Rozdział 4
Porty standardowe oraz związane z nimi usługi

Podejrzewam, że po przeczytaniu Rozdziału 1. oraz Rozdziału 3. zaczynasz myśleć, mówić, a może nawet zachowywać się jak haker. Najwyższy więc czas, by zastosować zdobytą wiedzę dla poprawienia bezpieczeństwa własnej sieci. W części tej przyjrzymy się dokładniej mechanizmom powodującym, że porty standardowe oraz odpowiadające im usługi są tak wrażliwe na różnego rodzaju ataki. Następnie, w rozdziale 5., poznasz oprogramowanie, technikę, oraz wiedzę używaną przez hakerów i im podobnych.

Przegląd portów

Porty wejścia-wyjścia są kanałami, przez które przepływają dane pomiędzy różnorodnymi urządzeniami i procesorem. Hakerzy poszukują otwartych, lub „nasłuchujących", a tym samym podatnych na atak portów, aby następnie wykorzystać je do swoich celów. Narzędzia, takie jak np. skanery portów (opisane dokładniej w rozdziale 5.) pozwalają w krótkim czasie przeszukać wszystkie z ponad 65 000 portów komputera. Poszukiwania te skupiają się jednak głównie na pierwszych 1024 portach nazywanych również *portami standardowymi*. Porty te zarezerwowane są dla usług systemowych, z tego też powodu połączenia wychodzące realizowane są poprzez porty o numeracji wyższej niż 1023. Oznacza to również, że wszystkie pakiety przychodzące poprzez porty ponad 1023. są odpowiedzią na wewnętrzne żądania.

Skanowanie portów polega na zebraniu informacji o otwartych, półotwartych oraz zamkniętych portach komputera. Program tego typu wysyła do każdego przeszukiwanego portu zapytanie o jego status. Komputer, nie mając żadnych dodatkowych informacji, automatycznie wysyła żądaną odpowiedź. Ofiara skanowania w, bez żadnych dodatkowych kroków, prawdopodobnie nigdy się o tym nie dowie. W paru kolejnych punktach skupię się na opisaniu najbardziej znanych portów standardowych wraz z odpowiadającymi im usługami i lukami przez nie powodowanymi. Przybliżę też podstawowe techniki wykorzystujące zdobytą wiedzę.

Wiele portów uważanych jest za wystarczająco bezpieczn[illegible]y pominąć je w niniejszym opracowaniu. Zajmiemy się więc jedynie tymi, które mogą stanowić prawdziwe zagrożenie dla bezpieczeństwa systemu.

Porty TCP oraz UDP

Aby połączenie pomiędzy dwoma komputerami mogło dojść do skutku, strona pragnąca nawiązać połączenie musi znać numer portu gospodarza do którego powinna się połączyć. Z tego powodu powstała specjalna lista (opracowana przez IANA[1], a dostępna w RFC1700 oraz pod adresem *ftp://ftp.isi.edu/inotes/iana/assignments*) wiążąca porty standardowe i odpowiadające im usługi lub protokoły internetowe. Z każdym portem można się komunikować na wiele różnych sposobów nazywanych *protokołami*. Istnieją dwa szczególnie powszechne

[1] IANA — Internet Assigned Numbers Authority — jest centralnym koordynatorem przydzielającym unikalne wartości liczbowe związane z protokołami internetowymi.

protokoły internetowe — TCP oraz UDP (opisane odpowiednio w RFC793 i RFC768).

Należy pamiętać o tym, że połączenie przy pomocy protokołu TCP jest realizowane w trzech stopniach pozwalających na dokładne zsynchronizowanie strumienia pakietów wysyłanych przez obie strony. Taki sposób postępowania pozwala otrzymać pewny, stabilny, *zorientowany na połączenie* kanał informacji. Odmienną strategię wykorzystuje protokół UDP. Nie inicjuje się tutaj połączenia, nie ma też pewności, że datagramy będą przychodzić we właściwej kolejności. Wynikiem takiego postępowania jest szybki, *zorientowany na transmisję* kanał informacji.

Tabele 4.1 oraz 4.2 zawierają skróconą listę portów standardowych, odpowiednio TCP i UDP, wraz z usługami z nimi związanymi (pełna lista znajduje się w Dodatku C na końcu tej książki).

Tabela 4.1. Standardowe porty TCP oraz usługi z nimi związane

Numer portu	Usługa TCP	Numer portu	Usługa TCP
7	echo	115	sftp
9	discard	117	path
11	systat	119	nntp
13	daytime	135	loc-serv
15	netstat	139	nbsession
17	qotd	144	news
19	chargen	158	tcprepo
20	FTP-data	170	print-srv
21	FTP	175	vmnet
23	telnet	400	vmnet0
25	SMTP	512	exec
37	time	513	login
42	name	514	shell
43	whois	515	printer
53	domain	520	efs
57	mtp	526	temp
77	rje	530	courier
79	finger	531	conference
80	http	532	netnews
87	link	540	uucp
95	supdup	543	klogin
101	hostnames	544	kshell
102	iso-tsap	556	remotefs
103	dictionary	600	garcon
104	X400-snd	601	maitrd
105	csnet-ns	602	busboy
109	pop2	751	kerberos
110	pop3	752	kerberos-mast
111	portmap	754	krb_prop

113	auth	888	erlogin

Tabela 4.2. Standardowe porty UDP oraz usługi z nimi związane

Numer portu	Usługa UDP	Numer portu	Usługa UDP
7	echo	514	syslog
9	discard	515	printer
13	daytime	517	talk
17	qotd	518	ntalk
19	chargen	520	route
37	time	525	timed
39	rip	531	rvd-control
42	name	533	netwall
43	whois	550	new-rwho
53	dns	560	rmonitor
67	bootp	561	monitor
69	tftp	700	acctmaster
111	portmap	701	acctslave
123	ntp	702	acct
137	nbname	703	acctlogin
138	nbdatagram	704	acctprinter
153	sgmp	705	acctinfo
161	snmp	706	acctslave2
162	snmp-trap	707	acctdisk
315	load	750	kerberos
500	sytek	751	kerberos_mast
512	biff	752	passwd_server
513	who	753	userreg_serve

Luki w bezpieczeństwie związane z portami standardowymi

Na potrzeby książki opisy portów i usług zostaną przedstawione z punktu widzenia hakera. Taka konstrukcja opisów ma za zadanie uświadomić, jakie szanse ma osoba postronna na przełamanie zabezpieczeń i na dostanie się do naszego systemu, lub jego uszkodzenie.

Numer portu: 7

Usługa: echo

Port ten wykorzystywany jest do analizowania bieżącej kondycji połączenia internetowego. Zadaniem usługi jest wysyłanie do nadawcy wszelkich otrzymanych od niego pakietów[1]. Programem wykorzystującym jej właściwości jest PING (Packet InterNet Groper). Podstawowy problem dotyczący tego portu związany jest z

[1] Dokładniejsze informacje na ten temat znajdują się w RFC792

niektórymi systemami operacyjnymi, które dopuszczają przetwarzanie pakietów o nieprawidłowych rozmiarach. Najbardziej znanym sposobem wykorzystania tej luki jest wysłanie do portu ofiary pojedynczego pakietu o rozmiarach przekraczających 65 536 bajtów podzielonego na wiele fragmentów. System operacyjny ofiary nie może oczywiście przetworzyć częściowo otrzymanego pakietu, oczekuje więc na pozostałą część. Jeżeli przydzielony jest statyczny bufor pakietu, powoduje to jego przepełnienie, co w efekcie może doprowadzić do zawieszenia działania systemu, lub ponownego jego uruchomienia. Taktyka taka bardzo często nazywana jest „Ping of Death". Innym poważnym zagrożeniem jest tzw. „Ping Flooding". Sposób ten polega na masowym wysyłaniu w kierunku portu ofiary pakietów PING. Ponieważ usługa odpowiada na każdy pakiet, może to spowodować wyczerpanie zasobów systemowych i sieciowych (np. odcięcie komputera od Internetu, lub spowolnienie jego pracy).

Przykład działania programu PING pokazany jest na rys. 4.1.

```
C:\>ping task.gda.pl

Badanie task.gda.pl [153.19.253.204] z użyciem 32 bajtów danych

Odpowiedź z 153.19.253.204: bajtów=32 czas=762ms TTL=247
Odpowiedź z 153.19.253.204: bajtów=32 czas=763ms TTL=247
Odpowiedź z 153.19.253.204: bajtów=32 czas=693ms TTL=247
Odpowiedź z 153.19.253.204: bajtów=32 czas=704ms TTL=247

Statystyka badania dla 153.19.253.204:
    Pakiety: Wysłane = 4, Odebrane = 4, Utracone = 0 (0% utraconych),
Szacunkowy czas błądzenia pakietów w milisekundach:
    Minimum = 693ms, Maksimum =  763ms, Średnia =  730ms
```

Rys. 4.1 Przykład działania programu ping.

Numer portu: 11

Usługa: systat

Usługa ta została zaprojektowana do udzielania informacji o bieżących procesach. Przy jej pomocy można więc otrzymać informacje np. na temat zainstalowanego w systemie oprogramowania, czy też zalogowanych użytkowników.

