802.11. Bezpieczeństwo

Autorzy: Bruce Potter, Bob Fleck
Tłumaczenie: Marcin Jędrysiak
ISBN: 83-7361-412-5
Tytuł oryginału: 802.11 Security
Format: B5, stron: 215

Sieci bezprzewodowe otwierają nowe możliwości dla wszystkich użytkowników i odgrywają coraz większą rolę w naszym życiu. Najpopularniejszy protokół sieci WLAN – 802.11 – zmienia całkowicie sposób postrzegania tradycyjnych sieci lokalnych.

Sieci bezprzewodowe stanowią poważne wyzwanie zarówno dla użytkowników, jak i administratorów. Brak zabezpieczeń fizycznych, dostęp do darmowych narzędzi, które można wykorzystać do przeprowadzenia ataku, a także możliwość monitorowania ruchu sieciowego bez ryzyka wykrycia przez administratora sprawiają, że sieci bezprzewodowe stanowią łatwy cel ataku dla hakerów. Oznacza to konieczność dokładnego zabezpieczenia każdego elementu sieci w celu zapewnienia ochrony danych.

W niniejszej książce znajdują się podstawowe informacje na temat bezpieczeństwa sieci bezprzewodowych. Poznasz sposób działania sieci w standardzie 802.11 oraz ich słabe punkty. Bardzo ważną kwestią jest zrozumienie typowych metod włamań oraz najważniejszych zagrożeń związanych z wdrażaniem sieci bezprzewodowych.

Książka „802.11. Bezpieczeństwo" zawiera praktyczne rozwiązania dla wszystkich podstawowych komponentów sieci bezprzewodowych. Książka prezentuje też najlepsze aplikacje do zabezpieczania różnych systemów operacyjnych, omówiono użytkowanie sieci bezprzewodowych pod kontrolą Linuksa, FreeBSD, Mac OS X i Windows

W książce omawiane są również bardziej zaawansowane tematy, takie jak:

- zabezpieczanie punktów dostępowych,
- bezpieczeństwo bramy,
- konfigurowanie zabezpieczeń dla stacji roboczych Linux, OpenBSD, FreeBSD, Mac OS X i Windows,
- monitorowanie SNMP,
- ataki DoS i próby ataków socjotechnicznych,
- konfiguracja sieci VPN i protokołu 802.1x służącego do uwierzytelniania i autoryzacji użytkowników.

Książka „802.11. Bezpieczeństwo" jest przeznaczona dla wszystkich osób zajmujących się wdrażaniem sieci bezprzewodowych. Prezentuje teorię oraz praktyczne przykłady pozwalające zabezpieczyć zarówno sieć, jak i cenne dane.

Wydawnictwo Helion
ul. Chopina 6
44-100 Gliwice
tel. (32)230-98-63
e-mail: helion@helion.pl

Spis treści

5

Zabezpieczanie systemu Linux

Komputery pracujące w sieci bezprzewodowej są narażone na ataki wszystkich znajdujących się w pobliżu użytkowników. Dzieje się tak, gdyż w przeciwieństwie do sieci przewodowych nie istnieją żadne fizyczne ograniczenia dostępu, co znacznie zwiększa zagrożenie hosta. Linux jest potężnym i złożonym systemem operacyjnym. Prawidłowa konfiguracja tego systemu pozwoli zabezpieczyć komputer przed wieloma atakami hakerów. Należy jednak pamiętać, że źle skonfigurowany system linuksowy może stać się potężną bronią w ręku włamywacza.

Konfiguracja klienta linuksowego

Obsługa urządzeń bezprzewodowych w Linuksie znacznie się poprawiła w ciągu ostatnich kilku lat. Jeszcze do niedawna FreeBSD był zalecanym system dla sieci WLAN, ale zmiany dokonane przez programistów sprawiły, że Linux stał się świetnym narzędziem do obsługi sieci 802.11. Linux pozwala na użycie wielu typowych kart 802.11b, a większość producentów urządzeń 802.11a i 802.11g projektuje sterowniki dla tego systemu równolegle do sterowników dla Windows. Inni producenci dostarczają zmodyfikowane wersje Linuksa z wbudowaną obsługą sieci bezprzewodowych.

Jeżeli nie wspomniano inaczej, wszystkie przykłady przedstawione w tym rozdziale odnoszą się do systemu RedHat Linux 7.2 z jądrem 2.4.18. Oczywiście możliwe jest użycie tych przykładów w innych dystrybucjach Linuksa, ale zwykle wymaga to dokonania małych zmian w skryptach lub położeniu plików. Więcej informacji na temat dystrybucji RedHat można znaleźć pod adresem *http://www.redhat.com*, natomiast informacje o jądrze 2.4.18 umieszczono pod adresem *http://www.kernel.org*.

Konfiguracja jądra

Aby możliwe było bezpieczne korzystanie z sieci bezprzewodowej, należy zapewnić prawidłową konfigurację hosta. Podstawą bezpieczeństwa każdego komputera jest stabilna i dobrze zaplanowana konfiguracja jądra. Wprowadzane zabezpieczenia jądra muszą być zgodne z zasadą najmniejszego przywileju. Zasada ta mówi, że użytkownik lub system powinny otrzymać tylko te przywileje i uprawnienia, które są niezbędne do wykonywania określonych zadań. Oznacza to konieczność usunięcia z jądra wszystkich niepotrzebnych opcji konfiguracji; na przykład, jeżeli w komputerze nie ma żadnych urządzeń SCSI, należy usunąć z konfiguracji jądra wszystkie sterowniki SCSI.

Konfiguracja jądra z obsługą sieci bezprzewodowych

Zanim możliwe będzie użycie bezprzewodowych kart sieciowych, należy skompilować jądro z odpowiednimi opcjami. Proces kompilacji jądra Linuksa wykracza jednak poza zakres niniejszej książki. Więcej informacji na ten temat można znaleźć w pliku */usr/src/linux-2.4/README* w komputerze z Linuksem lub pod adresem *http://www.tldp.org/HOWTO/Kernel-HOWTO.html*. Jądro należy skonfigurować i skompilować z jak najmniejszym zestawem opcji. Po uzyskaniu okrojonego jądra można wykonać procedury przedstawione w dalszej części tego rozdziału.

