2. fejezet - Tartalom

2 A Windows-rendszerek (9x, NT, 2000) gyenge pontjai

Míg a Windows 95/98/ME fejlesztésénél a Microsoft a felhasználóbarátság kedvéért elhanyagolta a biztonságot, a professzionális területre készült termékek (Windows NT 4.0 és Windows 2000) tervezésénél sokkal tudatosabban koncentrált erre a témára. A hackereket egyenesen csalogatják a gyenge pontok, hogy behatoljanak a rendszerekbe. Ráadásul a felhasználói operációs rendszerek gazdái is nagyon megkönnyítik a támadók dolgát. A Windows 95/98/ME felhasználóinak (és valószínűleg azok nagy részének is, akik a Windows XP Home Editionnel fognak dolgozni) többnyire csak csekély ismeretei vannak a biztonságról, és azokról a veszélyekről, amelyeknek az adataikat kiteszik.

Mivel az adataink nem csak az internetes szörfözés közben vannak veszélyben, ez a fejezet az *adatbiztonság egészével* foglalkozik, ami a BIOS-jelszónál kezdődik.

2.1 A hackeren túl - merevlemez-fejreállás, adatbetekintés vagy lopás

A biztonság tulajdonképpen az adatok biztosítási lehetőségeinek az alapvető mérlegelésénél kezdődik, ami sok - a legtöbb? - esetben egyáltalán nem történik meg. Manapság szinte minden számítógép-használónak vannak olyan adatok a gépén, amelyeknek az elvesztése, illetve az újbóli előállítása a PC árának többszörösébe kerülne. És akkor a további kockázatokat, például egy lopását, még figyelembe se vettük: ugyan ki szeretné az utolsó adóbevallását vagy bizonyos leveleit rossz kezekben tudni?

Az egyedülálló PC-t ugyan inkább a külső hatások (vírusok, lopás stb.) vagy a hibás kezelés veszélyezteti, ennek ellenére rengeteg más lehetőség is van hozzáférni a személyes adatokhoz: otthon vagy az irodában alapvetően mindenki odaülhet a géphez - és még a legfifikásabb BIOS-jelszó sem ér sokat, ha a számítógép ebédszünetben bekapcsolva marad. Hogy mennyire biztonságosak a jelszóval védett képernyőkímélők, azt a későbbiekben megmutatjuk.

A magánfelhasználók, de gyakran még a vállalatok is visszariadnak egy jó tűzfal költségeitől, vagy a kényelem kedvéért lemondanak a BIOS-jelszóról, Így a felhasználók ezekkel az operációs rendszerekkel a jövőben is könnyű prédái lesznek mindenfajta hackertámadásnak.

2.1.1 Különbségek a Windows 9x, az NT és utódai között

A különböző operációs rendszerek közötti alapvető különbség, ami igazán csak most, az XP-vel fog megszűnni: az eddigi Windows 9x vonal *csak korlátozott védelmet* (BIOS-jelszó) kínál a jogosulatlan felhasználás ellen. Az NT vagy a Windows 2000-es gépeknél ott van még a jelszavas bejelentkezés, mint köztes fokozat, amely növeli a biztonságot. Emellett az NT-nél és a Windows 2000-nél az adatokat már eleve zárolni lehet, ami a 9x-nél kiegészítő szoftvertől függ.

A Windows 95/98/ME-t érő támadásoknak két fajtáját kell megkülönböztetni. Az egyik a *fizikai támadás,* amit olyan valaki hajt végre, akinek közvetlen elérése van a rendszerre, a másik a *távoli elérésű támadás,* amelyet az internetről indítanak.

2.1.2 A fizikai támadás

A számítógépek védelmének nem túl gyakori módja a *BIOS-jelszó beállítása,* amelyet a felhasználónak a számítógép minden indításához be kell írnia, mielőtt a grafikus felület megjelenne.

Sajnos, a hackereknek arra is vannak módszereik, hogy ezt a védelmet megkerülve jussanak be a rendszerbe. Alapigazság, hogy minél öregebb egy számítógép, és vele együtt a BIOS, annál könnyebb kikerülni, illetve feltörni a védelmet.

A BIOS-jelszavas lezárás megkerülésének, illetve feltörésének három alapvető módját különböztetjük meg:

- általános jelszó használata
- a jelszó megszerzése a memóriából
- a CMOS szoftverének törlése

Általános jelszó használata

A különböző BIOS-verziók gyártói adnak egy *általános* vagy *defaultjelszót,* arra az esetre, ha a biztonságáért aggódó felhasználó egyszer el találná felejteni a jelszavát. Ezekkel a jelszavakkal a számítógépet az utoljára használt és mentett jelszótól függetlenül lehet elindítani. Ezeket a jelszavakat számos oldalról be lehet szerezni az interneten, de valójában a legtöbbnél kérdéses, hogy vajon még működnek-e, vagy már teljesen elavultak.

Ezeknek a jelszavaknak a többségét sikerrel teszteltük, a használatuknál azonban figyelni kell az amerikai billentyűzetkiosztásra.

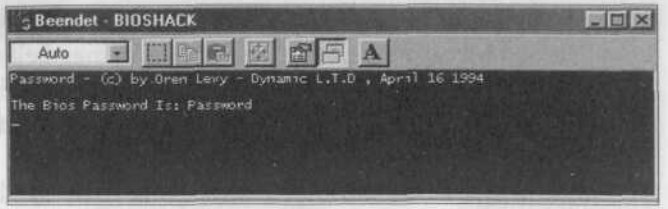
Gyártó: Award	Gyártó: AMI	Gyártó: Phoenix	Általános jelszavak
BIOSSTAR	PASSWORD	PHOENIX	aLLy
BIOSTAR	Ami	phoenix	Wodj
ALFAROME	A.M.I.	CMOS	SZYX
q_127&z	AMI?PW	BIOS	Syxz
J64	AMI?SW		Sxyz
J262	AMI_SW		SKY_FOX
J256	AMI		setup
j262			SER
j256			LKWPETER
AWARD_SW			lkwpeter
589589			HLT
AWARD_PW			CONDO
AWARD_PS			awkward
AWARD?SW			BIOSTAR
AWARD SW			
AWARD			
589721			

Általános BIOS-jelszavak

A jelszó megszerzése a memóriából

A jelszó memóriából történő megszerzése feltételezi, hogy a gép már elindult, ilyenkor ugyanis segédprogramokkal el lehet érni a memóriában tárolt jelszót. A különböző BIOS-verziókhoz különböző programok vannak, amelyeket könnyen be lehet szerezni az internetről.