Numer portu: 15

Usługa: netstat

Podobnie do usługi połączonej z portem 11, netstat podaje informacje dotyczące pracy systemu operacyjnego, takie jak np. informacje o aktywnych połączeniach, obsługiwanych protokołach, i wiele innych równie przydatnych z punktu widzenia atakującego informacji. Typowy wynik otrzymany z tego portu dla standardowego systemu Windows przedstawiony jest na rys. 4.2.

```
Protokół  Adres lokalny         Obcy adres        Stan
TCP    pavilion:135           PAVILION:0             NASŁUCHIWANIE
TCP    pavilion:1025          PAVILION:0             NASŁUCHIWANIE
TCP    pavilion:1035          PAVILION:0             NASŁUCHIWANIE
TCP    pavilion:1074          PAVILION:0             NASŁUCHIWANIE
TCP    pavilion:138           PAVILION:0             NASŁUCHIWANIE
TCP    pavilion:nbsession     PAVILION:0             NASŁUCHIWANIE
TCP    pavilion:137           PAVILION:0             NASŁUCHIWANIE
UDP    pavilion:1035          *:*
UDP    pavilion:1074          *:*
UDP    pavilion:nbname        *:*
```

```
  UDP    pavilion:nbdatagram   *:*
```

Rys. 4.2 Informacje zdobyte przy pomocy portu usługi netstat dla standardowego systemu Windows.

Numer portu: 19

Usługa: chargen

Port numer 19, oraz związana z nim usługa chargen wydają się być zupełnie nieszkodliwe. Jak sama nazwa wskazuje, działanie tej usługi polega na ciągłym generowaniu strumienia znaków przydatnym podczas testowania połączenia internetowego. Niestety, usługa ta jest podatna na atak przy pomocy bezpośredniego połączenia telnetowego. Jeśli wygenerowany w ten sposób strumień znaków zostanie skierowany np. na port 53 (DNS — Domain Name Service) może to spowodować błąd ochrony w usłudze DNS, a w konsekwencji utratę zdolności systemu do tłumaczenia nazw symolicznych na numery IP i odwrotnie.

Numery portów: 20, 21

Usługi (w kolejności): FTP-data, FTP

Usługi powiązane z portami 20 i 21 stanowią podstawę działania protokołu FTP (File Transfer Protocol). Aby odczytać, lub zapisać plik na serwerze FTP, musi zostać nawiązane równoległe połączenie służące do transmisji danych. Tak więc w typowej sytuacji port 21 służy jedynie do wysyłania rozkazów, oraz odbierania odpowiedzi, podczas gdy rzeczywista transmisja danych odbywa się poprzez port 20. Protokół FTP umożliwia między innymi na kopiowanie, usuwanie i zmianę plików oraz katalogów. W Rozdziale 5. omówione zostaną dokładniej luki w bezpieczeństwie powodowane przez serwery FTP, oraz techniki pozwalające atakującemu niepostrzeżenie kontrolować system plików ofiary.

Numer portu: 23

Usługa: telnet

Usługa właściwa dla portu 23 jest powszechnie znanym protokołem służącym do zdalnego logowania. Telnet działając jako emulator terminalu pozwala na logowanie się, oraz używanie interpretera poleceń na zdalnym systemie. W zależności od prekonfigurowanych ustawień bezpieczeństwa, serwer ten może pozwalać, i z regóły pozwala na kontrolę dostępu do systemu operacyjnego. Niestety, wykonanie specjalnie zaprojektowanych skryptów przygotowanych dla konkretnych wersji serwera potrafi doprowadzić do przepełnienia bufora, co w niektórych wypadkach doprowadza do uzyskania pełnego dostępu do systemu. Przykładem może być program TigerBreach Penetrator (rys. 4.3), który jest częścią pakietu TigerSuite (pakiet ten zamieszczony został na CD dołączonym do książki, a jego dokładniejszy opis znajduje się Rozdziale 12.).

Rys. 4.3 TigerBreach Penetrator w akcji.

Numer portu: 25

Usługa: SMTP

Protokół SMTP (Simple Mail Transfer Protocol) jest głównie używany do przenoszenia poczty elektronicznej. Standardowo serwery SMTP oczekują na przychodzącą pocztę na porcie 25, zaś odebraną pocztę kopiują do odpowiednich skrzynek pocztowych. Jeśli wiadomość nie może zostać dostarczona, nadawcy zwracany jest komunikat błędu zawierający początkowy fragment wiadomości. Po uzyskaniu połączenia poprzez protokół TCP, komputer wysyłający pocztę (klient) czeka na komputer odbierający pocztę (serwer), aby wysłać wiersz tekstu identyfikujący klienta oraz informujący, że klient jest gotowy wysłać pocztę. W mechaniźmie tym sumy kontrolne nie są wymagane do nawiązania kontaktu z powodu wewnętrznych mechanizmów kontrolujących przepływ danych w protokole TCP. Kiedy poczta zostanie w całości odebrana przez serwer, połączenie zostaje zwolnione. Podstawowymi problememi dotyczącymi wymiany poczty elektronicznej są m.in. „mail bombing”[1]

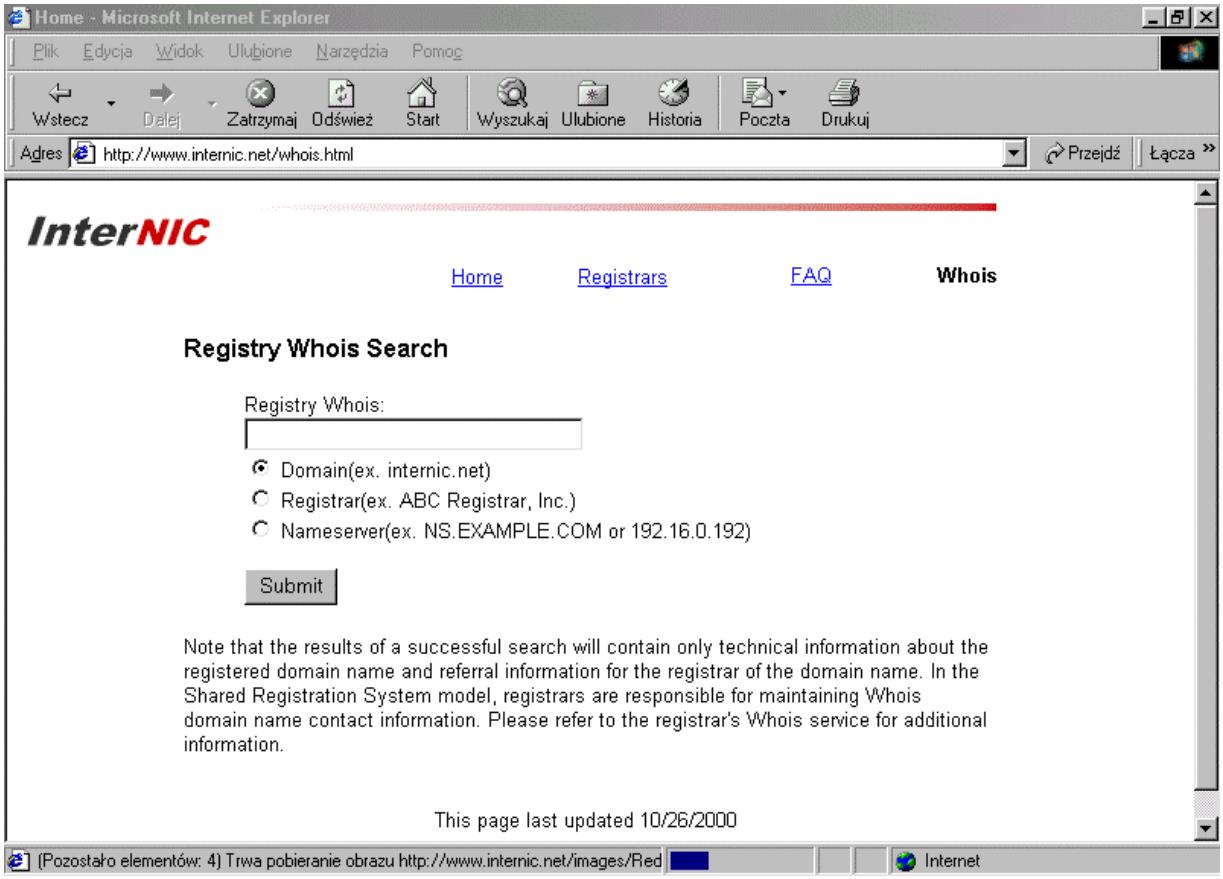
[1] „mail bombing” — atak typu DoS (Denial of Service) wykonywany poprzez wysyłanie na pojedyńczy serwer lub skrzynkę pocztową dużej ilości poczty w celu ograniczenia dostępności serwera, lub przepełnienia skrzynki pocztowej.

oraz „mail spamming”[1], ale nie brakuje również wielu innych ataków typu DoS (Denial of Service)[2]. Problemy te zostaną dokładniej omówione w dalszej części książki.

Numer portu: 43

Usługa: whois

Usługa Whois (*http://rs.Internic.net/whois.html*) jest opartym na protokole TCP serwerem działającym na zasadzie „pytanie-odpowiedź” pracującym na niewielkiej liczbie specyficznych komputerów centralnych. Jej zadaniem jest udostępnianie informacji o usługach dostępnych w sieci. Wiele domen utrzymuje swoje własne serwery Whois zawierające informacje o usługach lokalnych. Serwisy tego typu są wykorzystywane przez hakerów i im podobnych podczas zbierania informacji o potencjalnych ofiarach. Najpopularniejsze i największe bazy danych Whois dostępne są na serwerze InterNIC (rys. 4.4).



Rys. 4.4 Na tej stronie można wysyłać zapytania do usługi Whois położonej na serwerze InterNIC.

Numer portu: 53

Usługa: domain

Nazwa domeny jest ciągiem znaków identyfikującym jeden lub więcej adresów IP. Istnienie takiej usługi jest uzasadnione choćby z tego powodu, że łatwiej jest zapamiętać nazwę symboliczną domeny, niż cztero- lub

---

[1] „mail spamming” — to nie jest atak sam w sobie. „mail spamming” to wysyłanie dużej ilości w gruncie rzeczy zbędnej poczty (takiej, jak np. reklamy) na skrzynki pocztowe wielu użytkowników przyczyniając się do obciążenia serwerów i przepełniania skrzynek.