Istnieje wiele sposobów konfiguracji jądra. Niezależnie od tego, czy używane są metody *make menuconfig*, *make xconfig* czy też po prostu *make config*, wszystkie zmiany zostają zapisane w pliku konfiguracyjnym, który znajduje się zwykle w */usr/src/linux-2.4/configs/kernel-[ver].config*. Opisane w niniejszym rozdziale opcje stanowią dyrektywy umieszczone w tym pliku. Sposób wprowadzania tych opcji do pliku jest zależny od Czytelnika; możliwa jest zarówno bezpośrednia edycja pliku konfiguracyjnego, jak i użycie skryptów make *_config.

Bezprzewodowe karty sieciowe są zwykle montowane w wewnętrznym złączu PCI lub w gnieździe PCMCIA (karta PC). Pierwszym krokiem będzie wybranie typu interfejsu. Obsługa złączy PCI została już prawdopodobnie skompilowana w jądrze, a włączenie odpowiednich funkcji odbywa się za pomocą następującego polecenia:

```
CONFIG_PCI=y
```

Jądro Linuksa zapewnia obsługę bezprzewodowych kart PCI wielu producentów, włącznie z urządzeniami firm Lucent, Cisco i Linksys. W dokumentacji jądra można znaleźć informacje dotyczące sposobu włączenia obsługi konkretnego modelu karty.

Karty PCMCIA mogą być obsługiwane na wiele sposobów. W przypadku jądra 2.4 najprostszym sposobem będzie zainstalowanie pakietu do obsługi bezprzewodowych kart PC o nazwie *pcmcia-cs*, który jest dostępny pod adresem *http://pcmcia-cs.sourceforge.net/*. Aby możliwe było użycie tego pakietu, należy włączyć obsługę ładowanych modułów i wyłączyć macierzystą obsługę kart PC:

```
CONFIG_MODULES=y
CONFIG_CARDBUS=y
```

Kolejnym krokiem jest włączenie obsługi sieci bezprzewodowych (funkcja ta jest znana również jako „non-hamradio"):

```
CONFIG_NET_RADIO=y
```

W tym momencie należy skonfigurować i zainstalować jądro. Za obsługę wszystkich niezbędnych funkcji będzie odpowiedzialny pakiet *pcmcia-cs*.

Większość dystrybucji Linuksa zawiera wstępnie skompilowane moduły *pcmcia-cs*. Ich użycie nie powinno sprawiać żadnych większych problemów. Jeżeli jednak konieczne jest samodzielne skompilowanie pakietu *pcmcia-cs*, można wykonać poniższą procedurę.

Ze strony *http://pcmcia-cs.sourceforge.net/* należy pobrać kod źródłowy pakietu. Uzyskany plik należy rozpakować w katalogu, który zawiera katalog główny kodu źródłowego Linuksa (zwykle */usr/src*). Przejście do tego katalogu i wpisanie polecenia *make config* spowoduje rozpoczęcie kompilacji, podczas której wyświetlane będą następujące pytania:

Alternate target install category?

Możliwe jest podanie alternatywnego miejsca, w którym znajduje się kod źródłowy Linuksa. Domyślnie jest to katalog */usr/src/linux*.

Build "trusting" versions of card utilites?

Zwykle narzędzia tworzone w tym pakiecie muszą być uruchamiane przez użytkownika root, który może dokonać zmian w konfiguracji karty. Wybranie tej opcji pozwala na modyfikację konfiguracji przez dowolnego użytkownika. Należy się jednak zastanowić, czy będzie to bezpieczne.

Include 32-bit (CardBus card support)?

Jeżeli posiadane urządzenie pracuje w standardzie CardBus, konieczne jest włączenie tej funkcji. Jej użycie nie powinno jednak sprawiać żadnych problemów nawet w przypadku, gdy używana karta nie jest typu CardBus.

Include PnP BIOS resource checking?

Dzięki kontroli zasobów BIOS-u PnP, jaka jest wykonywana przez pakiet *pcmcia-cs*, możliwe jest uniknięcie konfliktów zasobów. Opcja ta może jednak spowodować pewne problemy w przypadku niektórych komputerów. Decyzję o jej włączeniu należy więc podjąć w zależności od posiadanego sprzętu.

Module install directory?

W razie potrzeby możliwe jest podanie alternatywnego katalogu dla modułu.

Po udzieleniu odpowiedzi na wszystkie pytania należy wydać polecenia *make all* i *make install*. Przejrzenie pliku */etc/pcmcia* pozwoli ustalić, czy konieczne jest dokonanie

dodatkowych zmian dla posiadanego urządzenia. Ostatnim krokiem będzie zrestartowanie komputera i sprawdzenie, czy karta jest rozpoznawana przez hosta.

Konfiguracja zabezpieczeń jądra

Jeżeli urządzenia bezprzewodowe działają poprawnie, należy dodać do jądra wymagane opcje zabezpieczeń, które zostaną wykorzystane przez inne narzędzia klienta.

Firewall stanowi podstawową linię obrony przeciwko atakom sieciowym. Odgrywa to szczególną rolę w przypadku sieci bezprzewodowych. Systemy klienckie korzystające z tego samego punktu dostępowego nie mają zwykle żadnego mechanizmu kontroli dostępu na poziomie sieci, który zapobiegałby ich komunikacji. Oznacza to, że zabezpieczenia przeciwko atakom złośliwych użytkowników bezprzewodowych należy włączyć bezpośrednio w systemie klienta.