Password-BIOS-Hacker Oren Levytől



Program	BIOS	Szerző	Forrás
AMIDECOD	AMI	Danny Soft	www.hackerzbook.de
Award Modular Bios crack tool	Award	The Immortal	www.hackerzbook.de
CrackAmiBios 1.1	AMI	Ismeretlen	www.hackerzbook.de
Password	általános	Oren Levy - Dynamic	www.hackerzbook.de
Password (C)alculator for AWARD BIOS	AWARD	FalCoN 'N' AleX	www.hackerzbook.de

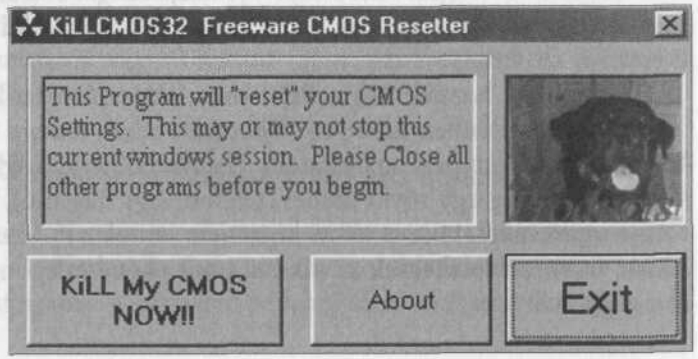
Programok a jelszó kiderítéséhez a memóriából

A CMOS szoftverének törlése

Ha a hacker nem talál általános jelszót vagy megfelelő segédprogramot, nem marad más hátra, mint törölni a BIOS-t, és azzal együtt a jelszót is. Azt persze figyelembe kell vennie, hogy ilyenkor a rendszerbeállítások is elvesznek.

A BIOS törléséhez megint csak segédprogramokat használnak a „betörők", ezek közül az egyik legismertebb a *KiLLCMOS32.* Ez a segédprogram minden beállítást töröl, és minden BIOS-verzióhoz használható. Mindenesetre a rendszernek már futnia kell a használatához.

A KiLLCMOS32 minden BIOS-beállítást megbízhatóan töröl



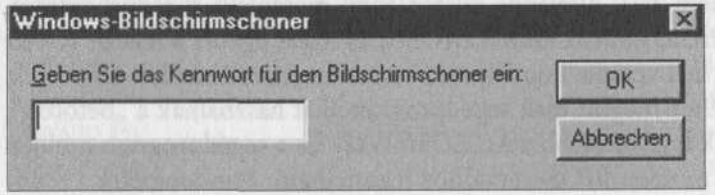
A program egy érvénytelen értéket helyez el a CMOS-ban, és ez úgy hat, hogy minden ott tárolt adatot (a jelszót is) újra meg kell adni. A használatának a feltétele azonban az, hogy a számítógép már működik, és szabad a hozzáférés.

A http://www.memosys.com/passwort/faq.htm címen további információk találhatók a BIOS-jelszavakról.

A jobban informált internet-felhasználók néha azt hiszik, hogy egy rendszert csak az internetről érhetnek támadások, és ez ellen egy tűzfallal jól meg is védik a gépüket. De mi van akkor, ha valaki mondjuk az ebédszünetben fizikailag fér hozzá a számítógéphez? Milyen módszereket fog alkalmazni, hogy kikerülje a képernyővédőt és jelszavakat olvasson ki?

2.1.3 Képernyővédő-jelszó- a bennfenteseknek nem okoz problémát

Hogy a számítógépünk rövid távolléteink alatt is védve legyen a kíváncsi szemektől, arról a Windows 95/98/ME alatt a legegyszerűbben *képernyővédő-jelszóval* gondoskodhatunk. Ez a képernyővédő bekapcsolása után csak a megfelelő jelszót megadó felhasználónak engedi meg a rendszer elérését.



Ha a Windows csővezetéket épít vagy Bezier-görbéket mutat - csak jelszóval lehetséges a visszatérés

Windows 95/98/ME alatt a *Képernyő tulajdonságai* ablakban a *Képernyőkímélő* regiszterlapon a képernyőkímélő bekapcsolása után zárolni lehet a rendszer elérését.

Ha mások is hozzáférnek a PC-nkhez, alapvetően be kell állítanunk ezt a jelszót, mert különben könnyen űzhetnek velünk csúnya tréfát: képzeljük el, hogy valaki három perc után induló jelszavas képernyővédőt állít be a gépünkön. Ezután elég egy rövid szünet (telefon vagy hasonló), és máris megakasztotta a munkánkat. Hiszen jelszó híján nem jutunk a PC-hez újraindítás nélkül. Akkor viszont elveszhetnek az adatok, amelyeket esetleg még nem mentettünk el - nagy az ár.

A Windows a jelszó megerősítését kéri

így lehet feltörni a jelszóvédelmet

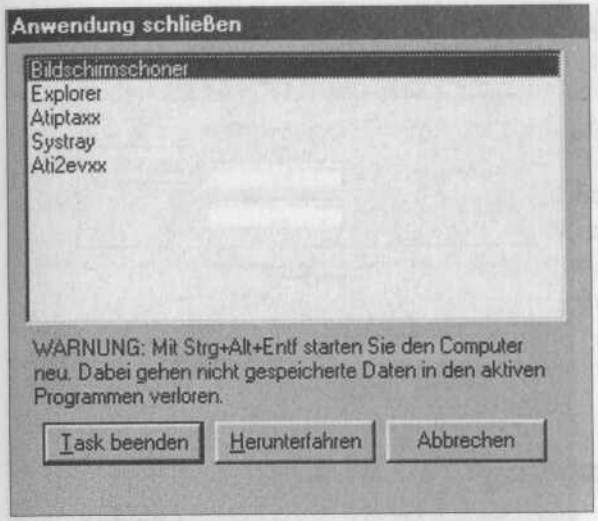
Az alábbiakban megvilágítjuk, milyen könnyű egy képernyőkímélő jelszavát kikapcsolni, illetve kikerülni, ha a hackernek ehhez elég ideje és tudása van.

Újraindítás

Igazán dühödt, primitív, de hatásos módszer a képenyőkímélő-jelszó kikerülésére: a számítógép újraindítása a *reset* gombbal. Figyelembe kell venni, hogy a nem mentett adatok minden esetben elvesznek, így például a nem mentett Word-dokumentumok vagy a nyitott fájlok stb. Szerencsére ilyenkor a rendszer felhasználója észreveszi a behatolást.

Taskmanager - kapu a betörőnek Windows 95 alatt

Windows 95 alatt a Microsoft még egyszerűbb módot kínál a képernyőkímélő kikerülésére: a Ctrl+Alt+Del billentyűkombináció lenyomásával •- mondhatni „majomfogással" - célzottan be lehet zárni a képernyőkímélő program taskját.



