Dodatek nr 4

Słowniczek

A

Administrator systemu — sprawuje opiekę nad systemem, przydziela prawo użytkowania, katalog domowy oraz powłokę-shell; określa udział użytkownika w systemie; ma dostęp do wszystkich plików.

Adres internetowy — 32-bitowy adres umożliwiający identyfikację sieci i komputerów.

Adres podsieci — W TCP/IP fragment adresu IP identyfikującego wydzieloną część sieci (podsieć), poziomu przypisanego do każdego węzła w sieci. Adres ten zwykle odnosi się do karty sieciowej węzła. Przykładem adresu sprzętowego jest 48-bitowy adres ethernetowy.

Adres sieciowy — w sieciach TCP/IP jest to adres IP węzła.

Architektura klient/serwer — jest to określenie często używane w przypadku, gdy na przykład jeden z programów służy do wydawania poleceń (klient), a drugi (serwer) je wykonuje. Mogą one być od siebie oddalone, ale muszą być połączone w tej samej w sieci.

ARPANET — W latach 1966-67 Departament Obrony sfinansował prace nad eksperymentalnym łączeniem odległych od siebie komputerów. Wykorzystano w nich wcześniejsze doświadczenia z systemami wielodostępnymi (*timesharing*), w których przyłączano wiele terminali do jednego komputera. Okazało się, że nie było problemów z łączeniem komputerów rożnych typów, ale pojawiły się one w przypadku używanych linii telefonicznych (były zbyt wolne i zawodne). W 1967 roku zaprezentowano plan sieci pakietowej ARPANET, która miała ze sobą połączyć początkowo cztery wybrane centra: Uniwersytet Kalifornii w Los Angeles (UCLA), Stanford Research Institute (SRI), Uniwersytet Kalifornii w Santa Barbara (UCSB) i Uniwersytet Utach. W każdym z nich do dużego komputera klasy mainframe miał

zostać dołączony minikomputer pełniący funkcję węzła przełączającego, określany mianem IMP (*interface message processor*). W odróżnieniu od systemów wielodostępnych, opartych na architekturze klient-serwer, miała to być sieć komputerów równorzędnych (peer-to-peer). Miały one zostać połączone liniami dzierżawionymi o przepustowości 50 kbps, dostarczonymi przez AT&T.

ASCII — (*American National Standart Code for Information Interchange*) — najbardziej rozpowszechniony standard kodowania znaków. Zestaw ASCII zawiera litery alfabetu, cyfry oraz różnorodne znaki i symbole. Początkowo było to 128 znaków i odpowiadających im kodom. Praktycznie jest to „czysty" plik tekstowy, w którym w przeciwieństwie na przykład do plików tekstowych Worda, nie występują różne czcionki, tabele, rysunki itp. Plik ASCII ma dokładnie taki sam rozmiar (w bajtach), co ilość znaków zapisanych w pliku z uwzględnieniem spacji, przecinków itp.

Asynchroniczność — jest to brak jakiejkolwiek regularności występowania w czasie.

Atak Denail of Service — jest to rodzaj ataku, powodujący odmowę usługi na zaatakowanym komputerze. Można zablokować komputer tak, by przez pewien czas (póki np. nie zostanie zrestartowany system) nikt nie mógł skorzystać z części lub wszystkich jego usług. Najbardziej znanym przykładem może być tu np. Nuke, Land, Hanson, Boink, Jolt, Newtear, Pong, Teardrop.

B

Back Door — to dosłownie: tylne drzwi. Jest to program (często koń trojański) instalowany głównie na serwerze, a jego zadaniem jest umożliwienie dostania się do niego (z ominięciem zabezpieczeń) hakera. Jest to bardzo często stosowana technika, za pomocą której haker może wielokrotnie powracać nawet na bardzo zabezpieczony serwer.

Backup — tworzenie kopii zapasowej danych (archiwizacja).

BBS (Bulletin Board System) — komputer odbierający telefony (a właściwie modemy) z oprogramowaniem pozwalającym użytkownikowi na wysyłanie i odbieranie poczty oraz plików. Niektóre BBS-y oferują inne dodatkowe możliwości.

