

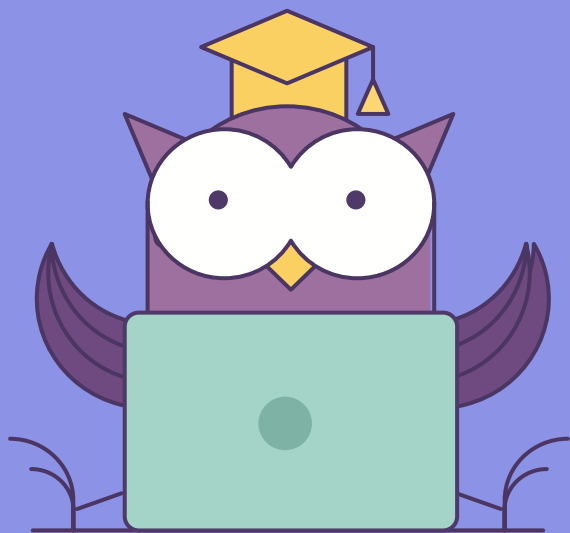


ОНЛАЙН-ОБРАЗОВАНИЕ

Основные сетевые протоколы



Меня хорошо слышно && видно?



Напишите в чат, если есть проблемы!

Ставьте если все хорошо

- **Сетевое взаимодействие**
 - Сетевые модели
 - Основные протоколы
 - Что такое трафик и зачем его разбирать
- **Утилиты для анализа трафика**
 - WireShark
 - Некоторые полезные утилиты для анализа
- **Практика**
 - Сканирование сети
 - Разбор трафика

1. Разобраться со стеком протоколов сетевого взаимодействия
2. Получить представление о том как нестандартно можно использовать информацию из протоколов для идентификации хостов в сети
3. Получить навыки работы с утилитами для обработки сетевого трафика



1. Что такое модель

В теории:

- Набор правил
- Схема работы правил
- Куча абстракций

2. Зачем нужна

В теории:

- Для того чтобы можно было делить действия на составные части
- Для создания алгоритма изучения взаимодействия систем

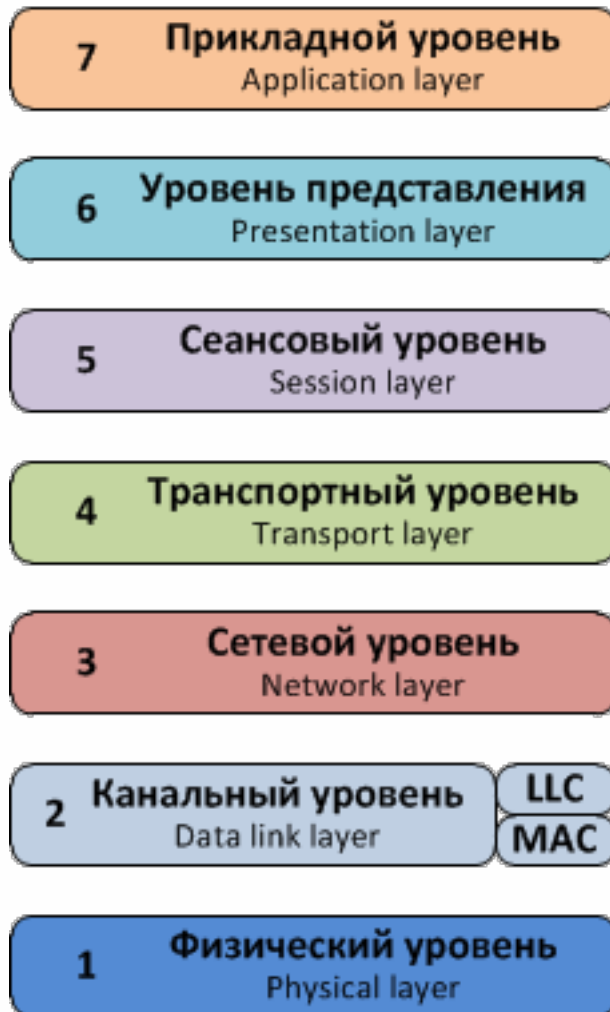
3. Какие бывают

На практике:

- TCP/IP
- IPX/SPX
- DOD



OSI



TCP/IP (DOD)



Прикладной	Захват имен пользователей и паролей
Представительский	Захват трафика сессий SSL/TLS
Сеансовый	Захват трафика Telnet и FTP
Транспортный	Захват TCP-сессий и UDP-трафика
Сетевой	Захват IP-адресов и номеров портов
Канальный	Захват MAC-адресов и ARP-запросов
Физический	Получение сведений о сети

01

Сетевое взаимодействие

Основные данные:

1. Протокол сетевого уровня модели TCP/IP
2. Основная задача протокола - адресация в сети
3. Популярные версии: v4, v6, безопасная версия - IPSec
4. Основные понятия протокола:
 - ip адрес
 - маска подсети
 - класс сети (v4)
 - маршрут



1. Адресация в протоколе возможна в пределах: $2^{32}-1$.
2. Чтобы расширить диапазон адресов можно использовать механизм NAT (Network Address Translation)
3. Для выдачи нового адреса нуждается в DHCP сервере
4. Создает адрес для каждого хоста с помощью адреса и маски подсети.
5. Хотя и задумывался как протокол с классификацией сетей, на данный момент используется с бесклассовой адресацией.