Rossz csillagzat alatt született a védelem: egy egérkattintással be lehet zárni a képernyőkímélőt

Védelmi lehetőség Windows 95 felhasználóknak

Ez ellen a támadás ellen csak a Windows 95 Windows 98/ME-re frissítése nyújt védelmet. A képernyőkímélő-jelszó elkerülésének ilyen kísérletei az NT/2000-nél is hatástalanok.

A későbbiekből az is ki fog derülni, hogyan is lehet feltörni az ilyen jelszót, mert a jelszavas védelem is csak korlátozott mértékben nyújt biztonságot. A jelszó megfejtése a megfelelő szoftvereszközzel igazán egyszerű, jobb, ha tudjuk, hogy mennyire az. így persze rögtön magunkon is segíthetünk, ha elfelejtettük a saját jelszavunkat.

2.1.4 Automatikus lejátszás - a betörés előkészítése CD-vel

A PC-t a BIOS-szal, a képernyőkímélőt jelszóval zároltuk, és talán még a jelszót is úgy választottuk meg, hogy az betűk és számok kombinációjából álljon - most aztán a PC-nk szünetben is bevehetetlen, vagy lehet, hogy mégsem? A következőkből kiderül, hogy milyen eszközöket vethet be ebédszünetben egy potenciális hacker, hogy minden igyekezetünk ellenére hozzáférjen az adatainkhoz.

A Windows 95/98/ME a CD-ROM-meghajtóhoz alapértelmezésként az *autoplay* (automatikus lejátszás) opciót használja, amelyet *a Microsoft Knowledge Base Article Q141059* a következőképpen definiál:

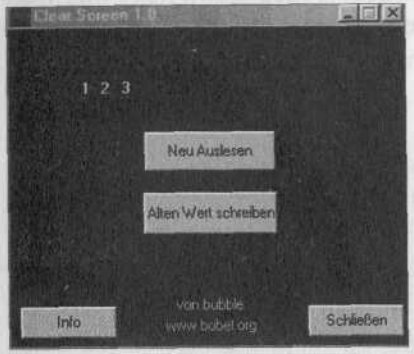
„A Windows folyamatosan ellenőrzi a CD-ROM-meghajtót, hogy megállapítsa, helyeztek-e bele CD-ROM-ot. Ha ilyen lemezt fedez fel, ellenőrzi, hogy van-e rajta *autorun.inf*-fájl. Ha a CD tartalmaz ilyen fájlt, akkor végrehajtja a fájl *open*= sorába írt parancsokat."

Megjegyzés: ezt a témát még a 4.fejezet is tárgyalja, mert az automatikus lejátszás funkciót gyakran használják trójai vírus becsempészésére idegen rendszerekbe. Ehhez lehet a rendszer esetleg futó internetkapcsolatait (vagy hálózatoknál a LAN-kapcsolatokat) használni, és így a PC-hez a képernyőkímélő-jelszó ellenére hozzá lehet férni. Ha a trójai már bent van, a képernyőkímélő-jelszót egészen egyszerűen ki tudja kerülni. Egy ilyen hozzáféréssel a képernyőkímélő-jelszót is ki lehet kapcsolni úgy, hogy: *HKEY_CURRENT_USER/Control Panel/desktop/ScreenSaveActive* Registry-kulcs értékét nullára állítjuk.

Van néhány program, amelyeket az automatikus lejátszás funkcióval, a jelszómegadást kikerülendő, fel lehet másolni. Ezeknek a programoknak egyike a *Clean Screen*. Íme, a használati utasítás, amellyel szükség esetén magunkat is kiszabadíthatjuk (az előkészületeket azonban *előre* meg kell megtenni, nehogy túl késő legyen):

1. Letölteni **(www.hakerzbook.de)** és kicsomagolni a ZIP fájlt!
2. Az *EXE* fájlt és az *autostart-ini*-t CD-re írni. A két fájlnak a könyvtárfán egészen felül kell lennie, tehát ne valamilyen alkönyvtárba másoljuk.
3. Ha a CD-írás elkészült, akkor egyszerűen próbáljuk ki egyszer a saját PC-nken.
4. Képernyőkímélő-jelszó beállítása, majd várakozás, míg a képernyőkímélő elindul.
5. Tegyük az újonnan megírt CD-t a meghajtóba, és várjunk, amíg a PC hangszórója sípolni kezd. Ha nincs bekötve, egyszerűen várjuk ki, míg a CD-ROM-meghajtó leáll.
6. Ezután már csak írjuk be a jelszó lekérdezésére az 123-at, és a képernyőkímélőnek el kell tűnnie!

7. Ezután a program kiírja a régi jelszót, és a *Régi érték beállítása* paranccsal vissza lehet állni rá. Ha ezt nem tesszük meg, aktuális jelszóként a 123-at tárolja.



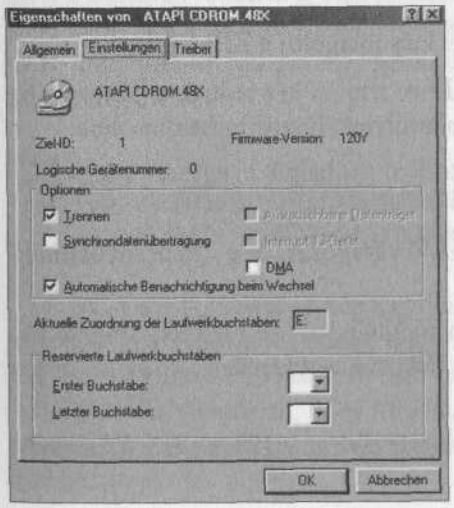
A képernyőkímélő-jelszó megszerzése autoplay CD-vel

Védekezés az automatikus indítások támadások ellen

Ezeket a támadásokat úgy védhetjük ki, ha a Windows 95/98/ME alatt kikapcsoljuk az automatikus lejátszás funkciót. Ez a következőképpen működik:

A *Vezérlőpulton* kattintsunk duplán a *Rendszerre,* válasszuk az *Eszközkezelő fület,* kattintsunk duplán a *CD-ROM-ra,* és aztán a *CD-ROM meghajtófára.*

A *Beállítások* regiszterlapon távolítsuk el a pipát az ***Automatikus*** *lejátszás elől.*



Itt találjuk a döntő fontosságú pipácskákat

A képernyőkímélő jelszó kikódolása

A képernyőkímélő jelszót a Windows 95/98/ME alapértelmezésként a *HKEY\USERS\.Default\Control Panel\Sreen_Save_Data* Registry-kulcsban tárolja. A kódolása nagyon egyszerű, és számos programmal feltörhető.