[2] Celem ataku typu DoS jest zablokowanie możliwości korzystania z określonych, lub wszystkich usług atakowanego serwera, lub nawet doprowadzenie serwera do stanu, w którym atakujący będzie mógł poszerzyć swoje uprawnienia do korzystania z serwera (z uzyskaniem uprawnień administratora włącznie).

sześcioczłonowy[1] adres IP. Zadaniem usługi DNS (Domain Name Service) jest tłumaczenie nazw symbolicznych na adresy IP i odwrotnie. Tak jak to zostało wyjaśnione w poprzednich rozdziałach, datagramy wędrujące poprzez sieć Internet używają adresów IP, dlatego też każdorazowo gdy użyty zostaje adres symboliczny, należy przetłumaczyć go na odpowiadający mu adres IP. W uproszczeniu — kiedy użytkownik wprowadza adres symboliczny, na przykład w przeglądarce, nazwa symboliczna wysyłana zostaje do serwera DNS, który po odszukaniu odpowiedniego rekordu w swojej bazie danych odsyła właściwy adres IP. Niedawno prowadzono śledztwo w sprawie podmieniania adresów DNS[2]. Podmienianie datagramów wędrujący od, lub do serwera DNS daje atakującemu, przykładowo, możliwość oszukania użytkownika próbującego połączyć się ze swoim serwerem pocztowym. Tak naprawdę będzie się próbował połączyć do innego serwera, zdradzając przy okazji hasło do swojego konta pocztowego. Częste są też przypadki różnego rodzaju ataków typu DoS, powodujących czasami niedostępność usługi DNS. Przykład typowego zapytania DNS pokazany jest na rys 4.5.

```
Lista odpowiedzi:

Nazwa zasobu: tigertools.net
Typ: A  Klasa: IN
Adres IP: 207.155.252.47

Nazwa zasobu: tigertools.net
Typ: A  Klasa: IN
Adres IP: 207.155.252.14

Nazwa zasobu: tigertools.net
Typ: A  Klasa: IN
Adres IP: 207.155.248.7

Nazwa zasobu: tigertools.net
Typ: A  Klasa: IN
Adres IP: 207.155.248.9
```

Rys. 4.5 Typowa odpowiedź na zapytanie DNS.

Numer portu: 67

Usługa: bootp

Protokół bootp pozwala komputerom bez pamięci stałej na otrzymanie własnego adresu IP. Serwer bootp rozpoznaje takie maszyny na podstawie ich konfiguracji sprzętowej (najczęściej jest to adres MAC[3]). Słabym punktem protokołu bootp jest moduł kernela, który podatny jest na przepełnienia bufora, powodujące błędy systemu. Jakkolwiek większość tego typu przypadków jest wynikiem ataków z sieci lokalnej, starsze systemy mogą być również podatne na ataki z Internetu.

Numer portu: 69

Usługa: tftp

Protokół TFTP (Trivial File Transfer Protocol) jest uproszczoną wersją protokołu FTP służącą głównie do inicjowania i uaktualniania systemów operacyjnych różnego rodzaju urządzeń sieciowych (głównie ruterów i przełączników). TFTP został zaprojektowany tak, aby było możliwe zaimplementowanie go do pamięci ROM.

---

[1] Nowa wersja protokołu IP — IPv6 przewiduje 6 bajtów adresu w przeciwieństwie do 4 w używanym powszechnie protokole IPv4.

[2] Podmienianie adresów DNS określa się jako „DNS spoofing". „Spoofing" polega na podmienianiu pakietów na odcinku pomiędzy serwerem i klientem.

[3] Adres MAC (Media Access Control) jest sześcio-bajtowym unikalnym numerem identyfikacyjnym niejako „wbudowanym" w każdą dostępną na rynku kartę sieciową.

Pozwala to wprawdzie na inicjowanie urządzeń nie posiadających pamięci dyskowej, ponieważ jednak urządzenia tego typu nie mogą się posiadać własnej nazwy użytkownika i hasła, protokół ten nie posiada jakiejkolwiek kontroli dostępu. Przy pomocy prostych sztuczek każdy użytkownik Internetu może skopiować ważne dla bezpieczeństwa systemu pliki (np. */etc/passwd*).

Numer portu: 79

Usługa: finger

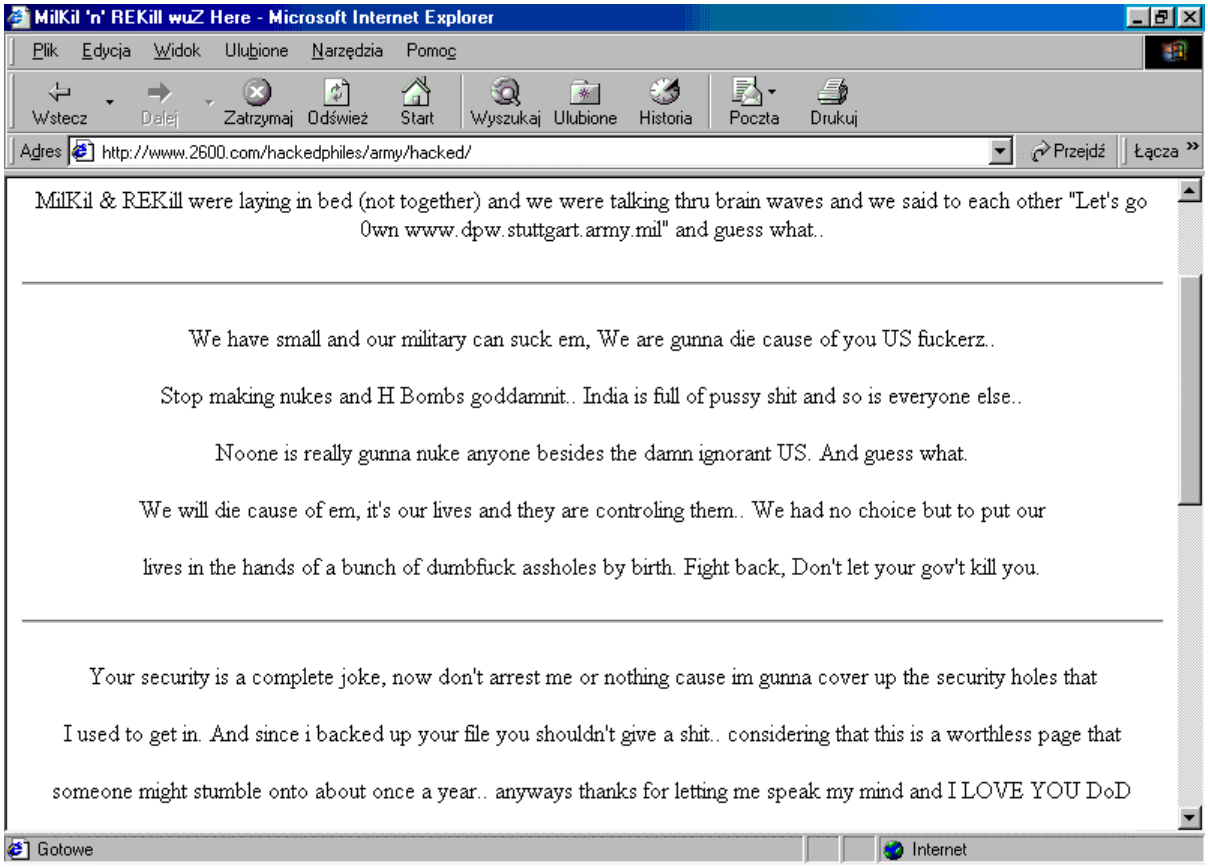
Finger jest usługą podającą informacje o kontach użytkowników. Informacje udzielane przez tą usługę w dużej mierze zależą od wersji i konfiguracji serwera, oraz preferencji użytkownika. Jednakże w większości przypadków można otrzymać co najmniej część informacji spośród takich, jak: pełna nazwa użytkownika, adres, numer telefonu, oraz informację, czy użytkownik jest w danym momencie zalogowany na serwerze. Operacja otrzymywania informacji poprzez protokół finger jest bardzo prosta: klient otwiera połączenia do serwera i wysyła odpowiednie zapytanie, po czym serwer przetwarza zapytanie, wysyła odpowiedź i zamyka połączenie. Przykład danych otrzymanych przy pomocy tej usługi przedstawiony został na rys. 4.6. Część informacji została zakryta dla zachowania anonimowości użytkownika.

Rys. 4.6 Przykładowa odpowiedź na zapytanie serwera finger.

Numer portu: 80

Usługa: http

Protokół HTTP (Hypertext Transfer Protocol) stanowi serce ogólnoświatowej sieci WWW (World Wide Web). Działanie serwera HTTP polega na przyjmowaniu od klientów i wykonywaniu pojedyńczych rozkazów. Każdy rozkaz jest wykonywany niezależnie od pozostałych. Dobrym przykładem działania serwera jest otwarcie dowolnej strony WWW po wprowadzeniu w oknie przeglądarki właściwego adresu URL. Powoduje to wysłanie do serwera komendy inicjującej pobranie z serwera określonego przez URL pliku (strony WWW). Jednym z problemów związanych z serwerami HTTP są przypadki podmieniania stron udostępnianych na serwerach. Przykład można znaleźć na stronie *www.2600.com/hacked_pages* (podmieniona strona Armii Stanów Zjednoczonych — rys. 4.7).



Rys. 4.7 Podmieniona strona armii Stanów Zjednoczonych.

