Bezpieczeństwo w Linuksie. Podręcznik administratora

Autor: Bob Toxen
Tłumaczenie: Marcin Jędrysiak (rozdz. 6-11), Marek Pętlicki (rozdz. 12-14), Piotr Pilch (rozdz. 17-19), Rafał Szpoton (rozdz. 1-5,dod. F), Grzegorz Werner (rozdz. 15-16, 20, dod. A, C-D)
ISBN: 83-7361-333-1
Tytuł oryginału: Real World Linux Security
Format: B5, stron: 888

Twój Linux zostanie zaatakowany – możesz być tego pewien. Może to nastąpić za kilka miesięcy, ale może dzieje się to właśnie teraz. Bądź więc przygotowany. Niniejsza książka omawia zarówno rozwiązania, jak i wyjątkowe oprogramowanie służące do ochrony systemu Linux lub sieci komputerowej. Autor poświęcił wiele czasu, aby ostateczna wersja książki opisywała najgroźniejsze ataki w internecie. Dzięki niej uzyskasz wszystkie informacje potrzebne do skutecznej obrony.

W książce omówiono:

- Nowe funkcje IP tables
- Nowe techniki oraz oprogramowanie służące do wykrywania oraz blokowania ataków ARP oraz ataków na przełączniki
- Usprawnienia zapór sieciowych opartych na systemie Linux filtrujących zawartość pakietów
- Opis bezpieczeństwa usługi Samba dla klientów systemu Windows.
- Bezpieczeństwo w sieciach bezprzewodowych (standard 802.11b)
- Sposób wykorzystania programów Logcheck, Portsentry oraz innych, nowych narzędzi monitorujących sieć komputerową
- Bezpieczeństwo sieci VPN oraz komunikatorów internetowych; program GPG; funkcje jądra 2.4 i wiele innych zagadnień
- Zabezpieczenia fizyczne

Dołączona do książki płyta CD-ROM zawiera własne oprogramowanie autora, służące do natychmiastowego zablokowania poczynań hakerów oraz powiadomienia administratorów systemu. Płyta zawiera również niepublikowane wcześniej skrypty IP Tables oraz IP Chains oraz nowe narzędzia służące do monitorowania stanu sieci komputerowej, wykrywania podejrzanych działań oraz raportowania o nich, zabezpieczania kopii i uproszczenia odtwarzania systemu.

O autorze:
Bob Toxen ma ponad 28 lat doświadczenia w zakresie systemów UNIX (Linux). Jest jednym ze 162 twórców systemu Berkeley UNIX. O zabezpieczeniach dowiedział się na uniwersytecie w Berkeley, gdzie złamał kilka oryginalnych systemów UNIX. Obecnie jest prezesem firmy Fly-By-Day Consulting specjalizującej się w zabezpieczeniach systemu Linux oraz sieci komputerowych, sieci VPN, monitorowaniu w trybie 24/7 oraz wykonywaniu czynności administracyjnych dla wielu klientów na całym świecie. W roku 2002 jego zalecenia zostały dołączone do raportu na temat udoskonalania wywiadu Stanów Zjednoczonych przedstawionego prezydentowi Bushowi.

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

Spis treści

Rozdział 5.

Ataki powszechnie stosowane przez włamywaczy

W niniejszym rozdziale przedstawione zostaną najczęściej wykonywane ataki, których przypuszczenia na nasz system wręcz należy oczekiwać i być zawsze przygotowanym na ich odparcie. O wielu z nich mogłeś już słyszeć, lecz być może nie rozumiałeś, na czym w rzeczywistości polegają. W tym miejscu zostaną one omówione ze wszystkimi szczegółami; ponadto zostaną tu przedstawione specjalne techniki służące zabezpieczaniu się przed nimi.

A oto wykaz tematów poruszanych w tym rozdziale:

5.1. Ataki przypuszczane przy użyciu predefiniowanych narzędzi

Poziom zagrożenia: 

Opracowany przez NSA słownik terminów związanych z zagadnieniami zabezpieczeń oraz wykrywania włamań w następujący sposób definiuje pojęcie *Rootkit*:

Rootkit — narzędzie służące do łamania zabezpieczeń (używane przez krakera), które przechwytuje hasła oraz dane w sieci komputerowej przekazywane do oraz z komputera. Zestaw narzędzi, umożliwiający krakerowi utworzenie tylnego wejścia do systemu, pobieranie informacji z innych systemów w sieci komputerowej, maskowanie faktu złamania zabezpieczeń systemu oraz wiele innych czynności. Rootkit jest klasycznym przykładem oprogramowania typu koń trojański.

Najczęściej używana jest druga definicja, określająca Rootkit jako zestaw narzędzi służących do tworzenia tylnych wejść do systemu oraz zmniejszania jego bezpieczeństwa. Inaczej mówiąc, narzędzia te pozwalają krakerowi ukryć przed tobą fakt, że cały czas dysponuje on kontrolą nad systemem. Zainstalowanie zestawu Rootkit jest drugą fazą włamania. Pierwszą, rzecz jasna, jest samo złamanie zabezpieczeń. Bardzo często jest to wynik działania „script kiddie".

Mianem takim określa się osobę, która nie jest wystarczająco utalentowana lub zmotywowana, aby utworzyć swój własny program służący do przeprowadzenia ataku, wykorzystującego na przykład błąd powodujący przepełnienie bufora (lub inny), niepoprawne ustawienia programu, łatwe do złamania hasło itp. „Script kiddie" używa raczej przygotowanego wcześniej programu, służącego do wykonania ataku; po prostu uruchamia go wielokrotnie, przypuszczając kolejne ataki na różne systemy, aż do chwili odnalezienia takiego, który nie będzie dobrze zabezpieczony i dzięki temu może zostać złamany. W środowisku krakerów status takich osób jest tylko jeden stopień powyżej najniższego, jaki posiadają osoby wykonujące najprostsze ataki DoS, polegające na zalaniu sieci fałszywymi pakietami.

Rootkit nie jest, ściśle mówiąc, atakiem, lecz większość tworzących go procesów to procesy złożone, które nie mogą być w prosty sposób wykryte, chyba że programy podmienione na konie trojańskie oraz pliki konfiguracyjne zostaną porównane z ich poprawnymi wersjami. Porównanie to jest zazwyczaj wykonywane przy użyciu sumy kontrolnej MD5 (bardziej trafnie nazywanej skrótem), za pomocą programu `md5sum` lub `cmp`. Ten ostatni wykonuje porównanie bajt po bajcie, co jest niezwykle czasochłonne. Należy również być przygotowanym na fałszywe alarmy. Sprawdzałem kiedyś system, który został złamany, w przypadku którego archiwum zawierające programy przeznaczone do przywrócenia było jedynie przynętą. Prawdziwy koń trojański umieszczony był w prawie każdym programie wykonywalnym, zaś program `sshd` przesyłał go do wszystkich plików wykonywalnych kopiowanych do systemu.

Również program Tripwire dysponuje możliwością porównywania sumy MD5, zaś jego niewątpliwą zaletą jest to, że działa dwa razy szybciej od `cmp`, ponieważ musi jedynie

odczytać podejrzany plik i porównać ze znanym wcześniej jego poprawnym skrótem. Należy jeszcze wspomnieć, że program `sum` nie jest godny zaufania, ponieważ niektóre konie trojańskie są tak zaprojektowane, aby w rezultacie dawały tę samą wartość skrótu co właściwe programy. Opis sposobu użycia programu Tripwire znajdziesz w podrozdziale zatytułowanym „Narzędzie Tripwire", na stronie 738.

Jest bardzo ważne, by zdać sobie sprawę z tego, że w przypadku podejrzenia włamania do systemu mamy do czynienia z sytuacją analogiczną do odkrycia szpiegów w firmie. W gruncie rzeczy w pierwszym przypadku jest jeszcze gorzej — nie wiadomo, komu można ufać. Każdy program mógł zostać zmodyfikowany w taki sposób, że w efekcie będzie dawać fałszywe wyniki. Bardzo często w charakterze koni trojańskich wykorzystywane są programy `ls`, `ps`, `login` oraz `inetd`. Oczywiście, włamywaczowi mogą posłużyć także inne aplikacje, jak choćby `sum`, `mount` lub umieszczona na dysku kopia Tripwire. Oznacza to, że nawet zamontowanie dyskietki z programem Tripwire w celu sprawdzenia systemu nie jest całkowicie bezpieczne, ponieważ podmieniony mógł zostać również program `mount`. W gruncie rzeczy przeprowadzana co noc procedura sprawdzania systemu przy użyciu programu Tripwire powinna umożliwić wykrycie wszystkich problemów, a jeżeli sam program jest wywoływany z nośnika umożliwiającego jedynie odczyt danych, takiego jak zabezpieczona dyskietka lub płyta CD-R, ryzyko otrzymania w wyniku sprawdzenia systemu niewłaściwych danych jest niewielkie.

Jak częste są ataki przypuszczane przy użyciu narzędzi typu Rootkit? Trzeba powiedzieć, że są one przeprowadzane bardzo często, szczególnie w celu umożliwienia krakerom pozostania w systemie, zaś od 20 do 70 procent włamań kończy się przejęciem uprawnień administratora. W jaki sposób uzyskać taki program? Krakerzy przeglądają witryny typu *www.rootkit.com/*[1]. Oczywiście istnieje znacznie więcej witryn tego typu.

Olbrzymia liczba witryn wykorzystywanych przez krakerów oraz potężne możliwości stosowanych przez nich narzędzi są przerażające. Chociaż najczęściej wykorzystywanym sposobem walki z takimi programami jest przeinstalowanie systemu od podstaw, nie zawsze aż tak radykalne działanie jest rzeczywiście konieczne. W części III oraz IV niniejszej książki zostaną szczegółowo omówione zagadnienia wykrywania włamań oraz naprawiania systemów, które padły ich ofiarą; trzeba pamiętać, że każde z takich włamań mogło spowodować spowodować pozostawienie w systemie koni trojańskich.

5.2. Fałszowanie pakietów

Poziom zagrożenia: ☠☠☠☠☠

Prawie każdy słyszał o fałszowaniu pakietów, lecz niewielu administratorów naprawdę dobrze rozumie tę technikę. Z fałszowaniem pakietów mamy do czynienia wtedy, gdy kraker wysyła pakiet danych w sieci komputerowej, na przykład do systemu *server.*

[1] Wydaje się, że ta witryna nie jest już dostępna. Co za szkoda! Być może jej sponsorzy pracują teraz w kamieniołomach. Wciąż jednak istnieje wiele innych witryn tego typu, jak choćby *www.thenewbiesarea.com*.

pentacorp.com z systemu *cracker.com*, twierdząc, że pochodzi on z systemu *client.pentacorp.com*. Takie działanie ma na celu uzyskanie uprawnień dostępu do serwera *server.pentacorp.com* właściwych dla *client.pentacorp.com*.