Bod (Baud) — jednostka miary określająca liczbę zmian stanu sygnału w jednej sekundzie. Jeśli sygnał może przyjmować tylko dwa stany, to szybkość transmisji w baudach odpowiada szybkości mierzonej w bitach na sekundę.

Bramka — to określenie tradycyjnie oznaczało w Internecie urządzenie spełniające funkcję rutera. Obecnie jednak terminu tego używa się w odniesieniu do urządzeń sieciowych dokonujących konwersji wszystkich protokołów sieci jednego typu na protokoły innej sieci.

Brute-Force — jest to technika stosowana przy łamaniu haseł. Polega ona na sprawdzaniu kolejno wszystkich możliwych kombinacji liter, cyfr i znaków (w do-

wolnej konfiguracji). Technika jest w 100% skuteczna, ale warto stosować ją tylko do złamania krótkich haseł, gdyż wraz ze wzrostem długości hasła, niewyobrażalnie rośnie długość jego wynajdywania,

BSD (Berkley Software Distribution) — jest to oprogramowanie dla systemu Unix.

C

Crack — dosłownie: złamać, rozwalić, roztrzaskać itp. Crackować można zarówno hasła (w tym przypadku cracker je wynajduje), jak i programy (poprzez odpowiednią modyfikację można uzyskać różne efekty, ale najczęściej jest to odblokowanie funkcji niedostępnych w wersji demo).

Cracker — właściwie pod tym hasłem kryją się dwie osoby:
— człowiek zajmujący się nielegalnym udostępnianiem programów (czyli łamaniem zabezpieczeń, omijaniem praw autorskich itp.);
— człowiek bardzo podobny do hakera, którego zamiary są jednak bardziej złośliwe — włamuje się do systemów, niszczy i kradnie dane.

CRC (Cyclic Redundancy Check) — cykliczna kontrola nadmiarowa. Funkcja matematyczna używana do weryfikacji bezbłędności transmisji w sieci. CRC pełni także rolę „porównawczą" (uprzednio trzeba stworzyć ciąg CRC na podstawie 100% pewnego pliku) na przykład wtedy, gdy chcemy być pewni, że ważny program na naszym serwerze nie został zmodyfikowany czy zarażony wirusem itp.

Cyberkultura — to kultura wieku informacji. Początkowo kojarzona jedynie z cyberpunkiem, dzisiaj obejmuje działania o charakterze twórczym związane ze światem komputerów, sieci, Internetu, multimediów, itp.

Cyberpunk — początkowo nurt w literaturze fantastyczno-naukowej, zainicjowany na początku lat 80. nowelami i książkami Williama Gibsona i Bruce'a Sterlinga. Termin powstał przez skojarzenie prefiksu słowa cyberprzestrzeń z nihilistycznym światopoglądem punków.

Cyberprzestrzeń — „przestrzeń informacyjna" zrealizowana w sposób pozwalający na jej eksplorację oraz odczuwanie wrażeń za pomocą zmysłów pobudzanych wspomaganymi komputerowo urządzeniami.

D

Deamon — typ programu często spotykanego w różnych implementacjach systemu Unix. Program taki działa samodzielnie i bez nadzoru wykonuje określone, standartowe usługi.

Debugger — program umożliwiający śledzenie funkcji programu. Jest on bardzo przydatny przy programowaniu, jak i przy crackowaniu innych programów.

Denail of Service — patrz: *Atak Denail of Service*.

DNS (Domain Name Service) — jest to serwer nazw, przyporządkowujący poszczególnym adresom IP odpowiednie nazwy. Dzięki niemu odwołanie się do serwera może się odbyć po wpisaniu np. *www.blabla.co.pl,* a nie tylko po wpisaniu adresu IP (czyli ciągu liczb).

DoS — patrz: *Atak Denail of Service.*

Dostawca internetu — patrz: *Provider.*

Dziennik — jest to program, który rejestruje zdarzenia na danym komputerze. Może on zapisywać połączenia, otwierane pliki itp. Dzięki niemu administrator może zobaczyć, co działo się pod jego nieobecność. Jest on zapisywany jest do plików, zwanych także logami.