Numery portów: 109, 110

Usługi (w kolejności): pop2, pop3

POP (Post Office Protocol) jest protokołem służącym do przenoszenia poczty elektronicznej z serwera pocztowego na komputer użytkownika. Z historycznych powodów istnieją dwie wersje protokołu POP: POP2 (zaproponowany w dokumencie RFC937 z 1985 roku), oraz nowszy — POP3 (opisany w RFC1939). Podstawowa różnica pomiędzy nimi polega na tym, że korzystanie z protokołu POP2 wymaga uruchomionego serwera SMTP, w przeciwieństwie do POP3, który może samodzielnie odbierać pocztę. Protokół POP oparty jest na architekturze klient-serwer, w której pocztę odbiera serwer pocztowy, a następnie przechowuje ją do momentu, w którym użytkownik zaloguje się na serwerze i ją pobierze. Większość współczesnych przeglądarek internetowych posiada wbudowaną obsługę protokołu POP3 (należą do nich m.in. produkty Netscape'a i Microsoftu). Niedociągnięcia w protokole pozwalają na zdalne zalogowanie się na serwerze nawet wtedy, gdy zmienione zostało hasło dostępu do skrzynki pocztowej. Port usługi POP3 jest również podatny na atak przy pomocy bezpośredniego połączenia telnetowego, możliwe jest wtedy uzyskanie niektórych ważnych z punktu widzenia bezpieczeństwa systemu informacji (rys. 4.8).

```
+OK.   XXX   POP3 server (Netscape Massaging Server - Version 3.6) ready at. 26 Aug 2000
14:13:05-0500
```

Rys. 4.8 Bezpośrednie połączenie może zdradzić wiele krytycznych dla bezpieczeństwa systemu informacji.

Numery portów: 111, 135

Usługi (w ko  ści): portmap, loc-serv

Głównym zadaniem usługi portmap jest tłumaczenie numerów identyfikacyjnych RPC (Remote Procedure Call — system zdalnego wywoływania procedur) na odpowiadające im numery portów. Kiedy uruchomiony zostanie serwer zgodny ze standardem RPC[1] przekazuje on swój numer identyfikacyjny usłudze portmap, która w odpowiedzi przydziela mu właściwy numer, lub numery portów, które program może obsługiwać. Z tego powodu portmap musi znać kompletną listę zarejestrowanych usług i przydzielone do nich porty. Loc-serv jest odmianą usługi portmap używaną w systemie operacyjnym Windows NT. Bez należytej kontroli dostępu do usługi portmap możliwe jest przechwycenie bieżącej nazwy domeny NIS, co w pewnych okolicznościach może pozwolić atakującemu na skopiowanie pliku haseł (*/etc/passwd*).

Numery portów: 137, 138, 139

Usługi (w kolejności): nbname, nbdatagram, nbsession

Usługa związana z portem numer 137 (nbname), nazywana też WINS lub serwisem nazw NetBIOS, używana jest głównie w systemach opartych na systemie operacyjnym Windows jako alternatywa dla usługi DNS. Węzły TCP/IP protokołu NetBIOS używają pakietów UDP rozprzestrzenianych przez komputery z portu numer 137 do rozpoznawania ich nazw. Wadą tego rozwiązania jest brak właściwej identyfikacji komputerów w sieci. Każdy komputer może bowiem rozprzestrzeniać swoje własne pakiety identyfikacyjne w imieniu innego komputera, lub w jego imieniu wysyłać odpowiedzi na zapytania, nim prawdziwy adresat zapytań będzie w stanie na nie odpowiedzieć. W uproszczeniu: nbname jest używane do rozprzestrzeniania nazw komputerów w sieci, nbdatagram — do dystrybucji pozostałych informacji, nbsession służy zaś do właściwej komunikacji, i przesyłania zasobów. Wykonanie komendy `netstat -a` (przykład na Rys. 4.9) na komputerze z uruchomionym systemem operacyjnym Windows może potwierdzić powyższe informacje, a nawet ujawnić potencjalne zakażenie koniem trojańskim.

```
C:\>netstat -a


Aktywne połączenia
```

[1] Programy takie posiadają swoje własne, unikalne numery identyfikacyjne (zarządzane przez Sun Microsystems, Inc). Dokładniejsze informacje na temat standardu RPC dostępne są w RFC1831.

```
Protokół  Adres lokalny         Obcy adres        Stan
TCP    ursa:epmap             ursa:0                 NASŁUCHIWANIE
TCP    ursa:microsoft-ds      ursa:0                 NASŁUCHIWANIE
TCP    ursa:1025              ursa:0                 NASŁUCHIWANIE
TCP    ursa:1027              ursa:0                 NASŁUCHIWANIE
TCP    ursa:netbios-ssn       ursa:0                 NASŁUCHIWANIE
UDP    ursa:epmap             *.*
UDP    ursa:microsoft-ds      *.*
UDP    ursa:1026              *.*
UDP    ursa:microsoft-ns      *.*
UDP    ursa:microsoft-dgm     *.*
UDP    ursa:isakmp            *.*
```

Rys. 4.9 Przykładowy wynik wykonania polecenia `netstat -a`.

Numer portu: 144

Usługa: news

Usługa news (Network-extensible Window System) jest nakładką okienkową na system operacyjny UNIX opracowaną przez Sun Microsystems. Jej jądro stanowi wielowątkowy interpreter języka PostScript z możliwością obsługi grafiki ekranowej oraz nawet bardzo skomplikowanych zdarzeń wejściowych. Istnieją powody, by obawiać się ataków hackerów skierowanych na tą usługę.

Numery portów: 161, 162

Usługi (w kolejności): snmp, snmp-trap

Simple Network Management Protocol (SNMP) jest, w skrócie, protokołem służącym do zarządzania i monitorowania urządzeń sieciowych. Jego działanie opiera się na wysyłaniu do różnych urządzeń sieciowych (agentów) specjalnych wiadomości. Urządzenia te przechowują bazy danych informacji o sobie, za pomocą których w razie potrzeby udzielają odpowiedzi na zapytania serwerów SNMP koordynujących pracą sieci. Ponieważ poprzez protokół SNMP transmituje się bardzo ważne dla pracy sieci dane, porty te cieszą się zainteresowaniem ze strony hakerów, dają potencjalnie duże możliwości do nadużyć (takich jak np. przekonfigurowywanie urządzeń sieciowych).

Numer portu: 512

Usługa: exec

Port numer 512 jest używany przez funkcję rexec() do zdalnego wykonywania poleceń. Jeśli port bardzo często nasłuchuje, lub jest aktywny, może to oznaczać że serwer startuje automatycznie. W takich przypadkach sugeruje to pracę *X-Windows*. Jeśli na dodatek port ten nie jest w żaden dodatkowy sposób chroniony, możliwe jest np. zdalne robienie zrzutów ekranowych, przechwytywanie bufora klawiatury, a nawet uruchamianie programów. Dla informacji — jeśli usługa exec jest dostępna w systemie, a dodatkowo port 6000 akceptuje połączenia telnetowe możliwy jest atak DoS z możliwością zawieszenia działania systemu włącznie.

Numery portów: 513, 514

Usługi (w kolejności): login, shell

Porty 513 i 514 są uważane za uprzywilejowane, gdyż za ich pomocą możliwe jest zdalne wykonywanie poleceń na systemach typu UNIX. Z tego też powodu porty te są celem bardzo wielu różnego rodzaju ataków, szczególnie podmieniania pakietów. Port 514 używany jest przez usługę rsh, działającą jako interaktywna powłoka, dostępna bez jakiejkolwiek konieczności logowania. Identyfikację przeprowadza głównie przy pomocy adresu klienta (stąd częste przypadki „spoofingu”). Obecność tej usługi w systemie sugeruje aktywność serwera *X-Windows*. Korzystając z tradycyjnych metod, przy użyciu jedynie telnetu możliwe jest nawiązanie połączenia z usługą (rys. 4.10 — część danych została zakryta dla zachowania anonimowości celu ataku).

```
Trying XXX.XXX.XXX.XXX
Connected to XXX.XXX.XXX.XXX

Escape character is '^]'
```

Rys. 4.10 Przykład udanego sprawdzenia statusu określonego portu (port otwarty).

Numer portu: 514

Usługa: syslog

Jako część wewnętrznego mechanizmu rejestracji zdarzeń, port 514 może być celem ataków typu DoS. Podatność na ataki tego typu sprawdzić można w prosty sposób przy pomocy skanera UDP.

Numery portów: 517, 518

Usługi (w kolejności): talk, ntalk

Serwery talk są interaktywnymi programami komunikacyjnymi zadaniem których jest umożliwianie konwersacji w trybie tekstowym i czasie rzeczywistym pomiędzy dwoma użytkownikami systemów UNIX. Całość składa się z serwera oraz klienta talk (nowsze serwery — ntalk — nie są kompatybilne z poprzednimi wersjami). Mimo, że serwer wydaje się być bezpiecznym, w rzeczywistości tak nie jest — klient inicjuje połączenie z serwerem poprzez przypadkowy port TCP co daje pole dla różnego rodzaju zdalnych ataków.

Numer portu: 520

Usługa: route

Proces wyznaczania tras pakietów pomiędzy dowolnymi dwoma komputerami w Internecie realizowany jest przy pomocy ruterów, oraz specjalnego protokołu, kontrolującego przesył danych o bieżącej topologii sieci pomiędzy sąsiadującymi ruterami. Chyba najczęściej używanym w takich sytuacja protokołem jest RIP (Routing Information Protocol), używający portu UDP numer 520. Również wiele ruterów sprzętowych używa do komunikacji tego samego portu. Dzięki programom przechwytującym pakiety w sieci można uzyskać bardzo ważne dane na temat topologii sieci.