Fałszowanie pakietów jest możliwe dzięki lukom w zabezpieczeniach wywodzących się z projektu (słabego) protokołów w rodzaju UDP, TCP, ICMP oraz protokołów i algorytmów routujących. Przyczyną występowania tej luki nie jest używanie jądra systemu Linux lub samego oprogramowania. Należy zrozumieć, że wspomniane protokoły zostały utworzone ponad 20 lat temu, kiedy sieć internet była mniejsza, bardziej przyjazna oraz bezpieczniejsza niż obecnie.

Protokół TCP został zaprojektowany dla potrzeb projektu ARPA, prowadzonego w Ministerstwie Obrony Stanów Zjednoczonych. Główny nacisk został położony na jego właściwości umożliwiające przetrwanie ataku nuklearnego i zniszczenia części sieci. Miał on umożliwić szybką i efektywną zmianę routowania pakietów poprzez ominięcie zniszczonych miast, bez straty pakietów przesyłanych właśnie przez zaatakowany obszar. Z drugiej strony, w przeciwieństwie do korzystających obecnie z protokołu TCP krakerów, przedstawiciele ministerstwa oraz naukowcy byli osobami zaufanymi.

Możliwość zmiany trasy przesyłania pakietów z pominięciem zniszczonych obszarów oraz brak wrażliwości na ewentualne przerwy w działaniu sieci w trakcie ataku zostały przetestowane z pozytywnym wynikiem. Podczas wojny w Zatoce Perskiej, pomimo masowych bombardowań Iraku, na terenie tego państwa wciąż istniał dostęp do sieci internet.

Każdy pakiet zawiera adres źródłowy składający się z adresu IP oraz numeru portu, z którego wydaje się pochodzić pakiet, a także adres docelowy, określający miejsce jego przeznaczenia. Problem stanowi to, że system nadawcy tworzy pakiet i może sfałszować informacje o swoim adresie źródłowym. Takie oszustwo może być trudne do wykrycia. W jaki więc sposób można się przed nim ochronić?

Nowoczesne zapory sieciowe (włączając do nich mechanizmy wbudowane w jądro systemu Linux) oraz niektóre routery mogą zostać skonfigurowane w ten sposób, aby dysponowały informacją o tym, jaki zakres adresów powinien być traktowany jako zakres adresów „wewnętrznych"; wszystkie inne będą traktowane jako „zewnętrzne". Kiedy zapora zarejestruje pakiet zawierający adres wewnętrzny przychodzący na interfejs zewnętrzny, rozpozna go jako pakiet sfałszowany i jako taki odrzuci. Właśnie do takiej konfiguracji służy parametr `--interface` programu `ipchain`. Umożliwia on administratorowi określenie interfejsu (na przykład karty Ethernet, ppp lub T1), z którego pakiety z określonym adresem źródłowym będą akceptowane.

Przed fałszowaniem pakietów można zabezpieczyć się w dużym stopniu poprzez użycie dobrego połączenia następujących reguł:

- Nie należy ufać adresom źródłowym UDP, z wyjątkiem *bardzo* bezpiecznych sieci.
- Należy upewnić się, czy wszystkie systemy w sieci używają nowych stosów IP, które nie wykorzystują możliwych do przewidzenia numerów sekwencji TCP (system Linux zawiera poprawkę tego błędu począwszy od jądra w wersji 2.0.36).

- Należy używać zaszyfrowanego tunelu w sieciach niezaufanych, takich jak internet. Jest to niezbędne w celu uniknięcia podsłuchiwania lub nawet przechwycenia sesji TCP. Możemy skorzystać np. z SSL oraz różnego rodzaju produktów tworzących VPN, jak chociażby FreeS/WAN. Zostaną one omówione w podrozdziałach „Zabezpieczanie sesji użytkownika za pomocą SSH" na stronie 481 oraz „VPN z wykorzystaniem FreeS/WAN IPSec" na stronie 502. Przechwytywanie sesji TCP zostanie omówione w podrozdziale „Przechwytywanie sesji TCP" na stronie 305.

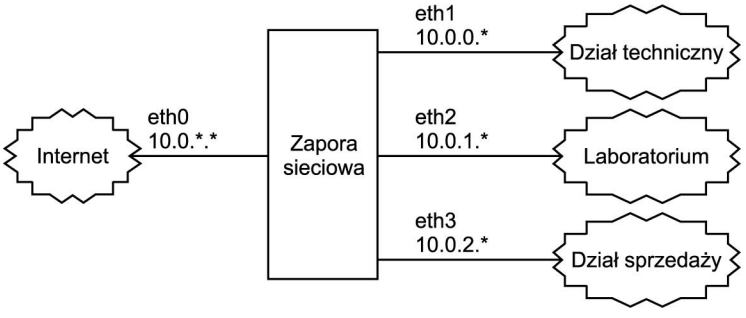
Administratorzy systemów powinni również skonfigurować swoje zapory sieciowe w ten sposób, aby poszukiwały fałszywych pakietów z adresami źródłowymi pochodzącymi spoza sieci komputerowej, przesyłanych na interfejsy „wewnętrzne" i odrzucały je przy jednoczesnym zapisaniu ich adresów MAC (adresów Ethernet). Pakiety te są tworzone przez źle skonfigurowany system w sieci lub przez użytkownika z sieci wewnętrznej, który ma niezbyt dobre zamiary. Włamywacze na zewnątrz firmy usiłujący sfałszować pakiety tak, aby wydawały się pochodzić z adresów IP wewnątrz firmy mogą zostać zablokowani w prosty sposób przy użyciu tylko jednego polecenia, co zostało omówione w podrozdziale zatytułowanym „Blokowanie fałszowania adresów IP" na stronie 180. Powinieneś również zapoznać się z podrozdziałem „Zapora sieciowa oraz DMZ za pomocą IP Chains", który znajdziesz na stronie 595. Żadna z omawianych dotychczas technik nie ochroni przed atakiem na sesje, których jeden uczestnik znajduje się poza siecią wewnętrzną firmy. Tego rodzaju problem rozwiązuje wykorzystanie komunikacji szyfrowanej.

Na szczęście większość dostawców ISP oraz dużych organizacji dokonuje filtrowania pakietów pochodzących z sieci wewnętrznych. Taka czynność zmniejsza znacznie ilość systemów, które mogą zostać wykorzystane przez krakerów chcących fałszować pakiety. Ochrona własnych systemów przed włamaniem, a tym samym możliwością ich wykorzystania w innych atakach, jest wręcz obowiązkiem każdego użytkownika komputera. Trzeba pamiętać, że złamanie zabezpieczeń systemowych może wiązać się z koniecznością poniesienia konsekwencji natury prawnej. Firmy, które nie są w stanie ochronić swoich systemów przed ich wykorzystaniem do przeprowadzenia ataków przeciw innym systemom, są często pozywane do sądu. Aby uzupełnić poruszane tutaj zagadnienia, zapoznaj się również z podrozdziałami zatytułowanymi „Blokowanie routingu źródłowego w IP" na stronie 178 oraz „Blokowanie fałszowania adresów IP" na stronie 180.

Dla podsumowania spróbuj naszkicować szkielet sieci komputerowej, zaznaczając połączenia z siecią internet. Narysuj okrąg dookoła każdego jej segmentu, który może być ochroniony za pomocą zapory sieciowej (włączając w to również wewnątrzfirmowe firewalle) lub routera, wykonujących filtrowanie pakietów pod kątem ich adresów. Dla każdej z granic, na przykład dla każdej zapory sieciowej, określ zakresy dopuszczalnych adresów pochodzących z obu jej stron. Rozważ również podsieci oraz serwery pośredniczące. Postaraj się być tak dokładnym, jak to tylko możliwe.

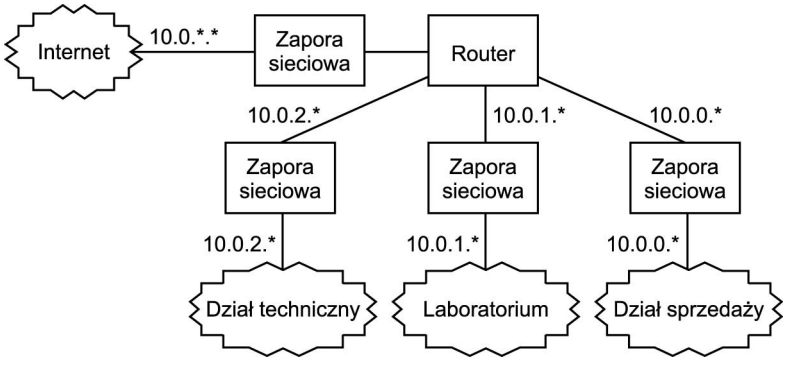
Czy na wszystkich zaporach sieciowych zostały wymuszone odpowiednie reguły? Zapoznaj się z podrozdziałem zatytułowanym „Zasady dotyczące topologii sieci", który znajdziesz na stronie 414. W charakterze zapory sieciowej oraz routera, chroniąc różne działy firmy przed zagrożeniami z internetu oraz złamaniem zabezpieczeń wewnątrz sieci

firmowej, może służyć pojedynczy komputer z systemem Linux, dysponujący wieloma kartami sieciowymi. Takie właśnie rozwiązanie zostało przedstawione na rysunku 5.1.



Rysunek 5.1. *Zapora sieciowa (router) z wieloma podsieciami*

Jak widać na rysunku 5.1, jeden serwer działający pod kontrolą systemu Linux, kosztujący około 500 dolarów lub mniej, może wykonać zadania innych, bardziej dedykowanych urządzeń. W przypadku większych firm może jednak wystąpić konieczność używania wielu zapór sieciowych lub oddzielnego routera. Taka konfiguracja została przedstawiona na rysunku 5.2.



Rysunek 5.2. *Wiele zapór sieciowych oraz router*

Jak widać, zapory sieciowe utworzone na bazie systemu Linux mogą zostać umieszczone wszędzie tam, gdzie istnieje konieczność stosowania tego rodzaju systemów.

5.2.1. Dlaczego udaje się fałszowanie pakietów UDP

Poziom zagrożenia: ☠☠☠☠☠

Możliwość wykrycia sfałszowanych pakietów UDP jest ograniczona do zapory sieciowej sprawdzającej, czy pakiet z określonym adresem źródłowym powinien pochodzić z systemów wewnętrznych, czy też zewnętrznych, oraz odrzucającej wszystkie pakiety łamiące określone dla niej reguły.

