Практическое занятие 5
«Сетевая анонимность»

Для выполнения заданий студентам понадобится основной ПК, виртуальная машина Practic5_anonymous и смартфон с доступом в сеть Интернет.

Результаты выполнения заданий записываются в отчет.

Задание 0. Создайте файл отчета с названием в формате «ФамилияИмяОтчество».

Задание 1. Считывание идентификаторов аппаратных компонентов ПК.
Шаг 1. Запустите консоль Windows (Win+R, cmd)
Шаг 2. Выполните следующие команды:
wmic cdrom get deviceid
wmic cdrom get volumeserialnumber
wmic diskdrive get serialnumber
wmic diskdrive get pnpdeviceid
wmic cpu get name
wmic cpu get revision
wmic memorychip get
wmic cpu get serialnumber
Шаг 3. Определите MAC-адрес сетевой карты.
Выполните *ipconfig /all* или воспользуйтесь графическим интерфейсом «Панель управления > Сеть»
Шаг 4. Запишите полученные идентификаторы в файл отчета.

Задание 2. Считывание идентификаторов аппаратных компонентов смартфона.
Способ 1. Для определения IMEI наберите в телефоне *#06#
Способ 2. Посмотрите IMEI/MEID, MAC, Serial в настройках «Настройки» > «Основные» > «О программе»
Способ 3. Посмотреть IMEI на корпусе телефона, лотке SIM-карты или на коробке.

Результат определения IMEI, MAC, Serial и IMSI запишите в отчет. В соответствии со справочной информацией опишите IMEI (марку и модель телефона, TAC, FAC, SNR, CD), по IMSI определите оператора сотовой связи и страну, по MAC адресу определите производителя сетевой карты.

Справочно:

Стандартный код IMEI состоит из 15 цифр, есть также вариант IMEISV, который имеет 16 цифр.

Код IMEI содержит модель, происхождение и серийный номер устройства. Стандартный формат AA-BBBBBB-CCCCCC-D для IMEI и AA-BBBBBB-CCCCCC-EE для IMEISV.

Первые 8 цифр (A и B) представляют TAC (код распределения типа), который однозначно идентифицирует устройство. До 2002 года последние 2 цифры относились к FAC (Код окончательной сборки), в котором указывалось, где был собран телефон. Следующие 6 цифр (C) содержат серийный номер устройства. Последняя цифра (D) в IMEI представляет контрольную сумму Luhn. Вместо этого последние 2 цифры (E) IMEISV указывают номер версии программного обеспечения .

Пример IMEI – 861647030675728

Пример проверки IMEI по базе https://www.imei.info/ru/?imei=861647030675728

(M3 MEIZU IMEI: TAC: 861647 FAC: 03 SNR: 067572 CD: 8)

IMSI – International Mobile Subscriber Identity. Телекоммуникационная компания присваивает уникальный номер SIM-карте, которую они выдают своим абонентам. Номера IMSI состоят из 15 цифр (не всегда).

Пример: 250-01-1234567890. Первые три цифры это MCC (Mobile Country Code, мобильный код страны). В примере 250 – Россия. За ним следует MNC (Mobile Network Code, код мобильной сети), 01 – МТС, 02 – Мегафон, 20 – Теле2, 99 – Билайн.

MAC-адрес (Media Access Control) – уникальный идентификатор, присваиваемый каждой единице активного оборудования или некоторым их интерфейсам в компьютерных сетях Ethernet. Стандарты IEEE определяют 48-разрядный (6 октетов) MAC-адрес. Первые 3 октета содержат 24-битный уникальный идентификатор организации (OUI), или код MFG (Manufacturing, производителя), который производитель получает в IEEE. Следующие три октета – выбираются изготовителем для каждого экземпляра устройства.

https://www.wireshark.org/tools/oui-lookup.html

Задание 3. Определение местоположения смартфона и компьютера.

Шаг 1. Определение местоположения узла на основе IP-адреса в сети Интернет

Для определения местоположения по IP-адресу на основе базы MaxMind посетите отдельно на смартфоне (сотовая сеть) и компьютере (сеть университета) один из ресурсов:

https://2ip.ru/geoip/

https://ip2geolocation.com/

https://ip-go.ru/

https://whoer.net/

Результаты определения местоположения (страна, город, координаты) запишите в отчет.

Шаг 2. Определение местоположения в смартфоне на основе данных сотовой сети

Воспользуйтесь программами типа NetMonitor (рекомендуется), OpenSignal, Network Cell Info в Android для определения параметров сотовых вышек поблизости (MCC, MNC, LAC, CellID) и найдите их в базе

https://opencellid.org

https://cellidfinder.com/

https://www.mylnikov.org/

Справочно:

Для того, чтобы найти координаты сектора базовой станции необходимо знать 4 параметра:

MCC (Mobile Country Code) – код, определяющий страну, в которой находится оператор мобильной связи.

MNC (Mobile Network Code) – код, присваиваемый оператору мобильной связи.

LAC (Location Area Code) – код локальной зоны. В двух словах LAC - это объединение некоторого количества базовых станций, которые обслуживаются одним контроллером базовых станций (BSC). Этот параметр может быть представлен как в десятичном, так и в шестнадцатеричном виде.

