

Молдавский Государственный Университет Молдовы
Факультет Математики и Информатики
Департамент Информатики

Лабораторная работа №6

по предмету “Безопасность Информационных Систем”

тема: “Обнаружение и предотвращение вторжений в компьютерные системы.

Системы защиты от вредоносного ПО и журналирования. IDS/IPS (Intrusion Detection Systems / Intrusion Prevention Systems) (Windows, Linux и т. д.)”

Преподаватель: Dr Conf. Unif. Новак Л.
Выполнила: Павлышина Александра I2302

Кишинев, 2024

Цель работы

1. Изучение характеристик и принципа работы систем обнаружения и предотвращения вторжений. Анализ их рабочих параметров (IDS/IPS).
2. Сравнительная характеристика систем обнаружения или предотвращения вторжений IDS/IPS .
3. Изучение функциональности некоторых систем обнаружения/предотвращения вторжений.
4. Описание принципа работы систем обнаружения/предотвращения вторжений.
5. Установление классификации по степени популярности в использовании и эффективности эксплуатации перечисленных ниже SDI/SPI.

Ход работы

IDS (Intrusion Detection System) — система обнаружения вторжений, предназначенная для мониторинга сетевого трафика и выявления подозрительной активности.

IPS (Intrusion Prevention System) — система предотвращения вторжений, которая не только обнаруживает угрозы, но и может блокировать их в реальном времени.

Типы IDS:

- NIDS (Network-based IDS): Система, которая мониторит сетевой трафик и анализирует сетевые пакеты, проверяя их на наличие признаков угроз.
- HIDS (Host-based IDS): Устанавливается на конкретные хосты (серверы или рабочие станции) и контролирует их состояние, отслеживая изменения в файлах, а также поведение системных процессов.

Классификация методов детектирования:

1. Сигнатурные системы. Обнаруживают угрозы на основе известной базы сигнатур.
2. Аномальные системы. Ищут подозрительные активности, отличающиеся от нормального поведения.
3. Гибридные системы. Комбинируют сигнатурный и аномальный подходы для более эффективного обнаружения угроз.

Основные отличия IDS и IPS заключаются в том, что IDS выполняет функции анализа и уведомления, не влияя на поток данных, а IPS, в дополнение к этому, может активно вмешиваться, блокируя опасный трафик или завершая подозрительные процессы.

Для более подробного сравнительного анализа IDS/IPS были взяты следующие системы:

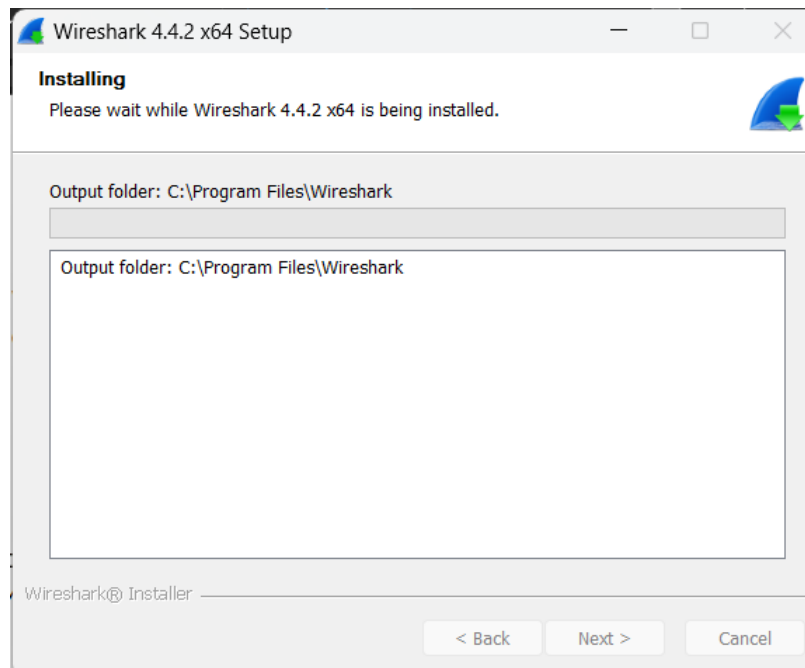
Критерий	Wireshark	NetworkMiner
Условия использования	Бесплатное ПО с открытым исходным кодом (GPL).	Бесплатная версия с ограниченными функциями, платная версия для расширенного функционала.
Совместимость с ОС	Поддержка Windows, macOS, Linux, UNIX.	Поддержка Windows; возможно, работает через Wine на Linux, но официально не поддерживается.
Предлагаемые услуги/принципы работы	Анализ сетевого трафика в реальном времени; мощные инструменты фильтрации и декодирования.	Анализ захваченных пакетов, фокус на восстановлении файлов и данных из сетевых сессий.
Преимущества	<ul style="list-style-type: none"> - Мощный и гибкий анализ трафика. - Поддерживает тысячи протоколов. - Огромное сообщество. 	<ul style="list-style-type: none"> - Простота для анализа pcap-файлов. - Поддержка восстановления данных (например, изображений).
Недостатки	<ul style="list-style-type: none"> - Сложное обучение для новичков. - Может быть ресурсоемким. 	<ul style="list-style-type: none"> - Ограниченная функциональность в бесплатной версии. - Ограниченная поддержка ОС.