Zastanów się przez chwilę nad taką sytuacją: dysponujesz zdalnym serwerem, który łączy się głównym serwerem przy użyciu internetu. Załóżmy, że ten zdalny komputer

zamierza używać do komunikacji UDP. Taka sytuacja może wystąpić w przypadku stosowania NFS[2] lub własnej aplikacji użytkownika.

W jaki sposób zapora sieciowa lub aplikacja mogłaby określić, że pakiet został sfałszowany? Otóż **nie może** tego wykryć, ponieważ wie, że zdalny serwer znajduje się na zewnątrz sieci i zaakceptuje pakiet (jeżeli użytkownik pragnie uruchomić aplikację wykorzystującą pakiety tego rodzaju), lecz poprawny pakiet nie będzie się niczym różnił od sfałszowanego.

Właśnie z tej przyczyny protokół **UDP jest uznawany za niebezpieczny**; ponadto głównie z tego samego powodu za niebezpieczną jest uznawana również usługa NFS, ponieważ używa jedynie[3] UDP. Wszystkie tak starannie skonfigurowane procedury kontroli dostępu, na przykład plik */etc/exports* pozwalający utworzyć połączenie NFS jedynie niektórym serwerom (inne aplikacje mogą używać podobnych plików konfiguracyjnych), zostaną pokonane, ponieważ wszystkie one bazują na polu adresu źródłowego pakietu, a właśnie ono zostało sfałszowane.

Oczywiście serwer (NFS lub inny) odeśle odpowiedź do komputera o adresie źródłowym określonym w fałszywym pakiecie klienta i — co także jest oczywiste — rzeczywisty system klienta, którym jest system krakera, nie ujrzy odpowiedzi (chyba że kraker może podsłuchiwać sieć). Nie stanowi to zazwyczaj problemu, ponieważ większość aplikacji działających na warstwie protokołu UDP implementuje prosty protokół, którego zazwyczaj używa klient do wysłania żądania, zaś serwer odpowiada za pomocą komunikatu `ok`, komunikatu o wystąpieniu błędu lub danych stanowiących odpowiedź na żądanie. Zazwyczaj kraker może dokonać wielu zniszczeń nawet nie dysponując odpowiedzią. Jeśli używa NFS, jest w stanie wysłać żądanie `rm /etc/init`, które spowoduje, że następnym razem system się nie uruchomi. Kraker w tym przypadku nie martwi się tym, czy otrzyma odpowiedź `ok`. Ponadto mógłby utworzyć nowy plik */etc/passwd*, zawierający wybrane przez siebie hasło administratora, wykorzystać NFS do umieszczenia go w systemie docelowym i przejąć dzięki temu kontrolę nad systemem. Większości poważnych problemów zapobiegnie ustawienie poprawnych uprawnień (przy użyciu opcji `root_squash`) w pliku */etc/exports*.

Opcja `root_squash` powoduje, że zdalny użytkownik podający się za użytkownika o UID 0 lub root będzie traktowany jako użytkownik `nobody`. Jest to domyślne zachowanie serwera NFS. Opcja `root_squash` nie zabezpieczy jednak w pełni systemu NFS. Kraker musi jedynie wykorzystać lukę w systemie, która nie wymaga uprawnień administratora. Jedna z takich „łatwych zdobyczy", które mogą okazać się dlań pomocne, polega na tym, że wielu użytkowników systemu używa źle skonfigurowanej zmiennej środowiskowej `$PATH`, zawierającej `.` (znak kropki) przed nazwą katalogów systemowych.

---

[2] NFS jest skrótem od Network File System — nazwy protokołu utworzonego przez firmę Sun Microsystems w celu umożliwienia programom działającym w systemach klientów uzyskanie dostępu do plików serwera, tak jakby stanowiły one pliki lokalne w systemach klienta. Protokół ten wykorzystuje UDP, ponieważ ten ma prawie dwukrotnie większą przepustowość niż TCP przy użyciu tego samego sprzętu dla potrzeb aplikacji klient-serwer. Protokół ten nie jest również oparty na połączeniu, co sprawia, że serwer nie natrafi na sytuację wyczerpania wszystkich gniazd plików, ponieważ potrzebuje tylko jednego dla całej usługi, a nie osobnego dla każdego systemu klienta.

[3] NFS w wersji 3 może używać również TCP — *przyp. red.*

Zostało to omówione w podrozdziale zatytułowanym „$PATH: Katalog . grozi nieszczęściem” na stronie 177.

Craker musi jedynie sfałszować adres źródłowy NFS i umieścić fałszywą wersję powszechnie używanego programu narzędziowego, takiego jak `ls` lub `pwd`, w katalogu */tmp* i czekać, aby administrator użył jednego z tych zmodyfikowanych poleceń w tym właśnie katalogu. Wykonanie przedstawionego tu polecenia spowoduje wyświetlenie wszystkich usług sieciowych wykorzystujących UDP, które mogłyby działać na twoim komputerze, z wyjątkiem tych, które nie posiadają nazw symbolicznych w pliku */etc/services*:

```
grep udp /etc/services
```

Bardziej wydajny sposób polega na użyciu programu `ports` lub `netstat`; oba zostały omówione w podrozdziale „Wyłączanie niepotrzebnych usług” na stronie 125. Programy te umożliwią określenie portów rzeczywiście używanych w systemie. Wszystkie osoby, które chciałyby napisać swoje własne programy analizujące otwarte porty, będą musiały odczytywać pseudopliki */proc/net/udp* oraz */proc/net/tcp*. Pola o nazwach `local_address` oraz `rem_address` są polami określającymi lokalny oraz zdalny adres komputera. Część pola umieszczona przez znakiem `:` określa adres IP, zaś część występująca za nim jest numerem portu. Oba numery są podane w postaci szesnastkowej.

5.2.2. Fałszowanie sekwencji TCP

Poziom zagrożenia:

Jedna z różnic pomiędzy protokołami TCP a UDP polega na tym, że pierwszy z nich dysponuje algorytmem potwierdzenia (ponowienia) transmisji, dzięki któremu nadawca dysponuje informacją o tym, czy każdy z pakietów został odebrany, zaś wszystkie opuszczone pakiety są wykrywane wskutek określenia brakujących pakietów z potwierdzeniami. W takim przypadku są one wysyłane ponownie (algorytm powtarzania). Częścią tego rodzaju algorytmu są numery sekwencji wbudowane w protokół w celu upewnienia się, że pakiet został dostarczony i czy w sekwencji nie ma brakujących pakietów.

Aby sfałszować pakiety TCP, osoba dokonująca tej operacji musi znać schemat numerowania sekwencji lub po prostu ją odgadnąć. Jeszcze nie tak dawno nikt w rzeczywistości nie przejmował się kwestią fałszowania i dlatego też numerowanie sekwencji było przewidywalne, chociaż jego sposób zależał od systemu operacyjnego (dlatego właśnie niektóre z programów używanych przez krakerów na podstawie charakteru tej sekwencji potrafiły określić nawet rodzaj używanego systemu).

Sposób nawiązywania połączenia TCP polega na wysłaniu przez klienta komunikatu TCP postaci `SYN`; jest to pakiet TCP z ustawionym bitem `SYN` w nagłówku (wartość `1`). W komunikacie tym klient umieszcza swój „numer początkowy sekwencji”, używany do śledzenia sekwencji pakietów.

Serwer odpowiada za pomocą komunikatu SYN/ACK (włączone bity SYN oraz ACK), zawierającego początkowy numer sekwencji serwera. Stare systemy używały początkowego numeru sekwencji *X* dla *N*-tego połączenia, *X*+64000 dla połączenia *N*+1 itd.

Ostatecznie klient wysyła komunikat ACK. W tym momencie każda ze stron może rozpocząć wysyłanie danych. Gdy każda wyśle *Y* bajtów swoich danych, musi zwiększyć numer sekwencji o wartość *Y*. Należy zauważyć, że zostały wysłane trzy pakiety, i dlatego to właśnie trójstopniowa wymiana komunikatów ACK inicjuje połączenie.

Jak przypominasz sobie z podrozdziału zatytułowanego „Dlaczego udaje się fałszowanie pakietów UDP", sfałszowanie adresu źródłowego pakietu jest trywialne. Jedynym utrudnieniem podczas przeprowadzania takiej operacji w przypadku połączenia TCP jest to, że klient musi znać numer początkowy sekwencji serwera lub spróbować go odgadnąć. Jeżeli klient używa fałszywego adresu źródłowego, odpowiedź SYN/ACK serwera, która będzie zawierać cenny początkowy numer sekwencji, wysyłana jest pod fałszywy adres źródłowy i kraker nigdy jej nie zobaczy.

Najnowsze wersje systemu Linux używają trudnego do odgadnięcia schematu tworzenia numerów sekwencji; takie rozwiązanie ma zwiększyć ochronę przed fałszowaniem. Szczegółowe informacje zostaną podane w podrozdziale „Zapobieganie fałszowaniu sekwencji TCP" na stronie 307. Ponieważ numer sekwencji jest liczbą 16-bitową, włamywacz musi odgadnąć 65536 liczb.

Jeśli jednak włamywacz mógł nie został wykryty przez dostatecznie długi okres czasu, mógł odgadnąć ten numer. Z tego powodu w sytuacji, w której wymagane jest stosowanie mocnych zabezpieczeń, nie polegać jedynie na adresach IP. Powinniśmy wykorzystać zaporę sieciową blokująca pakiety pochodzące z internetu (lub podsieci, do których mamy niewystarczająco duże zaufanie), które wydają się pochodzić z systemu umieszczonego w sieci wewnętrznej. Jedynie połączenia ssh pochodzące z sieci zewnętrznej powinny być przepuszczane do Strefy Zdemilitaryzowanej (DMZ), w której należy umieścić serwery pocztowe oraz WWW. Więcej szczegółowych informacji znaleźć można w podrozdziale „Zbuduj niezależne twierdze" na stronie 349. Wciąż jednak zapora sieciowa lub program TCP Wrappers będzie filtrować znaczną część prób włamania się do sieci.

5.2.3. Przechwytywanie sesji TCP

Poziom zagrożenia:

Trzeba w tym miejscu wspomnieć o jednej bardzo istotnej rzeczy: otóż jeżeli kraker może podsłuchać ruch w sieci komputerowej, może również określić kolejny numer sekwencji w połączeniu wychodzącym, niezależnie od tego, po której stronie połączenia się znajdzie. Jeżeli ma dostęp do jednego z serwerów sieci serwera lub klienta, obserwowanie ruchu w tej sieci nie sprawi mu najmniejszego problemu. Następnie kraker będzie w stanie wprowadzić do niej swój własny pakiet. Na przykład jeżeli istnieje otwarta oraz aktywna sesja telnet, zapoczątkowana choćby przez administratora

logującego się ze swojego komputera domowego, kraker mógłby wprowadzić pakiet używający polecenia powłoki powodującego wprowadzenie do systemu konia trojańskiego. Takie przechwycenie sesji nie będzie trwać długo — jedynie do czasu, gdy dwa uprawnione systemy zostaną zdezorientowane i zamkną sesję. Z tego samego powodu możliwe jest wykorzystanie tej techniki do przeprowadzenia ataku DoS.