Numer portu: 540

Usługa: uucp

Protokół uucp (UNIX-to-UNIX Copy Protocol) wymaga zestawu programów do transmisji plików pomiędzy różnymi systemami UNIX-owymi lecz, co ważniejsze, również wykonywania poleceń na zdalnych systemach. I mimo, że protokół ten został wyparty przez inne, bardziej uniwersalne i poręczne, takie jak na przykład FTP i SMTP, na wielu systemach dalej spotyka się aktywną usługę UUCP używaną w celach administracyjnych. W zależności od systemu i wersji serwera istnieją różne sztuczki pozwalające użytkownikom kont UUCP na powiększenie swoich uprawnień.

Numery portów: 543, 544, 750

Usługi (w kolejności): klogin, kshell, kerberos

Usługi powiązane z powyższymi portami reprezentują system identyfikacji Kerberos. Głównym założeniem tego projektu jest stworzenie środowiska pozwalającego na bezpieczną wymianę poufnych informacji przy pomocy sieci publicznej. Metoda polega na przydzielaniu każdemu użytkownikowi unikalnych kluczy lub tzw. „biletów". Następnie, dla identyfikacji i autentyfikacji, dane są przy pomocy tychże biletów szyfrowane. Należy jednakże filtrować dostęp do tych portów, gdyż podatne są one na różnego rodzaju ataki, włączając w to przepełnienia buforów, podmienianie pakietów, ukryte sesje i podkradanie biletów[1].

---

[1] W nowocześniejszych metodach stosuje się dodatkowy element bezpieczeństwa — bilety (hasła) jednorazowe — dzięki takiemu postępowaniu podkradanie biletów staje się w znacznej mierze nieskuteczne.

Niezidentyfikowane usługi

Różnego rodzaju programy hakerskie, których celem jest przedostanie się do systemu ofiary, zwykle zaprojektowane są do zainstalowania w systemie tylnych drzwi lub innej luki w bezpieczeństwie. Nie zawsze wprawdzie intencje atakującego są groźne, może on jednak działać złośliwie i wyrządzić poważne szkody. Oprogramowanie opisane w tej części zaklasyfikować można do jednej z trzech kategorii: wirusów, robaków i koni trojańskich. Podział ten zostanie dokładniej omówiony w dalszych częściach książki. Na razie wystarczy wiedzieć, że:

- *wirusy* są programami rozprzestrzeniającymi się poprzez zarażanie innych programów, użytkowych lub też systemowych,
- *robaki* potrafią się rozprzestrzeniać nie wymagając przy tym nosiciela, potrafią również już w momencie infekcji kompilować swój kod, lub w inny sposób rozprzestrzeniać swoje kopie, zachowując w ten sposób cokolwiek duże tempo rozprzestrzeniania,
- *konie trojańskie* są zwykłymi (lub wyglądającymi na zwykłe) programami, udającymi często przydatne oprogramowanie, lecz wykonującymi pewne operacje bez wiedzy ich użytkownika.

Większość programów opisanych w tej części książki dostępna jest na płycie CD dołączonej do książki, lub poprzez TigerTools Repository, które jest również dostęne na płycie CD.

Numery portów: 21, 5400-5402

Programy: Back Construction, Blade Runner, Fore, FTP Trojan, Invisible FTP, Larva, WebEx, WinCrash

Programy te (pokazane na rys. 4.11) używają głównie portu 21, funkcjonalnie stanowią zaś serwery FTP. Dzięki temu atakujący może kopiować pliki na komputer ofiary, jak i w odwrotnym kierunku. Niektóre z tych programów posiadają moduły serwera, jak również klienta, większość z nich używa kluczy *Rejestru Systemowego*. Przykładowo, powszechne wersje programu Blade Runner używają jako punktu startowego następującego klucza *Rejestru*:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
```

Rys. 4.11 Back Construction, Blade Runner oraz WebEx.

Numer portu: 23

Program: Tiny Telnet Server (TTS)

TTS jest emulatorem terminala pozwalającym na zdalne wykonywanie poleceń tak, jak gdyby były one wykonywane lokalnie na zainfekowanym systemie. Wykonywane komendy mają uprawnienia administratora, lub użytkownika uprzywilejowanego. Program instaluje się jako *C:\WINDOWS\windll.exe*. Używa też następującego klucza *Rejestru*:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run -
windll.exe="C:\WINDOWS\windll.exe"
```

Numery portów: 25, 110

Programy: Ajan, Antigen, Email Password Sender, Haebu Coceda, Happy 99, Kuang2, ProMail Trojan, Shtirlitz, Stealth, Tapiras, Terminator, WinPC, WinSpy

Ukrywając się pod postacią dowcipu, lub ładnej grafiki programy te przesyłają atakującemu hasła systemowe, pozwalają mu kontrolować skrzynki pocztowe użytkowników, przechwytują sekwencje naciskanych kawiszy, pozwalają inicjować ataki typu DoS, i stanowią zdalne lub lokalne tylne wejście do systemu. Każdy z wyżej wymienionych programów używa różnych nazw dla swoich plików, różnych kluczy *Rejestru* i różnej przestrzeni pamięci operacyjnej. Jedynym elementem wiążącym jest współużywany port TCP numer 25.

Numery portów: 31, 456, 40421-40426

Programy: Agent31, Hackers Paradise, Masters Paradise

Tego rodzaju złośliwe programy, używające portu 31 obejmują swoim działaniem zdalną administrację, jak na przykład przekierowywanie aplikacji i plików czy edycję *Rejestru Systemowego* (na rys. 4.12 znajduje się przykład systemu zdalnej administracji z możliwością przeglądania usług zakażonego komputera). W wypadku zarażenia atakujący może przejąć pełną kontrolę nad systemem swojej ofiary...

Rys. 4.12 Kontrolowanie ofiary przy pomocy portu 31 może być dla niej wielce szkodliwe.

Numery portów: 41, 999, 2140, 3150, 6670-6671, 60000

Program: Deep Throat

Deep Throat posiada wiele funkcji, włączając w to ukryty serwer FTP (z możliwością kasowania plików, oraz kopiowania w obie strony). Z pozostałych funkcji wymienię choćby możliwość zdalnego robienia zrzutów ekranu, podglądania haseł, operowania przeglądarką internetową, wyłączania komputera a nawet kontrolowanie obsługi zdarzeń innych uruchomionych programów.

Rys. 4.13 Panel kontrolny programu Deep Throat.

Numer portu: 59

Program: DMSetup

DMSetup został zaprojektowany, by udawać klienta mIRC. Raz uruchomiony, instaluje się w różnych miejscach drzewa katalogów powodując duże spustoszenia w plikach startowych i jednocześnie uszkadzając pliki konfiguracyjne programu mIRC. W rezultacie zaś program stara się rozprzestrzenić do wszystkich osób kontaktujących się z zarażonym komputerem.

Numery portów: 79, 5321

Program: Firehotker

Program ten znany jest również jako Firehotker Backdoorz. Prawdopodobnie został zaprogramowany jako narzędzie służące do zdalnej administracji systemem zainfekowanego komputera, lecz w większości przypadków jedynie zużywa zasoby spowalniając działanie systemu. Program występuje pod postacią pliku *server.exe* nie używając przy tym kluczy *Rejestru*.

Numer portu: 80

Program: Executor

Ten bardzo niebezpieczny program, służący do zdalnego wykonywania poleceń, powstał z myślą o zniszczeniu plików systemowych i konfiguracyjnych zaatakowanego komputera. (rys. 4.14). Serwer instaluje się jako plik *sexec.exe* używając jednocześnie następującego klucza *Rejestru*:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run -
<>Executer1="C:\windows\sexec.exe"
```

Rys. 4.14 Executor jest zawsze gotowy by zniszczyæ twoje pliki systemowe.

Numer portu: 113

Program: Kazimas

Kazimas jest robakiem rozprzestrzeniającym się pomiędzy użytkownikami mIRC-a. Występuje pod postacią pliku *milbug_a.exe*, o rozmiarach w przybliżeniu 10 KB. Po zarażeniu kopiuje się do następujących katalogów:

```
C:\WINDOWS\kazimas.exe
C:\WINDOWS\SYSTEM\psys.exe
C:\icqpatch.exe
C:\MIRC\nuker.exe
C:\MIRC\DOWNLOAD\mirc60.exe
C:\MIRC\LOGS\logging.exe
```

```
C:\MIRC\SOUND\player.exe
C:\GAMES\spider.exe
C:\WINDOWS\freemem.exe
```

Program uszkadza pliki konfiguracyjne mIRC-a, i stara się rozprzestrzenić do wszystkich użytkowników komunikujących się z zarażoną maszyną.

Numer portu: 119

Program: Happy99

Happy99 ukrywa swoją destrukcyjną naturę udając nieszkodliwy program wyświetlający okno i sekwencję ogni sztucznych. W tle zaś instaluje się jako aplikacja udostępniająca atakującemu hasła systemowe, dostęp do poczty elektronicznej, obsługę ataków DoS, oraz tylne wejście do systemu operacyjnego ofiary.

Rys. 4.15 Happy99 ukrywający się ukrywający się pod postacią seerii bardzo efektownych ogni sztucznych.

Numer portu: 121

Program: JammerKillah

JammerKillah jest koniem trojańskim opracowanym i skompilowanym dla unieszkodliwienia programu Jammer. Po wykonaniu odszukuje i unieszkodliwia programy Back Orifice oraz NetBus.

Numery portów: 531, 1045

Program: Rasmin

Wirus ten, napisany w Visual C++, używa portu TCP numer 531 (normalnie używany przez usługę konferencji). Chodzą pogłoski, że serwer ten pozostaje bierny do momentu otrzymania specjalnego rozkazu od swojego twórcy. Badania wykazały, że ukrywa się pod następującymi nazwami plików:

```
Rasmin.exe
Wspool.exe
Winsrvc.exe
Inipx.exe
Upgrade.exe
```

Numery portów: 555, 9989

Programy: Ini-Killer, NeTAdmin, phAse Zero (na rys. 4.16), Stealth Spy

Głównym zadaniem tych programu, poza szpiegowaniem i kopiowaniem plików, jest zniszczenie zaatakowanego systemu. Należy więc pamiętać, że jedynym sposobem, by zarazić się trojanem, jest jego uruchomienie.

Rys. 4.16 Niektóre możliwości programu phAse Zero.

Numer portu: 666

Programy: AttackFTP, Back Construction, Cain&Abel, Satanz Backdoor (rys. 4.17), ServeU, Shadow Phyre

Działanie AttackFTP ogranicza się do zainstalowania serwera FTP z pełnymi prawami do kopiowania w obie strony. Back Costruction został omówiony przy okazji portu 21. Cain został napisany do przechwytywania haseł, podczas gdy Abel jest serwerem umożliwiającym pełny dostęp do plików ofiary. Oba programy (Cain&Abel) nie potrafią się replikować. Satanz Backdoor, ServeU i Shadow Phyre znane są z tego, że instalują serwery umożliwiające zdalny dostęp, zużywając przy tym bardzo niewiele zasobów systemowych.

Rys. 4.17 Satanz Backdoor.

Numer portu: 999

Program: WinSatan

WinSatan jest programem potrafiącym łączyć się do różnych serwerów IRC, pozostawiając połączenia nawet po własnym zamknięciu. Program uruchamia się w tle, bez jakichkolwiek śladów w *Menadżerze Zadań*. Po krótkiej obserwacji można zauważyć, że program jedynie rozprzestrzenia się, zużywając zasoby i powodując chaos w systemie.

Numery portów: 1001

Programy: Silencer, WebEx

WebEx został już opisany przy okazji portu 21. Silencer służy zaś do zdalnej kontroli zasobów, i jako taki ma bardzo ograniczone funkcje (rys. 4.18).

Rys. 4.18 Silencer został napisany do zdalnej kontroli zasobów.

Numery portów: 1010-1015

Program: Doly Trojan

Ten trojan znany jest z umiejętności przejmowania całkowitej kontroli nad zainfekowanym komputerem, z tego też powodu uważany jest za jeden z najbardziej niebezpiecznych. Program używa różnych portów, potrafi też prawdopodobnie zmieniać nazwę swojego pliku. Do *Rejestru Systemowego* dołączany jest podczas instalacji Doly Trojan następujący klucz[1]:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run - tesk.exe
```

Rys. 4.19 Opcje programu Doly Trojan.

Numery portów: 1024, 31338, 31339

Program: NetSpy

NetSpy (rys. 4.20) jest kolejnym serwerem przeznaczonym do szpiegowania zarażonego systemu. Program pozwala atakującemu na zdalne kontrolowanie nawet do 100 komputerów. NetSpy posiada m.in. następujące możliwości:

- pokazuje listę otwartych i zminimalizowanych okien,
- pozwala zmieniać katalog roboczy,
- pozwala na zdalną kontrolę serwera (włącznie z jego natychmiastowym usunięciem),
- pozwala uzyskać pełną listę plików i katalogów,
- pozwala uzyskiwać podstawowe informacje na temat systemu,
- pozwala wysyłać komunikaty użytkownikowi zarażonego komputera,
- pozwala ukrywać i pokazywać klawisz *Start*,
- pozwala ukrywać *pasek zadań*,
- pozwala wykonać (i ukryć) dowolną aplikację Windows lub DOS.

Rys. 4.20 Klient NetSpy.

Numer portu: 1042

Program: BLA

---

[1] Zakładając, że główny plik programu nazywa się tesk.exe oraz, że znajduje się on w którymś z katalogów w ścieżce wyszukiwania (przeważnie jest to c:\windows\), ale jak już wspomniano, nazwa ta może się zmieniać.

BLA jest serwerem, który po zainstalowaniu w systemie ofiary pozwala atakującemu m.in. na zdalne sterowanie, wysyłanie pakietów ICMP, zdalne wyłączenie komputera, oraz bezpośrednie wysyłanie wiadomości użytkownikowi. BLA używa następujących kluczy *Rejestru*:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run -
System=„c:\windows\system\mprdll.exe”

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run -
SystemDoor=„c:\windows\system\rundll argp1”
```

Rys. 4.21 Trojan BLA jest u¿ywany do wywo³ania zamieszania u ofiary.

Numery portów: 1170, 1509

Programy: Psyber Stream Server, Streaming Audio Trojan

Programy te zaprojektowane zostały dla jednego celu — wysłania ofierze strumienia audio. Po udanym zainstalowaniu programu, atakujący może odtworzyć na głośnikach ofiary cokolwiek tylko zechce.

Numer portu: 1234

Program: Ultors Trojan 

Ultors jest jeszcze jednym programem zaprojektowanym do umożliwienia zdalnego uruchamiania programów i poleceń systemowych, kontrolowania uruchomionych procesów oraz wyłączania zarażonego komputera. Z biegiem czasu jego możliwości zostały poszerzone o zdolność do wysyłania komunikatów oraz wyświetlania komunikatów błędów.

Numery portów: 1243, 6776

Programy: BackDoor-G, SubSeven, SubSevenApocalypse

Programy te są różnymi odmianami niesławnego programu Sub7 (rys. 4.22). Po zarażeniu dają one atakującemu za pośrednictwem Internetu nieograniczony dostęp do komputera ofiary. Programy instalacyjne są z regóły zamaskowane jako różnego rodzaju dowcipy, głównie rozprzestrzeniając się poprzez załączniki do poczty elektronicznej. Występują pod następującymi nazwami plików (ich nazwy mogą się zmieniać):

```
C:\WINDOWS\nodll.exe

C:\WINDOWS\ server.exe  lub  kernel16.dl  lub te¿  window.exe

C:\WINDOWS\SYSTEM\watching.dll  lub  lmdrk_33.dll
```

Rys. 4.22 SubSevenApocalypse.

Numer portu: 1245

Program: VooDooDoll

VooDoo Doll jest połączeniem możliwości swoich poprzedników. Głównym zadaniem programu jest spowodowanie jak największego zamieszania (rys. 4.23). Społeczność hakerska twierdzi, że niektórzy rozprowadzają go wraz z dodatkowymi programami, znanymi z tego, że po uruchomieniu przez VooDoo Doll usuwają nieodwracalnie zawartość dysku (poprzez zapisanie zawartości oryginalnych plików), niszcząc czasem pliki systemowe.

Rys. 4.23 Wybór funkcji VooDoo Doll.

Numer portu: 1492

Program: FTP99CMP

FTP99CMP jest prostym serwerem FTP używającym następującego klucza *Rejestru*:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run - windll_16
```

Numer portu: 1600

Program: Shivka-Burka

Ten koń trojański udostępnia proste możliwości (kopiowanie i kontrola plików), i z tego pewnie powodu jest rzadko spotykany. Program nie używa *Rejestru Systemowego*, ani też portu innego niż 1600.

Numer portu: 1981

Program: Shockrave

Znana jest tylko jedna kompilacja tego programu, funkcjonalnie będącego ukrytym sewerem telnet. Podczas konfiguracji używany jest następujący klucz *Rejestru*:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices - NetworkPopup
```

Numer portu: 1999

Program: BackDoor

Jako jeden z pierwszych koni trojańskich instalujących tylne wejścia do systemów, BackDoor (rys. 4.24) został rozprzestrzeniony na całym świecie. Mimo, że napisany w języku Visual Basic, serwer ten ma całkiem spore możliwości, włączając w to:

- kontrolę napędu CDROM,
- kontrolę kombinacji *CTRL-ALT-DEL* oraz *CTRL-ESC*,
- wysyłanie wiadomości,
- rozmowę z użytkownikiem zaatakowanego komputera,
- wyświetlanie listy uruchomionych aplikacji,
- zarządzanie plikami,
- kontrolę API Windows,
- zamrażanie pozycji myszy.

Podczas konfiguracji używany jest następujący klucz *Rejestru*:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run - notps
```

Rys. 4.24 Ba[illegible]or jest jednym z pierwszych koni trojańskich udostêpniaj¹cych opcje zdalnego sterowania.

Numery portów: 1999-2005, 9878

Program: Transmission Scout

Niemieckiej produkcji koń trojański udostępniający zdalną kontrolę. Transmission Scout posiada wiele niebezpiecznych funkcji. Podczas swojej instalacji używa klucza *Rejestru*:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run - kernel16
```

Jakkolwiek program jest raczej rzadko spotykany, został uzupełniony tak, by posiadać następujące funkcje:

- restartowanie i wyłączanie komputera,
- uzyskiwanie informacji o systemie,
- reagowanie na wiadomości ICQ i pocztę przychodzącą,
- uzyskiwanie haseł,
- kontrola dźwięku,
- kontrola myszy,
- kontrola *paska zadań*,
- kontrolę otwartych okien,

- wysyłanie wiadomości,
- edycja *Rejestru*,
- zmienianie zawartości *pulpitu*,
- wykonywanie zrzutów ekranu.

Numer portu: 2001

Program: Trojan Cow

Ten koń trojański, tak jak większość innych, pozwala na zdalne wykonywanie różnego rodzaju poleceń. W zakres jego możliwości wchodzą m.in.:

- otwieranie i zamykanie napędu CDROM,
- włączanie i wyłączanie monitora,
- usuwanie i przywracanie ikon *pulpitu*,
- otwieranie i zamykanie menu *Start*,
- ukrywanie i przywracanie *paska zadań*,
- ukrywanie i przywracanie *zegara*,
- zamienianie pozycjami klawiszy myszy,
- zmiana tapety *pulpitu*,
- uchwycenie wskaźnika myszy w rogu ekranu,
- usuwanie plików,
- uruchamianie programów,
- ukrywanie działania programów,
- zamykanie systemu ofiary,
- restartowanie komputera ofiary,
- wylogowywanie się z systemu,
- wyłączanie komputera.

Podczas konfiguracji, program używa następującego klucza *Rejestru*:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run - SysWindow
```

Numer portu: 2023

Program: Ripper

Ripper jest jednym ze starszych programów. Jego zadaniem jest rejestrowanie sekwencji naciśniętych klawiszy, głównie w celu przechwytywania haseł. Ma jednak poważną wadę, utrudniającą jego wykorzystanie — nie potrafi on mianowicie uruchomić się po restarcie systemu.