Возможные записи адреса: 192.168.1.1 255.255.255.0 или 192.168.1.1/24

Октет	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	Версия		IHL		Differentiated Services Code Point				ECN		Длина пакета																					
4	Идентификатор								Флаги		Смещение фрагмента																					
8	Время жизни (TTL)				Протокол				Контрольная сумма заголовка																							
12	IP-адрес отправителя																															
16	IP-адрес получателя																															
20	Параметры (от 0 до 10 32-битных слов)																															
	Данные																															

1. Адресация в протоколе возможна в пределах: $2^{128}-1$.
2. Не нуждается в NAT
3. Самостоятельно конфигурирует сеть и выдает адреса
4. Имеет отдельные адреса для передачи данных выбранным нодам
5. Адрес состоит только из адреса, маски подсети не используются

Возможные записи адреса: 2001:0DB8:AA10:0001:0000:0000:0000:00FB или 2001:0DB8:AA10:0001:::00FB

Позиция в октетах	Позиция в битах	0				1				2				3																	
		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29
0	0	Версия				Класс трафика				Метка потока																					
4	32	Длина полезной нагрузки								След. заголовок				Число переходов																	
8	64	IP-адрес отправителя																													
12	96																														
16	128																														
20	160																														
24	192																														
28	224	IP-адрес получателя																													
32	256																														
36	288																														

IPv4	IPv6
32 битный адрес	128 битный адрес
Статические адреса и динамические от DHCP	Автоконфигурация
Не гарантирует целостности	Предоставляет механизм целостности
Безопасность реализуется приложением	IPSec встроена в протокол
Десятичное представление адреса	Шестнадцатеричное представление адреса
Фрагментация на совете передающего	Фрагментация задается отправителем
Нет механизмов идентификации конкретного пользователя	Есть система тегирования в заголовке
Контрольная сумма пакета возможна	Контрольная сумма недоступна
Есть бродкастовая схема	Есть мультикастовая и эникастовая схема
Шифрование и аутентификация недоступны	Встроенная аутентификация и шифрование

1. Address Resolution Protocol
2. Протокол используется для обнаружения хостов в сети
3. Основные понятия:
 - ARP таблица
 - ip адрес
 - Mac адрес

+	Bits 0 – 7	8 – 15	16 – 31
0	Hardware type (HTYPE)		Protocol type (PTYPE)
32	Hardware length (HLEN)	Protocol length (PLEN)	Operation (OPER)
64	Sender hardware address (SHA)		
?	Sender protocol address (SPA)		
?	Target hardware address (THA)		
?	Target protocol address (TPA)		

1. Internet Control Message Protocol
2. Протокол помогает идентифицировать ошибки в сети
3. Основные понятия:
 - код ошибки

Октет (байт)	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
[0–3]	Тип							Код								Контрольная сумма																
...	Данные (формат зависит от значений полей «Код» и «Тип»)																															

1. Transmission Control Protocol
2. Позволяет контролировать соединение
3. Основное понятие протокола: порт

Примечание: Первая 1000 портов используется популярными сервисами и благодаря этому их можно с высокой точностью определять.

Бит	0 – 3	4 – 9	10 – 15	16 – 31
0	Порт источника, Source Port			Порт назначения, Destination Port
32	Порядковый номер, Sequence Number (SN)			
64	Номер подтверждения, Acknowledgment Number (ACK SN)			
96	Длина заголовка	Зарезервировано	Флаги	Размер Окна
128	Контрольная сумма			Указатель важности
160	Опции (необязательное, но используется практически всегда)			
160/192+	Данные			

1. User Datagram Protocol
2. Часто используется для передачи потоковых данных (звук, видео)
3. Основные понятия протокола: порт

Примечание: Протокол не требует ответа от целевого хоста. Так же таймаут отправки таких пакетов регулируется параметрами ядра операционных систем.