Dziura — jest to z reguły błąd w programie, który może zostać wykorzystany przez hakera.

E

Exploit — jest to program, który wykorzystuje różne dziury w systemie (może mieć wpływ na ich działanie, zawieszać je lub nawet przejąć nad nimi kontrolę). Najczęściej exploitem jest program dla Uniksa lub Linuksa, gdyż najwięcej ludzi zajmujących się nimi „na poważnie" to użytkownicy tych systemów. Jednocześnie są stanowią one często źródło poznania dla każdego administratora (lub hakera), które pozwala zapoznać się z działaniem i wykorzystać do własnych celów.

F

Faq (Frequency Asked Questions) — jest to plik tekstowy, którego teoretycznym celem jest odpowiedź na najczęściej zadawane pytania dotyczące wybranego tematu.

G

Geek — osoba, której praca oraz pasje koncentrują się na komputerach, sieciach i nowoczesnych technologiach w stopniu znacznie przekraczającym tradycyjnie pojmowane hobby.

Grupa dyskusyjna — wyodrębnione formalnie miejsce, w którym można wymieniać z innymi osobami informacje i poglądy na określone tematy. Najbardziej popularne fora dyskusyjne należą do sieci Usenet.

H

Haker — jest to człowiek, który za sprawą swoich zdolności informatycznych (czasami nie tylko!) potrafi włamać się do innych komputerów, nie kradnąc jednocześnie z niego danych. Nie niszczy ich, lecz robi to dla sprawdzenia samego siebie.

Hardware — sprzęt, technika, elektronika, urządzenia.

Hash — to po prostu znaczek „#".

Host — jest to komputer podłączony do sieci, posiadający własny adres IP należący do odpowiedniej domeny.

HTML (Hyper Text Markup Language) — jest to najbardziej rozpowszechniony język programowania w sieci. Stosowany na każdej stronie WWW pozwala na proste i wygodne formatowanie tekstów, tworzenie powiązań pomiędzy nimi, przesyłanie grafiki, dźwięku oraz wielu innych rodzajów danych.

I

ICQ (I Seek You) — coraz bardziej popularny program do komunikacji w sieci. Jest wielo platformowy, szybki i sprawny. Można za jego pomocą wysyłać krótkie wiadomości, pliki, URL, a także porozmawiać „na żywo" za pomocą funkcji chat. Program zupełnie nie zależny od standartowych usług typu e-mail czy IRC, w przeciwieństwie do którego sami ustalamy listę naszych przyjaciół.

IP Spoofing — jest to bardzo skuteczna i często stosowana technika pozwalająca na podszycie się pod inny komputer. Jest kilka jego odmian — można stosować odpowiednie oprogramowanie na własnym komputerze, lecz także odpowiednio „podkręcić" rutera tak, by zamiast przekazywać pakiety do komputera XXX, przekazywał je hakerowi. Do spoofingu należy także wysyłanie poprzez otwarty port ICQ dowolnych informacji (wystarczy podać jako nadawcę cudzy numer UIN).

IRC (Internet Really Chat) — program, za pomocą którego możemy porozmawiać (pisząc na klawiaturze) z wieloma ludźmi z całego świata. Wchodząc na ogólnoświatowe kanały IRC widzimy wszystkie wypowiedzi każdej osoby (a każdy widzi nasze), dzięki czemu IRC można by nazwać swego rodzaju konferencją. Porządku na kanale pilnują IRC Opy oraz Boty.

IRC kanał — jest to wirtualne miejsce w sieci, w którym spotykają się często dziesiątki ludzi z różnych miejsc świata. Każda nazwa kanału IRC jest poprzedzona znaczkiem hash, po czym następuje właściwa nazwa kanału np. #techno, #teqnix,

itp. Gdy chcemy zlokalizować rejon, dla którego kanał jest przeznaczony (a dokładniej język) dodawana jest końcówka symbolizująca język np.#hakpl, #amigapl itp. Aby wejść na kanał IRC musimy posiadać specjalny program, który po zalogowaniu się do serwera IRC przyłączy nas do wybranych kanałów. Należy także pamiętać, że gdy chcemy się łączyć z kanałami polskimi, najlepiej łączyć się z polskimi serwerami IRC.