Linux zapewnia elastyczny mechanizm firewalla o nazwie Netfilter. Jest on zaimplementowany w jądrze i kontrolowany za pomocą programu o nazwie *iptables*. Wcześniejsze wersje Linuksa (2.2 i starsze) korzystały z firewalla IPFW, który był zarządzany za pomocą programów *ipfwadmin* i *ipchains*. Wszystkie te narzędzia zostały jednak usunięte z nowszych wersji systemu. W tym rozdziale skoncentrujemy się wyłącznie na opisie firewalla Netfilter i programu *iptables*, które wspólnie zapewniają zabezpieczenia klienta. Informacje dotyczące bardziej skomplikowanych zastosowań firewalla Netfilter przedstawiono w rozdziale 11., który jest poświęcony konfiguracji bramy z systemem Linux. Włączenie firewalla odbywa się za pomocą następującej opcji:

```
CONFIG_NETFILTER=y
```

Firewall Netfilter zapewnia wiele opcji konfiguracji. Niektóre z nich są wymagane, aczkolwiek większość z nich można dodać w zależności od potrzeb:

CONFIG_IP_NF_IPTABLES

Opcja ta zapewnia podstawową strukturę jądra, jaka jest wykorzystywana przez program *iptables* do zarządzania firewallem. Użycie tej opcji jest wymagane.

CONFIG_IP_NF_FILTER

Dzięki tej opcji firewall może filtrować wszystkie pakiety, które host próbuje wysłać lub odebrać. Użycie tej opcji jest wymagane.

CONFIG_IP_NF_MATCH_MAC

Użycie tej opcji sprawia, że firewall dopasowuje pakiety na podstawie źródłowego i docelowego adresu MAC. Funkcja ta będzie bardzo przydatna w sieci bezprzewodowej, gdzie bardzo łatwe jest podszywanie się pod inne adresy IP.

CONFIG_IP_NF_MATCH_STATE

Parametr ten przekształca Netfilter w firewall z kontrolą stanu (ang. *stateful firewall*), który może śledzić wszystkie aktywne i poprawne połączenia. Po przesłaniu

i odebraniu pakietu tworzącego transakcję dwukierunkową firewall dodaje tę sesję do tablicy stanu. Pozwala to na szybsze przetwarzanie pakietów dla ustanowionej sesji, a także zapobiega przekazywaniu fałszywych pakietów (stanowi to poważny problem w przypadku firewalli filtrujących pakiety, takich jak IPFW). Użycie tej opcji nie jest wymagane, ale w większości przypadków zalecane. Wszystkie przedstawione w tym rozdziale przykłady wykorzystują funkcje firewalla tego typu.

CONFIG_IP_NF_CONNTRACK

Opcja ta pozwala na śledzenie połączeń przez firewall. W połączeniu z funkcjami kontroli stanu pozwala to programowi Netfilter na bardziej efektywne śledzenie ustanowionych połączeń.

CONFIG_IP_NF_FTP

Ten moduł dodaje funkcje logiczne wymagane do śledzenia połączeń FTP. Firewalle od zawsze miały problemy z takimi połączeniami, ponieważ wykorzystują oddzielne kanały poleceń i danych. Dzięki temu modułowi możliwe jest śledzenie trybów aktywnego i pasywnego FTP.

CONFIG_IP_NF_IRC

Moduł ten przypomina przedstawiony powyżej moduł do obsługi połączeń FTP i zapewnia funkcje logiczne wysokiego poziomu do prawidłowego śledzenia połączeń IRC.

CONFIG_IP_NF_TARGET_LOG

Dzięki tej opcji firewall protokołuje wszystkie pakiety w dziennikach syslog w celu ich późniejszego zbadania. Pozwala to uzyskać ogromną ilość informacji, które mogą być wykorzystane do szczegółowej analizy przeprowadzanych prób włamania.

Dzięki użyciu powyższych opcji możliwe jest uzyskanie elastycznego firewalla klienta. Przykład konfiguracji firewalla Netfilter przedstawiono w podrozdziale „Konfiguracja firewalla" w dalszej części tego rozdziału. Poniżej przedstawiono dodatkowe parametry firewalla.

CONFIG_SYN_COOKIES

Opcja ta umożliwia użycie techniki migracji SYN flood o nazwie SYN Cookies. Powoduje to utworzenie wyzwania kryptograficznego w pakiecie ACK w celu zweryfikowania, czy pakiet SYN stanowi część poprawnej sesji. Użycie tej opcji w hoście powoduje jednak znaczne obciążenie zasobów. Technika SYN Cookies jest domyślnie wyłączona, nawet po jej włączeniu w jądrze. Aby ją wywołać, należy wprowadzić następujące polecenie:

```
echo 1 >/proc/sys/net/ipv4/tcp_syncookies
```

Użycie tej opcji nie jest wymagane w komputerze, który służy wyłącznie jako stacja robocza i nie jest wykorzystywany jako serwer. Jeżeli jednak uruchomiono jakiekolwiek usługi sieciowe, należy włączyć obsługę SYN Cookies.

CONFIG_PACKET=y

Ta opcja konfiguracji umożliwia przechwytywanie pakietów pierwotnych z interfejsu. W pewnym sensie jest więc to odpowiednik opcji BPF w jądrze FreeBSD. Użytkownik *root* może użyć tej funkcji do nasłuchu ramek skierowanych do innych komputerów sieci. Włączenie tej opcji jest wymagane do prawidłowego działania niektórych programów narzędziowych, takich jak *tcpdump* i *arpwatch*.