Интерфейс/удобство	- Графический интерфейс. - Поддержка работы с командной строкой.	- Удобный графический интерфейс, но без CLI.
Степень безопасности	- Высокий уровень безопасности, но возможны ошибки анализа, если данные повреждены.	- Минимальный риск ложных тревог, но ограничен в реальном времени.
Популярность /категории пользователей	- Популярен среди сетевых инженеров, ИБ-специалистов, преподавателей.	- Используется исследователями кибербезопасности, экспертами по анализу данных.
Общая простота использования	Высокая сложность для новичков, но огромный потенциал для профессионалов.	Прост в освоении, особенно для восстановления файлов и анализа содержимого.

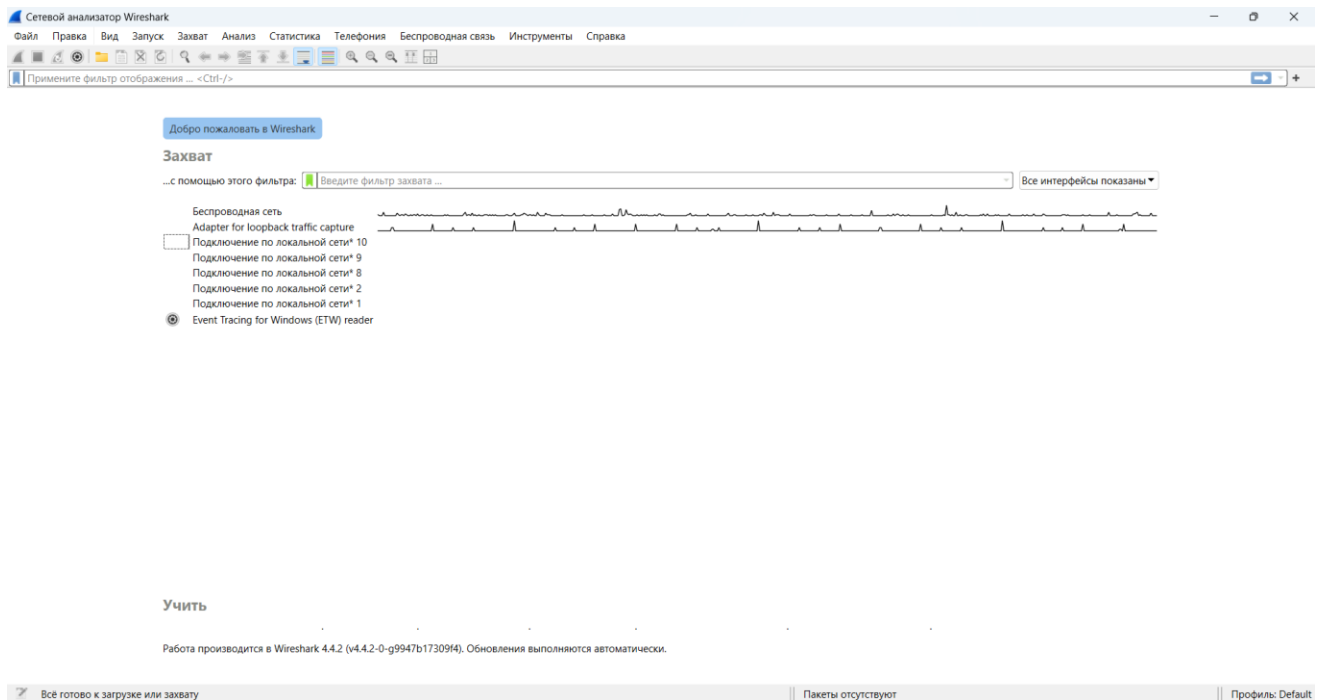
Wireshark — это мощный инструмент для детального анализа сетевого трафика, идеально подходящий для профессионалов, которым важны широкие возможности и гибкость. NetworkMiner больше подходит для тех, кто занимается восстановлением данных из захваченных пакетов, и является удобным инструментом для анализа пост-фактум.

