



ОНЛАЙН-ОБРАЗОВАНИЕ

Основные сетевые протоколы. Разбор трафика.



Меня хорошо слышно && видно?



Напишите в чат, если есть проблемы!

Ставьте если все хорошо

- **Утилиты для анализа трафика**
 - WireShark
 - Некоторые полезные утилиты для анализа
- **Практика**
 - Разбор тестового трафика
 - Фильтры
 - Форматы
 - Вспомогательные утилиты

1. Вспомнить основы протоколы сетевого взаимодействия
2. Собрать информацию о сеть посредством анализа трафика
3. Получить навыки работы с утилитами для обработки сетевого трафика



01

Утилиты для анализа трафика

Типы утилит:

1. Снифферы

- WireShark
- Net-Miner
- tcpdump
- netsniff-ng

2. Респондеры

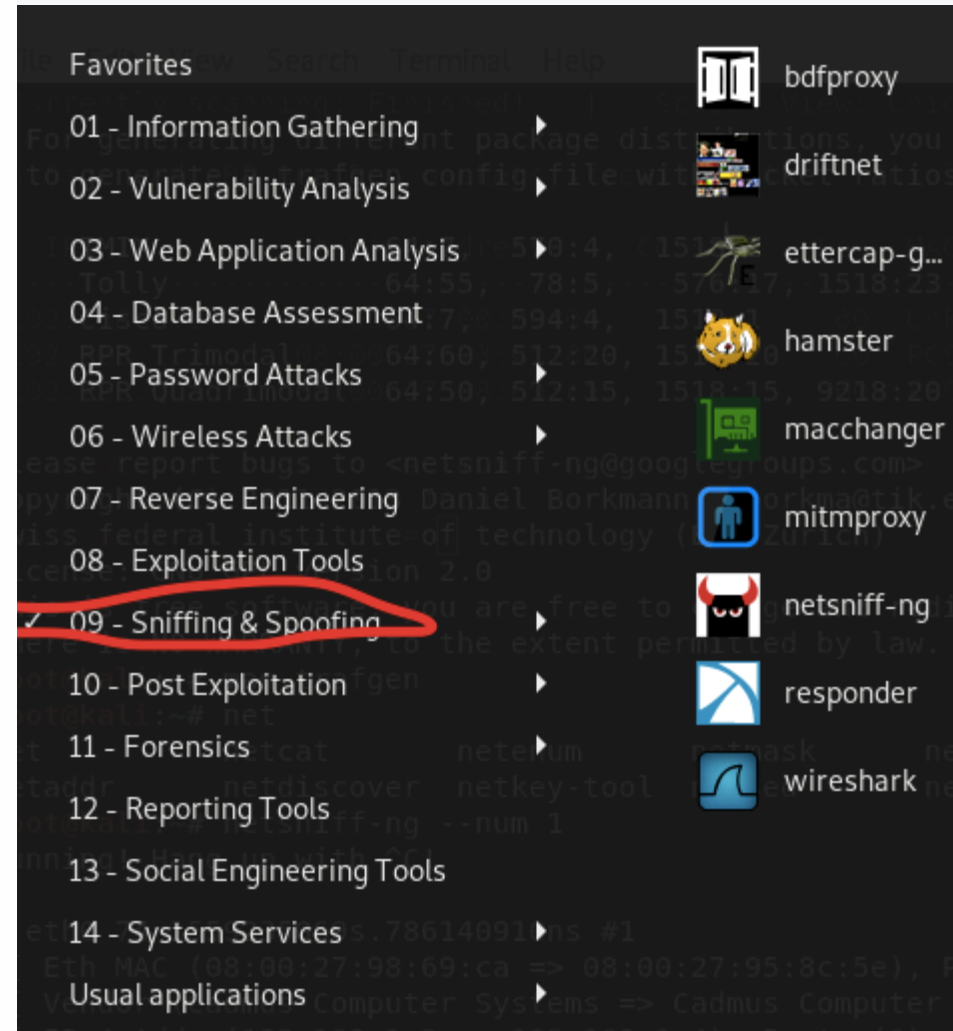
- Responder
- Ettercap

3. Прокси

- Burp Suite
- Owasp ZAP
- mitmproxy

4. Библиотеки

- libpcap
- NpCap



Панель инструментов

Фильтр
Данные из сети

| No. | Time | Source | Destination | Protocol | Length |
|-----|-----------|-----------------------|----------------|----------|-------------|
| 215 | 3.339917 | 172.20.10.5 | 2.18.74.168 | TCP | 54 |
| 216 | 3.616795 | 172.20.10.5 | 172.20.10.1 | UDP | 46 08010310 |
| 217 | 3.620284 | 172.20.10.1 | 172.20.10.5 | ICMP | 70 |
| 218 | 4.120451 | 172.20.10.5 | 172.20.10.1 | UDP | 46 10010310 |
| 219 | 4.128043 | 172.20.10.1 | 172.20.10.5 | ICMP | 70 |
| 220 | 4.453751 | 172.20.10.5 | 172.20.10.15 | NBNS | 110 |
| 221 | 4.694150 | 172.20.10.5 | 224.0.0.251 | MDNS | 530 |
| 222 | 5.958685 | 172.20.10.5 | 17.248.150.119 | TLSv1... | 1273 |
| 223 | 5.959368 | 172.20.10.5 | 17.248.150.119 | TLSv1... | 423 |
| 224 | 6.017687 | 17.248.150.119 | 172.20.10.5 | TCP | 66 |
| 225 | 6.017692 | 17.248.150.119 | 172.20.10.5 | TCP | 66 |
| 226 | 6.198965 | 17.248.150.119 | 172.20.10.5 | TLSv1... | 1094 |
| 227 | 6.199050 | 172.20.10.5 | 17.248.150.119 | TCP | 66 |
| 228 | 8.073192 | 172.20.10.1 | 224.0.0.251 | MDNS | 180 |
| 229 | 8.073197 | fe80::10e3:7e9f:ff... | ff02::fb | MDNS | 200 |
| 230 | 9.628508 | 172.20.10.5 | 172.20.10.1 | UDP | 46 08010310 |
| 231 | 9.633171 | 172.20.10.1 | 172.20.10.5 | ICMP | 70 |