Ponieważ jednak pojedynczy pakiet może wprowadzić konia trojańskiego do sesji telnet, jest ona bardzo niebezpieczna. W podobny sposób może zostać przechwycona również sesja WWW, np. podczas wykonywania operacji transakcji płatniczej. W obu przypadkach powinniśmy zabezpieczyć się stosując mocne algorytmy szyfrujące, takie jak SSL, SSH lub sieci VPN w rodzaju FreeS/WAN. Ich użycie zapobiegnie zarówno podsłuchiwaniu, jak i przejmowaniu sesji. Wspomniane tu rozwiązania zostaną omówione w podrozdziałach zatytułowanych „Zabezpieczanie sesji użytkownika za pomocą SSH" na stronie 481, „Pobieranie pakietu SSL" na stronie 830 oraz „VPN z wykorzystaniem FreeS/WAN IPSec" na stronie 502.

5.3. Ataki typu SYN Flood

Poziom zagrożenia: 

Przypomnij sobie dyskusję o trójstopniowej wymianie pakietów `ACK`, omówionej w podrozdziale „Fałszowanie sekwencji TCP" na stronie 304. Po wysłaniu przez klienta pakietu `SYN` do serwera, ten ostatni odnotowuje to w kolejce połączeń oczekujących na dokończenie, odsyła do klienta pakiet `SYN/ACK` oraz oczekuje na pakiet `ACK` kończący nawiązywanie połączenia. Co więcej, podczas oczekiwania przydziela pewne tymczasowe zasoby, „wiedząc", że pakiet `ACK` zostanie przesłany za sekundę lub dwie.

W przypadku ataku typu `SYN` Flood, czyli ataku polegającego na użyciu półotwartych połączeń, klient (kraker) nie wysyła nigdy ostatniego komunikatu `ACK`. Zamiast tego wysyła ponownie kolejny pakiet `SYN` z innym sfałszowanym adresem źródłowym, co powoduje przydzielenie kolejnych zasobów serwera. Zauważ, że klient nie zarezerwował żadnych swoich zasobów, ponieważ w celu wysłania dowolnych pakietów używał surowych gniazd.

Ponieważ aż do ostatnich czasów większość systemów operacyjnych nie mogła obsługiwać więcej niż tylko pewnej małej ilości tego rodzaju „w połowie otwartych" gniazd zanim zasoby nie zostały wyczerpane całkowicie, z pewnością zaistnienie takiej sytuacji bardzo szybko spowoduje wyłączenie serwera. Obrona przed atakami tego typu zostanie omówiona w kolejnym podrozdziale. Atak zrealizowany przy użyciu pakietów `SYN` został zaobserwowany po raz pierwszy wtedy, gdy podatny na niego serwer firmy Panix (dostawcy ISP w Nowym Jorku) został przy jego użyciu wyłączony. W firmie tej do dziś nikt nie wie, kto zaatakował ją po raz pierwszy.

5.4. Obrona przed atakami typu SYN Flood

Poziom zagrożenia: 

W poprzednim podrozdziale omówiłem działanie ataku DoS typu SYN Flood. Aby się przed nim uchronić, gdy jeśli używasz wersji jądra starszej niż 2.0.36, powinieneś po prostu je uaktualnić. Należy podkreślić, że już jądra o wersji wyższej niż 2.0.30 udostępniają poprawkę zabezpieczającą przed tym atakiem, lecz oprócz tego zawierają inny błąd umożliwiający fałszowanie pakietów TCP, dlatego też należy używać wersji przynajmniej 2.0.36, w której wspomniany błąd nie występuje. Po pobraniu jądra 2.0.36 lub nowszego konieczne jest przekompilowanie go ze zdefiniowaną stałą `CONFIG_SYN_COOKIES`. Zazwyczaj uzyskamy to wykonując podczas konfiguracji jądra następujące polecenia, wywoływane z */usr/src/linux*:

```
make xconfig      w przypadku używania X Windows
make menuconfig   menu
make config       stara metoda
```

Stała `CONFIG_SYN_COOKIES` powoduje rozpoznanie, że kolejka „w połowie otwartych" połączeń, w której zapamiętywane są szczegóły dotyczące nawiązywanego połączenia, przekroczyła odpowiedni rozmiar. Połowa z tej kolejki jest dedykowana do obsługi komunikacji z systemami, z którymi ostatnio pomyślnie nawiązano połączenie, przy założeniu, że systemy te są prawdopodobnie do tego uprawnione.

Jeżeli serwerowi zaczyna brakować przestrzeni w kolejce, koduje dane przy użyciu 32 bitów i dołącza tę informację do pakietu `SYN/ACK` jako numer początkowy sekwencji. Jeżeli pakiet ten trafi do właściwego klienta, który nie jest koniem trojańskim, ten zwiększy numer pakietu i umieści go w kolejnym pakiecie `ACK`. Serwer następnie odejmuje jeden od numeru pakietu i dysponuje wszystkimi informacjami niezbędnymi do zakończenia procesu nawiązywania połączenia. Jeżeli pakiet `SYN` spowodowany był atakiem typu `SYN` flood, w przypadku gdy jądro odsyła z powrotem pakiet `SYN/ACK`, serwer „zapomina" o okolicznościach połączenia (zamiast zapisywać do pliku z logiem komunikatu z ostrzeżeniem „Uwaga: możliwy atak typu SYN Flood."). Większość ostatnich wersji jądra ma tę opcję włączoną domyślnie.

5.5. Zapobieganie fałszowaniu sekwencji TCP

Poziom zagrożenia: 

Starsze jądra systemu Linux (i wiele innych systemów operacyjnych) używają przewidywalnego schematu tworzenia numerów sekwencji pakietów TCP, co otwiera

system na możliwość sfałszowania przez krakera pakietów oraz przejęcia połączenia. Szczegółowe wyjaśnienie tej techniki zostało umieszczone w podrozdziale „Fałszowanie sekwencji TCP" na stronie 304. Rozwiązanie polega na uaktualnieniu jądra systemu Linux przynajmniej do wersji 2.0.30.

Trzeba jednak pamiętać, że w stosie protokołu TCP starszych jąder istnieje błąd umożliwiający przeprowadzenie fałszowania pakietów TCP przy użyciu innej metody — klient (używający fałszywego adresu źródłowego) mógłby wysłać pakiety, które zostałyby dostarczone do nasłuchującego serwera przed zakończeniem trójetapowego nawiązywania połączenia TCP. Ponieważ klient, jeśli jest narzędziem krakera, nie musi oczekiwać na zakończenie tej procedury, nie musi również oczekiwać na otrzymanie pakietu SYN/ACK i w ten sposób omija zabezpieczenia TCP. Ten ostatni błąd został poprawiony w wersji 2.0.36 jądra. Dlatego też jeżeli używasz jądra w starszej niż ta wersji, jeśli chcesz zapewnić sobie ochronę przez fałszowaniem pakietów TCP, powinieneś dokonać jak najszybszego uaktualnienia.

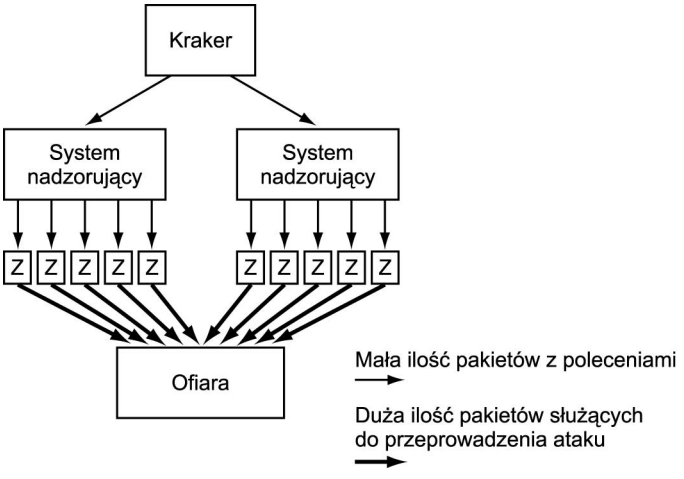
5.6. Sztormy pakietów, ataki smurfów oraz fraglesi

Poziom zagrożenia:

Sztorm pakietów (ang. *packet storm*) to określenie, którym nazywa się technikę wykorzystywaną przez włamywacza (lub osobę z nim współpracującą) w celu zalania systemu fałszywymi pakietami i zajęcia dzięki temu całego dostępnego pasma łącza sieciowego. Uniemożliwi to obsługę uprawnionych pakietów, ponieważ upłynie czas ich obsługi. Jest to jeden z rodzajów ataków typu DoS. Jeżeli atak przypuszczony został z wielu systemów, jest nazywany rozproszonym atakiem DoS (DDoS). Niektóre z brutalnych ataków typu DDoS polegają na złamaniu przez krakera wielu systemów, zainstalowaniu na nich programów pozostających w utajnieniu, a następnie wykorzystaniu ich po pewnym okresie czasu (niekiedy po miesiącach) do wykonania jednoczesnego ataku na system ofiary. Metoda ta została przedstawiona na rysunku 5.3, na którym każdy z prostokątów reprezentuje inny system. Zauważ, że kraker musi wysłać jedynie kilka komunikatów w celu spowodowania zalania systemu ofiary milionem pakietów. Może skorzystać z pakietów ICMP lub UDP zawierających sfałszowane adresy źródłowe, co praktycznie uniemożliwi wyśledzenie źródła ataków. Prostokąty z literą „Z" oznaczają „zombie" — systemy ze złamanymi zabezpieczeniami, atakujące ofiarę po wydaniu stosownego polecenia.

Jak wynika z rysunku 5.3, po skonfigurowaniu komputerów nadzorujących atak oraz komputerów zombie, wysłanie kilku zaledwie pakietów z systemu krakera może wyłączyć nawet największy system. Ponieważ możliwe jest wykorzystanie wielu poziomów „pośrednich" pomiędzy włamywaczem a ofiarą, ten pierwszy prawdopodobnie nie zostanie schwytany, chyba że zaatakował niewłaściwą osobę.