Numer portu: 2115

Program: Bugs

Serwer ten (rys. 4.25) jest jeszcze jednym udostępniającym zdalny dostęp, z funkcjami pozwalającymi między innymi na zarządzanie plikami, oraz oknami programów. Podczas instalacji używany jest następujący klucz *Rejestru*:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run - SysTray
```

Rys. 4.25 Interferjs u¿ytkownika programu Bugs.

Numery portów: 2140, 3150

Program: The Invasor

Invasor jest programem, który w zestaw swoich możliwości włącza przechwytywanie haseł, wysyłanie komunikatów, kontrolę dźwięku, zmienianie rozdzielczości ekranu oraz przechwytywanie jego zawartości (rys. 4.26).

Rys. 4.26 Wybór funkcji programu Invasor.

Numer portu: 2155, 5512

Program: Illusion Mailer

Programu Illusion Mailer pozwala atakującemu wysyłać pocztę posługując się adresem IP ofiary (w szczególności wysyłać pocztę w jej imieniu). Ponieważ nagłówek tak wysłanego listu zawiera adres ofiary, więc bardzo trudno jest odnaleźć prawdziwego nadawcę. Podczas instalacji wykorzystywany jest klucz *Rejestru*:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices – Sysmem
```

Numer portu: 2565

Program: Striker

Głównym zadaniem tego programu jest zniszczenie systemu Windows. Na szczęście program nie aktywuje się więcej po restarcie systemu, tak więc jego znaczenie jest raczej niewielkie.

Numer portu: 2583, 3024, 4092, 5742

Program: WinCrash

WinCrash pozwala przejąć atakującemu pełną kontrolę nad systemem. Posiada wiele możliwości, m.in. opcje powodujące znaczne obciążenie systemu. Z tego powodu uważany jest za stosunkowo niebezpieczny.

Rys. Narzędzia udostępniane przez program WinCrash.

Numer portu: 2600

Program: Digital RootBeer

Kolejny bardzo irytujący program. W zakres jego możliwości wchodzą:

- wysyłanie komunikatów, oraz możliwość prowadzenia rozmowy z użytkownikiem zaatakowanej maszyny,
- kontrolowanie pracy urządzeń takich jak monitor, modem czy karta dźwiekowa,
- zatrzymywanie pracy systemu,
- kontrolowanie okien aplikacji.

Podczas instalacji wykorzystywany jest następujący klucz *Rejestru*:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices – ActiveX
Console
```

Numer portu: 2801

Program: Phineas Phucker

Program ten (rys. 4.28), przysparzający użytkownikom zaatakowanych komputerów wiele problemów, posiada większość funkcji typowych dla koni trojańskich umożliwiających zdalny dostęp.

Rys. 4.28 Phineas Phucker.

Numer portu: 2989

Program: RAT

Program ten jest bardzo niebezpiecznym serwerem zdalnego dostępu, ponieważ jego głównym celem jest zniszczenie zawartości twardych dysków zaatakowanego komputera. Podczas instalacji używane są następujące klucze *Rejestru Systemowego*:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run - Explorer="C:\Windows\System\msgsvr16.exe"
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices - Default=" "
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices - Explorer=" "
```

Numery portów: 3459-3801

Program: Eclipse

Eclipse jest kolejnym ukrytym serwerem FTP. Po wykonaniu udostępnia wszystkie pliki w systemie, zezwalając nie tylko na odczyt i zapis, ale również na ich uruchamianie. Podczas instalacji programu używany jest następujący klucz *Rejestru*:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run - Rnaapp="C:\Windows\System\rmaapp.exe"
```

Numery portów: 3700, 9872-9875, 10067, 10167

Program: Portal of Doom

Możliwości tego progamu (rys. 4.29) to między innymi:

- kontrola napędu CD-ROM,
- kontrola urządzenia dźwiękowego,
- eksploracja systemu plików komputera,
- kontrola *paska zadań*,
- kontrola *pulpitu*,
- przechwytywanie haseł oraz naciskanych przez użytkownika klawiszy,
- zarządzanie plikami.

Rys. 4.29 Możliwości programu Portal of Doom.

Numer portu: 4567

Program: File Nail

File Nail jest programem atakującym i rozprzestrzeniającym się wśród użytkownikó ICQ (rys. 4.30). Efektem działania programu jest uszkodzenie klienta ICQ na zaatakowanym komputerze.

Rys. 4.30 File Nail został zaprojektowany do uszkodzenia serwerów ICQ.

Numer portu: 5000

Program: Bubbel

To jeszcze jeden program integrujący w systemie tzw. „tylne drzwi" posiadający możliwości podobne do programu Trojan Cow włączając w to:

- wysyłanie wiadomości,
- kontrolę pracy monitora,
- kontrolę okien programów,
- zatrzymywanie pracy systemu,

- kontrolę pracy modemu,
- możliwość prowadzenia rozmowy z użytkownikiem opanowanego komputera,
- kontrolę dźwięku,
- przechwytywanie haseł i naciskanych klawiszy,
- drukowanie,
- kontrolowanie pracy przeglądarki.

Numery portów: 5001, 30303, 50505

Program: Sockets de Troie

Sockets de Troie jest wirusem, który rozprzestrzeniając się integruje w zaatakowanych systemach "tylne drzwi" służące do zdalnej administracji systemem. Raz wykonany kopiuje się do katalogu *Windows\System* jako plik *mschv.exe*, oraz modyfikuje *Rejestr Systemu*. Podczas instalacji używane są z regóły następujące klucze *Rejestru*:

```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunLoadMschv32 -
Drv="C:\Windows\System\MSchv32.exe"

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunLoad -
Mgadeskdll="C:\Windows\System\Mgadeskdll.exe"

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunLoad -
Rsrcload="C:\Windows\Rsrcload.exe"

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServicesLoad -
Csmctrl32="C:\Windows\System\Csmctrl32.exe"
```

Numer portu: 5569

Program: Robo-Hack

Robo-Hack jest jednym ze starszych trojanów napisanych w języku Visual Basic. Program nie potrafi się samodzielnie rozprzestrzeniać, ani też nie uruchamia się po ponownym uruchomieniu systemu. Jego ograniczone funkcje (rys. 4.31) obejmują:

- monitorowanie pracy systemu,
- edycję plików,
- restartowanie i wyłączanie systemu,
- wysyłanie komunikatów,
- kontrolowanie pracy przeglądarki,
- otwieranie i zamykanie napędu CD-ROM.

Rys. 4.31 Ograniczone możliwości programu Robo-Hack.

Numer portu: 6400

Program: The tHing

The tHing jest małym, lecz niebezpiecznym, serwerem pozwalającym skopiować na dysk komputera docelowego dowolny program, a następnie go uruchomić. Podczas instalacji używany jest następujący klucz *Rejestru*:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices - Default
```

Rys. 4.32 The tHing potrafi skopiowaæ na dysk komputera dowolny program a nastêpnie go uruchomiæ.

Numer portu: 6912

Program: Shit Heep

Ten dosyć powszechnie spotykany, napisany w języku Visual Basic, koń trojański próbuje zamaskować się jako systemowy *Kosz*. Po zainfekowaniu użytkownik otrzymuje komunikat o rzekomym „uaktualnieniu Kosza" (rys.4.33). Do ograniczonych możliwości tego programu należą m.in.:

- kontrola *Pulpitu*,
- kontrola działania myszy,
- wysyłanie komunikatów,
- zamykanie wybranego okna,
- otwieranie i zamykanie napędu CD-ROM.

Rys. 4.33 Komunikat systemowy po zarażeniu programem Shit Heep.

Numery portów: 6969, 16969

Program: Priority

Pritority jest trojanem napisanym w języku Visual Basic pozwalającym na:

- zamykanie i otwieranie napędu CD-ROM,
- odtwarzanie na zaatakowanym komputerze dowolnych dźwięków,
- chowanie i przywracanie *paska zadań*,
- kontrolowanie zawartości *pulpitu*,
- przechwytywanie naciskanych klawiszy i haseł systemowych,
- zarządzanie plikami,
- zarządzanie aplikacjami,
- kontrolowanie przeglądarki,
- restartowanie systemu,
- skanowanie portów.

Rys. 4.34 Priority charakteryzuje się stosunkowo dużym wyborem funkcji.