Konfiguracja startowa

Bezprzewodowe karty sieciowe należy zainicjalizować podczas startu systemu, podając właściwe informacje. Wszystkie te dane są zapisywane w pliku */etc/pcmcia/wireless.opt*. Plik dołączony do danej dystrybucji systemu może zawierać wpisy dla różnych modeli kart. Choć możliwość wybrania odmiennych ustawień sieciowych dla różnych kart może być przydatna, zwykle nie jest potrzebna. Większość użytkowników woli stosować identyczne ustawienia sieciowe niezależnie od używanego urządzenia. Poniżej przedstawiono szablon dla informacji w pliku *wireless.opt*:

```
case "$ADDRESS" in
*,*,*,*)
    # INFO - nazwa opisujaca to polaczenie
    INFO="Siec bezprzewodowa"
    ESSID - Nazwa sieci ESSID, z ktora nastapi polaczenie
    ESSID="Przyklad"
    # MODE - tryb dzialania. Typowe wartosci to Managed dla powiazan
    # z punktem dostepowym i ad hoc dla polaczen z siecia iBSS.
    MODE="Managed"
    # RATE - szybkosc danych polaczenia. Wartosc auto pozwala karcie
    # na automatyczne wybranie szybkosci w zaleznosci od warunkow.
    RATE="auto"
    # KEY - klucz WEP. Klucze szesnastkowe sa podawane w postaci
    # 0123-4567-89. Klucze ASCII sa poprzedzone litera s,
    # na przyklad s:secrt
    KEY="s:secrt"
    ;;
esac
```

Domyślny plik *wireless.opt* zawiera również dodatkowe opcje, które można skonfigurować w zależności od potrzeb. Wszystkie wartości ustawione w tym pliku są przekazywane do programu *iwconfig* w celu konfiguracji karty. Więcej informacji na temat tego narzędzia można znaleźć w podrozdziale „Konfiguracja karty”.

Domyślne pliki startowe powodują automatyczne włączenie interfejsu i ustawienie niezbędnych opcji sieciowych. Interfejs jest zwykle skonfigurowany w taki sposób, aby adres IP był przydzielany przez DHCP. Aby skonfigurować statyczny adres IP, należy dokonać edycji pliku */etc/sysconfig/network-scripts/ifcfg-[urządzenie]*. Poniżej przedstawiono parametry urządzenia `ifcfg-eth0` dla statycznego adresu IP:

```
DEVICE=eth0
IPADDR=192.168.0.100
NETMASK=255.255.255.0
NETWORK=192.168.0.0
```

```
BROADCAST=192.168.0.255
GATEWAY=192.168.0.1
ONBOOT=yes
```

Jeśli klient wymaga DHCP do uzyskania adresu IP, należy użyć następującego zestawu opcji:

```
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=DHCP
```

Konfiguracja karty sieciowej

Konfigurowanie bezprzewodowej karty sieciowej w systemie Linux to proces składający się z dwóch etapów. Najpierw należy ustawić parametry połączenia bezprzewodowego za pomocą narzędzia *iwconfig*. Kiedy karta utworzy poprawne powiązanie z punktem dostępowym, należy użyć programu *ifconfig* do skonfigurowania informacji odnoszących się do IP.

Poniżej przedstawiono najważniejsze parametry konfiguracji programu *iwconfig*:

interfejs

Jest to nazwa interfejsu, który należy skonfigurować. Zwykle jest tu podawana wartość typu *eth0*. Jeżeli do programu *iwconfig* przekazano tylko nazwę interfejsu bez żadnych parametrów konfiguracji, zostanie wyświetlona bieżąca konfiguracja interfejsu bezprzewodowego.

essid `identyfikator_essid`

Jest to identyfikator sieci ESSID (ang. *Extended Service Set ID*), z którą należy się połączyć. Wartość ta musi być zgodna z wartością ustawioną w punkcie dostępowym. Podanie wartości `any` sprawi, że klient będzie się łączył z punktem dostępowym o najwyższej mocy sygnału. Użycie takiej opcji nie jest zalecane, ponieważ znajdujący się w pobliżu haker może zmusić stację roboczą do połączenia z wrogim punktem dostępowym.

nwid `identyfikator_nwid`

Jest to identyfikator sieci; jest to mechanizm używany do identyfikacji określonych punktów dostępowych w sieci SSID. Wiele punktów dostępowych może mieć identyczny identyfikator SSID, zapewniając w ten sposób usługi dla tej samej sieci. Z kolei identyfikatory *nwid* poszczególnych punktów dostępowych mogą się różnić, dzięki czemu użytkownicy mogą wybrać urządzenie, z którym chcą się połączyć. Podanie wartości `off` spowoduje wyłączenie sprawdzania *nwid*. Użycie tego parametru nie jest wymagane.

channel `kanał`

Jest to kanał służący do komunikacji z punktem dostępowym. Specyfikacja PHY w standardzie 802.11b określa kanały w paśmie 2,4 GHz, jakie mogą być używane przez urządzenia radiowe. W Stanach Zjednoczonych możliwe jest użycie 11 kanałów, podczas gdy w Europie aż 14 kanałów. Aby komunikacja pomiędzy klientem a punktem dostępowym była możliwa, konieczne jest określenie tego samego kanału dla obu urządzeń.

mode `tryb`

Parametr ten określa typ sieci, z jaką będzie się łączył klient. Dostępne wartości obejmują `managed` dla powiązań z punktami dostępowymi oraz `ad hoc` dla powiązań tworzonych w trybie IBSS.

ap `adres_mac`

Jest to adres MAC wybranego punktu dostępowego. Poprzez określenie tego parametru klient będzie łączył się tylko z jednym punktem dostępowym. Pozwoli to znacznie zminimalizować ryzyko związane z obecnością wrogich punktów dostępowych, które próbują podszywać się pod identyfikatory SSID i NWID. Wartość tego parametru jest podawana w formie `00:08:20:4e:5e:1f`. Użycie parametru `ap` nie jest wymagane.

key `[klucz_wep] [indeks] [tryb]`

Ten znacznik służy do ustawiania wszystkich opcji konfiguracji WEP. Klucz WEP można podawać zarówno szesnastkowo (na przykład `0123-4567-89`), jak i w postaci łańcucha ASCII poprzedzonego znakami `s:` (na przykład `s:secrt`). Dzięki indeksom w zakresie od 0 do 3 możliwe jest wprowadzenie i użycie czterech kluczy WEP. Ostatnia opcja pozwala na ustawienia trybu powiązania, który decyduje o sposobie obsługi przez klienta pakietów WEP i innych. Wartości `on` i `off` wyłączają zabezpieczenia WEP, wartość `open` pozwala karcie sieciowej na zestawianie połączeń w zależności od obecności punktów dostępowych, natomiast wartość `restricted` wymusza tworzenie powiązań tylko z zabezpieczeniami WEP.