Rysunek 5.3.
Atak typu DDoS



Ataki smurfów (ang. *smurf attacks*) to swoiste ataki typu sztorm pakietów; włamywacz używa w nich fałszywego adresu podczas wysyłania pakietu echo protokołu ICMP na adres rozgłoszeniowy IP. O ile sieć docelowa nie została zabezpieczona przed takimi atakami, żądanie to zostanie dostrzeżone przez wszystkie systemy w niej umieszczone i każdy z nich odpowie przy użyciu fałszywego adresu nadawcy, co spowoduje zalanie tego serwera (zamierzonej ofiary) olbrzymią ilością fałszywych pakietów. Atak ten może być jeszcze zwielokrotniony poprzez wykorzystanie adresu rozgłoszeniowego w charakterze sfałszowanego adresu źródłowego, co spowoduje zwielokrotnienie liczby systemów dotkniętych atakiem.

Więcej informacji na temat omawianych tu ataków oraz przeciwdziałania im zawiera witryna Craiga Huegena, znajdująca się pod adresem *http://www.pentics.net/denial-of-service/*. Łącza do niej umieszczane są na wielu innych witrynach, zaś jej autor wspaniałomyślnie zgodził się na użycie jego materiałów w tej książce.

Wykorzystanie rozgłoszeniowego adresu docelowego w celu spowodowania przez początkowy pakiet wygenerowania wielu odpowiedzi (w tym przypadku odpowiedzi na polecenie echo protokołu ICMP) jest nazywane wzmocnieniem (ang. *amplification*). Dzięki wykorzystaniu takiej metody osoba dokonująca ataku nie musi wykorzystywać zbyt wielu zasobów swojego komputera. Jeżeli przy użyciu adresu rozgłoszeniowego wysłała ona wiadomość rozgłoszeniową do 100 serwerów w sieci, ofiara otrzyma 100 odpowiedzi. Jeżeli w ten sposób zostanie wykorzystana duża sieć komputerowa, na przykład sieć uniwersytetu lub jednej z firm z listy Fortune 500, uzyskane zwielokrotnienie może wynosić nawet 1000 razy. Dzięki temu atak może zostać zapoczątkowany przy użyciu połączenia wdzwanianego do sieci T1 i spowodować zatrzymanie działania olbrzymiej sieci docelowej z łączem T3. Jeżeli sieć komputerowa `10.*.*.*` klasy A pozwala na użycie rozgłoszeniowych adresów docelowych, odpowiedź na polecenie echo zostałaby wysłana pod adres `10.255.255.255`.

System, do którego jest wysyłane żądanie *echo*, jest nazywany wzmacniaczem. W celu zwiększenia efektu osoba atakująca może wykorzystać równolegle wiele wzmacniaczy, wysyłając pakiet najpierw do pierwszego systemu, później do drugiego itd. Jednak

jest to wciąż zaledwie pierwszy poziom wzmocnienia. Jeżeli natomiast również sieć zamierzonej ofiary obsługuje docelowe pakiety rozgłoszeniowe, możliwe jest uzyskanie wzmocnienia dwupoziomowego.

Mechanizm taki polega na wysłaniu pakietów pod adres rozgłoszeniowy sieci komputerowej ofiary, z wykorzystaniem sfałszowanego adresu źródłowego, którym jest adres rozgłoszeniowy innej sieci komputerowej. Jeżeli sieć ofiary obejmuje 50 systemów, zaś druga sieć komputerowa 100, każdy z 50 systemów wyśle odpowiedź na żądanie *echo* przy użyciu komunikatu skierowanego do drugiej sieci komputerowej, powodując wysłanie odpowiedzi przez każdy z jej 100 systemów. Daje to w rezultacie wzmocnienie 50×100, czyli 5000 razy. W przypadku, gdyby sieć dysponowała 1000 systemów, uzyskane zostałoby wzmocnienie 1 000 000 razy. Większość wykorzystywanych obecnie dużych sieci zabezpieczono jednak przed atakami tego typu.

Nazwa omawianego tu typu ataku pochodzi z bajki o Smurfach, w której wiele tych niebieskich stworzonek zdawało się wypełniać niemal całą przestrzeń.

Istnieje odmiana ataku smurfów zwana *atakiem fraglesów*, używająca żądań echo protokołu UDP w sposób podobny do żądań ICMP wykorzystywanych w przypadku ataku smurfów.

5.6.1. Zapobieganie wykorzystaniu systemu w charakterze wzmacniacza

W celu wykluczenia możliwości wykorzystania systemu w charakterze wzmacniacza należy wykonać wiele czynności. Każda z nich zostanie omówiona w dalszej części tej sekcji.

Na routerze lub zaporze sieciowej należy blokować wszystkie pochodzące z internetu pakiety z rozgłoszeniowym adresem docelowym lub rozgłoszeniowym adresem źródłowym.

Jeżeli pomiędzy systemami twojej sieci a siecią internet nie jest umieszczony żaden system zapory sieciowej lub router (w przypadku dysponowania więcej niż kilkoma systemami nie zasługuje to na pochwałę), poprzednia rada powinna zostać zastosowana w odniesieniu do każdego systemu. Na każdej z maszyn bez wątpienia powinien zostać uruchomiony program IP Chains, pozwalający na wykonanie stosownego filtrowania. (Należy pamiętać, że dowolny komputer z systemem Linux z rozsądnie nowej dystrybucji, używający jądra w wersji 2.2 lub późniejszej, może być w prosty sposób skonfigurowany w charakterze zapory sieciowej pomiędzy siecią wewnętrzną LAN a oddzielna kartą Ethernet obsługującą połączenie z internetem lub połączeniem PPP, ISDN, T1 lub T3. Nawet system dysponujący procesorem 386 poradzi sobie w przypadku połączenia ISDN, zaś system Pentium będzie w stanie obsłużyć połączenie T3.)

Używana przez ciebie zapora sieciowa powinna zostać również skonfigurowana w celu blokowania pakietów nadchodzących z sieci „zewnętrznej", które zawierają adres źródłowy, jaki powinien pochodzić jedynie z systemów twojej firmy i vice versa (jest to

częsta technika fałszowania pakietów). Blokowanie pakietów z sieci wewnętrznej z adresami właściwymi sieciom zewnętrznym ma na celu wykluczenie możliwości przeprowadzenia ataku przez nieprzyjaznych użytkowników z twojej sieci. Jeżeli obsługujesz system firmy ISP lub uniwersytetu, oczywiście musisz bronić się przed takimi użytkownikami. Ta sama reguła dotyczy dużych firm. Należy wyłączyć możliwość ustalania adresów źródłowych dla wszystkich pakietów przesyłanych do sieci (oraz wychodzących z niej, ponieważ osoby atakujące inne systemy mogą pracować w twojej sieci wewnętrznej).

Możesz również wyłączyć możliwość używania bezpośrednich adresów rozgłoszeniowych wewnątrz obsługiwanych podsieci, dysponujących więcej niż (na przykład) pięcioma systemami (wcześniej sprawdź, czy nie używasz żadnej aplikacji polegającej na tego rodzaju metodach rozgłoszeniowych, na przykład DHCP). Więcej informacji na temat konfiguracji zapór sieciowych, jak również przykłady reguł, zawierać będzie podrozdział zatytułowany „Zapora sieciowa oraz DMZ za pomocą IP Chains", który znajdziesz na stronie 595.

W przypadku powszechnie wykorzystywanych routerów odpowiednie polecenia wyglądają następująco:

```
Cisco:
      Polecenie interfejsu "no ip directed-broadcast"

Proteon:
      Konfiguracja protokołu IP "disable directed-broadcast"

Bay Networks:
      Ustaw falszywy adres statyczny ARP dla adresu rozgloszeniowego
```

Mógłbyś zapobiec żądaniom *echo* protokołu ICMP oraz przedostaniu się do sieci odpowiedzi na nie po prostu je ignorując, jednak takie podejście nie jest zalecane, o ile nie stanowi ostatniej deski ratunku — spowoduje bowiem utrudnienie rozwiązywania problemów zarówno przez ciebie, jak i inne osoby, które napotykają na kłopoty z połączeniem się z twoją siecią. Powodem ignorowania (odrzucania) odpowiedzi jest to, że będą one wysyłane przez niektórych krakerów, oczekujących, że twój system odpowie komunikatem informującym, że nie wysyłał żadnego żądania ICMP. Można zezwolić na wykonywanie normalnych poleceń *echo* i zablokować ataki Smurfów poprzez zablokowanie odpowiedzi echo ICMP o rozmiarze przekraczającym 100 bajtów, jako że ataki takie wydają się używać pakietów o rozmiarze ok. 1000 bajtów.

Należy wyłączyć odpowiedzi na komunikaty echo ICMP wysyłane na adresy rozgłoszeniowe. Takie działanie zostało zaakceptowane w dokumencie RFC-1122, w którym, w sekcji 3.2.2.6, użyto terminu *multicast* zamiast *broadcast*. Odpowiedzi na wspomniane komunikaty mogą być blokowane począwszy od jądra 2.2. Dla niektórych starszych jąder dostępna jest odpowiednia poprawka. Kontrolowanie tej oraz innych właściwości zostało opisane w podrozdziale „Opcje jądra dotyczące protokołów" na stronie 116. W celu powstrzymania tego określonego typu ataku, podczas każdego uruchamiania systemu powinno być użyte następujące polecenie:

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

Dokument RFC 1122 jest dostępny po adresem:

www.faqs.org/rfcs/rfc1122.html

5.6.2. Obrona przed atakiem używającym sztormu pakietów

Jeżeli odkryłeś, że jesteś ofiarą ataku przeprowadzonego przy użyciu sztormu pakietów, powinieneś zdawać sobie sprawę z tego, że znalazłeś się w trudnej sytuacji. Atak tego typu spowoduje wykorzystanie całego pasma łącza. Z tego powodu nie istnieje możliwość uratowania sieci komputerowej. Niektóre firmy usiłują sprzedawać urządzenia, które „ochronią sieć przeciwko rozproszonym atakom DoS przeprowadzanym przy użyciu sfałszowanych pakietów oraz podobnym atakom". Nie daj się zwieść takim reklamom. Chociaż urządzenia te mogą chronić przeciwko atakom Smurfów, atakom przeprowadzanym za pomocą sfragmentowanych pakietów oraz podobnym, polegającym na naruszaniu standardów protokołów, to jednak zapora sieciowa oparta na systemie Linux skonfigurowanym w sposób przedstawiony w tej książce spełni te same zadania za znacznie mniejszą cenę.

