

Модуль 3. Виртуальные защищенные каналы связи, DMZ, Wi-Fi (HW)

Лабораторная работа №2 (HW)

Шаг 13 Создайте словарь из символов алфавита aehikrrsw

Создаем словарь из заданного алфавита с помощью утилиты **crunch** и сохраняем словарь в директорию рядом с pcap-файлом

```
astepanov@kali: /mnt/shared/2 semester/Network security/Module 3/HW 2
File Actions Edit View Help Wireless Tools Help
astepanov...-configs x astepanov@...figs/files x astepanov@kali: /mnt/shared...work security/Module 3/HW 2 x

(astepanov@kali)-[~/2 semester/Network security/Module 3/HW 2]
$ crunch 9 9 -p aehikrrsw > ./wordlist.txt Protocol Length Info
Crunch will now generate approximately the following amount of data: 3628800 bytes | 37824 -> 1194 [SYN]
3 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 362880
(astepanov@kali)-[~/2 semester/Network security/Module 3/HW 2]
$ ls
dump.pcap  image.png  README.MD  README.pdf  wordlist.txt
(astepanov@kali)-[~/2 semester/Network security/Module 3/HW 2]
$ 
```

Шаг 14 Произведите атаку на полученный pcap файл при помощи сгенерированного (скачанного) словаря

Перебираем ключи с помощью утилиты **aircrack-ng**, передав параметром -w - словарь, по которому мы будем перебирать значения...

Спустя пару минут ключ найден: **wireshark**