Wireshark

Я скачиваю Wireshark с официального сайта и устанавливаю программное обеспечение, выбрав стандартные параметры.



Запускаю программу и меня встречает стартовое меню, на котором можно увидеть доступные для захвата интерфейсы компьютера, руководства от разработчиков программы и множество других вещей.



Из всего имеющегося меня интересует пока только эта область. Здесь нужно выбрать тот сетевой интерфейс, через который я подключены к интернету.

Добро пожаловать в Wireshark

Захват

...с помощью этого фильтра:

Беспроводная сеть

Adapter for loopback traffic capture


☐ Подключение по локальной сети* 10

Подключение по локальной сети* 9

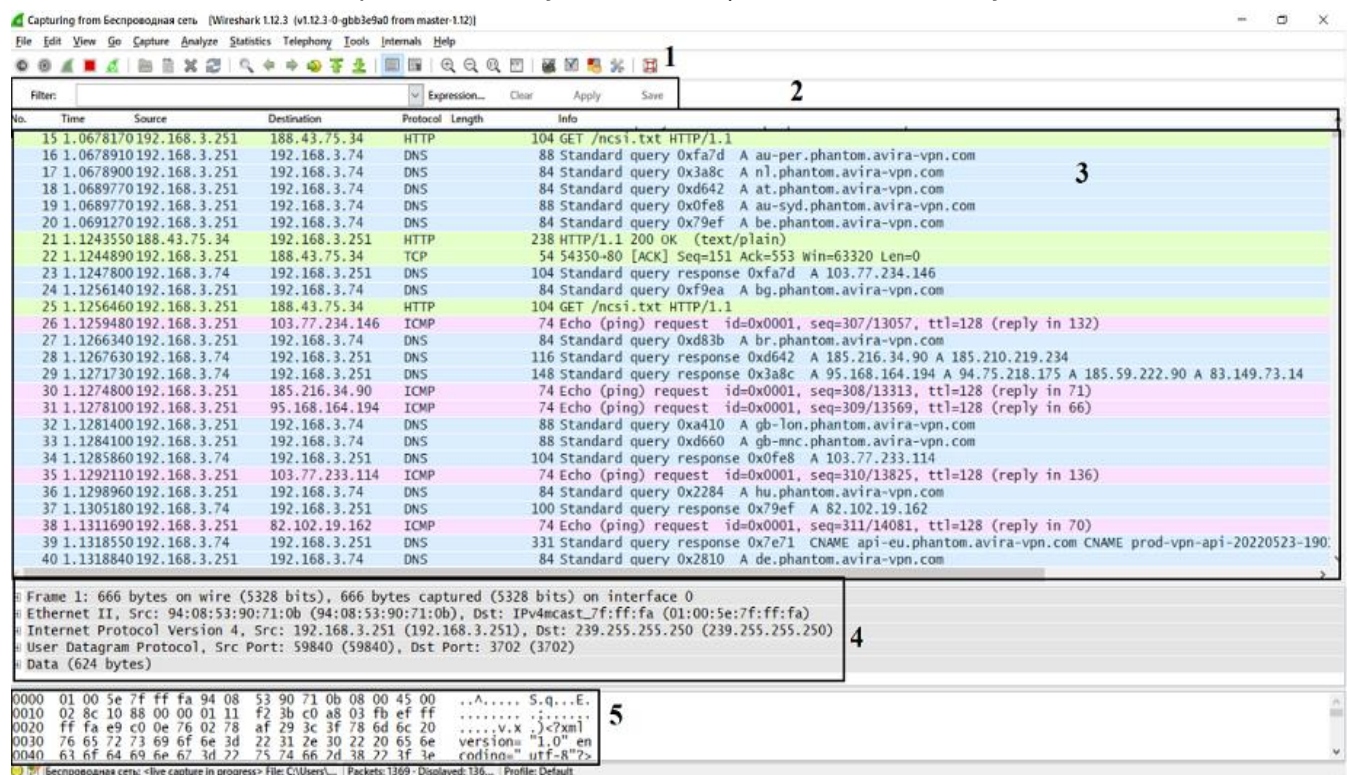
Подключение по локальной сети* 8

Подключение по локальной сети* 2

Подключение по локальной сети* 1

 Event Tracing for Windows (ETW) reader

Выбрав подходящий интерфейс, в моем случае это беспроводная сеть (есть возможность также выбрать кабельную - Ethernet), появляется следующее окно



1. Filter: Expression... Clear Apply Save

2. Packet list table:

No.	Time	Source	Destination	Protocol	Length	Info
15	1.0678170	192.168.3.251	188.43.75.34	HTTP	104	GET /ncsi.txt HTTP/1.1
16	1.0678910	192.168.3.251	192.168.3.74	DNS	88	Standard query 0xfa7d A au-per.phantom.avira-vpn.com
17	1.0678900	192.168.3.251	192.168.3.74	DNS	84	Standard query 0x3a8c A nl.phantom.avira-vpn.com
18	1.0689770	192.168.3.251	192.168.3.74	DNS	84	Standard query 0xd642 A at.phantom.avira-vpn.com
19	1.0689770	192.168.3.251	192.168.3.74	DNS	88	Standard query 0x0fe8 A au-syd.phantom.avira-vpn.com
20	1.0691270	192.168.3.251	192.168.3.74	DNS	84	Standard query 0x79ef A be.phantom.avira-vpn.com
21	1.1243550	188.43.75.34	192.168.3.251	HTTP	238	HTTP/1.1 200 OK (text/plain)
22	1.1244890	192.168.3.251	188.43.75.34	TCP	54	54350->80 [ACK] Seq=151 Ack=553 Win=63320 Len=0
23	1.1247800	192.168.3.74	192.168.3.251	DNS	104	Standard query response 0xfa7d A 103.77.234.146
