# 7. fejezet - Tartalom

# 7 Jelszófeltörés

Ez a fejezet *a jelszavak biztonságosságát* tárgyalja. A hackereknek változatlanul az okos jelszavas védelem jelenti az egyik legnagyobb akadályt, mivel az interneten és a helyi számítógépeken is gyakran védik jelszavakkal a fájlokat a jogosulatlan hozzáférések ellen..

A jelszavak kiderítésére, illetve feltörésére különböző lehetőségek vannak. Az egyik legfontosabb a *Social Engineering,* amellyel a fontos adatok jelszó-tulajdonosoktól való megszerzését jelölik. A kreativitás, amivel ilyenkor eljárnak, hihetetlen. Tehát ne hagyjuk, hogy ismeretlenek olyan információkat csaljanak ki tőlünk, amelyeket senkinek sem adnánk meg önként. Ez történhet mondjuk egy telefonhívással, amelyben a főnökünk keresztnevét kérdezik - kulcsszó: e-mail-cím.

A klasszikus *jelszótörő* egy olyan program, amely egy lista segítségével minden lehetséges variációt megjátszik. Hogy hogyan is működnek ezek a programok, az a fejezet *7.3* pontjából derül ki. Természetesen a jelszófeltörők elleni legjobb védelem, a „biztos jelszó" sem fog kimaradni.

A jelszófeltörésről oldalakat lehetne írni. A legfontosabb azonban az, hogy *egy jelszó ne legyen túl egyszerű*. Ezért itt csak a valóban fontos információkat szeretnénk bemutatni, és a jelszóválasztás biztonságát a középpontba állítani.

## 7.1 Hackelt security-site - jelszófeltöréssel ez is lehetséges

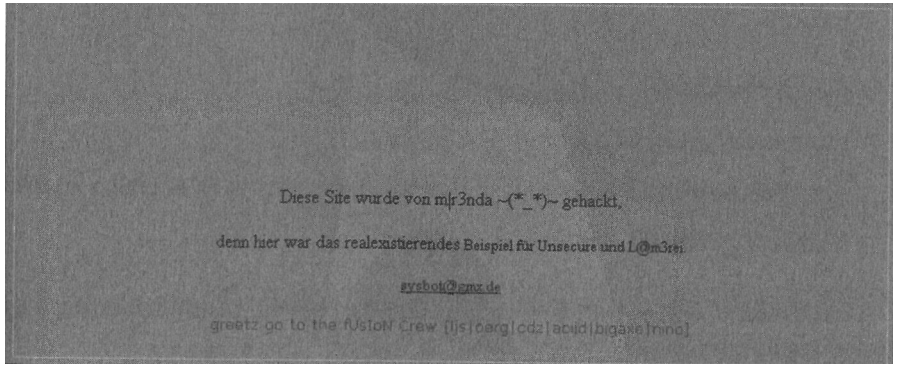
Egy ismert példa a *th-security* „átváltozása" (deface) volt. Itt a következő történt.

Az áldozat, amelyet egy *m \ r3nda* nevű hacker kinézett magának, a **www.th-security.de** volt, egy ismert biztonsági és trójai információs oldal, amelyen semmiféle scripthibát vagy szerverhibát nem lehetett találni. Tehát a hackernek más eszközökhöz kellett folyamodnia. Kutatás közben megállapította, hogy a webmesternek két GMX-fiókja van: **tobias.haennle@gmx.de** és **pegasuss.flieger@dmx.de** (a címeket az adatvédelem miatt megváltoztattuk). Az első címet kontaktcímként adta meg a weboldalon, a második a *Denic-nél (www.denic.de)* és a *Puretec (www.puretec.de)* szolgáltatónál szerepelt kontaktcímként.

A támadó először megnézte a GMX-titkos kérdést, és látta, hogy a kérdés mindkét postafióknál így hangzott: *Mi a keresztnevem?* Az oldalon megadott kontaktcímből, tehát **tobias.haennle@gmx.de,** hamar rájött, hogy milyen névről van szó. Tehát fogta *Tobias-t,* megváltoztatta a jelszót, és máris büszke tulajdonosa lett egy GMX-accountnak. Most egy kicsit körülnézett a GMX felhasználói menüben, ahol a valódi tulajdonos a nevétől kezdve a telefonszámáig tulajdonképpen minden adatot hátrahagyott, amelyekre a Social Enineering-hez szükség van.

