ОНЛАЙН-ОБРАЗОВАНИЕ

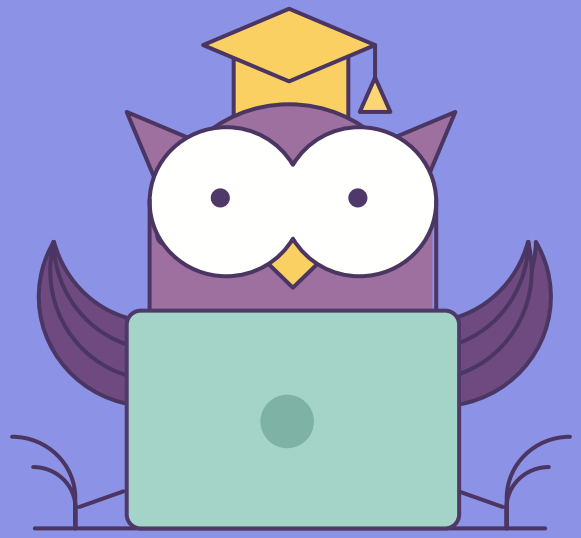
OTUS

Модификация пакетов и работа с их структурой

Основные приемы при исследовании сетевого трафика

Колесников Александр Александрович

Меня хорошо слышно && видно?



Напишите в чат, если есть проблемы!

Ставьте + если все хорошо

Содержание

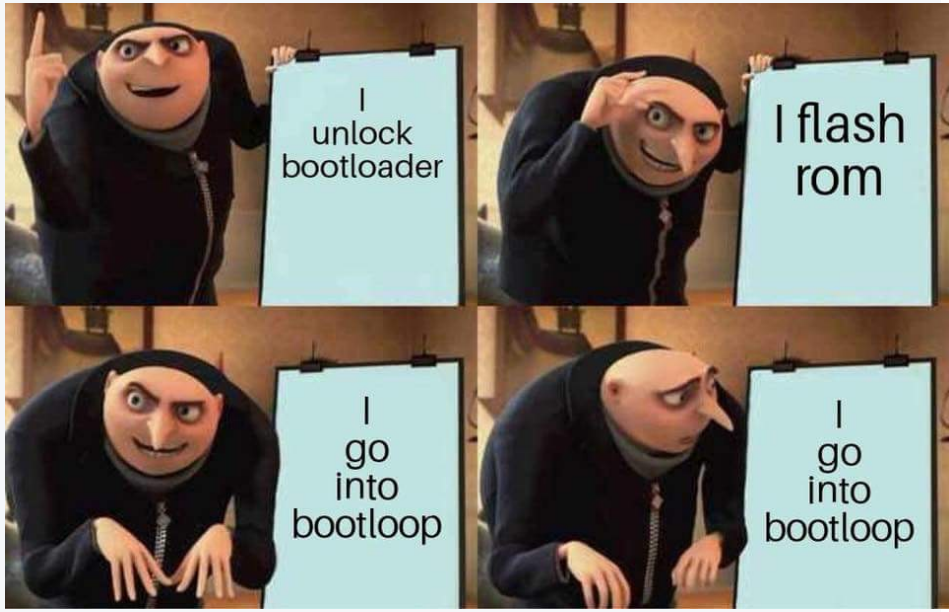
- **Исследование трафика**
  - Система фильтров WireShark
  - Практика
- **Модификация пакетов**
  - Scapy основные понятия
  - Scapy генерация пакетов
  - Практика

Цель занятия

1. Научиться модифицировать данные передаваемые по сети

2. Освоить основные подходы к фильтрации трафика

3. Закрепить полученные навыки на практике



01

Исследование трафика

Ответы на вопросы

Система фильтров

Фильтры:

1. Меню расположено над окном со списком пакетов

2. Само меню предоставляет возможность получить весь список фильтров

3. Возможно создание фильтров для быстрого доступа

Application	HTTP, SMTP, FTP, Telnet
Presentation	ASCII, MPEG, JPEG, MIDI
Session	NetBIOS, SAP, SDP, NWLink
Transport	TCP, UDP, SPX
Network	IP, ICMP, ARP, RIP, IPX
Data Link	Ethernet, Token Ring, FDDI, AppleTalk

Сложные фильтры

WireShark поддерживает сложные фильтры. Фильтры организуются в последовательность логических выражений.

```
Допустимые символы в выражениях:

Операторы сравнения: ==, !=, <, >, >=, <=
Логические операторы: or, and, xor, not


Пример фильтра: tcp.port==80 || udp.port == 80
```

02

Модификация пакетов

Описание

- Фреймворк на Python
- Имеет интерактивную оболочку
- Поддерживает более 300 протоколов
- Позволяет проводить некоторые атаки прямо из коробки

Дополнительные бонусы:

- 90% кода уже написано за программиста
- Присутствует функционал фаззера
- Может работать с любым типом сети

Application	HTTP, SMTP, FTP, Telnet
Presentation	ASCII, MPEG, JPEG, MIDI
Session	NetBIOS, SAP, SDP, NWLink
Transport	TCP, UDP, SPX
Network	IP, ICMP, ARP, RIP, IPX
Data Link	Ethernet, Token Ring, FDDI, AppleTalk

Основные команды

Команды, которые позволяют изучить набор функций и освоиться с окружением

```
help() - получение информации по объектру в скобках
ls() - список поддерживаемых протоколов
lsc() - список готовых функций
```

Создание пакета и кастомизация полей заголовка

OTUS

```
>>> ip = IP(src="192.168.56.102")
>>> ip.dst="192.168.56.101"
>>> ip.display()
###[ IP ]###
  version= 4
  ihl= None
  tos= 0x0
  len= None
  id= 1
  flags=
  frag= 0
  ttl= 64
  proto= hopopt
  chksum= None
  src= 192.168.56.102
  dst= 192.168.56.101
  \options\
```

```
>>> tcp = ip/TCP()
>>> tcp.display()
###[ IP ]###
  version= 4
  ihl= None
  tos= 0x0
  len= None
  id= 1
  flags=
  frag= 0
  ttl= 64
  proto= tcp
  chksum= None
  src= 192.168.56.102
  dst= 192.168.56.101
  \options\
###[ TCP ]###
     sport= ftp_data
     dport= http
     seq= 0
     ack= 0
     dataofs= None
     reserved= 0
     flags= S
     window= 8192
     chksum= None
     urgptr= 0
     options= {}
```

01

Создание пакетов и отправка: TCP, UDP, ICMP, ARP

03

ARP Poison

Александр Колесников

Спасибо
за внимание!