24	1.1256140	192.168.3.251	192.168.3.74	DNS	84	Standard query 0xf9ea A bg.phantom.avira-vpn.com
25	1.1256460	192.168.3.251	188.43.75.34	HTTP	104	GET /ncsi.txt HTTP/1.1
26	1.1259480	192.168.3.251	103.77.234.146	ICMP	74	Echo (ping) request id=0x0001, seq=307/13057, ttl=128 (reply in 132)
27	1.1266340	192.168.3.251	192.168.3.74	DNS	84	Standard query 0xd83b A br.phantom.avira-vpn.com
28	1.1267630	192.168.3.74	192.168.3.251	DNS	116	Standard query response 0xd642 A 185.216.34.90 A 185.210.219.234
29	1.1271730	192.168.3.74	192.168.3.251	DNS	148	Standard query response 0x3a8c A 95.168.164.194 A 94.75.218.175 A 185.59.222.90 A 83.149.73.14
30	1.1274800	192.168.3.251	185.216.34.90	ICMP	74	Echo (ping) request id=0x0001, seq=308/13313, ttl=128 (reply in 71)
31	1.1278100	192.168.3.251	95.168.164.194	ICMP	74	Echo (ping) request id=0x0001, seq=309/13569, ttl=128 (reply in 66)
32	1.1281400	192.168.3.251	192.168.3.74	DNS	88	Standard query 0xa410 A gb-lon.phantom.avira-vpn.com
33	1.1284100	192.168.3.251	192.168.3.74	DNS	88	Standard query 0xd660 A gb-mnc.phantom.avira-vpn.com
34	1.1285860	192.168.3.74	192.168.3.251	DNS	104	Standard query response 0x0fe8 A 103.77.233.114
35	1.1292110	192.168.3.251	103.77.233.114	ICMP	74	Echo (ping) request id=0x0001, seq=310/13825, ttl=128 (reply in 136)
36	1.1298960	192.168.3.251	192.168.3.74	DNS	84	Standard query 0x2284 A hu.phantom.avira-vpn.com
37	1.1305180	192.168.3.74	192.168.3.251	DNS	100	Standard query response 0x79ef A 82.102.19.162
38	1.1311690	192.168.3.251	82.102.19.162	ICMP	74	Echo (ping) request id=0x0001, seq=311/14081, ttl=128 (reply in 70)
39	1.1318550	192.168.3.74	192.168.3.251	DNS	331	Standard query response 0xe71 CNAME api-eu.phantom.avira-vpn.com CNAME prod-vpn-api-20220523-190
40	1.1318840	192.168.3.251	192.168.3.74	DNS	84	Standard query 0x2810 A de.phantom.avira-vpn.com