A legtöbb programnak az a hátránya, hogy csak akkor működik, ha a képernyőkímélő még nem aktív (hogy mit tehetünk, ha már az, azt már tudjuk).

Jelszófeltörő program működés közben

Néhány program a képernyőkímélő-jelszó feltöréséhez:

Program	Szerző	weboldal
SCR-it! - 1 .0 verzió	Yoto Yotov	www.hakerzbook.de
SCRNLOCK	Yoto Yotov	www.hakerzbook.de
SS_D 1.0	Bubble	www.hakerzbook.de
Win95 Screen Saver Password Cracker v1 . 1	nobody	www.hakerzbook.de

Programok a képernyőkímélő-jelszó feltöréséhez

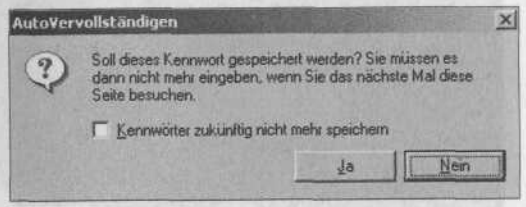
2.2 A jelszavak kikémlelése

2.2.1 Érdekes jelszavak szinte mindenütt akadnak

A helyi támadásoknál nagy szerepe van *a jelszavak kikémlelésének.* Jelszófeltörők segítségével a hackerek szinte minden, Windows alatt tárolt jelszót meg tudnak szerezni, hogy azután elérjenek velük jelszóval védett fájlokat, az

internetet vagy a hálózatot, illetve ezek bizonyos területeit. Sajnos, a Microsoft nagyon megkönnyíti a betolakodóknak, hogy hozzáférjenek ezekhez az információkhoz, a felhasználóknak pedig egyre nehezebbé teszi a jelszavak elrejtését. Erre egyszerű példák találhatók az Internet Explorernél és a telefonos kapcsolatnál.

Az Internet Explorer a 4. verziótól kezdve egy ***automatikus*** *kiegészítést* használ, amely a belépési adatok megadása után megkérdezi a felhasználótól, hogy szeretné-e menteni ezeket.



Praktikus segítség a felhasználóknak és a betörőknek - az automatikus kiegészítés

Az így tárolt információkat egy jelszófeltörő segítségével nagyon könnyű kiolvasni. Különösen veszélyes ez a telefonos kapcsolatnál, mert akár odáig vezethet, hogy valaki, az adatokat kiolvasva, a felhasználó költségén szörfözhet az interneten.

íme egy aktuális példa:

2001. november *5.* hétfő de. 10:30

Németország: Hackerek milliós csalása

... Jelszavak ezreit törték fel

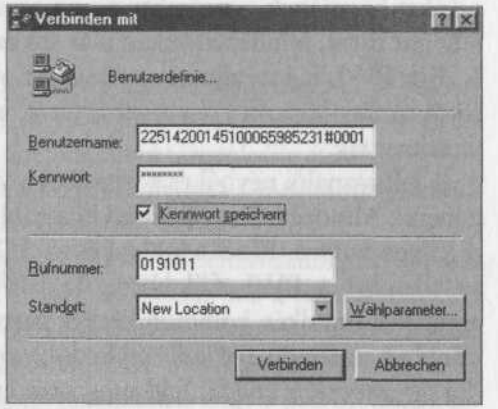
A nyomozók hackerek nagy szabású csalásainak a nyomára bukkantak, akik mit sem sejtő PC-tulajdonosok költségére szörföztek az interneten. Egy kb. 30 feltételezett tettesből álló kör több ezer számítógép-felhasználó jelszavát törte fel - számol be a *Der Spiegel* hírmagazin nemrégiben megjelent tudósítása.

A dortmundi és a münsteri államügyészség két nagy ügyében kerek kétmillió márkára becsüli a károkat. A mit sem sejtő felhasználók számlájára esetenként akár havi 20 ezer márkáért is interneteztek. A hackerek a jelszavakat még az idevágó weboldalakon is nyilvánossá tehették - mondják. Münsterben már 3600 nyomozási eljárás lezárult. Ezek az ügyek azonban az államügyész adatai szerint már egy fél évvel ezelőttiek.

A dortmundi államügyészségnél több mint 1000 eljárás van folyamatban gyanúsítottak ellen egész Németországban. (dpa)

Forrás: www.silicon.de

Internetezzünk olcsón - sokkal több nem is kell hozzá

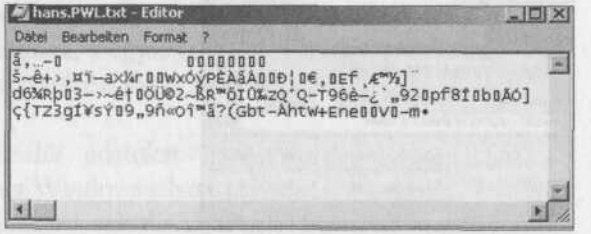


2.2.2 A jelszófájlok

A Windows 95/98/ME *PWL fájlokban* tárolja a jelszavakat és a felhasználói neveket. A PWL a *PassWord Library* rövidítése. Minden felhasználói profil tartalmaz egy saját *PWL* fájt, a fájlnév pedig a mindenkori felhasználó neve lesz. Példa: ha a Windowsba *Jani* néven jelentkezünk be, a PWL fájl *nevejani.pwl* lesz. A Windows minden PWL-fájlt a Windows könyvtárban tárol, tehát a *c:\windows* alatt.

A Windows 95/98/ME alatt minden program eléri a PWL fájlokat, hogy adatokat tudjon elhelyezni bennük, így tárolódnak például a meghajtók és a nyomtatók hozzáférési jelszavai, a telefonos kapcsolat jelszavai és a Windows bejelentkező nevek.

A kódolt jelszó az első pillantásra még ártalmatlan



A kódolás

A Microsoft a Windows 95 első verzióiban nem nagyon strapálta magát a kódolás algoritmusával, ami viszonylag egyszerűvé tette a hackereknek ezek megfejtését, illetve feltörését. A következő verziókban már olyan kódolási technikákat használtak, amelyeket ugyan továbbra is számos segédprogrammal fel lehetett törni, mindez azonban már sokkal több időbe telt.