A hacker most a webtárhely szolgáltatójától kapott mail-eket kereste, mert ezekben szerepelt az ügyfélszám, amire szüksége volt ahhoz, hogy a Puretec-kel „elfelejtett" jelszavakat lehessen a kontaktcímre küldetni. De nem voltak mail-ek a szolgáltatótól, így két lehetőség adódott - az első: várni pár napot egy mail-re a szolgáltatótól, mert a Puretec általában havonta egyszer mail-ben elküldi a számlainformációkat. De ez biztosan feltűnne a felhasználónak, és megváltoztatná a kontaktcímét. A másik lehetőség: a jó szerencsében bízva egyszerűen megpróbálkozni néhány jelszóval. A hacker a felhasználó születési dátumával kezdett, amelyet a GMX-adatokból megtudott.

És nézzenek oda: ez megint telitalálatnak bizonyult, mert a legtöbb felhasználó nagyon lazán veszi a jelszó kiválasztását. Hogy ezek után mit csinált az oldalból? íme az eredmény:




**Itt egy honlap volt**

Ez bizony egy nagyon jó példa arra, hogy hogyan válik lehetségessé egy „deface" a rosszul megválasztott titkos kérdés, az alkalmatlan jelszó révén.

## 7.2 Mire kell ügyelni a felhasználói oldalról?

A legtöbb felhasználó nem túl ötletes egy értelmes jelszó kitalálásánál. Ezért a rosszul választott jelszavak kihasználása a hackerek egyik legjobban elterjedt támadófegyvere.

A jelszavak megadásánál a következő alapszabályokat kellene betartani:

- ne legyen öt karakternél rövidebb,
- semmi duplázás, tehát ne legyen „hhaalloo",
- ne legyen szabványos,
- semmi születésidátum és hasonlók,
- ne legyenek olyan szavak, amelyek benne lehetnek a jelszólistákban vagy a szótárakban.

A jó jelszavak

- több mint tíz karakterből,
- alfanumerikus karaktersorból, pl. kml34Hs9,
- vegyesen kis- és nagybetűkből állnak.

Teljesen értelmetlen a jelszóhasználat, ha

- mindenütt ugyanazt a jelszót használjuk,
- egy cetlit teszünk a billentyűzet alá vagy a monitorra, és ráírjuk a jelszót,
- a jelszó egy fájlban van mentve a gépen.

A jelszót *kettő-négy hetente cserélni kell.* Ezzel a fogással meghiúsíthatjuk a korábban kikémlelt jelszó felhasználását.

### A titkos kérdések legyenek titkosak

Az interneten a különböző oldalak biztonságra ügyelő *szolgáltatói jelszókérdések* vagy *titkos kérdések* megadását kínálják, hogy a felhasználónak lehetővé tegyék, megváltoztatni a jelszavát, ha elfelejtette. Gyakran lehet ilyen kérdésekkel találkozni: „Mi a hideg ellentéte?" Ez természetesen rossz választás, mert így minden támadónak lehetővé tesszük a jelszavunk tetszés szerinti megváltozatását.

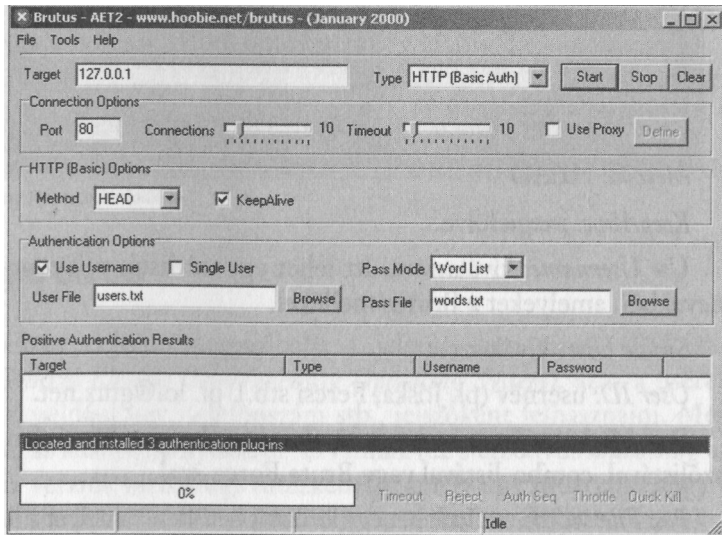
## 7.3 A jelszófeltörők

A jelszófeltörők olyan programok, amelyek jelszavakat fednek fel, hogy ki kerüljék az alkalmazott biztonsági intézkedéseket. A jelszót a legritkább esetben fejtik vissza, ehelyett egy névről nagyon jól ismert eljárást, a *Brute Force-ot* használják. A Brute Force annyit jelent: nyers erőszak. E programok nem tesznek mást, mint nagyon nagy sebességgel próbálják ki az egyik lehetséges jelszót a másik után, amíg megtalálják az igazit.

Egy példa az ilyesfajta programra a *Brutus.* A Brutus jelszófeltörő internet-accountok valamennyi variánsához (FTP, HTTP, POP3, Telnet, NetBios stb.). Az internetjelszavak minden fajtájához szívesen használják.