K

Kanał IRC — patrz: *IRC kanał.*

Key Logger — jest to program, którego zadaniem jest rejestrowanie wszystkich lub tylko niektórych wpisywanych tekstów za pomocą klawiatury. Najczęściej stosowane są Kay Loggery programowe (zgrywające wynik do pliku), ale istnieją także ich sprzętowe wersje (np. mały układ podłączony między klawiaturą a komputerem). Dzięki nim możemy zarejestrować wpisywane hasła, informacje itp.

Klient — patrz: *Architektura klient/serwer.*

Koń trojański — jest to program, którego celem jest pełnienie specjalnych funkcji „udających" inny program. Przykładem może tu być „podmieniony" program logujący, który poza tym, że działa jak oryginał, zapisuje wprowadzone hasło do pliku tak, żeby później mogło być przejrzane przez hakera. Stosowane są także konie trojańskie działające na zasadzie klient/serwer, które składają się z programu, jakim będziemy wydawać polecenia, oraz „sługi" zainstalowanego na komputerze ofiary, wykonującego różnego rodzaju zadania.

L

Lan (Local Area Network) — jest to sieć lokalna obejmująca komputery umieszczone w niewielkiej odległości od siebie.

Lamer — jest to bardzo ciekawe, choć dokładnie niesprecyzowane określenie człowieka, który nie zna się specjalnie na kwestiach związanych z programowaniem. Ogólnie jest ono obraźliwe.

Link — odnośnik, połączenie, hiperłącze.

Linux — system zupełnie niezależny od produktów Microsoft. Sposób jego działania jest zupełnie inny —darmowy, bez przerwy rozwijany. Istnieje jego wiele odmian, z czego najbardziej znanymi są Red Hat, S.u.S.E., Shockware, Debain. W działaniu nieco podobny do jest Uniksa.

Logi — są to pliki, w których utrzymywane są historie zdarzeń na danym komputerze. Są one wynikiem działania programów typu Dziennik.

M

MAN (Metropolitan Area Network) — jest to sieć miejska, obejmująca teren o zasięgu jednego miasta. Zapełnia ona lukę pomiędzy sieciami LAN oraz WAN.

MD5 — jest to 128-bitowy algorytm szyfrujący, stosowany między innymi w niektórych wersjach Uniksa.

Mirror — jest to kopia serwera lub samej strony, która znajduje się w innym miejscu w sieci. Jego stosowanie pozwala odciążyć serwer główny, zachowując wszystkie lub co najmniej część jego zasobów.

Modem — jest to urządzenie podłączane do komputera, które umożliwia przesyłanie danych w postaci cyfrowej przez analogowe sieci. Urządzenie to składa się z MODulatora oraz DEModulatora sygnału pozwalającego na nadawanie i odbiór zrozumiałego dla nich sygnału. Od tego zresztą pochodzi nazwa.

N

Nick — nazwa, pod którą rozpoznawany jest użytkownik sieci (np. na IRC-u).

O

Off-line — dosłownie: poza linią. W trybie off-line (a może być on w pojedynczym programie) pozostajemy odłączeni od sieci aż do momentu wejścia w tryb on-line,

On-line — dosłownie: na linii. W trybie tym jesteśmy podłączeni do sieci aż do momentu jej odłączenia, czyli przejścia w tryb off-line.

P

Pakiet (*TCP/IP)* — jest to najmniejsza porcja danych przesyłanych w sieci. Mogą to być np. różnego rodzaju komendy wymieniane pomiędzy komputerami.

Phreaking — jest to dziedzina podobna w konwencji do hakingu, lecz tycząca się... telekomunikacji.

Ping — jest to komenda, której zadaniem jest wysyłanie do innego komputera komunikatu przypominającego pytanie w stylu „żyjesz?" (Ping?). O ile drugi komputer będzie miał możliwość odpowiedzi, potwierdzi: „tak!" (Pong!).

