Początki

Sniffing i wardriving – zabezpiecz się!

Konrad Witaszczyk

stopień trudności

Wiele osób korzystających z Internetu nie zdaje sobie sprawy, że oprócz takich zagrożeń, jak robaki i wirusy istnieje również sniffing (ang. sniff – węszyć). Wykorzystując tę technikę można dowiedzieć się między innymi, jakie ktoś ma hasła.

Ostatnio, w związku z szerzącą się modą na *hotspoty*, popularny stał się również *wardriving*. Jest to nic innego, jak wyszukiwanie sieci bezprzewodowych. Należy pamiętać, że nie zawsze oznacza to włamywanie się do nich. Niektórzy jednak nie poprzestają na wyszukaniu sieci i kradną dane. Dalsza część artykułu naprowadzi Cię na sposób, w jaki powinniśmy się zabezpieczyć przed takimi atakami.

Jeśli chcemy się uchronić przed jakimś zagrożeniem, to musimy je najpierw poznać. *Sniffing* odbywa się poprzez przechwytywanie pakietów sieci lokalnej (Rysunek 1). Większość osób może odbierać jedynie własne pakiety, ponieważ współcześnie sieci są oparte o switche lub routery pozwalające na przesyłanie danych tylko do komputera, do którego zostały przekazane informacje. Jedynie huby wysyłają pakiety do wszystkich użytkowników, lecz aktualnie rzadko wykorzystuje się urządzenia tego typu.

Zabezpieczenia routera da się ominąć poprzez przepełnienie tablicy ARP lub ARP Poisoning. Nie będę tutaj opisywać tych metod, ponieważ mamy inny cel – a osoby bardziej zainteresowane tym tematem znajdą pożądane informacje w Internecie (ramka *W Sieci*). *Sniffing* często wiąże się z wardrivingiem. Napastnik najpierw wyszukuje sieć bezprzewodową, a następnie łączy się z nią. Jeśli sieć jest ogólnodostępna, to nie ma żadnego problemu, ponieważ potrzebne dane zostaną pozyskane dzięki *DHCP*. Często jednak zdarza się, że sieć jest chroniona kluczem, ponieważ za dostęp trzeba zapłacić lub po prostu ktoś nie chciał przyjmować niepowołanych gości.

Szyfrowanie połączenia

Pierwszym krokiem, jaki powinniśmy zrobić w kierunku zabezpieczenia swojego komputera, jest szyfrowanie czegokolwiek, co wysyłamy do sieci. Możemy w tym celu zastosować często używany standard SSL (*Secure Socket Layer*).

Z artykułu dowiesz się

- jak bezpiecznie korzystać z Sieci,
- jak zabezpieczyć własną sieć bezprzewodową.

Co powinieneś wiedzieć

- w jaki sposób wysyłane są dane do serwerów,
- powinieneś znać podstawowe pojęcia dotyczące sieci bezprzewodowych.

GPG - komendy

- `gpg - list-keys` – lista wygenerowanych kluczy,
- `gpg - export adres@adres.com -armour -output plik _ klucza` – eksport klucza publicznego do pliku,
- `gpg - import plik _ klucza` – import klucza z pliku,
- `gpg - edit-key adres@adres.com` – weryfikacja klucza,
- `gpg - delete-keys nazwa` – usuwanie klucza,
- `gpg - output wiadomość _ zaszyfrowana -encrypt wiadomość` – szyfrowanie wiadomości,
- `gpg - decrypt wiadomość _ zaszyfrowana` – odszyfrowanie wiadomości,
- `gpg - output wiadomość _ podpisana -clearsign wiadomość` – podpisywanie wiadomości,
- `gpg - verify wiadomość _ podpisana` – weryfikacja podpisanej wiadomości.

Literatura

- *802.11 Security* – Bruce Potter, Bob Fleck; 01/2004,
- *Hack Proofing Your Network* – 10/2002,
- *TCP/IP Unleashed* – Karanjit S. Siyan, Tim Parker; 12/2002,
- *Upgrading and Repairing Networks: Field Guide* – Scott Mueller, Terry W. Ogletree; 04/2004,
- *Wireless Hacks* – Lee Barken; 11/2006.

Jednak nie jest on już dłużej rozwijany, a jego miejsce zajął TLS (*Transport Layer Security*). Doskonale nadaje się on do szyfrowania takich protokołów, jak HTTP, SMTP czy POP3. Największą różnicą między SSL a TLS jest to, iż nowsza wersja używa algorytmu HMAC, który trudniej złamać w przeciwieństwie do wcześniej stosowanego algorytmu MAC. Różni je to, że pierwszy z nich wykorzystuje *hashe* (MD5 lub SHA1), do których są dołączane klucze oraz nie posiada ograniczeń długości tekstu.