Nie jest to pełna lista znaczników, jakie można przekazać do programu *iwconfig*. Pozostałe opcje konfigurują ustawienia oszczędzania energii, czułość oraz metody identyfikacji klienta. Aby uzyskać informacje o wszystkich dostępnych parametrach, należy wpisać polecenie *man iwconfig*.

Aby zestawić połączenie z zamkniętą siecią Ethernet z kluczem WEP *secrt*, należy wprowadzić poniższe polecenie, które pozwoli skonfigurować to powiązanie:

```
iwconfig eth0 essid Przyklad key s:secrt restricted
```

Program *iwconfig* może być także użyty do zbadania stanu bezprzewodowej karty sieciowej. W takim przypadku jako jedyny parametr należy przekazać nazwę żądanego interfejsu:

```
[root@mo root]# iwconfig eth0
eth0      IEEE 802.11-DS  ESSID:"Przyklad"  Nickname:"Prism 1"
          Mode:Managed  Frequency:2.412GHz  Access Point: 00:02:2D:04:3D:5D
          Bit Rate:2Mb/s   Tx-Power=15 dBm   Sensitivity:1/3
          RTS thr:off   Fragment thr:off
          Encryption key:3433-6435-64
          Power Management:off
          Link Quality:92/92  Signal level:-11 dBm  Noise level:-102 dBm
          Rx invalid nwid:0  invalid crypt:0  invalid misc:0
```

Program *iwconfig* wyświetla klucz WEP, ponieważ został uruchomiony przez użytkownika root. Klucz szyfrowania nie będzie dostępny, jeżeli program zostanie wywołany przez użytkownika z niższymi uprawnieniami.

Po skonfigurowaniu informacji dotyczących sieci bezprzewodowej należy w normalny sposób wprowadzić informacje o ustawieniach IP. Służy do tego narzędzie *ifconfig*. W systemie FreeBSD możliwe było skonfigurowanie wszystkich parametrów sieci i ustawień IP za pomocą pojedynczego programu. Linux wymaga jednak w tym samym celu użycia dwóch oddzielnych narzędzi.

Programy narzędziowe dla kart sieciowych

W Linuksie dostępnych jest wiele poleceń z rodziny *iw*, które mogą być przydatne w konfiguracji bezprzewodowej karty sieciowej:

iwgetid `interfejs`

To polecenie zwraca identyfikator SSID punktu dostępowego, z którym powiązany jest klient.

iwlist [`interfejs] [freq | ap | rate | key | power | txpower | retry]`

To polecenie zwraca różne statystyki interfejsu bezprzewodowego, dzięki którym można ustalić możliwości karty; na przykład polecenie `iwlist key` wyświetli listę dostępnych długości klucza oraz istniejące klucze, jakie zapisano na karcie. Z kolei polecenie `iwlist rate` wyświetla informacje o wszystkich szybkościach, z jakimi karta może przesyłać dane.

iwspy `interfejs [+] IPADDR | HWADDR […]`

Polecenie `iwspy` zapewnia mechanizm pozwalający na śledzenie jakości połączenia pomiędzy dwoma węzłami sieci bezprzewodowej. Najpierw należy podać adres IP lub MAC, który będzie śledzony (na przykład `iwspy 192.168.0.1`). Dodanie znaku + do listy adresów spowoduje ich dodanie na końcu istniejącego zestawu śledzonych adresów. Od tej chwili możliwe jest sprawdzenie stanu wybranego połączenia poprzez przekazanie nazwy interfejsu do polecenia *iwspy*, na przykład:

```
[root@mo root]# iwspy eth0
eth0      Statistics collected:
    00:60:1D:20:E0:00 : Quality:91/92  Signal level:-11 dBm  Noise level:-102 dBm
(updated)
```

iwpriv `interfejs prywatne_polecenie [prywatne_parametry]`

To polecenie powoduje ustawienie parametrów sterownika, które nie są dostępne poprzez standardowy zestaw poleceń *iwconfig*. Za pomocą polecenia *iwpriv* możliwe jest, na przykład, włączenie funkcji roamingu, jakie istnieją w pakiecie `wavelan_cs`.

Można również zbadać stan dowolnego interfejsu bezprzewodowego poprzez system plików */proc*:

```
[root@mo root]# cat /proc/net/wireless
Inter-| sta-|   Quality        |   Discarded packets               |\
Missed
 face | tus | link level noise |  nwid  crypt   frag  retry   misc|\ beacon
  eth0: 0000   92.  245.  154.       0      0      0      0      0 \      0
```

Ochrona systemu operacyjnego

Poprawnie skonfigurowane jądro to tylko część rozwiązania umożliwiającego bezpieczne korzystanie z sieci bezprzewodowej. Jest to wrogie środowisko pracy dla stacji roboczej, gdyż każda znajdująca się w pobliżu osoba może przeprowadzić atak przeciwko niej. Oznacza to, że nie można opierać się tylko na zabezpieczeniach zapewnianych przez sieć, ale trzeba zastosować również techniki chroniące stację roboczą przed wszystkimi wrogimi czynnościami, jakie są przeprowadzane przeciwko niej.

Konfiguracja firewalla

Konfiguracja firewalla dla klienta bezprzewodowego jest relatywnie prosta. Na większości stacji roboczych nie są uruchamiane żadne usługi sieciowe, takie jak serwery pocztowe i WWW. Wszystkie nowe połączenia powinny więc wychodzić od klienta, a przychodzące żądania połączenia nie powinny być obsługiwane. Jeżeli jednak na stacji roboczej uruchomiono jakieś usługi sieciowe, należy zmodyfikować odpowiednio konfigurację firewalla.