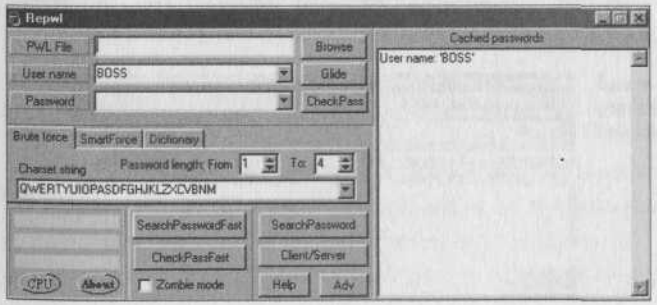
Egy PWL fájl tartalmaz egy *header*-t, valamint a fájl létrejöttének a dátumát, továbbá úgynevezett *rekordokat* is tárol, amelyek a tulajdonképpeni jelszavakat tartalmazzák.

A felhasználói névből és a jelszóból a Windows 9x egy *32 bit hosszúságii kódot* generál. Mindegy, hogy a jelszó hosszabb vagy rövidebb 32 bitnél, a kód mindig ilyen hosszú. Ezzel a kóddal és az *RC4 algoritmus* egy változatával kódolják az adatokat a PWL fájlokban. Az RC4 egy szimmetrikus kódolási eljárás, amelynél mindkét kommunikációs partner ugyanazt teszi - csak ellenkező irányban. A feladó egy kulccsal kódolja az átvitelre szánt adatokat, a fogadó pedig ugyanezzel a kóddal fejti meg az üzenetet. A szimmetrikus kódolás előnye mindenekelőtt a kódolás nagy sebessége, és az, hogy az eljárást könnyű implementálni. Hátrányként jelenik meg a kódkicserélés problémája és a ráfordításigényes kódnyilvántartás.

Sajnos ezt a kódot a megfelelő eszközzel másodpercek alatt fel lehet törni, ehhez számtalan eszköz áll a hackerek rendelkezésére a hálón, ráadásul a trójaiakba is gyakran integrálnak olyan programokat, amelyek lehetővé teszik a célszámítógép valamennyi jelszavának azonnali kiolvasását.

Jelszófeltörők

Mint már említettük, a Windowshoz *sok jelszófeltörő van,* amelyek lehetővé teszik a Windows jelszavak kikódolását, illetve kiolvasását. A nagyobb PWL



A számokból és betűkből álló kombinációk a jelszófeltőrőket is megizzasztják

fájloknál azonban sok idő kell a jelszavak kiolvasásához. Ilyenkor a hackerek gyakran lemezre menük a PWL fájlokat, amelyeket egy másik számítógépre másolhatnak, hogy ott zavartalanul és időkorlát nélkül kikódolhassák.

Védelmi lehetőségek

Hogy a jelszófeltörő programoktól megvédhessük magunkat, a Windows 95/98/ME alatt lehetőség van a *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Network\DisabledPwdCaching = 1* Registry-kulcs létrehozására. Ez a kulcs megakadályozza a megadott jelszavak tárolását, és ezzel lehetetlenné teszi a kiolvasásukat is.

Továbbra is ajánlatos azonban, főleg a Windows 95 felhasználóknak, a frissítés egy erősebb kódoló algoritmusra. Ehhez az update-hez a **http://support.microsoft.com/support/kb/artícles/Q132/8/07.asp** oldalon juthatunk hozzá.

Van egy program is, amely megakadályozza a jelszavak kiolvasását. A *PassSecure* a *Multimedia Network Systemstől* meggátolja, hogy a jelszófeltörők elérjék a PWL fájlokat.

2.2.3 Jelszavak a Windows 2000 alatt

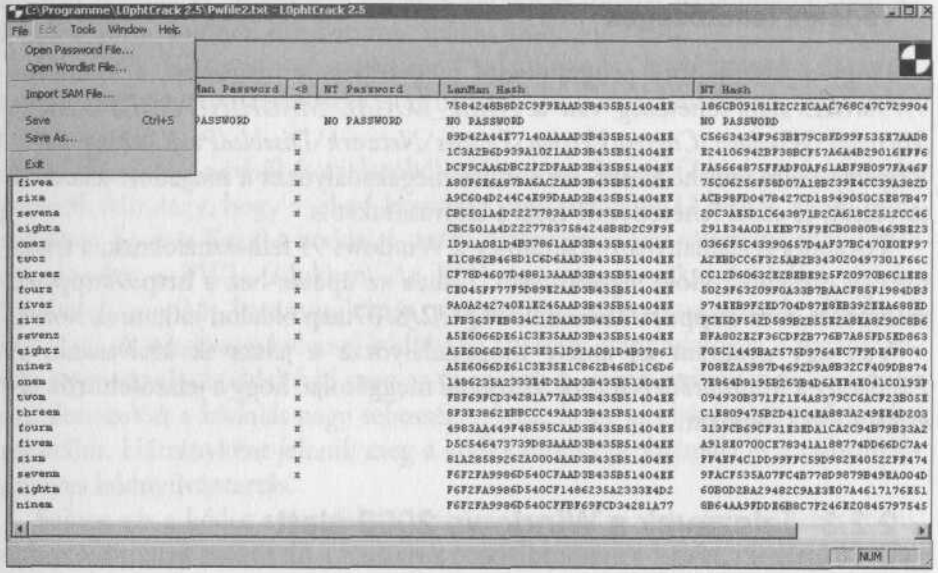
A *Windows 2000* alatt egészen más a jelszavak kezelése, mint a Windows 95/98/ME alatt. A Windows 2000 automatikusan ellenőrzi a jelszavak biztonságosságát, s automatikusan figyelmeztet az általános jelszóbiztonság elleni vétségekre. A Windows 2000 ellenőrzi minden jelszó hosszát, a jelszavak rendszeres változtatását és a karakterek sokszínűségét. Ezeknek az adatoknak az alapján a Windows 2000 ki tudja számítani a jelszavak biztonsági kockázatát, és szükség esetén figyelmezteti a felhasználót.

A Windows valamennyi jelszót egy *SAM (Security Account Manager)-adatbázisban* tárol, ez az adatbázis a *Registry* része.

Ha Windows 2000 alatt bejelentkezik egy felhasználó, az adatai a *Security Account Manager*-hez továbbítódnak, s egyfajta „jogosultsági igazolványt" kap, amelyben rögzítve vannak a hozzáférési jogai, és hogy melyik felhasználói csoporthoz tartozik.

A SAM azokat a felhasználói adatokat használja, amelyeket a *winnt/system32/config/sam* fájl tárol. Ez a Windows jelszó mellett a hálózati jelszót is őrzi. Ezt a fájlt nem lehet közvetlenül elérni, mivel a Windows állandóan használja.

Időközben azonban számos *Brute Force program* is íródott, amelyek az NT és a Windows 2000 alatt is lehetővé teszik jelszavak hackelését. Az egyik legismertebb közülük a legendás *LOphtCrack 2.5.* Ez a program úgy kerüli ki a hozzáférési védelmet, hogy a háttérben egyfajta másolatot készít a SAM-fájlról.