3. Packet details pane:

Frame 1: 666 bytes on wire (5328 bits), 666 bytes captured (5328 bits) on interface 0

Ethernet II, Src: 94:08:53:90:71:0b (94:08:53:90:71:0b), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)

Internet Protocol Version 4, Src: 192.168.3.251 (192.168.3.251), Dst: 239.255.255.250 (239.255.255.250)

User Datagram Protocol, Src Port: 59840 (59840), Dst Port: 3702 (3702)

Data (624 bytes)

4. Packet bytes pane:

0000 01 00 5e 7f ff fa 94 08 53 90 71 0b 08 00 45 00 ..A....S.q...E.
0010 02 8c 10 88 00 00 01 11 f2 3b c0 a8 03 fb ef ff:.....
0020 ff fa e9 c0 0e 76 02 78 af 29 3c 3f 78 6d 6c 20v.x.)<xml
0030 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e version="1.0" en
0040 61 6f 64 69 6e 67 3d 22 75 74 66 2d 38 22 3f 3e codinn="utf-8">

5. Status bar: Беспроводная сеть: <live capture in progress> File: C:\Users\... Packets: 1369 / Displayed: 136... Profile: Default

Wireshark — подробное руководство по началу использования / Хабр

, где:

1. Панель фильтров, позволяющая найти необходимую информацию.
2. Панель наименований, разделяющая информацию из пункта 3 на номер, времени с начала захвата трафика, источник и адресат, а также используемый протокол, размер пакета и небольшую информацию о сетевом пакете.
3. Панель пакетов, обновляющаяся в реальном времени. Здесь информация о пакетах разделена по столбцам, определённым на панели наименований.
4. Панель уровней, описывающая уровни модели OSI выбранного сетевого пакета.
5. Панель метаданных, представляющая данные в шестнадцатеричном коде и символах.

Для анализа трафика использую фильтр http. Это помогло выделить HTTP-запросы, в которых могли быть обнаружены подозрительные действия. Происходит анализ пакетов, из-за чего нужно обратить внимание на необычные IP-адреса и типы запросов.

The screenshot shows the Wireshark interface with the 'http' filter applied. The packet list pane displays several HTTP GET requests. The selected packet (No. 24403) is expanded in the packet details pane, showing the Ethernet II, Internet Protocol Version 4, and Hypertext Transfer Protocol layers. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
24403	0.74279	10.22.128.152	92.122.18.32	HTTP	455	GET /MFewTsBNMEswSTA3BgUdNgMCgUABBRr2bwARTxMteY9asprAZg5QfhagQQUgrWP2Fon89x6J13r%2F2ztwk1V8BCEDwt3udNB9q%2F1%2BERqxsHS%3D HTTP/1.1
24404	0.92415	92.122.18.32	10.22.128.152	HTTP	413	HTTP/1.1 304 Not Modified
24420	259.184528	10.22.128.152	142.250.187.131	HTTP	254	GET /r/r1.cr1 HTTP/1.1
24435	259.261864	142.250.187.131	10.22.128.152	HTTP	277	HTTP/1.1 304 Not Modified
24442	259.286227	10.22.128.152	92.122.17.28	HTTP	281	GET / HTTP/1.1
24444	259.298096	92.122.17.28	10.22.128.152	HTTP	317	HTTP/1.1 304 Not Modified
24445	259.305312	10.22.128.152	142.250.187.131	HTTP	256	GET /r/gsr1.cr1 HTTP/1.1
24455	259.385192	142.250.187.131	10.22.128.152	HTTP	277	HTTP/1.1 304 Not Modified
24457	259.393680	10.22.128.152	142.250.187.131	HTTP	254	GET /r/r4.cr1 HTTP/1.1
24459	259.471804	142.250.187.131	10.22.128.152	HTTP	276	HTTP/1.1 304 Not Modified