CellID (CID) – «идентификатор соты». Тот самый сектор базовой станции. Этот параметр также может быть представлен в десятичном, и шестнадцатеричном виде.

Результаты определения (MCC, MNC, LAC, CellID) и местоположения запишите в отчет.

Шаг 3. Определение местоположения на основе данных о видимых Wi-Fi сетях

Запишите ESSID и BSSID Wi-Fi сетей в Вашем окружении (можно для домашней сети).

Справочно:

Для определения BSSID (MAC-адресов точек доступа) можно воспользоваться снифером, например, WirelessNetView, airodump-ng или программой для смартфона типа WiFi Analyzer (VREM Software Development) – open source, либо посмотреть данные в настройках известных сетей.

Найдите местоположение сети в базе https://www.mylnikov.org/

Пример:

https://api.mylnikov.org/geolocation/wifi?v=1.1&data=open&bssid=00:0C:42:1F:65:E9

{"result":200, "data":{"lat": 45.22058921511, "range": 146.104, "lon": 16.54733338499, "time": 1639318756}}

или

с помощью скриптов https://github.com/GONZOsint/geowifi (порядок установки описан в документации)

Подготовительные мероприятия:

Импортировать и запустить виртуальную машину Practic5_anonymous с операционной системой Windows 10 и необходимыми программами в VirtualBox.

Параметры входа в ОС Windows:

Username: student

Password: 12345678

Задание 4. Подключение к заблокированным сайтам.

Шаг 1. Запустите Tor-браузер

Шаг 2. Подключитесь к сети Tor, следуя инструкциям на сайте torproject.org или tor.eff.org

Шаг 3. Выберите сайт, заблокированный Роскомнадзором (проверка блокировки eais.rkn.gov.ru). Зайдите на него с помощью обычного браузера без прокси и с помощью Tor-браузера. Сохраните скриншоты.

Примеры сайтов:

linkedin.com, rutracker.org

Задание 5. Изучение отпечатков браузера.

Определение идентификаторов CanvasFingerprint и FingerprintJS

1. Зайдите с помощью браузера на сайты https://fingerprintjs.com/demo/, https://browserleaks.com/canvas, https://ja3er.com/
2. Запишите значения Your ID, Your Fingerprint, JA3 SSL Fingerprint
3. Очистите историю, Cookie и закройте браузер.
4. Повторите посещение сайтов https://fingerprintjs.com, https://browserleaks.com/canvas, https://ja3er.com/
5. Сравните значение Your ID.

   Повторите пункты 1-5 в Tor-браузере или Brave.

   Запишите в отчет полученные результаты.

Задание 6. Создание скрытого сервиса в сети анонимизации TOR.

Шаг 1. Отредактируйте поле Title в index.html (напишите ФИО) и запустите Web-сервер Nginx из директории на рабочем столе виртуальной машины.

Шаг 2. Проверьте в браузере работоспособность Nginx посредством перехода по адресу http://127.0.0.1/

Шаг 3. Найдите файл конфигурации torrc в каталоге Tor-браузера («C:\Users\student\Desktop\Tor Browser\Browser\TorBrowser\Data\Tor»), добавьте директиву для настройки скрытого сервиса для порта web-сервера:

HiddenServiceDir C:\Users\student\Desktop\Tor Browser\Browser\TorBrowser\Data\Tor\hidden

HiddenServicePort 8888 127.0.0.1:80

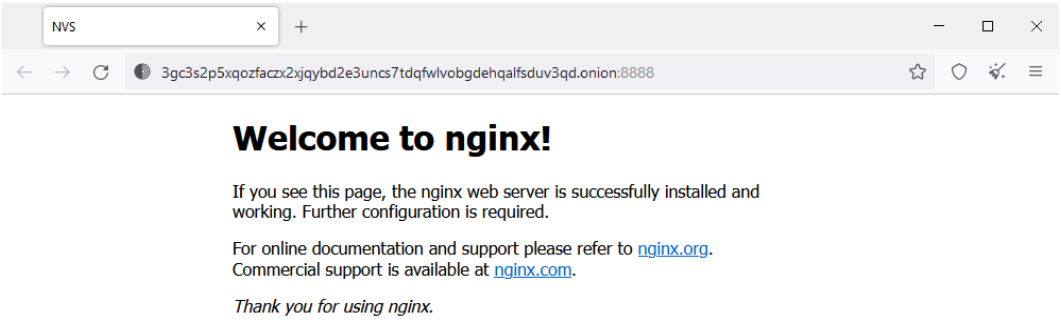
HiddenServiceVersion 3

Перезапустите Tor-браузер. В указанном каталоге появится адрес сайта в сети Tor (hostname).

Например, 3gc3s2p5xqozfaczx2xjqybd2e3uncs7tdqfwlvobgdehqalfsduv3qd.onion

Шаг 5. Проверьте работоспособность сайта через сеть Tor-браузер (порт 8888), сделайте скриншот браузера .

Например



Задание 7. Просмотр метаданных файла

Выберите любой файл в виртуальной машине или сети Интернет и с помощью утилиты exiftool просмотрите его метаданные. Результаты запишите в отчет.

Задание 8. Очистка временных файлов и затирание дискового пространства.

С помощью программы Privazer или BleachBit проведите очистку цифровых улик в пользовательском окружении. Результат работы программы сохраните в виде скриншота в отчет.