Coraz więcej banków, firm hostingowych czy nawet zwyczajnych serwisów używa SSL bądź TLS, co daje klientowi satysfakcję z ochrony danych. W celu wykorzystania tej technologii musimy dysponować przeglądarką internetową, która posiada pełną obsługę SSL 128-bit:

- Opera – SSL 2, SSL 3, TLS 1, TLS 1.1,
- Firefox – SSL 3, TLS 1,
- Internet Explorer – SSL 2, SSL 3, TLS 1.

Aktywowanie tej funkcji jest proste. Najpierw należy w ustawieniach przeglądarki włączyć szyfrowanie połączeń, a następnie przy otwieraniu strony zaakceptować certyfikat.

Komunikatory

Częstym przypadkiem ataku typu *sniffing* jest podsłuchiwanie rozmów. Niestety większość polskich użytkowników korzysta z komunikatora Gadu-Gadu, którego twórcy dopiero niedawno rozpoczęli testy wersji programu z szyfrowanym połączeniem. Jednak w tej sytuacji możemy wybrać inne rozwiązanie, a konkretnie – Jabbera (patrz *Terminologia*). Zaletami tego protokołu komunikacji są przede wszystkim bezpieczeństwo i wielofunkcyjność. Gdy zdecydujemy się na to rozwiązanie, możemy szyfrować połączenie, jeśli nam na to pozwoli serwer, a dodatkowo istnieje możliwość wykorzystywania PGP lub GPG (patrz *Terminologia*) w celu szyfrowania transmisji. Wybranie tej opcji nie wiąże się z rezygnacją z używania takich protokołów, jak Gadu-Gadu czy Tlen, ponieważ Jabber zawiera obsługę tzw. transportów, czyli przekazania użytkownikowi kontroli nad API danej sieci. Dodatkowym atutem Jabbera jest otwartość jego kodu (ang. *open source*). Dzięki temu powstało wiele ciekawych komunikatorów, które cieszą się znaczną popularnością.

Rysunek 1. *Przechwycony pakiet z odpowiedzią serwera HTTP po otworzeniu obrazka GIF*

GNU Privacy Guard

Jak wcześniej wspomniałem, GPG jest idealnym rozwiązaniem dla osób, które chcą mieć pewność, że nikt ich nie podsłuchuje. W tej części artykułu wygenerujemy swoją pierwszą parę kluczy.

Program ten jest wieloplatformowy, więc zarówno użytkownicy **nix*, jak i Windows nie będą mieć kłopotu z dostępem do niego. Obsługa aplikacji wygląda tak samo w każdym systemie. Gdy mamy zainstalowane odpowiednie oprogramowanie, wpisujemy w konsoli:

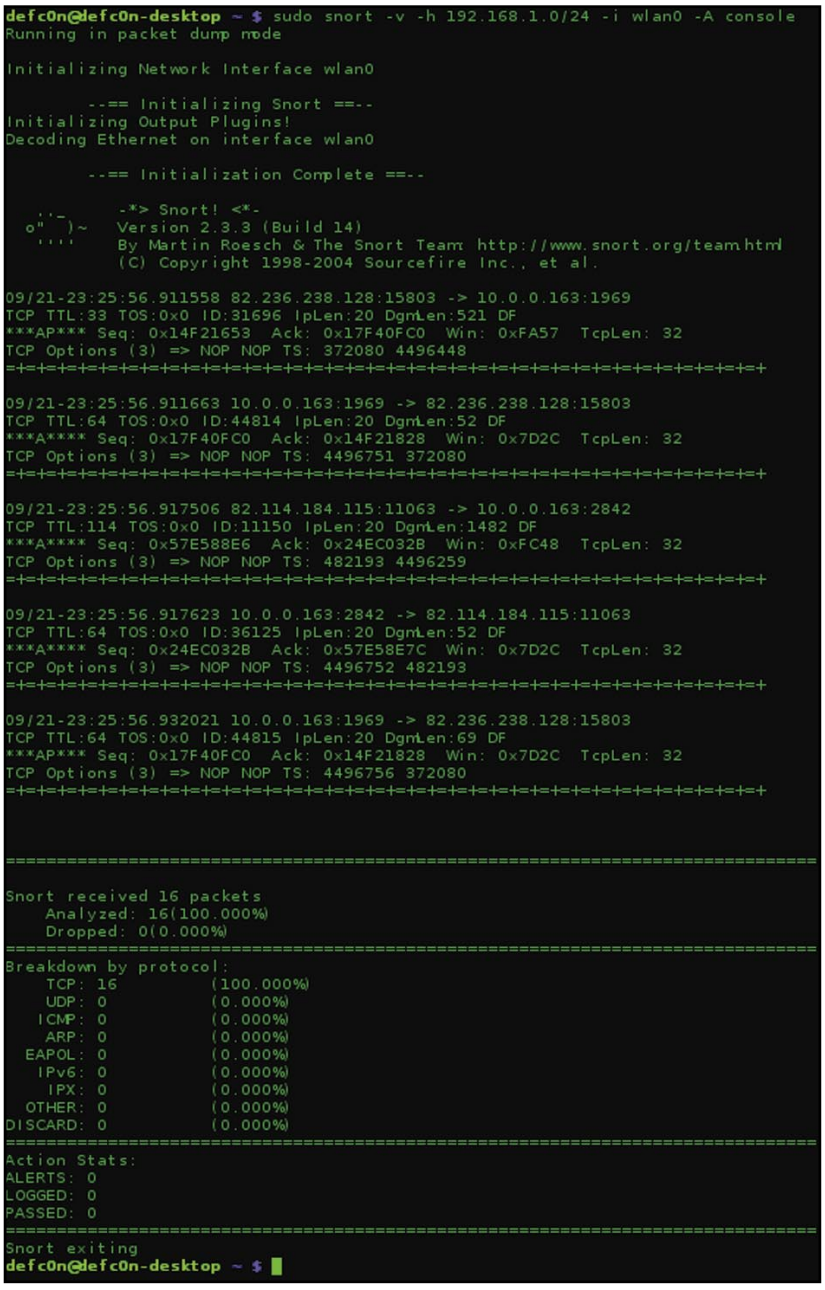
```
gpg - gen-key
```

Pojawia się numer wersji programu, trochę informacji na temat licencji i głów-

ne menu. Musimy w nim wybrać, jaki algorytm wykorzystamy. Wybierzemy pierwszą opcję (*DSA* i *Elgamal*), ponieważ dzięki niej będziemy mieć możliwość szyfrowania i podpisywania wiadomości. Następny krok to wybór długości klucza, a potem jego terminu ważności. Po tych czynnościach musimy wpisać swoje imię, nazwisko oraz e-mail. Dane nie muszą być prawdziwe, ważne, żeby osoby korzystające z klucza publicznego wiedziały, do kogo on należy. Jeśli wszystko się zgadza, akceptujemy wpisane dane oraz podajemy hasło dostępu, które powinno być odpowiednio skomplikowane, aby nikt poza nami go nie znał i nie mógł odgadnąć. Jeśli wszystko poszło dobrze, powinniśmy ujrzeć komunikat zwracający *fingerprint*. Posiadanie tego ciągu jest wymagane, by uchronić się przed atakiem *Man in the middle*. Eksport klucza do pliku wykonujemy za pomocą komendy:

```
gpg -export adres@adres.com -armour-
                              output plik
```

Teraz możemy udostępnić klucz publiczny znajomym i szyfrować swoje wiadomości. Pozostałe komendy potrzebne do korzystania z programu zostały przedstawione w ramce *GPG – komendy*.



Rysunek 2. *Wynik działania programu Snort*

W Sieci

- *http://www.gnupg.org* – GnuPG,
- *http://www.openssl.org*
- *http://tools.ietf.org/html/rfc4346* – TLS 1.1, RFC 4346,
- *http://tools.ietf.org/html/rfc1122* – warstwy komunikacji, RFC 1122.

IDS

System wykrywania włamań (ang. *Intrusion Detection System*) to pożyteczny mechanizm, który pomaga nam poprzez dostarczanie raportów o ewentualnych atakach na nasz komputer, wykrytych dzięki analizie ruchu sieciowego. Jedną ze słynniejszych aplikacji wykorzystujących tego typu mechanizm jest *Snort*, który pokazuje komunikaty w czasie rzeczywistym. Informują one nas m. in. o wysyłanych oraz odbieranych pakietach, próbach ataków typu *buffer overflow* (przepełnienie bufora), skanowaniu portów przez intruza czy próbie wykrycia wersji naszego systemu operacyjnego. Przykładowy wynik działania tego programu został przedstawiony na Rysunku 2. Dla osób, które są przyzwyczajone do okienek, został stworzony *front-end* tego programu o nazwie *IDScenter* (*http://www.engagesecurity.com/products/idscenter*). Istnieje jeszcze kilka aplikacji tego typu dla użytkowników systemu Windows, np. *KFSensor* (*http://www.keyfocus.net/kfsensor*), lecz jest on mniej popularny niż poprzednio wspomniany konkurent. Innym wartym uwagi programem tego typu jest *Kismet* (*http://www.kismetwireless.net*). Oprócz tego, iż posiada on mechanizm IDS, może wyszukiwać sieci bezprzewodowe, a także sniffować.