LOphtCrack 2.5 - tolvajkulcs a Windows 2000 jelszavakhoz

A LOphtCrack kétféleképpen tud jelszavakat feltörni. Az első módszer a *dictionary cracking,* amelynél gyakran használt jelszavak és karakterek listáját használja, hogy kitalálja a jelszót. A második a *brute force cracking,* ahol minden lehetséges szám és/vagy szókombinációt kipróbál. (A jelszófeltörés témáját a 7. fejezet részletesen újratárgyalja.)

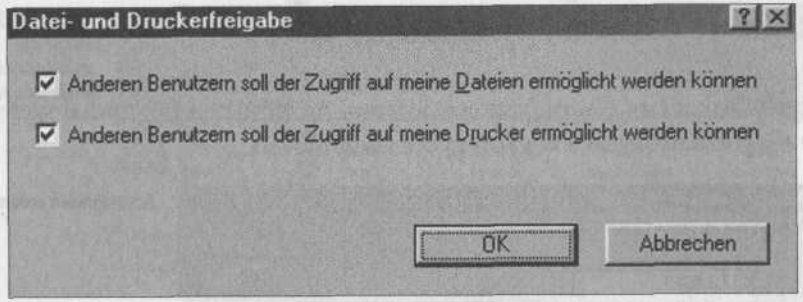
2.3 A távoli elérésű támadás - internet- vagy hálózati felhasználók, vigyázat!

Egyet világosan kell látni: egy távolból jövő támadás egy Windows 95/98/ME rendszer ellen, szabvány konfigurációban, egyedüli PC-ként és trójai nélkül, valóban nehéz. Azonban a strandard konfigurációt gyakran meg kell változtatni, például a rendszer hálózatra csatlakoztatása miatt. Az adathordozók minden védelem nélküli megosztása vagy a slamposan megadott jelszavak gyakran szélesre tárják a kaput a betolakodók előtt. Ebből a fejezetből kiderül, hogyan lehet felderíteni az ilyen megosztott erőforrásokat.

Ráadásul az ISDN, az xDSL és a flatrate-ek korában, amikor a felhasználók rendszerei gyakran folyamatosan kapcsolódnak az internethez, elég idejük van a hackereknek arra, hogy a cél érdekében számtalan támadási módot kipróbáljanak, így például a rendszer különböző réseinek a szkennelését.

2.3.1 A fájl- és nyomtatómegosztás - veszélyes biztonsági rések

A fájl- és nyomtatómegosztást tulajdonképpen arra használják, hogy lehetővé tegyék a felhasználóknak a mappák vagy az adathordozók elérését a hálózaton. Mióta egyre több felhasználó épít ki otthon is kis hálózatocskát, hogy továbbra is használni tudja a régi PC-jét, vagy hogy időnként csatlakoztatni tudjon egy notebookot, a megosztás a magánemberek számára is a biztonságot meghatározó témává vált.

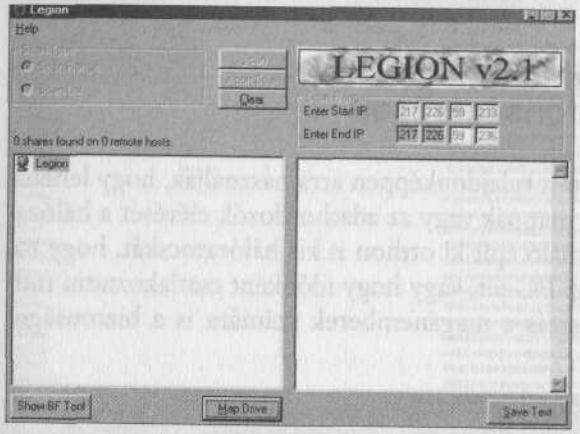


Itt egy kockázati tényező rejtőzik, amelyet nem veszünk észre

E szolgáltatások felhasználói általában nincsenek tisztában azzal, hogy milyen veszélyeknek teszik ki az adataikat az internethez kapcsolódással. A kár, amelyet a hackerek okoznak, főleg attól függ, hogy milyen megosztásokat használ a felhasználó. A könyvhöz végzett kutatások során valóban találtunk olyan rendszereket, amelyeknek a felhasználói minden meghajtót megosztottak, méghozzá minden jelszóvédelem nélkül. Az ilyen esetek természetesen durva gondatlanságról tanúskodnak, ugyanakkor újra bebizonyítják, hogy mennyire könnyelműen mozognak egyesek a hálón.

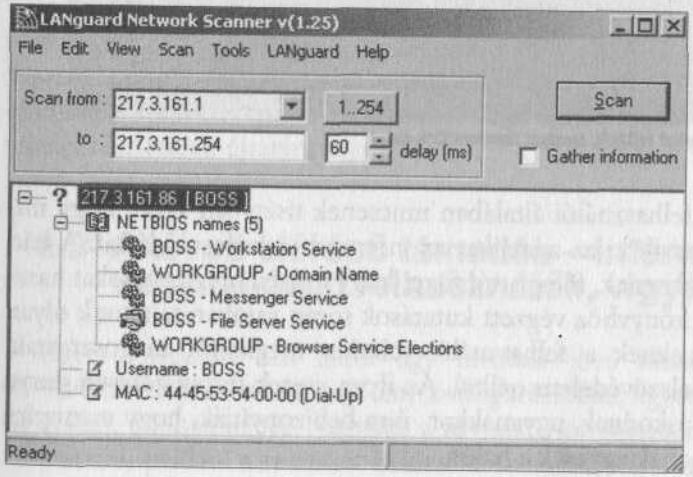
2.3.2 Mik azok a szkennerek, és hogyan működnek?

A megosztások felkutatása *szkennerprogramokkal* történik. Az egyik legismertebb ilyen a *Légion,* a *Rhino9* szerzeménye. A Légion minden megosztást szkennel a számítógépen, majd grafikusan megjeleníti ezeket. Sajnos, a Légion nagyon megbízhatatlan, és nem mindig találja meg azonnal a megosztott erőforrásokat, ami több szkennelést tesz szükségessé.



A megosztások felkutatásához elegendő a számítógép IP-területe

Egy másik a *Lan Guard Network Scanner.* Az előnyei a Légionnal szemben a nagy megbízhatóság és a nagyon gyors szkennelés.



A szkennelés eredménye

Csak a számítógépről szállít információkat, és semmilyen támadóeszköze nincs, ami azt jelenti, hogy a jelszófeltöréshez egy másik eszközt, például a Légiont kell használni.