W celu przeprowadzenia analizy pakietów możesz użyć programów `Snort`, `sniffit` lub `tcpdump`, szczególnie wtedy, gdy adresy źródłowe tych pakietów są podejrzane. Czy pakiety wydają się pochodzić z jednego adresu IP, czy z wielu? Jeżeli wydają się pochodzić z jednego lub małej liczby adresów, należy ustalić firmę, do której te adresy należą, używając w tym celu technik opisanych w rozdziale „Namierzanie komputera włamywacza" na stronie 801. Kiedy to zrobisz, skontaktuj się z jej przedstawicielami i zmuś do powstrzymania ataku. Nalegaj, aby w razie konieczności wyłączyli swoje komputery.

Trzeba pamiętać, że adres źródłowy może być sfałszowany, dlatego też istnieje możliwość, że atak pochodzi z zupełnie niezwiązanych z nim systemów. Jeżeli organizacja nie może zostać ustalona lub nie chce współpracować, należy użyć polecenia `traceroute` z argumentem w postaci podejrzanego adresu IP. Powinniśmy odnaleźć systemy występujące przed podejrzanym. Mogłyby one określać jego dostawcę ISP. W takim przypadku można ponowić opisane powyżej czynności, próbując nawiązać kontakt z firmą i poprosić jej przedstawicieli o potwierdzenie oraz powstrzymanie ataku.

Jeżeli adres źródłowy został sfałszowany, skontaktuj się z własnym dostawcą ISP. Powinien on dysponować planem działania podejmowanego w takiej sytuacji, lecz nie jest to obligatoryjne. Jeżeli adres źródłowy został sfałszowany, przedstawiciele dostawcy usług ISP muszą ustalić, jaki system ostatnio używał pakietu, a jaki jeszcze wcześniej — i tak aż do odnalezienia adresu systemu źródłowego. W przypadku, gdy w ataku uczestniczy wiele systemów atakujących, technika ta może zostać powtórzona dla każdego z nich, co jest jednak niezwykle czasochłonne. Chociaż blokowanie ataków przy użyciu określonego rodzaju pakietu jest proste, to kilka z ostatnich programów stosowanych do przeprowadzenia ataku DDoS może używać różnych typów pakietów.

Przyszłe programy umożliwiające ataki typu DDoS prawdopodobnie będą jeszcze bardziej różnicować pakiety, co jeszcze bardziej utrudni ich blokowanie. Już teraz trwają

dyskusje pomiędzy niektórymi specjalistami, zmierzające do rozszerzenia protokołów umożliwiających systemowi docelowemu wysłanie komunikatu z informacją: „Przestań przesyłać pakiety o takich parametrach". Taka metoda będzie mogła zostać wykorzystana do zablokowania omawianych tu ataków. Ponieważ większość systemów rozszerza używane zapory sieciowe w celu wykonywania filtrowania pakietów oraz blokowania złych pakietów pochodzących z ich własnych sieci, ataki tego typu będą się coraz trudniej rozprzestrzeniać.

5.6.3. Routery Cisco

Administratorzy wykorzystujący routery firmy Cisco mogą znaleźć wiele przydatnych informacji na jej stronie internetowej, poświęconej zwiększaniu zabezpieczeń; można ją znaleźć pod adresem:

www.cisco.com/warp/public/707/3.html

Na stronie tej znajdziemy m.in. omówienie techniki blokowania dostępu sieciowego, nazywanej w firmie Cisco „portem diagnostycznym UDP routera". Zaprezentowane w tabeli 5.1 powszechnie obsługiwane usługi systemów Linux (UNIX) są często wykorzystywane do przeprowadzania ataków typu DoS.

Tabela 5.1. *Usługi diagnostyczne w systemie Linux (UNIX)*

Usługa	Port	TCP	UDP	Przeznaczenie
Echo	7	T	T	Router odpowiada przy użyciu otrzymanych danych
Discard	9	T	T	Router odrzuca otrzymane dane
Daytime	13	T	N	Router wysyła datę oraz czas systemowy
Chargen	19	T	T	Router tworzy strumień znaków

W celu wyłączenia tych usług w routerze firmy Cisco, należy użyć następujących globalnych poleceń konfiguracyjnych:

```
no service udp-small-servers
no service tcp-small-servers
```

Usługi te możesz również wyłączyć w systemie Linux, obejmując ich wpisy, znajdujące się w pliku */etc/inetd.conf*, znakiem komentarza. Chociaż wspomniane usługi są przydatne dla administratorów innych systemów, próbujących przeanalizować problemy z siecią komputerową, to jednak mogą się one również przydać krakerom oraz innym osobom dokonującym ataków DoS.

Niestety, chociaż wszystkie są usługami wewnętrznymi `inetd`, niemożliwe jest wykorzystanie TCP Wrappers w celu zezwolenia na ich wykorzystanie przez określone, przyjazne serwery oraz domeny. Tym niemniej w celu przyznania praw do ich wykorzystania tylko określonym systemom mógłbyś użyć funkcji zapory sieciowej lub IP Chains.

5.6.4. Ataki DDoS: zasoby sieciowe z narzędziami do przeciwdziałania

Zapoznaj się ze wspomnianą już wcześniej, doskonałą stroną Craiga Huegena. Przypomnę, że znajdziesz ją pod adresem:

http://www.pentics.net/denial-of-service/

Wartościowe wyjaśnienie poruszanego tu problemu umieszczono także na stronie:

www.cert.org/tech_tips/denial_of_service.html

Sposób obrony opisany został pod adresem:

www.cert.org/reports/dsit_workshop.pdf

Sugestie dotyczące zwiększenia zabezpieczenia systemu zamieszczone zostały na stronie o adresie:

www.cert.org/security-improvement

zaś następujące dwie strony zawierają sugestie dotyczące sposobu przywrócenia poprawnego działania systemu:

www.cert.org/nav/recovering.html
www.sans.org/

Po wystąpieniu w lutym 2000 roku dobrze opisanych ataków DDoS zauważyłem, że niektórzy dostawcy zapór sieciowych twierdzili niezgodnie z prawdą, iż tylko ich urządzenia ochronią sieć przed takimi atakami. Większość ataków typu DDoS, które wspomniane zapory sieciowe mogą blokować, takich jak chociażby ataki przeprowadzane za pomocą pakietów `SYN` oraz sfragmentowanych pakietów, można zablokować również dzięki poprawnie skonfigurowanemu systemowi Linux. Nie ufaj zatem ślepo przedstawicielom takich firm — poszukaj niezależnego doradcy.

5.7. Przepełnianie buforów oraz niszczenie zawartości pamięci

Poziom zagrożenia: 

Jeden z najbardziej powszechnie wykorzystywanych sposobów włamania się do systemu Linux polega na wykorzystaniu tzw. przepełnienia bufora. Niektórzy programiści popełniają pomyłki i nie są w stanie ograniczyć ilości danych, które ktoś może wczytać do pamięci programu zarezerwowanej na bufor danych. Kolejne bajty będą umieszczane w kolejnych obszarach pamięci, niszcząc tym samym ich wcześniejszą zawartość. Kiedy ten obszar pamięci zostanie odczytany ponownie, zostaną wykonane instrukcje umieszczone

w nim przez osobę, która dokonała przepełnienia bufora. Przypomina to wprowadzanie poprawek do programu w najbardziej złośliwy i skomplikowany sposób.

Jedna ze stosowanych powszechnie (w języku C) praktyk programistycznych polega na przydzieleniu wielu buforów w pamięci na stosie, jak również wykorzystaniu stosu do przechowywanie adresów powrotnych z procedury. Umożliwia to sprytnemu krakerowi spowodowanie, że procedura zwróci to wszystko, czego on sobie zażyczy — zazwyczaj adres powrotu do własnego kodu umieszczonego w innym obszarze bufora. Inaczej mówiąc, w celu dokonania włamania modyfikowane są zmienne na stosie.

> Istnieje kilka sprytnych technik służących do odpierania ataków przeprowadzanych za pomocą przepełnienia bufora nawet w przypadku wadliwego kodu. Techniki te — niektóre bardzo proste — zostaną opisane w podrozdziale zatytułowanym „Ochrona przed przepełnieniem bufora za pomocą Libsafe" na stronie 397.

Atak przeprowadzany za pomocą przepełnienia bufora może być rozpoznany, jeżeli system zarejestruje obecność długiego pola wejściowego, zawierającego wiele znaków, które nie są drukowalne. Oto, co otrzymałem jako „prezent noworoczny" w roku 1999:

```
Jan 1 00:59:41 rabbit mountd[351]: Unauthorized access by NFS client 206.132.153.48
Jan 1 00:59:41 rabbit syslogd: Cannot glue message parts together
Jan 1 00:59:41 rabbit mountd[351]: Blocked attempt of 206.132.153.48 to mount
^P^P^P^P^P^P^P^P^P^P
[prawie 460 znaków ^P]
Jan 1 00:59:41 rabbit ^H(-^E^H(-^E^H(-^E^H(-^E^H(-^E^H(-^E^H(-^E...
```

Atak został zarejestrowany przez magazyn CERT numerze CA-1998-12; znajdziesz go pod adresem:

http://www.cert.org/advisories/CA-1998-12.html

W przypadku programów CGI na włamanie oraz na próbę obejścia filtrowania zawartości wskazują długie łańcuchy wejściowe, zawierające dużą liczbę sekwencji typu `%xy`. Metody zapobiegania skutkom działania tego typu programów, dokonujących filtrowania zawartości za pomocą sekwencji `%xy`, zostały opisane w podrozdziale zatytułowanym „Odszyfrowywanie adresów URL" na stronie 354.

5.8. Techniki fałszowania

Fałszowanie ma miejsce wtedy, gdy coś (ktoś) udaje coś innego. W przypadku interesujących nas zagadnień może to dotyczyć osoby, systemu lub pakietu. Przedstawiona w tym rozdziale dyskusja zostanie ograniczona jedynie do systemu generującego pakiety sieciowe lub komunikaty, które wydają się pochodzić z zupełnie innego miejsca. Komunikat taki byłby zestawem pakietów, który składa się z kompletnej porcji informacji, tak jak wiadomość e-mail może składać się z długiej sekwencji pakietów TCP.

5.8.1. Fałszowanie wiadomości pocztowych

Poziom zagrożenia:

Ze sfałszowaną wiadomością pocztową mamy do czynienia wtedy, gdy wydaje się ona pochodzić od zupełnie kogoś innego, od kogo w rzeczywistości pochodzi. Sfałszowanie wiadomość pocztowej jest trywialne, nawet dla nieuprzywilejowanego użytkownika, ponieważ to program pocztowy umieszcza w wiadomości nagłówek określający, od kogo ona pochodzi, kto jest jej adresatem, adres zwrotny oraz datę. W celu dokonania fałszerstwa należy jedynie połączyć się z programem `sendmail` bezpośrednio, z pominięciem programów typu Mail czy Netscape. Po kilku godzinach eksperymentowania można będzie zupełnie ominąć program `sendmail` i połączyć się bezpośrednio z portem 25, przy użyciu protokołu TCP.