A *Target* mezőbe be kell írni a kikémlelendő fél URL-jét vagy IP-címét. Ezután ki lehet választani a támadás fajtáját, és szükség szerint szólistákat is be le-

**A Brutus program: minden beállítás egy lapon**



het tölteni, amelyek, ha a jelszó a listán van, igencsak megrövidítik a feltörést. Egy további, a támadásokhoz hasznos tulajdonság egy beépített proxy, amely megakadályozza, hogy vissza lehessen követni a támadót.

### 7.3.1 Ismert felhasználói nevek jelszavainak a kitalálása

Mint már a neve is mutatja, a program ennél az eljárásnál csak egy user névvel próbálkozik, amelyet előre meg lehet adni, mert az már ismert, de nincs meg a hozzá tartozó jelszó. Így lenne ez például akkor is, ha elfelejtettük a fiók-jelszavunkat.

### 7.3.2 Beállítások áttekintésére

*Target:* a host URL-je vagy IP-je, amelyen pl. a POP3 vagy FTP-account van.

*Type:* itt lehet kiválasztani a cél típusát, HTTP, FTP, POP3, Telnet, SMB (NetBOIS) stb.

*Port:* a port megadása, HTTP esetén a 80-as port, FTP-nél a 21-es.

*Connection:* meg lehet adni, hogy milyen gyakran létesítsen kapcsolatot a program.

*Timeout:* megadható, hogy mennyi idő múlva szakítsa meg a program a kapcsolatot.

*Use Proxy:* nincs kiválasztva; a Brutus itt lehetővé teszi egy proxy bejegyzését.

*Method:* HEAD

*KeepAlive:* megjelölve.

*Use Username:* kiválasztva. Itt lehet egy névlistát választani különböző user nevekből, amelyeket a Brutus mellékel.

*Single User:* kiválasztva

*User ID:* usernév (pl. Jóska, Fercsi stb.), pl: lol@gmx.net.

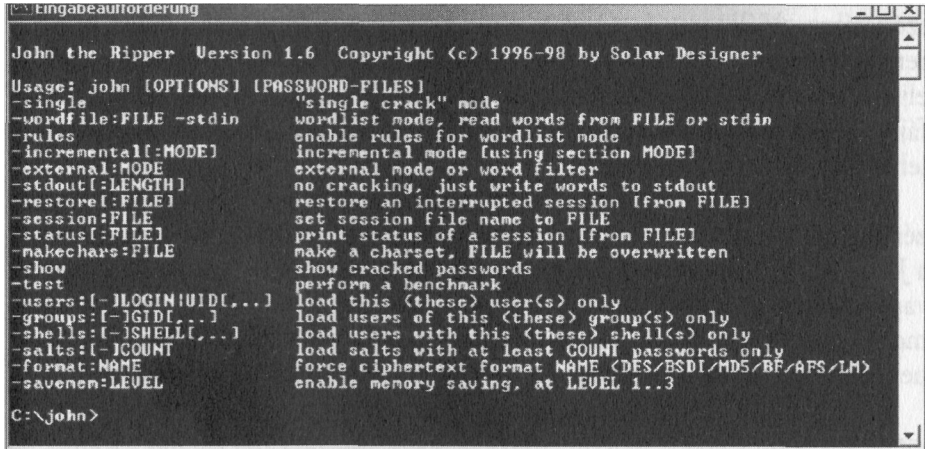
*Pass Mode:* szólista; itt lehet kiválasztani, hogyan történjen a feltörés. Lehet szólistával, combo-listával vagy Brute Force-szal.

*Pass Fik:* words.txt. Itt lehet egy szólistát betölteni, amelyet a Brutus mellé adnak.

## 7.4 Jelszavak megfejtése a John the Ripperrel

A *John the Ripper* egy jelszófeltörő, amely DES-sel *(Data Encryption Standard)* kódolt jelszavakat tud dekódolni. A DES-kódolások felhasználásának egyik területét a Unix-jelszavak jelentik.

Az idő, amelyre John the Rippernek szüksége van a jelszavak visszafejtéséhez, a rendelkezésre álló processzor sebességétől függ, ezért a program egyes verziói különböző processzorokra optimalizáltak. A John működése azon alapul, hogy a megadott jelszólehetőségeket például DES-sel kódolja, aszerint, hogy milyen módban indult el (single, szólista, incremental, external), és az eredményt összehasonlítja a megfejtendő jelszóval. Ha a jelszavak kódolt állapotban egyeznek, akkor visszafejtve is egyezniük kell, mert mindkettőnél ugyanazt a kódolási eljárást (DES) alkalmazták.