Plugin — dosłownie: wtyczka. Wiele programów (nie tylko do obróbki dźwięku) ma tzw. architekturę otwartą, co oznacza, że można dodać do nich tzw. podprogra-

miki (pluginy-wtyczki), które nie działają samodzielnie, tylko współpracują z programem-matką.

POP3 (Post Office Protocol Version 3) — protokół wykorzystywany do odbierania poczty zgromadzonej na serwerze pocztowym.

Port Scanning — jest to technika pozwalająca na zorientowanie się, które z portów innej sieci są aktualnie używane i udostępnione. Dzięki temu możemy się dowiedzieć, że działa tam np. FTP, finger, serwer pocztowy. Istnieje kilka odmian port scanningu, różniących się efektywnością, stopniem trudności, wysyłanymi pakietami, rodzajem skanowanych portów, itp.

Provider — jest to — najprościej mówiąc — dostawca Internetu. Może on świadczyć usługi poprzez różne połączenia (modem, łącze stałe), oraz w różnym zakresie (ograniczmy się jednak do komputerów) udostępniać konta e-mail, miejsce na strony WWW itp.

Przejęcie kanału IRC — patrz: *Takeover.*

Q

Quot — jest to obszar pamięci dyskowej wyznaczany przez administratora dla użytkownika na jego dane.

S

SATAN — jest to typ programu skanującego (Skaner portów TCP/IP), którego skrócony opis znajduje się poniżej.
Autor: Dan Farmer i Weitse Venema
Język programowania: C. Perl
Wyjściowy system operacyjny: Unix (ogólnie)
Docelowy system operacyjny: Unix
Wymagania: Unix, Perl 5.001, C+, pliki nagłówkowe IP, prawa administratora

Program skanujący SATAN ujrzał światło dzienne w kwietniu 1995 roku i od razu spowodował duże zamieszanie w środowiskach ludzi zajmujących się bezpieczeństwem w Sieci. Cieszył się on zainteresowaniem medialnym jak żaden inny program tego typu, gdyż był programem skanującym, który nie tylko sondował większość luk znanych już w systemach zabezpieczeń, ale także — jeśli odnalazł taką lukę — natychmiast przedstawiał szczegółowe wskazówki dotyczące tego, jak tę lukę wykorzystać i dla przeciwwagi — jak ją wyeliminować. Ponadto SATAN okazał się pierwszym programem skanującym, który zwracał efekty swej pracy w formacie przyjaznym dla użytkownika.
Program ten do interakcji z użytkownikiem wykorzystuje interfejs HTML z formularzami, w których wpisuje się serwery do gotowe skanowania, oraz z tabelami, w których zwraca wyniki. Pojawiają się tu również kontekstowe opisy znalezionej lu-

ki. Jest to świetne narzędzie z dobrze napisanym kodem i dużymi możliwościami rozszerzania.
SATAN został zaprojektowany dla platformy Unix i napisany w językach C i Perl, co pozwala uruchomić go pod kontrolą różnych odmian tego systemu operacyjnego.
Program skanuje odległe serwery w poszukiwaniu znanych luk w systemami zabezpieczeń, czyli:

- Luk w serwerze FTPD;
- Luk w sieciowym systemie plików — NFS;
- Wad NIS;
- Luk RSH;
- Wad pakietu Sendmail;
- Luk serwera X Window.

Script kiddie — jest to określenie stosowne dla ludzi, którzy nie są już tylko lamerami, ale jakimiś podstawowymi sztuczkami osiągają coraz lepsze efekty w hakowaniu. Ze względu na sposoby działania (np. korzystanie z gotowych skryptów) nie są do końca lubiani przez prawdziwych hakerów.

Secret Service — specjalny odział policji, ścigający przestępstwa komputerowe.

Serwer — aplikacja reagująca na żądania klientów. Jest on szeroko stosowany w szerokim wachlarzu usług — od drukowania, zarządzania plikami (np. FTP) po obsługę terminali i przesyłanie danych. Patrz: Architektura klient/serwer.

Serwer plików — program działający na komputerze głównym umożliwiający dostęp do plików z innych komputerów.