Firewall Netfilter, jaki stanowi część systemu Linux 2.4, jest zarządzany poprzez program *iptables*. Netfilter wykorzystuje do przetwarzania wszystkich pakietów zestaw reguł firewalla nazywanych *łańcuchami* (ang. *chains*). Dostępne są trzy różne łańcuchy:

INPUT

Pakiety przeznaczone dla danego hosta są obsługiwane przez łańcuch *INPUT*. Jeżeli w hoście uruchomiono, na przykład, serwer WWW, wszystkie pakiety przeznaczone dla portu 80 publicznego adresu IP hosta będą przetwarzane przez łańcuch *INPUT*.

OUTPUT

Łańcuch OUTPUT przetwarza wszystkie pakiety wygenerowane przez danego hosta dla innego hosta. Żądanie strony internetowej wysłane ze stacji roboczej do zdalnego serwera WWW zostanie obsłużone właśnie przez łańcuch wyjściowych hosta.

FORWARD

Łańcuch FORWARD przetwarza pakiety, które pochodzą z nielokalnego hosta i są skierowane do innego nielokalnego hosta w sieci. Jest to typowe działanie firewalla, który chroni całą sieć lokalną — ruch sieciowy przechodzi przez danego hosta, choć nie jest przeznaczony dla komputera, w którym uruchomiono firewall.

Aby możliwe było zarządzanie firewallem, należy utworzyć skrypt powłoki, który będzie wywoływał właściwe polecenia *iptables* w celu zaimplementowania żądanych reguł. Poniżej przedstawiono prosty przykład konfiguracji firewalla dla klienta bezprzewodowego, który wykorzystuje opcje kontroli stanu zapewniane przez Netfilter. Należy pamiętać o dołączeniu do firewalla właściwych modułów, które opisano w podrozdziale „Konfiguracja jądra z obsługą sieci bezprzewodowych" we wcześniejszej części tego rozdziału. Aby uzyskać więcej informacji na temat programu *iptables* i firewalla Netfilter, należy przejść do rozdziału 11., odwiedzić stronę *http://www.netfilter.org/* lub wyświetlić stronę pomocy *iptables*.

```
#!/bin/sh
# Prosta konfiguracja rc.firewall dla klienta bezprzewodowego

# Ustawienie zmiennych
IPTABLES=/sbin/iptables

# Oproznienie wszystkich lancuchow, aby zapewnic start od zera
$IPTABLES -flush

# Lancuchy INPUT i FORWARD zostana przeniesione do wlasnego
# lancucha "client"
# Utworzenie lancucha client
$IPTABLES -N client

# Dopuszczenie ustanowionego ruchu
$IPTABLES -A client -m state --state ESTABLISHED,RELATED -j ACCEPT

# Zaakceptowanie wszystkich polaczen, ktore nie przychodza
# do glownego interfejsu Ethernet (interfejs bezprzewodowy)
$IPTABLES -A client -m state -state NEW 01 ! eth0 -j ACCEPT

# Odrzucenie pozostalego ruchu
$IPTABLES -A client -j DROP

# Skok lancuchow INPUT i FORWARD do lancucha client
$IPTABLES -A INPUT -j client
$IPTABLES -A FORWARD -j client

# Dopuszczenie calego ruchu wychodzacego
$IPTABLES -A OUTPUT -j ACCEPT
```

Powyższy kod należy zapisać w pliku wykonywalnym o nazwie */etc/init.d/rc.firewall*. Następnie należy dodać następujące wpisy do pliku */etc/rc.d/rc.local*:

```
# Firewall IP
echo "uruchamianie Firewalla IP
/etc/init.d/rc.firewall
```

Reguły firewalla zostaną zastosowane po zrestartowaniu systemu. Aby natychmiast załadować te reguły, należy użyć polecenia */etc/init.d/rc.firewall*. Niektóre dystrybucje Linuksa wymagają użycia alternatywnych metod ładowania reguł firewalla podczas startu systemu. Więcej informacji na ten temat można znaleźć w dokumentacji dołączonej do danej dystrybucji.

Wyłączenie niepotrzebnych usług

Zasada najmniejszego przywileju odnosi się nie tylko do opcji jądra, ale również do usług uruchomionych w stacji roboczej. Niepotrzebne usługi mogą być wykorzystane przez hakerów do przeprowadzenia próby włamania do hosta. Uruchomienie każdej dodatkowej usługi znacznie zwiększa prawdopodobieństwo wystąpienia luki w zabezpieczeniach. Z tej przyczyny należy wybrać tylko naprawdę niezbędne usługi, a następnie wyłączyć wszystkie pozostałe. Pozwoli to na zredukowanie zagrożenia, a także uprości życie administratorowi systemu.

Aby ustalić wszystkie udostępniane usługi, należy uruchomić narzędzie *lsof* ze znacznikiem `-i`, na przykład:

```
[root@mo root]# lsof -i
COMMAND    PID USER   FD   TYPE DEVICE SIZE NODE NAME
portmap    639 root    3u  IPv4    913       UDP *:sunrpc
portmap    639 root    4u  IPv4    914       TCP *:sunrpc (LISTEN)
rpc.statd  668 root    4u  IPv4    939       UDP *:844
rpc.statd  668 root    5u  IPv4    966       UDP *:1024
rpc.statd  668 root    6u  IPv4    969       UDP *:1024 (LISTEN)
sshd       933 root    3u  IPv4   1198       TCP *:ssh (LISTEN)
xinetd     966 root    3u  IPv4   1222       TCP mo:1025 (LISTEN)
xinetd     966 root    3u  IPv4   1273       TCP *:echo
sendmail  1006 root    4u  IPv4   1274       TCP mo:smtp (LISTEN)
X         1233 root    1u  IPv4   1477       TCP *:x11 (LISTEN)
```

Polecenia wyświetlane po lewej stronie otworzyły porty podane po prawej stronie. Na przykładowym hoście uruchomiono usługi echo i sendmail (*smtp*), które prawdopodobnie nie są potrzebne i można je bezpiecznie wyłączyć. Według programu *lsof* port echa jest kontrolowany przez *xinetd*, natomiast port sendmail należy do samego programu *sendmail*. Aby wyłączyć te usługi, należy odnaleźć plik konfiguracyjny *sendmail* i zatrzymać ten program, a następnie zmodyfikować ustawienia demona *xinetd* i wyłączyć echo.