Numer portu: 6970

Program: GateCrasher

GateCrasher jest kolejnym programem pozwalającym zdalnie sterować zarażonymi komputerami. Maskuje się jako program rozwiązujący problem Y2k. Program posiada prawie każdą funkcję dostępną w innych programach tego typu. Podczas instalacji używa klucza *Rejestru*:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices - Inet
```

Rys. 4.35 GateCrasher posiada prawie ka¿d¹ funkcjê spotykan¹ w trojanach udostêpniaj¹cych zdalny dostêp.

Numer portu: 7000

Program: Remote Grab

Pogramu Remote Grab pozwala na zdalne wykonywanie zrzutów ekranu. Podczas instalacji kopiowany jest plik *\Windows\System\mprexe.exe.*

Numer portu: 7789

Program: ICKiller

Serwer ten został zaprojektowany do przechwytywania informacji o różnorodnych kontach internetowych. Program maskuje się jako... koń trojański, służący do atakowania użytkowników ICQ (rys. 4.36). Z tego też powodu program rozprzestrzenia się głównie wśród początkujących hakerów.

Rys. 4.36 ICKiller przechwytuje hasła, chociaż udaje narzędzie do atakowania użytkowników ICQ.

Numer portu: 9400

Program: InCommand

InCommand został napisany na podobieństwo programów z serii Sub7. W odróżnieniu jednak od nich zawiera dodatkowo prekonfigurowany moduł serwera.

Numer portu: 10101

Program: BrainSpy

BrainSpy posiada funkcje dostępne w typowych trojanach umożliwiających zdalny dostęp i kopiowanie plików. Dodatkowo, po uruchomieniu, program stara się uszkodzić zainstalowane skanery antywirusowe. Podczas instalacji wykorzystywane są następujące klucze *Rejestru*:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices - Dualji
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices - Gbubuzhnw
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices - Fexhqcux
```

Numer portu: 10520

Program: Acid Shivers

Trojan ten, oparty na usłudze Telnet, ma zdolność do wysyłania atakującemu komunikatów pocztowych powiadamiających go o uaktywnieniu atakowanego systemu (rys. 4.37).

Rys. 4.37 Acid Shivers potrafi wysyłać atakującemu komunikaty.

Numer portu: 10607

Program: Coma

Jeszcze jeden koń trojański napisany w języku Visual Basic, udostępniający zdalne sterowanie atakowaną maszyną. Jego możliwośći łatwo wydedukować z prostego interfejsu użytkownika (rys. 4.38).

Rys. 4.38 Ubogie możliwości programu Coma.

Numer portu: 12223

Program: Hack'99 KeyLogger

Trojan ten jest typowym programem przechwytującym kombinacje przyciśniętych klawiszy, w odróżnieniu jednak od innych produktów tego typu, potrafi on przekazywać atakującemu przechwycone informacje w czasie rzeczywistym (rys. 4.39).

Rys. 4.39 Hack'99 potrafi w czasie rzeczywistym wysyłać przechwycone kombinacje klawiszy.

Numery portów: 12345, 12346

Program: NetBus, NetBus2, NetBus Pro

NetBus, oraz jego późniejsze wersje, jest jednym z najbardziej znanych i rozpowszechnionych koni trojańskich udostępniających opcje zdalnego sterowania i monitoringu. Program ten obsługuje m.in. protokoły telnet oraz http. Za centrum dowodzenia programem NetBus uważana jest domena UltraAccess.net (więcej informacji można znaleźć na stronie *www.UltraAccess.net*).

Numer portu: 17300

Program: Kuang

Kuang jest mutacją prostego programu kradnącego hasła poprzez protokół SMTP.

Numery portów: 20000, 20001

Program: Millennium

Millennium jest kolejnym prostym koniem trojańskim napisanym w jezyku Visual Basic. Jego opcje zdalnego sterowania zostały uaktualnione, dzięki czemu potrafi m.in.:

- wysuwać i chować tackę napędu CD-ROM,
- odgrywać na głośnikach zaatakowanego komputera dowolny dźwięk lub utwór,
- kontrolować parametry *pulpitu*,
- podkradać hasła,
- monitorować aktywność klawiatury,
- kontrolować działanie innych aplikacji,
- kontrolować przeglądarkę,
- wyłączać i restartować system,
- skanować porty.

Podczas instalacji używany jest następujący klucz *Rejestru*:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices - millenium
```

Numer portu: 21544

Program: GirlFriend

Kolejny koń trojański, którego głównym zadaniem jest przechwytywanie haseł. Nowsze kompilacje zawierają serwer FTP, oraz możliwość wysyłania ofierze komunikatów. Podczas konfiguracji wykorzystywany jest następujący klucz *Rejestru Systemowego*:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices - Windll.exe
```

Numery portów: 22222, 33333

Program: Prosiak

Trojan o dosyć standardowych możliwościach:

- wysuwanie i chowanie tacki napędu CD-ROM,
- kontrolowanie urządzeń dźwiękowych komputera,
- kontrolowanie *paska zadań*,
- kontrolowanie *pulpitu*,
- monitorowanie klawiatury,
- przechwytywanie haseł,
- zarządzanie plikami,
- kontrolowanie pracy przeglądarki,
- wyłączanie i restartowanie systemu,
- skanowanie portów,

Podczas instalacji używany jest następujący klucz *Rejestru Systemowego*:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices - Microsoft DLL
Loader
```

Numer portu: 30029

Program: AOL Trojan

AOL Trojan zaraża DOS-owe pliki *.exe. Potrafi rozprzestrzeniać się poprzez sieci LAN, WAN, Internet oraz poprzez pocztę. Po uruchomieniu AOL Trojan natychmiast stara się zainfekować kolejne programy.

Numery potów: 30100-30102

Program: NetSphere

Ten potężny i bardzo niebezpieczny koń trojański posiada w swoim arsenale funkcje takie jak:

- wykonywanie zrzutów ekranu,
- wysyłanie wiadomości,
- ukrywanie i przywracanie *paska zadań*,
- kontrolowanie *pulpitu*,
- możliwość prowadzenia rozmowy z użytkownikiem zainfekowanego komputera,
- zarządzanie plikami,
- zarządzanie aplikacjami,
- kontrolowanie myszy,
- zamykanie i restartowanie systemu,
- odgrywanie na głośnikach dowolnego dźwięku,
- monitorowanie wszelkich dostępnych informacji o systemie.

Podczas instalacji używany jest następujący klucz *Rejestru Systemowego*:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices - nssx
```

Numery portów: 1349, 31337, 31338, 54320, 54321

Program: Back Orifice

Back Orifice jest jednym z najgroźniejszych i najbardziej rozpowszechnionych znanych koni trojańskich. Potrafi m.in. komunikować się przy pomocy szyfrowanych pakietów UDP, co znakomicie utrudnia wykrycie intruza. Potrafi również korzystać z wtyczek, dzięki czemu atakujący może wzbogacać już zainstalowanego na komputerze ofiary trojana o zupełnie nowe funkcje. Podczas instalacji wykorzystuje następujący klucz *Rejestru*:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices - bo
```

Numery portów: 31785-31792

Program: Hack'a'Tack

To jeszcze jeden powszechnie spotykany serwer udostępniający wszystkie typowe opcje zdalnego sterowania (rys. 4.40). Podczas instalacji używany jest następujący klucz *Rejestru Systemowego*:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices - Explorer32
```

Rys. 4.40 Możliwości programu Hack'a'Tack.

Numer portu: 33911

Program: Spirit

Ten dobrze znany trojan posiada unikalną, bardzo niebezpieczną funkcję — *monitor burn*. Jej działanie polega na ciągłym resetowaniu rozdzielczości ekranu, możliwe jest też, że zmieniana jest również częstotliwość odświeżania. Podczas instalacji używany jest klucz *Rejestru*:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices -
SystemTray="c:\windows\windown.exe"
```

Numer portu: 40412

Program: The Spy

Program ten jedynie rejestruje sekwencje naciśniętych przez użytkownika klawiszy po czym natychmiast wysyła je atakującemu. Jego możliwości są ograniczone, gdyż nie potrafi przechowywać sekwencji klawiszy gdy, przykładowo, system jest odłączony od Internetu. Klucz *Rejestru* używany podczas instalacji:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices - systray
```

Numer portu: 47262

Program: Delta Source

Trojan Delta Source został napisany na wzór Back Orifice, w rezultacie ma bardzo podobne możliwości. Podczas instalacji używa następującego klucza *Rejestru*:

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices - Ds admin tool
```

Numer portu: 65000

Program: Devil

Devil jest jednym ze starszych koni trojańskich napisanych w jezyku Visual Basic. Na szczęście nie uruchamia się ponownie po restarcie systemu. Ograniczone możliwości tego programu przedstawione zostały na rys. 4.41.

Rys. 4.41 Ograniczone możliwości trojana Devil.

Obeznani z problemami dotyczącymi portów i usług rozpoczniemy teraz odkrywanie tych dziedzin informatyki, których dogłębna znajomość pozwala hakerom dokonywać swoich "magicznych sztuczek". Jak to wielokrotnie w życiu bywa, przeciwnika można pokonać jego własną bronią. Opanowanie tych umiejętności jest konieczne, by poprawić bezpieczeństwo własnej sieci lub systemu operacyjnego oraz, by tworzyć bezpieczniejsze oprogramowanie. Należy jednak pamiętać, że *stosowanie większości technik i programów opisanych w tej książce bez wiedzy i przyzwolenia osób nimi atakowanych jest niezgodne z prawem obowiązującym w Polsce, oraz wielu innych krajach. Ani autor, ani wydawca nie może ponosić odpowiedzialności za użycie, lub niezrozumienie informacji przedstawionych w tej książce.*

Co dalej?

Zadaniem tego rozdziału było przekazanie podstawowej wiedzy dotyczącej portów wejścia-wyjścia oraz usług z nimi związanych. Warunkiem przejścia do kolejnego rozdziału jest zdobycie umiejętności pozwalających zidentyfikować potencjalne niebezpieczeństwa związane z portami. W kolejnym rozdziale, zajmiemy się technikami pozywającymi wykrywać niebezpieczne porty i usługi, by umieć przygotować system na ewentualne próby ataków ze strony hakerów.