Packet Details for Frame 24403:

- Ethernet II, Src: CloudNetwork_64:5d:a3 (cc:5e:f8:64:5d:a3), Dst: Cisco_42:41:5f (74:8f:c2:42:41:5f)
- Internet Protocol Version 4, Src: 10.22.128.152, Dst: 92.122.18.32
- Transmission Control Protocol, Src Port: 52474, Dst Port: 80, Seq: 1, Ack: 1, Len: 401
- Hypertext Transfer Protocol

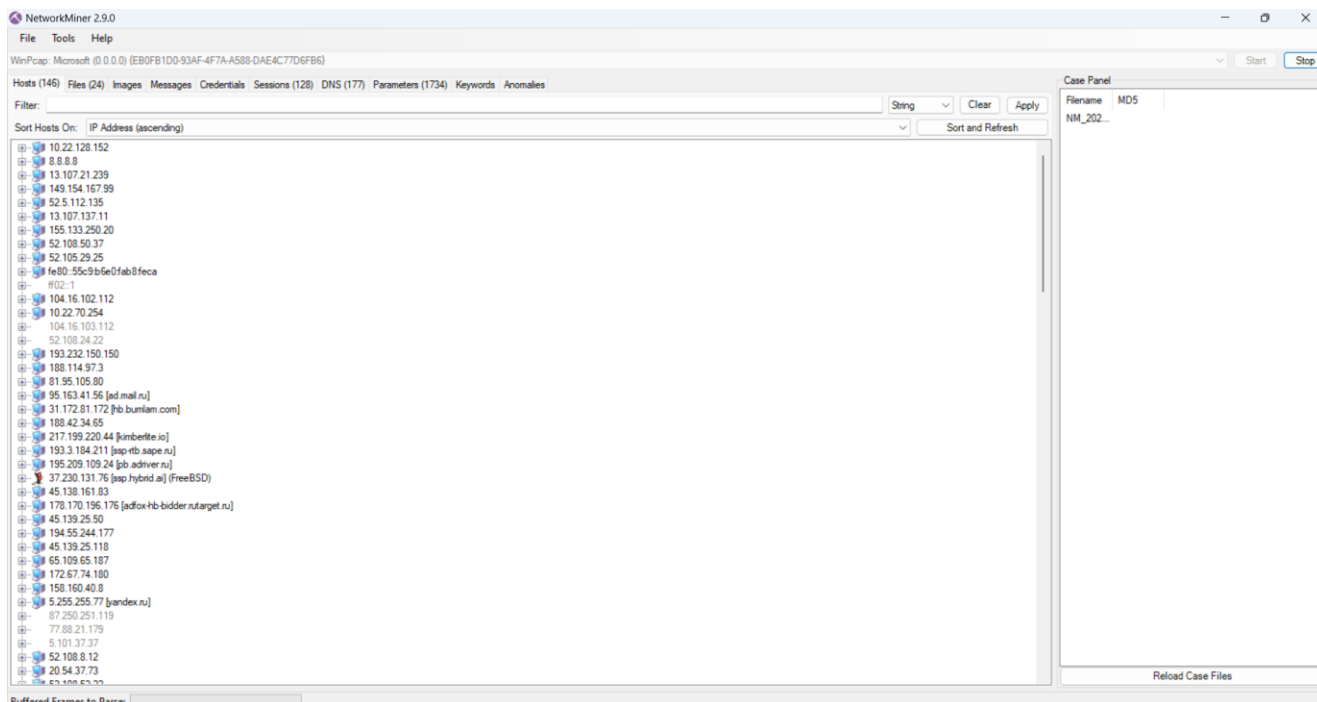
Packet Bytes:

```

0000  74 8f c2 42 41 5f cc 5e f8 64 5d a3 08 00 45 00  t..BA..^..d]...E
0010  01 b9 5e e8 40 00 80 06 a1 0e 0a 16 80 98 5c 7a  ...@... ..z
0020  12 20 cc fa 00 50 b2 57 6a 5f 29 89 fc 49 50 18  ...P.W j...-IP-
0030  02 00 fb 89 00 00 47 45 54 20 2f 4d 46 45 77 54  ....-GE T//MFewT
0040  7a 42 4e dd 45 73 77 53 54 41 4a 42 67 55 72 44  zBNMEswS TA7BgUrD
0050  67 4d 43 47 67 55 41 42 42 52 72 32 62 77 41 52  gMCGUAB BRr2bwAR
0060  54 78 4d 74 45 79 39 61 73 70 52 41 5a 67 35 51  TxMteY9a sprAZg5Q
0070  46 68 61 67 51 51 55 67 72 72 57 50 5a 66 4f 6e  FhagQQUg rrwP2Fon
0080  89x6J13r K2F2ztwk 1V8BCEDwt3udNB9q%2F1%2BERqxsHS%3D HTTP/1.1
0090  31 56 38 38 43 45 44 57 76 74 33 75 64 4e 42 39  1V8BCEDwt3udNB9
00a0  71 25 32 46 49 25 32 42 45 52 71 73 78 4e 53 73  q%2F1%2B ERqxsHS
00b0  25 33 44 20 48 54 54 50 2f 31 2e 31 0d 0a 43 61  %3D HTTP /1.1..Ca
00c0  63 68 65 2d 43 6f 6e 74 72 6f 6c 3a 20 6d 61 78  che-Cont rol: max
00d0  2d 61 67 65 20 3d 20 31 31 32 38 0d 0a 43 6f 6e  -age = 1 128..Con
  