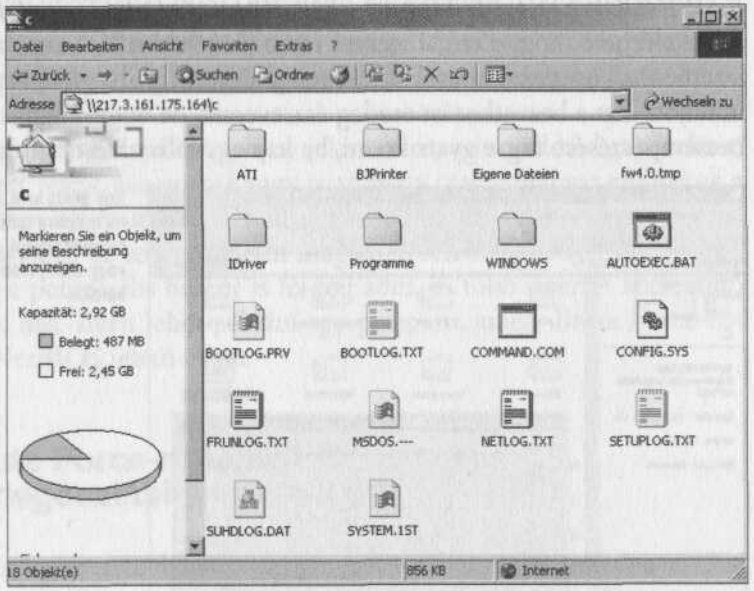
Név	URL	Operációs rendszer
Auto NetBIOS Hacker	www.hackerzbook.de	Windows 9x/NT/2000
Légion	www.hackerzbook.de	Windows 9x/NT/2000, UNIX/Linux
NAT	www.hackerzbook.de	Windows 9x/NT, UNIX/Linux
SharesFinder	www.hackerzbook.de	Windows 9x/NT/2000

Programok a megosztások felkutatásához

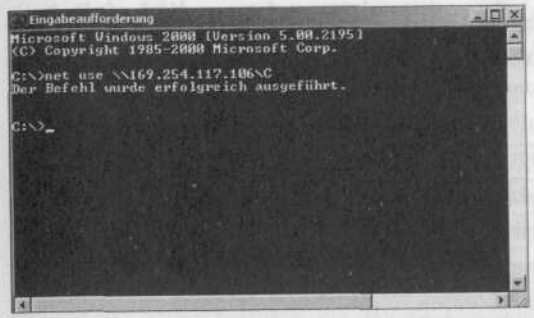
Hozzáférés a szabad erőforrásokhoz

A talált megosztott erőforrások elérése a következők szerint történik: a támadó egyszerűen beírja a talált IP-címet a Windows Intézőbe, például *\\217.3.161.59.* A következő ábra a megosztott C: merevlemez tartalmát mutatja egy, a hálózaton keresztül elért számítógépen. Nem nehéz felismerni a lehetséges kockázatokat és károkat.

Kapcsolódás egy másik számítógéphez, fájlmegosztással



A DOS alatt a *NET USE* paranccsal is lehet kapcsolatot teremteni.

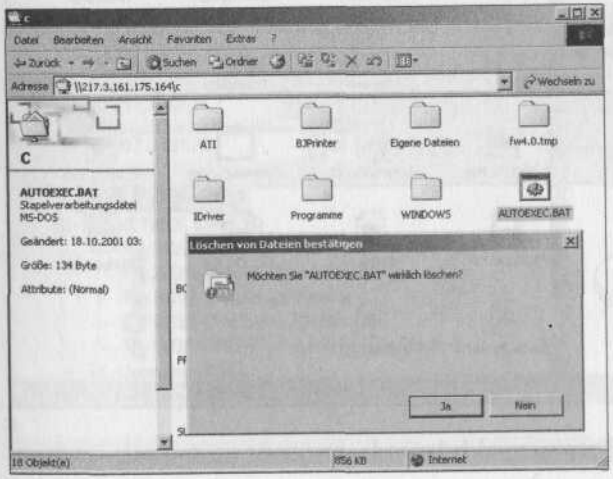


Így lehet DOS alól elérni a másik számítógépet

2.3.3 Milyen lehetőségeik vannak a betolakodóknak?

A megosztott mappát vagy meghajtófájlokat a megosztás módja szerint lehet elérni.

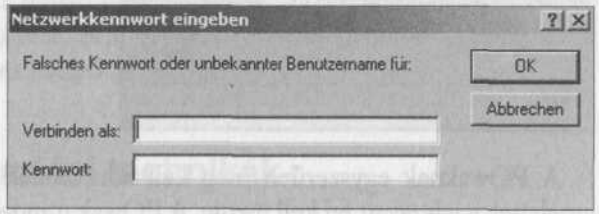
Annak megfelelően, hogy milyen hozzáférési módokat adtak meg, a betolakodó másolhat, feltölthet, vagy a kedve szerint törölhet, ahogy neki tetszik. Egy különösen kedvelt támadási mód egy trójai vírust elhelyezni a *C:\WINDOWS\STARTMENÜ\PROGRAMOK\INDÍTÓPULT* könyvtárban. Ezzel elérhető, hogy a trójai szerver része (közelebbit lásd a trójaiakról szóló fejezetben) a következő bootolás után telepítődjön, a fájl törlődjön, és a szerver elinduljon. Ezt a beavatkozást esetleg észreveszik, de hogy a felhasználó egy trójai becsempészésére fog-e gyanakodni, ha kap egy hibajelzést, az bizony kérdéses.



Egy példa arra, hogy mi mindent tudnak megváltoztatni, törölni, vagy manipulálni a behatolók

2.3.4 Jelszóval védett megosztások

A megosztott erőforrásokat természetesen jelszóval lehet védeni. Ezzel megvalósíthatjuk, hogy senki se férjen hozzájuk jogosulatlanul a hálózatról vagy az internetről.



A legegyszerűbb védelem: jelszavak az erőforrásokhoz

Persze ez a védelem a szimpla jelszavak esetén meglehetősen sovány, amit némi tudással vagy megfelelő programmal könnyen ki lehet kerülni. Az is köztudott, hogy a felhasználók kényelemszeretetből gyakran könnyen megjegyezhető jelszavakat adnak meg.

