Hesla ve Windows 2000/XP

Vložil/a Profik123 [1], 16 Listopad, 2005 - 18:46

- Cracking [2]
- Hacking [3]

V tomto článku se podíváme na to, jak vytáhnout hesla z počítače, ke kterému máme fyzický přístup, ale neznáme přihlašovací údaje do Windows.

V tomto článku se podíváme na to, jak vytáhnout hesla z počítače, ke kterému máme fyzický přístup, ale neznáme přihlašovací údaje do Windows. Celá akce se bude provádět ze systému, který nabootujeme z CD (předpokládá se tedy, že bude povolen boot z CD). Pravděpodobně se bude jednat o nějakou Linux Live distribuci. Budeme potřebovat následující věci:

Bkhive (Linux)
Samdump2 (Linux)
John the Ripper (Linux, Windows)
L0pthcrack (Windows)
Cain (Windows)
To všechno najdete v **Linuxové Live distribuci Auditor**, kterou stáhnete zde [4].

Hashe systémových hesel jsou ve Windows uloženy v **SAM** souboru (C:\Windows\System32\config\SAM). Podle toho by se zdálo, že **SAM** soubor stačí zkopírovat a hashe cracknout, ale Microsoft od jisté doby používá tzv. SYSKEY, což je 128 bitový klíč, kterým je celý SAM přešifrovám ještě jednou. Z toho vyplývá, že i když si **SAM** zkopírujete, tak vám to nebude k ničemu. K "čistým" hashím má ve Windows přístup pouze Administrator, a to vy nejste. Naštěstí existuje utilitka Bkhive pro Linux, která dokáže ze souboru **SYSTEM** (C:\Windows\System32\config\SYSTEM) vygenerovat BootKey, kterým dále celý soubor **SAM** dešifrujeme a získáme "čisté" hashe, které potom standardním způsobem crackneme.

Nyní přejděme k praktické ukázce celá akce.
Na začátku vložíme do mechaniky CD s Linuxem a restartujeme PC. Projdeme úvodním nastavením a počkáme několik minut než celý systém naběhne. Poté spustíme **Consoli** a namountuje pevný disk počítače následujícím způsobem:

```
mount /dev/hda1
```

A poté se přesuneme do složky **ramdisk**

```
cd /ramdisk/
```

Nyní se dostávám k použitý utilitky **Bkhive**. Chceme, aby nám BootKey uložila do souboru key.txt

```
bkhive-linux /mnt/hda1/WINDOWS/system32/config/system key.txt
```

Máme BootKey uložený v souboru **key.txt**, který dále využijeme v **Samdump2**. Výsledné hashe se nám uloží do souboru **hashes.txt**

```
samdump2-linux /mnt/hda1/WINDOWS/system32/config/sam key.txt > hashes.txt
```

Teď když máme hashe v souboru **hashes.txt** je můžeme standardním způsobem cracknout. Buď hned v Linuxu utilitkou **John the Ripper** příkazem:

```
john hashes.txt
```

Anebo si soubor **hashes.txt** zkopírujeme třeba na disketu nebo si ho pošleme mailem a pak ho v klidu crackneme v **L0pthcracku** nebo **Cainu** na Windows.

Dále bych chtěl upozornit na ntpasswd [5], který dokáže přepisovat hesla uživatelů a i administrátora, takže nemusíte louskat heslo.

Hiren's BootCD

Nejjednodušší je asi stáhnout Hirens Boot CD (http://www.hiren.info/pages/bootcd [6]) z torrentu, nabootujete, vyberete si program z kategorie Password Tools a přepíšete heslo administrátora. (pozn. redakce)

URL článku: https://www.security-portal.cz/clanky/hesla-ve-windows-2000xp

Odkazy:
[1] https://www.security-portal.cz/users/profik123
[2] https://www.security-portal.cz/category/tagy/cracking
[3] https://www.security-portal.cz/category/tagy/hacking
[4] http://www.remote-exploit.org/index.php/Auditor_mirrors
[5] http://home.eunet.no/~pnordahl/ntpasswd/
[6] http://www.hiren.info/pages/bootcd