Bezpieczne WiFi

Przy budowie sieci bezprzewodowej musimy rozważyć wszelkie możliwości dostania się do niej przez niepowołane osoby. Wielu administratorów popełnia błąd, tworząc sieci bezprzewodowe bez szyfrowania. Inni natomiast

Terminologia

- *Adres IP* – unikatowy numer komputera w danej sieci,
- *DHCP* – technologia pozyskiwania od serwera takich danych, jak IP, DNS czy adres domyślnej bramy po rozpoznaniu MAC,
- *Fingerprint* – suma kontrolna klucza PGP/GPG, dzięki niej możemy go zweryfikować,
- *HotSpot* – punkt dostępowy bezprzewodowej sieci, przykładowo prawie w każdym McDonaldzie można zaobserwować płatny hotspot sieci Era,
- *MAC* – unikatowy adres karty sieciowej,
- *PGP/GPG* – program do szyfrowania wiadomości wykorzystujący algorytm DSA lub RSA.

O autorze

Autor jest programistą PHP w firmie zajmującej się projektowaniem stron internetowych. Dodatkowo prowadzi kilka projektów, w tym *Ruby Movie Get* (*http://movieget.org*) oraz *wyklady.net*. Kontakt z autorem: *defc0n@defc0n.or*

stosują jedynie DHCP, które polega na pozyskaniu adresu sieciowego IP poprzez odczytanie MAC, czyli unikatowego numeru interfejsu. W tym wypadku osoba atakująca może zastosować MAC *Spoofing*, czyli ustawianie identyfikatora MAC innej osoby i podszywanie się pod nią. Jeśli sieć używa klucza WEP, to – przy odpowiedniej ilości przechwyconych pakietów – można go często odszyfrować w przeciągu minuty. Do tego służy program *Aircrack*–ng – wyszukiwarka sieci, *sniffer* i łamacz WEP oraz WPA-PSK (prostsza wersja WPA). Najlepszym sposobem przeciwdziałania jest zaszyfrowanie sieci standardem WPA (wersja *Enterprise*), który zaleca Wi-Fi Alliance. Został on stworzony jako następca WEP, który stał się mało bezpieczny. Każda osoba powinna mieć swój oddzielny klucz. Można go wygenerować za pośrednictwem strony *speedguide.net*, która zawiera generator z możliwością wyboru różnej długości klucza. Warto taką czynność powtarzać co jakiś czas, np. raz w miesiącu. Hasło powinno zawierać znaki specjalne i być długie, trudne do złamania. Dzięki temu istnieje mniejsza szansa na złamanie hasła metodą *brute–force*, czyli poprzez sprawdzenie wszystkich kombinacji, np:

```
aa; ab; ac (...) ba; bb; bc (...)
```

Niestety, nie we wszystkich urządzeniach jest dostępna obsługa WPA, jeżeli się jednak pojawiła, to bez zastanowienia należy ją włączyć.

Dodatkowym zabezpieczeniem może być ukrycie SSID, czyli identyfikatora sieci. Wydaje się to być dobrym wyjściem, choć nie do końca. Osoba atakująca ma możliwość stworzenia sieci z widocznym SSID o takiej samej nazwie, która będzie na tym samym kanale, co prawdziwa. Dzięki temu może przechwycić pakiety i odczytać poufne informacje.

Można również włączyć serwer DHCP z listą dostępową zawierającą dopuszczalne wartości MAC, która ułatwi proces uwierzytelnienia użytkowników. Jednak nie jest on potrzebny przy małej ilości osób korzystających z sieci. Każdy może sam wpisać potrzebne dane w konfiguracji karty sieciowej.

Podsumowanie

Przy korzystaniu z Internetu musimy być gotowi na wszelkiego rodzaju niebezpieczeństwa. Najlepszą obroną przed nimi jest logiczne myślenie i ostrożność w działaniu. Zabezpieczenie się przed zagrożeniami może wydawać się czasochłonne, ale podjęty trud zapewni nam spokój i ochroni naszą prywatność. Administratorzy muszą pamiętać, że brak dostatecznych zabezpieczeń stanowi pośrednio przyzwolenie na włamanie się do sieci. Poprawiając bezpieczeństwo zwiększają zaufanie do swoich usług. ●