| 232 | 10.134029 | 172.20.10.5 | 172.20.10.1 | UDP | 46 10010310 |
| 233 | 10.137914 | 172.20.10.1 | 172.20.10.5 | ICMP | 70 |
| 234 | 10.720858 | 172.20.10.5 | 224.0.0.251 | MDNS | 424 |
| 235 | 15.640068 | 172.20.10.5 | 172.20.10.1 | UDP | 46 08010310 |
| 236 | 15.645040 | 172.20.10.1 | 172.20.10.5 | ICMP | 70 |
| 237 | 16.141546 | 172.20.10.5 | 172.20.10.1 | UDP | 46 10010310 |
| 238 | 16.145207 | 172.20.10.1 | 172.20.10.5 | ICMP | 70 |

Текстовые данные по каждому протоколу

```
Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
  Ethernet II, Src: Apple_11:25:f8 (d4:61:9d:11:25:f8), Dst: ba:01:a7:0f:a7:64 (ba:01:a7:0f:a7:64)
  Internet Protocol Version 4, Src: 172.20.10.5, Dst: 172.20.10.1
  User Datagram Protocol, Src Port: 51112, Dst Port: 53
  Domain Name System (query)
```

Командная строка

```
root@kali:~# netsniff-ng --num 1
Running! Hang up with C!
< eth0 74 1559235069s.786140910ns #]
  Chr MAC (08:00:27:95:8c:5e) => (08:00:27:95:8c:5e), Proto (0x0800, IPv4) ]
  Vendor (Cadmus Computer Systems => Cadmus Computer Systems) ]
  IPv4 Addr (192.168.1.3 => 192.168.1.4), Proto (6), TTL (64), TOS (0), Ver (4), IHL (5), Tlen (60), ID (26140), Res (0), NoFrag (1), MoreFrag (0), Frag
  Off (0), CSum (0x5148) is ok ]
  TCP Port (47381 => 2222), SN (0x27abb21f), AN (0x0), DataOff (10), Res (0), Flags (SYN), Window (14600), CSum (0x3c05), UrgPtr (0) ]
  Chr ..... ]
  Hex 02 04 05 b4 04 02 08 0a 00 0e 04 03 00 00 00 00 01 03 03 03 ]

  1 packets incoming (17 unread on exit)
  18 packets passed filter
  0 packets failed filter (out of space)
  0.0000% packet droprate
  1 sec. 799774 usec in total
```

Данные пакета

Статистика

Информация о принятом пакете

00

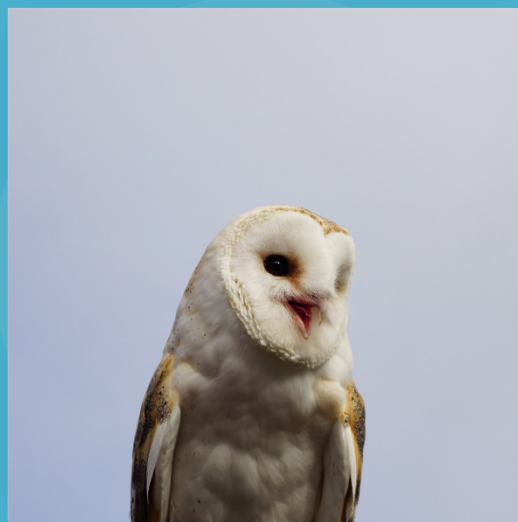
Анализ трафика

01

Разбор трафика

- Какие операционные системы есть в сети?
- Какие протоколы используются для общения?
- Можно ли установить название машин?
- Можно ли получить имена пользователей и другую пользовательскую информацию?
- Перечислить название общих ресурсов (шар)





Александр Колесников

**Спасибо
за внимание!**