Usługi w systemie Linux mogą być uruchamiane na wiele sposobów. Wiele z nich, na przykład telnet, ftp i portmapper, jest uruchamianych przez superdemona *inetd* lub *xinetd*. *inetd* to od dłuższego czasu standardowy demon systemowy. Twórcy niektórych dystrybucji (jak na przykład RedHat) zdecydowali się na migrację do demona *xinetd*, co było spowodowane rozbudowanym zestawem funkcji i lepszymi zabezpieczeniami.

Usługi uruchamiane poprzez demona *inetd* są kontrolowane za pomocą pliku *inetd.conf*, który zwykle znajduje się w katalogu */etc*. Aby zablokować uruchamianie wybranych usług, należy oznaczyć znakami komentarza (#) ich wpisy w pliku konfiguracyjnym *inetd.conf*. Wszystkie zmiany zostaną zastosowane po zresetowaniu komputera. Jeżeli

jednak konieczne jest natychmiastowe użycie zmodyfikowanych ustawień, należy wysłać do demona *inetd* sygnał HUP, co spowoduje ponowne odczytanie pliku konfiguracyjnego:

```
killall -s HUP inetd
```

Konfiguracja demona *xinetd* jest bardziej skomplikowana. W większości systemów istnieje plik osłony konfiguracji o nazwie */etc/xinetd.conf*, który wywołuje skrypty znajdujące się w katalogu */etc/xinetd.d/*. Aby wyłączyć usługę znajdującą się w katalogu *xinetd.d*, należy do pliku konfiguracyjnego tej usługi dodać następujący wiersz:

```
disable = yes
```

Również w tym przypadku wszystkie zmiany zostaną wykonane po zresetowaniu systemu. Demon *xinetd* nie odczytuje ponownie pliku konfiguracyjnego po odebraniu sygnału HUP. Aby natychmiast zastosować wprowadzone zmiany, należy unicestwić całkowicie proces i uruchomić go ponownie za pomocą następującego polecenia:

```
killall xinetd; xinetd -stayalive -reuse -pidfile /var/run/xinetd.pid
```

Przewodnik po funkcjach zapewnianych przez demona xinetd można znaleźć pod adresem *http://www.macsecurity.org/resources/xinetd/tutorial.shtml*.

Niektóre usługi nie są uruchamiane przez superdemona, ale poprzez jeden z katalogów startowych systemu. Pliki startowe są zapisywane w różnych miejscach w zależności od dystrybucji systemu; na przykład RedHat wykorzystuje katalogi */etc/rc.d/rc[0-6].d*, natomiast w przypadku Debiana są to katalogi */etc/rc[0-6].d*. Liczba w nazwie katalogu odpowiada poziomowi startu, z jakim wywoływane są skrypty. Większość niepotrzebnych usług jest uruchamiana poprzez skrypty w podkatalogach *rc2.d* i *rc3.d*. Aby wyłączyć usługę znajdującą się w katalogu *rc*, należy zmienić pierwszą literę nazwy skryptu z *S* na inną literę (zwykle *K*); na przykład, aby wyłączyć program *sendmail* w dystrybucji RedHat, konieczne są następujące polecenia:

```
cd /etc/rc.d/rc2.d
mv S80sendmail K80sendmail
```

Od tej chwili sendmail nie będzie się już uruchamiał przy starcie komputera.

Statyczne wpisy ARP

Ataki zatrucia ARP, które omówiono w rozdziale 2., stanowią poważne zagrożenie dla wszystkich użytkowników sieci bezprzewodowych. Skuteczne zatrucie pamięci podręcznej ARP hosta pracującego w takiej sieci umożliwia przeprowadzenie ataku DoS lub włamania za pośrednictwem człowieka. Na szczęście dzięki statycznemu odwzorowaniu adresów MAC na adresy IP dla najważniejszych hostów w sieci można w dużym stopniu zminimalizować ryzyko związane z atakami tego typu.

Podstawowym zadaniem jest ustawienie statycznego wpisu ARP dla bramy domyślnej. Poniżej przedstawiono przykładowy skrypt, który po umieszczeniu w pliku */etc/init.d/staticarp* może tworzyć niezbędne przypisanie. Zamiast wartości <*adres_IP _bramy*> i <*adres_MAC_bramy*> należy podać konkretne ustawienia sieci lokalnej:

```
#!/bin/sh
# Ten skrypt ustawia statyczne wpisy arp w systemie Linux
case "$1" in
start)

# Dodanie adresu MAC bramy do tablicy ARP

   echo -n 'dodawanie adresu MAC bramy do tablicy ARP'
   arp -s <adres_IP_bramy> <adres_MAC_bramy>
   ;;
stop)

# Usuniecie adresu MAC z tablicy ARP
   echo 'usuwanie statycznego adresu MAC z tablicy ARP'
   arp -d <adres_IP_bramy>
   ;;
*)

# Standardowe polecenie uzycia

   echo "Uzycie: `basename $0` {start|stop}" >&2
   ;;
esac

exit 0
```

Aby statyczne wpisy ARP były ładowane automatycznie podczas startu systemu, należy upewnić się, czy plik *staticarp* jest wykonywalny, a następnie dodać dowiązanie symboliczne do katalogu */etc/rc.d/rc2.d*. W tym celu należy wprowadzić następujące polecenia:

```
[root@mo rc2.d]# chmod 755 /etc/init.d/staticarp
[root@mo rc2.d]# cd /etc/rc.d/rc2.d
[root@mo rc2.d]# ln -s /etc/init.d/staticarp S98staticarp
```

Inne kwestie związane z bezpieczeństwem

Jeżeli jest to niezbędne, możliwe jest wprowadzenie kolejnych zabezpieczeń stacji roboczej. Ich omówienie wykracza jednak poza tematykę niniejszej książki. Wiele przydatnych informacji na temat bezpieczeństwa Linuksa można znaleźć na stronie Linux Security HOWTO, która jest dostępna pod adresem *http://www.tldp.org/HOWTO/Security-HOWTO.html*.