```

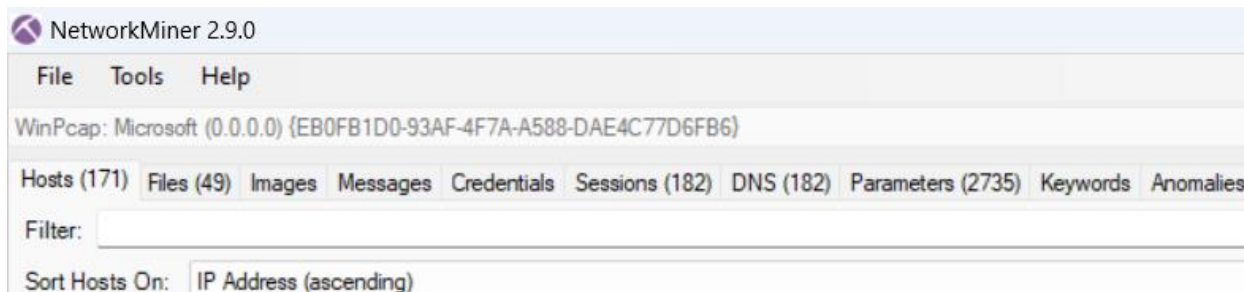
NetworkMiner

Я скачиваю NetworkMiner с официального сайта и распаковываю архив, захожу сразу в приложение, так как установка не требуется. После запуска нам предоставляется удобный интерфейс, который сразу же позволяет начать анализ данных.



В главном меню выбираю сетевой интерфейс, в моем случае это WIFI. Нажимаю кнопку Start для запуска анализа, после чего программа начинает пассивный сбор данных, отображая hosts, соединения и трафик.

Во вкладке “Hosts” отобразились устройства, подключенные к сети. Для каждого хоста указаны IP-адрес, MAC-адрес и общая информация о соединениях. А во вкладке “Files” показываются файлы, переданные в сети. Я анализирую переданные документы, чтобы выявить подозрительные данные. Во вкладке “Credentials” программа автоматически извлекает учетные данные, которые могли быть переданы по незащищенным протоколам.



В итоге я проверила не появляются ли неизвестные устройства в списке хостов и проанализировала подозрительные соединения, где был передан большой объем данных или использовались необычные порты.

Вывод

В процессе выполнения лабораторной работы я изучила принципы работы систем обнаружения и предотвращения вторжений (IDS/IPS), а также их роль в обеспечении информационной безопасности. Я провела анализ сетевого трафика с использованием таких инструментов, как Wireshark и NetworkMiner, которые предоставили работу с трафиком и базовое понимание анализа сетевых угроз.

Библиография

1. <https://habr.com/ru/articles/204274/>
2. <https://selectel.ru/blog/ips-and-ids/>
3. <https://www.wireshark.org/download.html>
4. <https://www.netresec.com/?page=NetworkMiner>
5. <https://spy-soft.net/networkminer/>