Nowsze wersje programu `sendmail` będą przekazywać użytkownikowi komunikat „may be forged", jeżeli różne elementy danych nie zgadzają się ze sobą. Wiele najnowszych konfiguracji programu `sendmail` określa rzeczywisty adres nadawcy oraz rzeczywistą nazwę serwera (za pomocą odwrotnego rozwiązania adresów), tak że będziesz mógł określić, czy dana wiadomość pocztowa została sfałszowana i umieścić ją na liście *Realtime Blackhole List*. Więcej szczegółowych informacji na ten temat zostało przedstawionych w podrozdziale „Fałszowanie adresu nadawcy wiadomości pocztowych" na stronie 234.

W celu nawiązania połączenia z portem 25 oraz wysłania wiadomości może być wykorzystany nawet program `telnet`, co zostało zademonstrowane w zaprezentowanym tu przykładzie. Dokonano w nim sfałszowania wiadomości pocztowej do prezesa firmy Pentacorp, udającej wiadomość wysłaną z Komisji Bezpieczeństwa oraz Wymiany, zawierającą informację, że przeciw firmie rozpoczęte zostało postępowanie w sprawie przestępstw handlowych.

```
telnet mail.pentacorp.com 25
EHLO mail.sec.gov
MAIL From:<jwebb@mail.sec.gov>
RCPT To:<pres@pentacorp.com>
DATA
From jwebb@mail.sec.gov Mon Oct 11 23:53:38 2000
Return-Path: jwebb@mail.sec.gov
Received: (from jwebb) by mail.sec.gov (8.8.9/8.8.9) id XAA19239 \
for pres@pentacorp.com; Mon, 11 Oct 2000 23:43:47 -0500 (EST)
Received: by mail.pentacorp.com (8.8.9/8.8.9) id XAA19239 \
from rootkit.com; Mon, 11 Oct 2000 23:43:58 -0500 (EST)
From: jwebb@mail.sec.gov (Jack Webb)
Message-Id: <200010120443.XAA19239@mail.sec.gov>
Subject: Postępowanie w sprawie przestępstw handlowych
To: pres@pentacorp.com
Date: Mon, 11 Oct 2000 23:43:47 -0500 (EST)

Szanowny Panie Rafale

Pragniemy poinformować Pana, że przeciwko Pana firmie zostało wszczęte postępowanie
z urzędu w sprawie możliwego naruszenia obowiązujących przepisów dotyczących handlu
```

```
wewnętrznego.
Nasi przedstawiciele skontaktują się wkrótce z Panem, pracownikami Pana firmy oraz
Pana brokerem w celu wyjaśnienia wątpliwości.

Z wyrazami szacunku

J. Webb
Starszy Inspektor
800-SEC-0330
```

W pierwszym komunikacie serwer przesyłający wiadomość poda swoją nazwę, lecz — w odróżnieniu od adresu IP — będzie mógł podać dowolną nazwę systemu. Istnieje jednak pewna przydatna funkcja, pozwalająca świadomemu odbiorcy wyśledzić wiadomość. Większość systemów pośredniczących będzie dodawać do nagłówka wiadomości wiersze `Received`. Chociaż osoba fałszująca wiadomość będzie mogła dodać swoje własne wiersze `Received`, to kolejne poprawne systemy dodadzą swoje:

```
Received: by mail.pentacorp.com (8.8.9/8.8.9) id XAA19239 \
from rootkit.com; Mon, 11 Oct 2000 23:43:58 -0500 (EST)
```

Zauważ że system pocztowy firmy Pentacorp dodał prawdziwy nagłówek, który pozwoli wyśledzić, że wiadomość dotarła z serwera *rootkit.com*, choć fałszerz zadał sobie trud, aby dodać nagłówek postaci:

```
Received: (from jwebb) by mail.sec.gov (8.8.9/8.8.9) id XAA19239 \
for pres@pentacorp.com; Mon, 11 Oct 2000 23:43:47 -0500 (EST)
```

Serwery pocztowe przekazujące wiadomość dodadzą poprawną nazwę serwera systemu, z którego ją otrzymały, a niektóre pokażą również adres IP w postaci liczbowej (a to jest już znacznie trudniejsze do sfałszowania). Niektóre systemy pośredniczące odmówią zaakceptowania wiadomości pocztowych z systemów, które nie podadzą poprawnej nazwy w wierszu `EHLO`. Nieliczne dokonają nawet weryfikacji, czy odpowiada ona numerowi IP systemu, z którym zostało nawiązane połączenie. Jedynym sposobem obrony przed tego rodzaju atakiem — oprócz sprawdzania danych podanych w wierszu `EHLO` — jest odpowiednia edukacja użytkowników oraz stosowanie PGP. Należy postarać się o to, by użytkownicy zrozumieli, że tego rodzaju fałszerstwo jest możliwe i nie należy bezgranicznie ufać wiadomościom pocztowym, chyba że są one wysyłane przy użyciu PGP.

5.8.2. Atak realizowany przy użyciu adresu MAC

Poziom zagrożenia: 

Skrót MAC pochodzi od określenia *Media Access Control* (ang. kontrola dostępu do medium) i oznacza rzeczywisty adres karty sieciowej. Czasem nazywa się go także adresem w sieci Ethernet. Jest on reprezentowany za pomocą 6 liczb w systemie szesnastkowym, na przykład: `28:44:29:31:0A:69`. Jest to rzeczywisty adres karty. Jeżeli nie zostanie zmieniony przez program konfiguracyjny, będzie to adres zapisany w pamięci PROM karty. Karta, a tym samym również komputer, otrzymuje dane przeznaczone

dla danego adresu IP komputera jedynie z tej przyczyny, że istnieje protokół pozwalający na skojarzenie adresu IP z adresem MAC. Protokół ten umożliwia systemowi wysyłającemu dane zadać pytanie: „Pod jaki adres MAC powinienem wysłać dane adresowane pod określony adres IP?". Następnie, po uzyskaniu odpowiedzi, system adresuje pakiet wykorzystując adres MAC.

Ataku omawianego tu typu ma miejsce w przypadku, gdy kraker dysponuje kontrolą nad systemem w sieci LAN i zmieni adres MAC (adres Ethernet) udostępniany przez kartę sieciową innym systemom. Jeżeli następnie wyśle pakiety, będą one pojawiać się tak, jakby pochodziły z systemu, pod który kraker się podszywa. W takim przypadku pomaga odłączenie zaatakowanego systemu od sieci komputerowej, uzyskiwane poprzez odłączenie jego karty Ethernet, wyłączenie zasilania lub uszkodzenie systemu. Pamiętaj, że większość kart Ethernet umożliwia zmianę ich adresów MAC; aby ją przeprowadzić, można wykorzystać na przykład parametr `hw ether` polecenia `ifconfig`.

W celu wykrycia ataków tego typu można użyć programu Arpwatch, omówionego w podrozdziale „Wykrywanie ataków ARP i MAC za pomocą programu Arpwatch" na stronie 715. Spójrz również do indeksu i odszukaj wpis *MAC*.

5.8.3. Zmiana pamięci podręcznej ARP

Poziom zagrożenia: ☠☠☠

Na najniższym poziomie dwa komputery używające sieci Ethernet komunikują się ze sobą używając adresów MAC, zwanych niekiedy adresami Ethernet. Adres MAC musi zostać przetłumaczony na adres IP, przedstawiany w postaci czterech liczb oddzielonych kropkami.

Mechanizm ten polega na tym, że w przypadku gdy system X zamierza wysłać wiadomość do systemu o adresie IP `205.180.58.231`, wysyła wiadomość rozgłoszeniową ARP (ang. *address resolution protocol*, czyli protokół rozwiązywania adresów), pytając: „Który komputer ma przydzielony adres IP `205.180.58.231`?"

System o takim adresie IP powinien odpowiedzieć: „Ja mam podany adres, a mój adres MAC to `00:87:72:13:16:F7`". System nadawcy wie w tym momencie, że pakiet danych powinien zostać wysłany na adres MAC `00:87:72:13:16:F7`.

Wszystkie komputery umieszczone w sieci komputerowej powinny nasłuchiwać przesyłanych danych i umieszczać wszystkie odwzorowania w pamięci podręcznej, tak aby nie były zmuszone do wysyłania swoich własnych zapytań. Ominięcie tego zabezpieczenia i oszukanie innego systemu polega na użyciu polecenia `ifconfig eth0 167.192.183.135`.

Jeśli system, który rzeczywiście ma przydzielony adres IP o numerze `167.192.83.135`, nie jest włączony, to komputer, który się pod niego podszywa, nabywa wszystkie jego uprawnienia.

Sprawdź również hasło *MAC* w indeksie.

5.8.4. Zmiana pamięci podręcznej DNS

Poziom zagrożenia: 

Istnieje szereg sposobów, przy użyciu których kraker mógłby sfałszować dane przechowywane w pamięci podręcznej DNS. Jeżeli niektóre z używanych serwerów znajdują się na zewnątrz domeny, możliwe jest wykorzystanie całkiem prostej techniki omówionej przez D. J. Bernsteina (*djb@cr.yp.to*). Jeżeli włamywacz może wpuścić do sieci komputerowej odpowiedzi systemu DNS, to znaczy, że istnieje również wiele innych luk w zabezpieczeniach. Oczywiście jedno z rozwiązań tego problemu polega na wymuszeniu, aby wszystkie serwery w sieci wewnętrznej używały wewnętrznego serwera DNS, a następnie zablokowaniu na serwerze zapory sieciowej wszystkich odpowiedzi przekazywanych przy użyciu portów 53 protokołów UDP oraz TCP pochodzących spoza sieci przesyłanych do komputerów pracujących w sieci wewnętrznej. Większość systemów powinna zablokować w systemie zapory sieciowej wszystkie dane przesyłane z i do sieci internet przy użyciu portu TCP o numerze 53.

