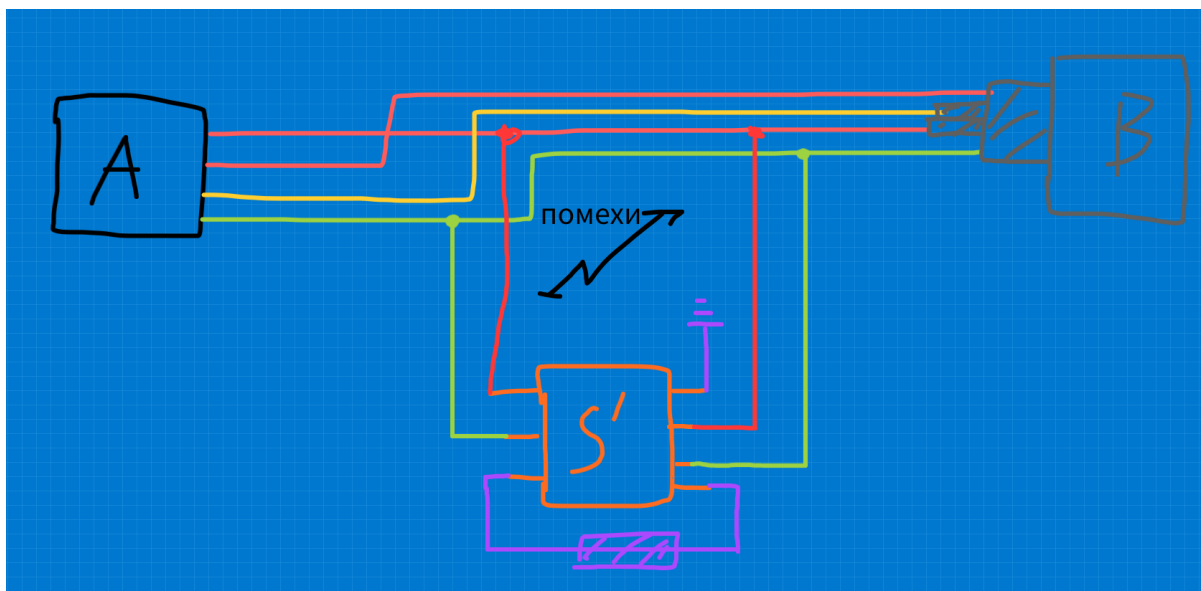
Если заряд устройства низкий, то перехват информации будет некачественным. Для более хорошего сигнала следует использовать устройство со 100% зарядом.

Согласно законам РФ запрещено применение таких устройств без определенного согласия компании, офиса, фирм, предприятия...

ЗАДАНИЕ НА ЛАБОРАТОРНУЮ РАБОТУ.

Цель задания: посмотреть как работает простой перехват информации на специально созданном безвредном эмуляторе сервера. (язык программирования PYTHON)

СХЕМА ПЕРЕХВАТА.



Есть источник сигнала А, и приемник сигнала – В.
S' – наше устройство перехвата которое подключается к каналам между А и В.

Техническое устройство перехвата информации S' создает модульные колебания которые в свою очередь создают высокие помехи в канале связи. Благодаря помехам появляется канал утечки информации. А благодаря каналу утечки злоумышленник может проникнуть в систему и перехватить важную информацию.

КОМАНДЫ CMD <SERVER>:

ipconfig – просмотр IP адреса устройства

port – для просмотра порта устройства (эмуляция перебора порта)

devices – просмотр устройств подключенных (технических средств)

connect <ip> <port> – команда для подключения к указанному <ip> <port> с целью прослушивания

connect device <number id> – команда подключения выбранного устройства (НЧ или ВЧ генератора)

start device – эмуляция перехвата информации с помощью технических средств.

decode <text decoding> – команда для расшифровки полученной информации.

CTRL+Z – команда для временной остановки действия (команды). Только в этом случае придется перезапустить эмулятор.

ХОД РАБОТЫ.

Скачать эмулятор CMD <SERVER>

<https://disk.yandex.ru/d/qnv-fDZvqxEw0Q>

(там два файла **server.py** и **interface.py** + файл data; **ЗАПРЕЩЕНО ВНОСИТЬ КАКИЕ ЛИБО ИЗМЕНЕНИЯ В ЭТИ ДВА ФАЙЛА + ФАЙЛ DATA**)

ЗАПУСКАЕТЕ INTERFACE.PY ФАЙЛ И ПРОДЕЛЫВАЕТЕ СЛЕДУЮЩИЕ ШАГИ:

1. получение **ip адреса** и **порта** устройства
2. подключиться по указанному **ip** и **порту** для прослушивания.
3. посмотреть список устройств (*технических средств*)
4. выбрав техническое средство для перехвата информации подключить устройство к каналу утечки.
5. запустить устройство перехвата информации.
6. расшифровать перехваченную информацию средствами PYTHON.
7. результат выполнения – это два расшифрованных текста.