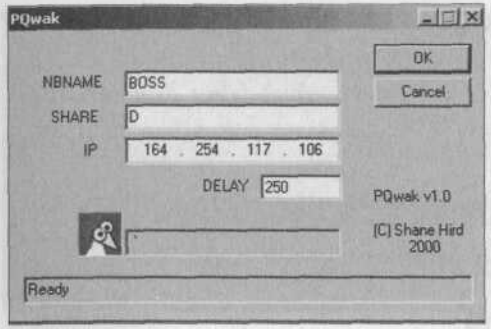
Az első, amit egy hacker programok segítsége nélkül is megtenne, a szisztematikus találgatás, ami a helyi hálózaton, ahol megvan a lehetősége, hogy a felhasználót személyesen is ismeri, rendkívül hatékony is lehet. Kezdhetné azzal, hogy végiggondolja a felhasználó minden ismert személyes adatát, és ezeket jelszóként végigpróbálgatja, pl. vezetékneveket, keresztneveket, barátnő, kutya nevét, születési adatokat...

De vannak gyakran használt szabvány jelszavak is, mint például *gast, admin, administrator, boss, jelszó, hónapnevek* vagy *teszt,* hogy csak néhányat említsünk a számtalan, gyakran hebehurgyán felhasznált jelszó közül.

Nehéz jelszavaknál ez természetesen meglehetősen értelmetlen vállalkozás, amit valamikor a potenciális hacker is fel fog adni, és több sikerrel kecsegtető módszerek után néz. Ilyen lehet például egy program, amely Brute Force-rohamot intéz a NetBIOS jelszó ellen.

2.3.5 Brute Porce-rohamok a megosztási jelszavak ellen

A legjobb és legismertebb ilyen programok egyike a *PQwak, Shane Hird* műhelyéből Ez az eszköz többek között a Windows 95/98 alatti fájlmegosztás egy implementációs hibáját használja ki.

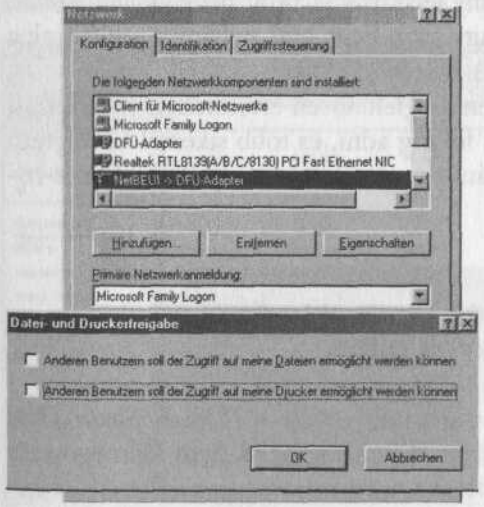


Előkészület a célzott támadásra

A PQwaknak egyszerűen meg kell adni annak a számítógépnek az IP-jét, amelynek a jelszavait fel kell törnie. A PQwak minden karaktert és különleges karaktert felismer, így azután a legrövidebb idő alatt szinte minden jelszót fel lehet vele törni. A PQwak 1.0-s verziója nincs túl gondosan programozva, sok különleges karakter hiányzik, és aki sikert akar elérni, annak gyakran kell újraindítania.

2.3.6 Óvintézkedések

A legegyszerűbb, amit tehetünk, ha védekezni akarunk az ilyen támadások ellen: a fájl- és nyomtatómegosztás megszüntetése a hálózati környezet beállításainál. Továbbá minden szükségtelen protokollt, köztük a NetBIOS-t is távolítsuk el.



Aránylag kényelmetlen, de veszélytelen - megszüntetjük a megosztásokat

Ez a megoldás azonban sok felhasználó számára szóba sem jöhet, mivel rá vannak utalva a megosztott erőforrások használatára. Tulajdonképpen csak erős jelszavak jöhetnek számításba, amelyek védik az erőforrásokat. Itt újból bizonyítást nyer az alfanumerikus kombinációk erőssége.

Szerverkörnyezetekben a rendszeradminisztrátor beállíthatja a jelszavak erősségét és futási idejét. Ez ugyan nem kínál százszázalékos védelmet, de jelentősen megnehezíti a betörést, és kiindulhatunk abból, hogy egy bizonyos idő múlva a még oly türelmes hacker is feladja.

2.4 További támadási technikák

A bemutatott biztonsági réseken kívül, amelyek az operációs **rendszer** felépítésében gyökereznek, természetesen vannak még más támadási lehetőségek is, amelyeket most csak bemutatunk.

Trójaiak - betörés a hátsó ajtón keresztül

Nagyon elterjedtek a támadások a hátsó ajtók, illetve a Remote Controll programok, ismertebb nevükön a *trójaiak* segítségével, amelyek külön fejezetet kaptak a könyvben (lásd 4. fejezet), és amelyekre most csak röviden szeretnénk kitérni.

A trójaiak a felépítésüknél fogva kitűnően alkalmasak arra, hogy jelszavakat kémleljenek ki, manipulálják a *Registry*-t, eljárásokat indítsanak vagy fejezzenek be, adatokat másoljanak, illetve töröljenek, és megosztásokat hozzanak létre.

Ezeknek a programoknak a problematikája az *egyszerűségükben* rejlik, ami azt jelenti, hogy a bonyolult támadásokkal ellentétben, itt semmiféle háttértudás megszerzésével nem kell foglalkozni.

Ez különösen a „szabadidős hackereknek" nyújt lehetőséget arra, hogy teljesen az uralmuk alá hajtsanak rendszereket. Az ilyen programok felhasználói ritkán gondolkodnak el cselekedetük következményeiről, és ennek megfelelő agresszivitással támadnak áldozataik rendszereire.

A felhasználók magatartása különösen a médiák felvilágosító tevékenysége nyomán az utóbbi években erősen megváltozott, és egyre gyakrabban figyelnek oda arra, hogy ne nyissák meg gondatlanul a mail-ékhez csatolt fájlokat. Mind gyakrabban használnak tűzfalakat, amelyek megakadályozzák a trójai szerver kapcsolódását a klienshez. Egyre jobban elterjednek a trójai-, illetve víruskere-

ső programok is, amelyek képesek észlelni és eltávolítani a szerveralkalmazásokat a rendszerben, illetve megfelelő figyelmeztetésekkel megakadályozni a telepítésüket.

De még mindig elég sok felhasználó van, akikben nem tudatosultak ezek a veszélyek, és fütyülve minden figyelmeztetésre, ismeretlen és komolytalan forrásból származó fájlokat nyitnak meg. A gyakorlatból ismerünk olyan eseteket, mikor már régóta ismert trójaiak, mint a *Sub7* vagy a *BackOrifice* (pontosabbat ezekről a programokról a trójaiakról szóló fejezetben) települtek olyan számítógépekre, amelyek vállalati hálózatokban működtek. Ez a magatartás durván felelőtlen, de a rendszergazdák valószínűleg csak a káresetekből fognak tanulni. A védekezés és a felismerés lehetőségeivel ugyancsak a trójaiakról szóló fejezetben foglalkozunk.