Zastosowanie tej poprawki nie jest konieczne, lecz zablokowanie wspomnianych żądań zapobiegnie zmianie danych w pamięci podręcznej DNS przy użyciu fałszywych żądań transferów strefy. (Jeżeli co najmniej jeden spośród twoich serwerów DNS jest udostępniany przez twoją firmę ISP, będziesz zmuszony współpracować z jej przedstawicielami w celu rozwiązania tego problemu.) Bernstain udostępnia swój własny program zastępujący `named`; nazwał go `dnscache`. Możesz pobrać go z witryny umieszczonej pod adresem:

http://cr.yp.to/dnscache.html

Pewne informacje na temat blokowania niepożądanych transferów stref są umieszczone na stronie:

http://www.faqs.org/rfcs/rfc2065.html

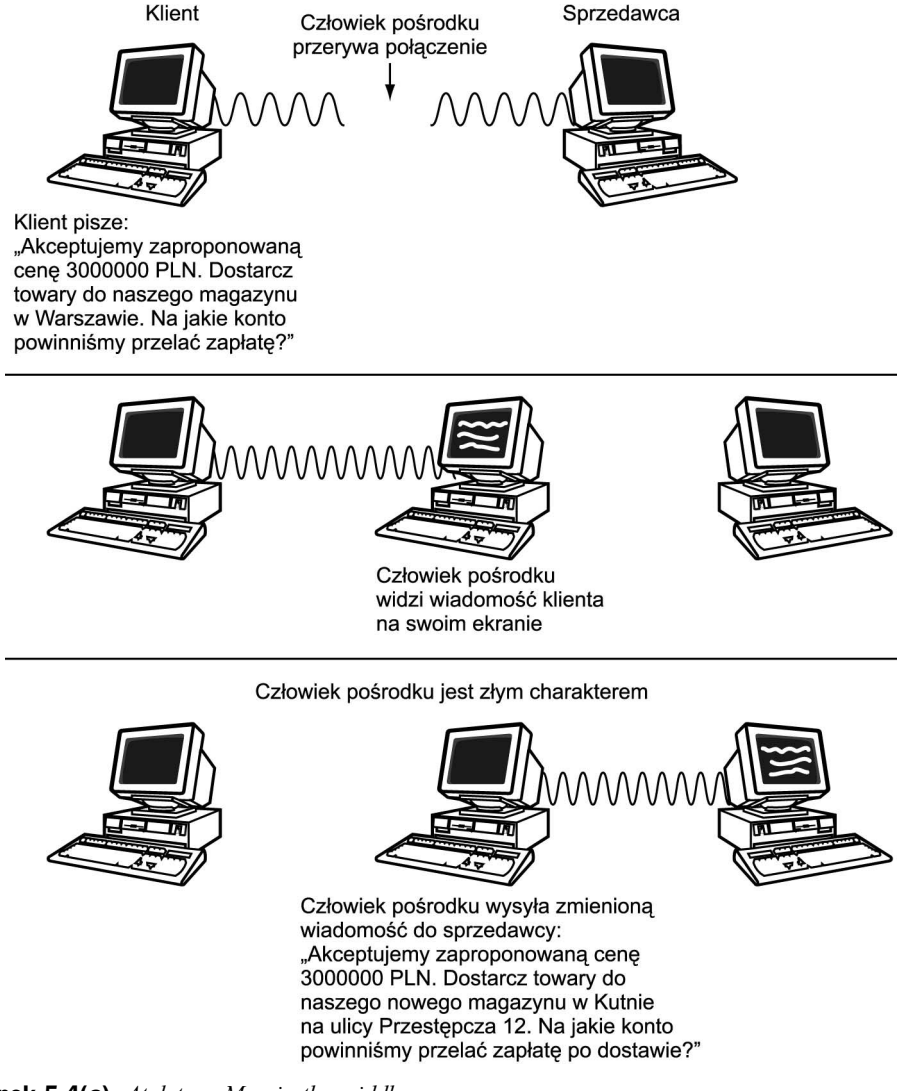
5.9. Atak typu Man-in-the-Middle

Poziom zagrożenia: 

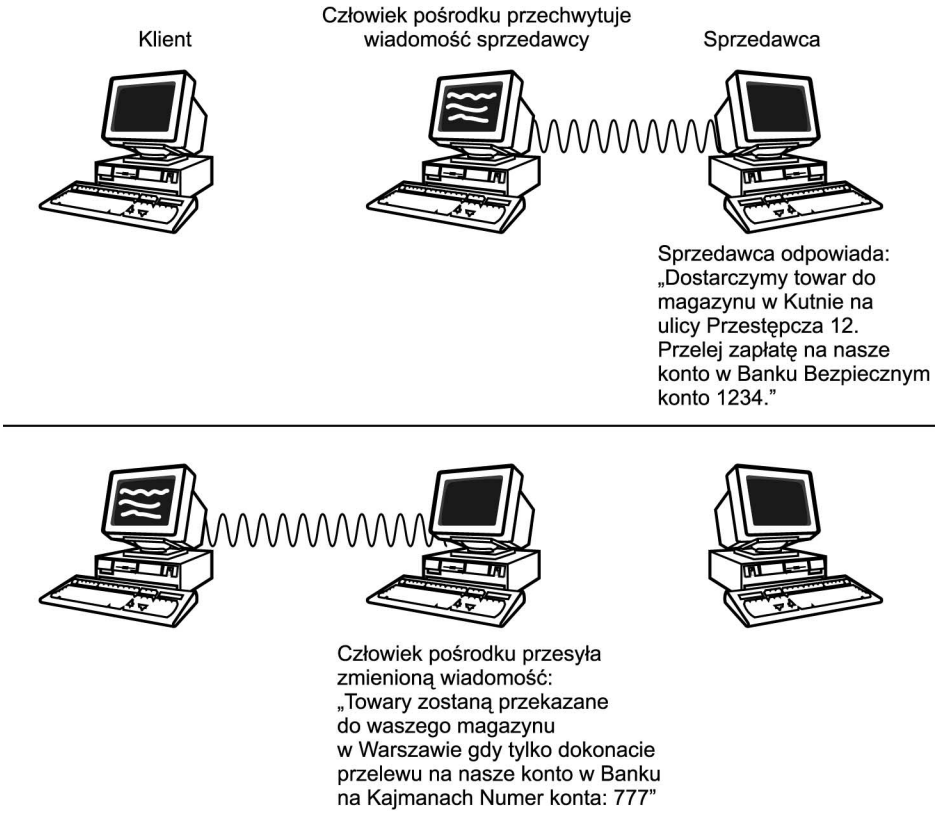
Atak typu Man-in-the-Middle ma miejsce w sytuacji, gdy wychodzące z twojej sieci pakiety nie trafiają do zamierzonego systemu docelowego, lecz raczej do kogoś, kto funkcjonuje jako pośrednik w komunikacji pomiędzy systemem twoim i odbiorcy, udając jednocześnie przed tobą system odbiorcy, a przed odbiorcą twój. Ten „człowiek znajdujący się pośrodku" (ang. *Man in the Middle*) może w takim przypadku kierować

do odbiorcy wiadomości inne niż te, które wysłałeś. Również odpowiedzi od odbiorcy docierają do człowieka znajdującego się pośrodku, który zmienia komunikat i odsyła go do ciebie. Na przedstawionym nieco dalej rysunku 5.4 sprzedawca oraz klient uzgadniają kontrakt biznesowy dotyczący dużej dostawy towarów. Określają adres doręczenia towaru, warunki płatności oraz konto bankowe sprzedawcy, na które ma zostać przelana zapłata za towar.

Zarówno dla sprzedawcy, jak i dla klienta wszystko wydaje się być zwykłą, prostą procedurą. Przeanalizuj rysunek 5.4 i postaraj się określić sposób, w jaki zarówno sprzedawca, jak i klient mógłby odkryć oszustwo.



Rysunek 5.4(a). *Atak typu Man-in-the-middle*



Rysunek 5.4(b). *Atak typu Man-in-the-middle*

Jak widać, ani klient, ani sprzedawca nie ma żadnego pojęcia, że rzeczywistym rozmówcą była niewłaściwa osoba. Ogólnie mówiąc metody uniknięcia takiego problemu wymagają bezpiecznego medium komunikacyjnego (takiego jak poczta polecona lub SSH) lub pewnej weryfikacji informacji, potwierdzającej, że została ona w sposób bezpieczny wymieniona pomiędzy dwiema stronami. Taka weryfikacja mogłaby polegać na użyciu sekretnego algorytmu tworzenia skrótu wiadomości (zobacz podrozdział zatytułowany „ Wykorzystanie GPG do łatwego szyfrowania plików” na stronie 505) lub innej techniki kryptograficznej. Ryzyko przeprowadzenia ataku Man-in-the-middle jest przyczyną, dla której akcentuję w tej książce konieczność zachowania ograniczonego zaufania do wiadomości pocztowych. Dlatego również mamy akty notarialne oraz kontrakty pomiędzy firmami.

Właśnie z tego powodu wynikało również znaczenie pieczęci królewskiej. W rzeczywistości definicja „pieczęci” mówi, że jest nią znak określający autentyczność dokumentu. Tego rodzaju atak może być bardzo trudny do uniknięcia, ponieważ najpierw, zanim nawiążesz pewny i bezpieczny kontakt z odbiorcą, musisz wymienić z nim pewne informacje w sposób mniej godny zaufania. Techniki PGP (GPG), SSH oraz VPN zapobiegną temu atakowi jedynie wtedy, gdy początkowe klucze zostaną wymienione w sposób bezpieczny. Narzędzia tego typu zostaną omówione w podrozdziałach „Pretty Good Privacy (PGP)” na stronie 504, „Wykorzystanie GPG do łatwego

szyfrowania plików" na stronie 505, „Zabezpieczanie sesji użytkownika za pomocą SSH" na stronie 481 oraz „VPN z wykorzystaniem FreeS/WAN IPSec" na stronie 502. Uniknięcie narażenia systemów końcowych oznacza również zabezpieczenie komunikacji pomiędzy każdym z systemów a klawiaturą użytkownika i ekranem. Zazwyczaj oznacza to więc bezpieczną konfigurację systemu X, co zostało omówione w podrozdziale „X oznacza lukę w zabezpieczeniach" na stronie 160.

Bardzo powszechne jest umieszczanie klucza publicznego PGP na domowej stronie WWW, a niektóre osoby dołączają go do wiadomości e-mail. Nie są to dobre rozwiązania. Potwierdzenie klucza publicznego przy użyciu faksu lub telefonu powinno wystarczyć w przypadku średniego stopnia zabezpieczenia aplikacji.

W przypadku aplikacji o wysokich zabezpieczeniach sugerowana jest wymiana kluczy publicznych PGP za pomocą poczty poleconej lub zaufanej firmy kurierskiej. Również rząd Stanów Zjednoczonych traktuje przesyłki polecone jako wystarczająco pewne medium do wysyłania tajnych dokumentów lub wiadomości poufnych, lecz muszą one zostać podwójnie opakowane. Taki wymóg wprowadzono by uniemożliwić sytuację, gdy ktoś przypadkowo otworzy zewnętrzną kopertę i zobaczy w niej poufne informacje.