**A John the Ripper szerény felhasználói felülete**

### 7.4.1 Single Mode

Ebben a módban a John megpróbálja a jelszófájlban tárolt GECOS-információkat *(General Electric Comprehensive Operating System),* azaz a userek személyes adatait, például név, telefonszám stb., jelszóként felhasználni. Még ha a *passwd* fájlban az adatok „árnyékolva" is vannak (ez a bizonyos *shadowing az* újabb Linux/Unix verziók biztonsági intézkedése, amely úgy működik, hogy a jelszavakat eltávolítja a *passwd* fájlból, és helyette a shadow-fájlban tárolja), a

GECOS-információk azonban még mindig a *passwd* fájlban vannak. Ebben az esetben az Unshadow program segít, mégpedig úgy, hogy összevezeti a *passwd* fájlt és a *shadow* fájlt, ezért a jelszavakat és a GECOS-információkat megint csak egyetlen fájl tartalmazza. Ez a mód természetesen csak akkor hatékony, ha a felhasználók személyes információikat használják jelszóként. Ez a módszer egyben nagyon gyors is, ezért nem szabad alábecsülni. Ennek a módnak a hatékonysága a jelszófájl tartalmazta felhasználók számával növekszik, mert minden felhasználó GECOS-információját az összes többinél is kipróbálja jelszóként.

### 7.4.2 A szólista módszer

Ennek a módszernek a hatékonysága teljes mértékben a felhasznált szólista méretétől és főleg a minőségétől függ. így lehet szerver- ill. adminspecifikus szólistákat előállítani, és ezzel a siker valószínűségét növelni, mert minden rendkelkezésre álló információt fel lehet használni. És éppen ez adja ennek az eljárásnak a erősségét: mivel valószínűtlen, hogy egy ausztráliai szerver *passwd* fájlja német jelszavakat tartalmaz, a szólista német részét ebben az esetben el lehet hagyni.

A szólistát úgy kell felépíteni, hogy minden sorban csak egyetlen karakterfüzér legyen. Arra is ügyelni kell, hogy a szólista ábécé-sorrendben legyen, mert a John egy kicsikét gyorsabban dolgozik, ha az egymás után következő szavak vagy karaktersorozatok nem különböznek túlzottan egymástól (vannak programok, amelyek a szólisták kezelésében segítenek, például több listát összefűznek, ábécé-sorrendbe rendezik, vagy eltávolítják a dupla bejegyzéseket).

### 7.4.3 Incremental mód

Ez a John leghatalmasabb üzemmódja. Minden létező jelszót, függetlenül attól, hogy betűkből, különleges karakterekből, számokból vagy kombinációkból áll, vissza tud fejteni úgy, hogy minden lehetséges kombinációt ellenőriz. Ezt az eljárást Brute Force-nak is nevezik. Azt mindenesetre figyelembe kell venni, hogy a szükséges idő (a processzor teljesítményétől, a jelszó hosszától és a jelszóban használt karakterektől függően) nagyon hosszú is lehet.

### 7.4.4 External mód

Ez a mód inkább tapasztalt felhasználóknak való, mert teljes mértékben konfigurálni kell.

### 7.4.5 A John legfontosabb parancsai

| Parancs | Leírás |
|---|---|
| John -single | Ez a parancs single módban indítja a Johnt. |
| John -i | Ez a parancs incremental módban indítja a Johnt. |
| John -w:aszólistaneve | Ez a parancs szólista módban indítja a Johnt. |
| John -e:MODE | Ez a parancs external módban indítja a Johnt, a LIST. EXTERNAL: előtt definiált MODE tulajdonságokkal. |
| John fájlnév | Ez a parancs először single, majd szólista, végül incremental módban futtatja le *a* Johnt. |
| John -show | Erre a parancsra mutatja meg a program a megfejtett jelszavakat. |

A John the Ripper legfontosabb parancsainak az áttekintése

Minden parancs után meg kell még adni a jelszófájlt is.
*A john* parancs kilistáz minden lehetséges paramétert.

### 7.4.6 A jelszófájl

Ennek a fájlnak tartalmaznia kell a megfejtendő jelszavakat a hozzájuk tartozó felhasználó-nevekkel. Ezeket kettősponttal elválasztva, a USERNAME: PASSWORD séma szerint kell tárolni. Hogy hány ilyen pár van a fájlban tárolva, az nem túl lényeges, csak arra kell figyelni, hogy egy sorban mindig csak egy USERNAME:PASSWORD pár legyen. A jelszavak „árnyékolva" sem lehetnek, hanem normál kódolt állapotban kell lenniük (pl: árnyékolva=*john:x* vagy john:* ; kódolva=*john:GjstuOeYjOEhc)*. Ha a single módot kell használni, akkor a GECOS-információknak és a user-könyvtár elérési útvonalának is mögötte kell állnia *(pl: john:OozDCtCCAa/lM:11202:0:99999:7:0:)*.