Kontrola zabezpieczeń i dzienników

Niezależnie od skuteczności zastosowanych zabezpieczeń zawsze można stać się ofiarą ataku nieznanego typu. Może to oznaczać poważne problemy, jeżeli użytkownik nie zapisuje informacji i nie monitoruje regularnie dzienników. Wykonywanie tych czynności

pozwoli reagować na ataki w czasie rzeczywistym, chroniąc w ten sposób zasoby, użytkowników i ich dane.

Narzędzie arpwatch

Ze względu na brak fizycznych zabezpieczeń sieci bezprzewodowych ataki niskiego poziomu stanowią znacznie poważniejsze zagrożenie niż w przypadku klasycznych sieci Ethernet. Dzięki zatruwaniu ARP (patrz rozdział 2.) złośliwy host może posłużyć do przeprowadzenia ataku za pośrednictwem człowieka na inne komputery znajdujące się w sieci. Użycie statycznych wpisów ARP w sposób opisany we wcześniejszej części tego rozdziału to jedna z metod zabezpieczenia się przed atakami tego typu.

Wykrywanie problemów z tablicami ARP to jedna z metod, dzięki którym administrator może przyjrzeć się ogólnemu bezpieczeństwu sieci. Wykrycie podejrzanych wpisów może oznaczać, że ktoś podsłuchuje wszystkie przesyłane pakiety, a dane są zagrożone. Do monitorowania sieci i sygnalizowania wszystkich nietypowych zdarzeń służy program o nazwie *arpwatch*. Aby możliwe było jego użycie, należy zapewnić dostęp do pierwotnych ramek, jakie są przesyłane poprzez sieć. W tym celu należy włączyć w jądrze obsługę opcji *CONFIG_PACKET*.

Szczegółowy opis konfiguracji i użycia programu *arpwatch* można znaleźć w podrozdziale „Narzędzie arpwatch” w rozdziale 4.

Narzędzie syslog

Program *syslog* to bardzo popularne narzędzie, które może być używane przez praktycznie każdą aplikację. Wiele standardowych aplikacji, włącznie z dziennikiem jądra, przesyła do tego narzędzia przydatne informacje. Przekierowanie uzyskanych danych do wybranego miejsca i regularne ich monitorowanie pozwala na uzyskanie przeglądu wszystkich czynności wykonywanych przez system i jego użytkowników, włącznie z osobami znajdującymi się w sieci.

Poszczególne dystrybucje Linuksa korzystają z odmiennych konfiguracji narzędzia *syslog*. W większości przypadków zebrane informacje są przesyłane do różnych plików dzienników na podstawie ich źródła i poziomu ważności. Czasami jednak przydaje się możliwość przesłania wszystkich danych do jednego pliku, gdyż pozwala to na ich przeglądanie za pomocą wybranych narzędzi, takich jak *grep* i *perl*. Samodzielnie przefiltrowane dane kontroli zabezpieczeń są zwykle znacznie bardziej przydatne niż informacje sortowane na podstawie założeń przyjętych z góry.

Aby przekierować do dziennika */var/log/messages* wszystkie informacje, jakie trafiają do narzędzia *syslog*, należy na początku pliku konfiguracyjnego */etc/syslog.conf* dodać następujący wiersz:

```
*.*                     /var/log/messages
```

Należy pamiętać o oznaczeniu znakami komentarza (#) wszystkich innych wierszy w pliku konfiguracyjnym programu *syslog*, jakie odwołują się do dziennika */var/log/messages*. Aby zastosować dokonane zmiany bez restartowania systemu, można jako użytkownik root wydać polecenie *killall syslogd; syslogd*.

Narzędzie swatch

Przeglądanie dzienników systemowych jest nudne. Jeżeli nie występują żadne ciekawe zdarzenia, szybko można stracić zainteresowanie tą pracą i przestać zwracać na dzienniki systemowe uwagę. Nie jest także możliwe przeglądanie dzienników przez cały czas. Na szczęście dostępny jest program *swatch*, który stale monitoruje wszystkie informacje zapisywane w dzienniku ASCII, oczekując na pojawienie się interesujących łańcuchów. Po wykryciu problemu program może wysłać wiadomość e-mail, wyświetlić komunikat w konsoli, a nawet odtworzyć sygnał dźwiękowy. Szczegółowy opis programu *swatch* można znaleźć w podrozdziale „Narzędzie swatch" w rozdziale 4.

Bezpieczna komunikacja

Nawet jeżeli firewall działa poprawnie, a jądro zostało skonfigurowane z minimalną ilością opcji, wysłanie do serwera niezaszyfrowanego hasła pocztowego może sprawić, że zaimplementowane systemowe mechanizmy zabezpieczeń staną się całkowicie bezużyteczne. Bezpieczna komunikacja stanowi podstawę dla bezpieczeństwa klienta. Szczegółowe przedstawienie mechanizmów komunikacyjnych można znaleźć w podrozdziale „Bezpieczna komunikacja" w rozdziale 3.

Przygotowanie niezbędnych zabezpieczeń stacji roboczych z systemami FreeBSD i Linux pozwoli pracować we wrogim środowisku, jakim jest sieć bezprzewodowa. Jeżeli stacja robocza będzie niedostępna i odporna na przeprowadzane próby włamania, haker szybko się zniechęci i spróbuje zaatakować inny komputer w sieci. Kolejnym krokiem procedury wdrażania chronionej sieci bezprzewodowej jest zbadanie bezpieczeństwa punktów dostępowych i bramy sieciowej.