Биты	0 - 15	16 - 31
0-31	Порт отправителя (Source port)	Порт получателя (Destination port)
32-63	Длина датаграммы (Length)	Контрольная сумма (Checksum)
64-...	Данные (Data)	

02

Утилиты для анализа трафика

Типы утилит:

1. Снифферы

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

2. Респондеры

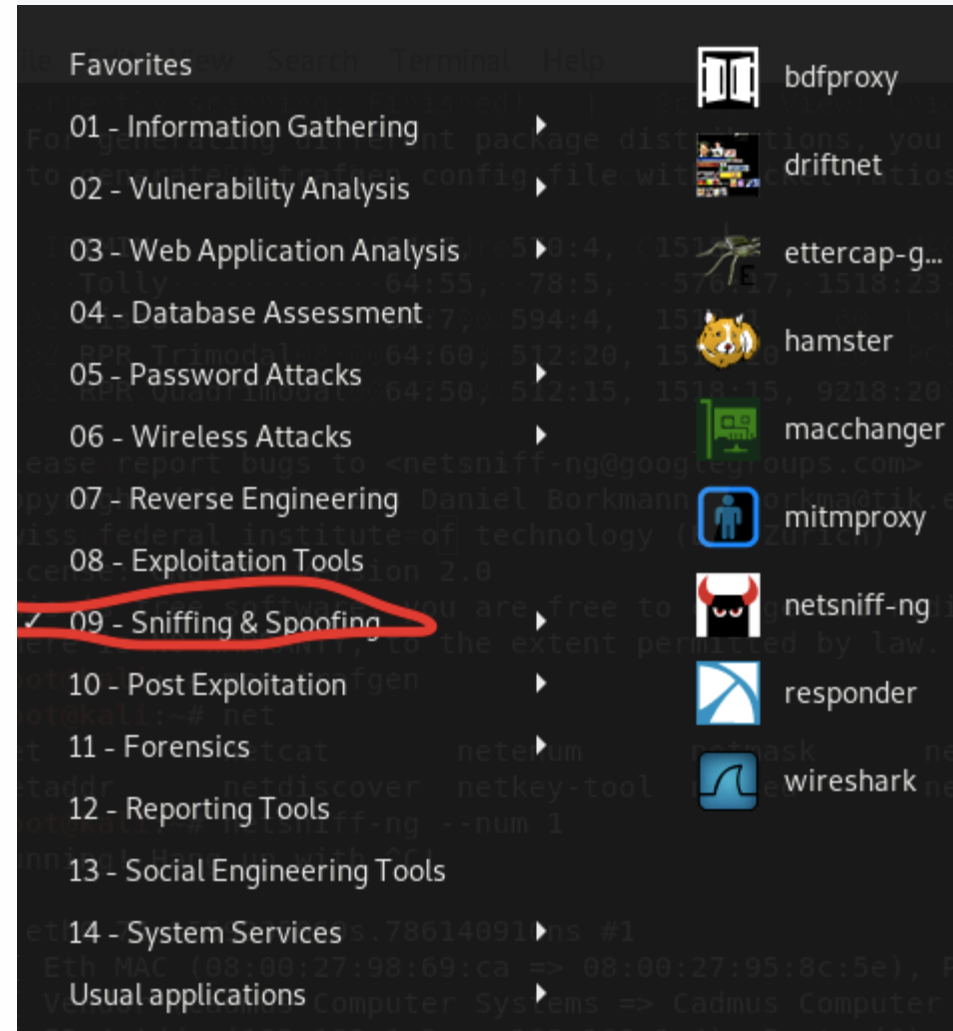
- Responder
- Ettercap

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

Информация о принятом пакете

Статистика

03

Сканирование сети

Сканирование:

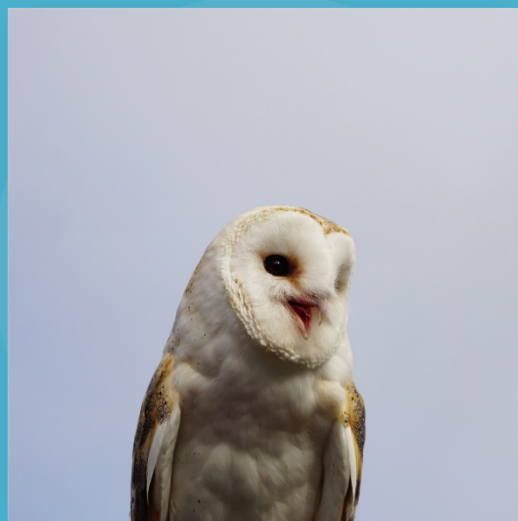
Типы сканирования:

1. Syn, Fin, Ack, Xmas, Mainmon
2. Ping scan
3. Zombie Scan



01

Сканирование



Александр Колесников

**Спасибо
за внимание!**