Serwer pocztowy — komputer najczęściej na stałe podłączony do Sieci zajmujący się przesyłaniem poczty elektronicznej pomiędzy konkretnymi użytkownikami. Można go znaleźć skanując Sieć pod kątem otwartego portu 25.

Sieć komputerowa — zbiór komputerów i innych urządzeń połączonych w celu umożliwienia wydajnej komunikacji.

Skanowanie portów — patrz: *Port Scanning.*

Słownik — jest to czysty plik tekstowy (ASCII) ze spisem najczęściej używanych słów, nazw, imion itp. Czym większy jest zestaw słów, tym większe prawdopodobieństwo, że za jego pomocą uda się złamać szukane hasło.

Słownikowe łamanie haseł — to technika słownikowa stosowana przy łamaniu haseł. Polega ona na pobieraniu kolejno słów ze spisu (słownika) i sprawdzaniu ich pod kątem podobieństwa z szukanym hasłem. Technika ta jest szybka i efektywna

tylko wtedy, gdy przypuszczamy, że prawdziwe hasło może znajdować się w naszym pliku (np. wiemy, że hasłem jest jakieś standartowe słowo, imię, nazwa itp.).

SMTP (Simple Mail Transfer Protocol) — protokół służący do wysyłania poczty elektronicznej.

SMTP Serwer — komputer, na którym działa serwer poczty elektronicznej umożliwiający jej wysyłanie.

Sniffer — patrz: *Sniffing.*

Sniffing — dosłownie: niuchacz. Jest to niezwykle efektywna technika służąca do podsłuchiwania pakietów wymienianych pomiędzy komputerami. Dzięki niej można przechwycić wysyłane dane. Sniffer umieszczony w newralgicznym miejscu Sieci staje się bardzo niebezpiecznym narzędziem.

Software — oprogramowanie.

Spam — jest to pewien rodzaj ataku, polegający na „zalewaniu" masą wiadomości (np. otrzymanie 1000 takich samych maili czy wiadomości w ICQ).

Stuff — oznacza to, samo co software, ale bardziej pieszczotliwie.

Spoofer — patrz: *IP—Spoofing.*

Spoofing — patrz: *IP—Spoofing.*

Sysop — System Operator, czyli osoba nadzorująca BBS, która ustala zasady korzystania z BBS-u, nadzoruje pracę systemu i użytkowników.

T

Tracerout — jest to proces pozwalający na określenie, przez jakie komputery przechodzi informacja zanim dotrze do odbiorcy.

Trojan horse — patrz: *Koń trojański.*

Tylne drzwi — patrz: *Back Door.*

U

UIN — jest to unikatowy numer identyfikacyjny dla poszczególnego posiadacza ICQ, który pełni funkcję podobną do adresu e-mail.

Underground — podziemie.

Upgrade — uaktualnienie.

W

Wan (Wide Area Network) — jest to sieć złożona z komputerów znajdujących się od siebie w dużej odległości (np. Internet). Do ich połączenia wymagane jest najczęściej zastosowanie publicznej sieci telekomunikacyjnej.

Warez — jest to określenie pełnej, komercyjnej wersji oprogramowania dostępnej w sposób nielegalny. *Webmaster* — dosłownie: mistrz sieci. Jest to człowiek, który zajmuje się tworzeniem i utrzymywaniem serwera oraz stron WWW.

X

X Window — nakładka typu klient/serwer opracowana dla systemów Linux czy Unix. Ułatwia pracę z tymi systemami za pomocą wygodnych interfejsów graficznych, mogących przybrać formę bardzo zbliżoną do Winsows. X Window pozwala na zdalną pracę z oddalonymi komputerami prowadzoną poprzez Sieć. Jako że wprowadza to „większy zamęt" w krystalicznie czystym systemie, hakerzy wolą z niego nie korzystać.

Y

Y2K (Year 2 thousand) — jest to ostatnio bardzo popularne określenie błędu w oprogramowaniu, które mogło poważnie zagrozić światu w roku 2000 (ale objęte problemem jest także kilka pochodnych dat).

Z

Zin hakerski — magazyn hakerski (gazeta, biuletyn) wydawany w wersji elektronicznej.