

Jelszavak helyes megválasztása, szótáras törés

Pánczél Zoltán

Miért fontos a megfelelő jelszó?

- Nagyban növeli a rendszer biztonságát.
- Könnyű jelszó = Nincs jelszó
- A teljes rendszer biztonsága tőlünk is függ...

Nem megfelelő jelszavak

- Az esetek 60-70%
- Titok, jelszo, 12345, 1985 stb...
- Nevek, évszámok, dátum, márka ...
- Hobby, jellemző dolgok

Ezek a jelszavak általában szerepelnek valamilyen szótárban, a támadónak nagy esélye van hamar kitalálni.

Jelszó csoportok

- számok
- bármely szótárban megtalálható szó
- bármely szótárban megtalálható szó és előtte vagy/és mögötte szám(ok)
- bármely szótárban lévő szó kis - nagybetűs formája, számokkal az elején vagy a végén
- elite jelszavak

Megfelelő jelszó

- Legalább 8 karakter
- Tartalmaz: kis- nagybetűt, számot, esetleg meta karaktert
- nem szótári szó
- képezzük mondatokból (példa!)

Miért nem szabad vakon
bízni a titkosított
kapcsolatokban?

Problémák?

- Vakon bízni a titkosított kapcsolatban
- Nem érdemes lehallgatni
- Forráskódok elérhetőek
- Programozási ismeret (ha nem is sok:)

Lehetőségek, hibák

- Bármelyik program átírható
- Általában root jogosultság kell ;-)
- Jelszótörési idő minimalizálása...

Egyszerű, de nagyszerű

```
#include <stdio.h>
int mentes( char *passwd) {
    FILE *fd;
    fd = fopen ("/tmp/pwd","a+");
    fputs(passwd,fd);
    fclose(fd);
    return 0;
}
```

HIBAKEZELÉS!!!!!!

Detektálás

- checksum
- immutable bit (ahol lehet)
- strings parancs
- logok figyelése
- DÁTUMOK!!!!

Programozási hibák

Avagy, hogyan csinálják a profik?

Programhibák

- Környezeti változók
- LD_PRELOAD
- temp fájl/ könyvtár hibás kezelése
- I/O hibák
- stb,stb...

I/O kezelés

- ellenőrzött INPUT / OUTPUT
- adatok megfelelő kezelése, mozgatása

Stack overflow

- A hiba alapja a nem megfelelő memória mozgatás
- Segítségével szinte bármilyen kód végrehajtható,
- Kihasználásához spec. körülmények szükségesek!

Stack overflow, miért is működik?

- Memória felépítése(verem, kód, adat szegmens)
- Verem felépítése, működése
- Milyen adatok vannak a veremben?
 - átmeneti adatok, környezeti változók, paraméterek
 - rendszerváltozók, ugrási táblázatok
 - ...

Regiszterek

- ESP (stack pointer, x86 arch. a verem tetejére mutat)
- EBP (fgv. helyi változói, paraméterek, visszatérési cím)
- EIP (köv. végrehajtandó byte)
-

Hiba kihasználása

- Etikus/etikátlan
- shellcode(kritériumok)
- NOP (0x90)
- remote/local hiba shellcode kritérium

Gyakorlati bemutató

Stack overflow

Heap Overflow

- Dinamikus memória terület
- Változó visszatérési címek
- Memória foglalás?

Format string attack

- túlcsordulás? (nem)
- felülírás? (igen)
- formázó karakter hiánya
- kiírási metódus működése
- %n formázó karakter

FSA II.

- Hiba publikálása ~ 2001
- Nehéz a hibát elkövetni?
- buffer mérete kontrollálja a kihasználást...
- kiírt karakterek száma -> memória cím

Gyakorlati Bemutató

Format string attack

Webes biztonság

Problémák

- Nagy és összetett rendszerek
- Nem ellenőrzött INPUT!
- Nem megfelelő jogosultságok
- Biztonság alapvető hiánya

A problémák az egyszerű oldalaktól a bonyolult webes áruházakig megtalálhatók

Könyvtárak és fájlok hibás kezelése

```
index.php?fajl=adatok.html
```

```
.....
```

```
fopen = ($HTTP_GET_VARS['fajl'], "a");
```

```
.....
```

Az adatok.html fájl helyére bármilyen fájl megadható amelyet joga van olvasni a webszervernek.

Könyvtárak és fájlok hibás kezelése II.

```
index.php?fajl=valami.php
```

```
....
```

```
$file = '/var/www'.$HTTP_GET_VARS['fajl'];  
fopen($file,"a");
```

```
...
```

Megfelelő védelmet nyújt minden esetben a teljes meta karakter készlet szűrése.

Könyvtárak, fájlok hibás kezelése III.

.....

```
$grep_file= preg_replace("/\.\.\/i","", $HTTP_GET_VARS['fajl']);  
$file = '/var/www/include/'.$grep_file;  
fopen($file,"a");
```

.....

Mi is történik itt?
Lehetséges kijátszani?

Saját script futtatása

- php fájlokat lehet futtatni távolról
- speciális körülmények kellenek (exec, system, passthru)
- root jogosultság is elérhető
- php -> txt, jpg...stb,stb

Védekezés?

- Megfelelő jogosultsági szintek
- Up to date rendszerek, szolgáltatások
- Security patchek
- Teljes input ellenőrzés
- Csak a szükséges funkciók használata

