Ako na zabudnuté heslo vo Windows?

Tipy a Triky
Ako postupovať, keď používateľ zabudne administrátorské heslo od svojho počítača, či nadobudne počítač, ku ktorému heslo nie je k dispozícii?

Nič nie je nemožné
Žiadna ochrana nie je neprelomiteľná, ak používateľ získa fyzický prístup k systému. Platí to i v tomto prípade. Ak sa vám už stalo, že ste zabudli heslo administrátora v operačnom systéme Microsoft Windows XP/2000/NT či 2003, vrátane serverových edícií, netreba zúfať. K dispozícii je viacero zaujímavých nástrojov, ktoré nám umožnia bez komplikácií problém vyriešiť.

V dnešnom príspevku sa zameriame na bootovaciu disketu s názvom „Offline NT Password & Registry Editor“. Ide o jednodisketovú linuxovú distribúciu obsahujúcu nástroj chntpw, ktorá je pre voľné stiahnutie k dispozícii na tejto adrese. Netreba sa zľaknúť pri prečítaní slovka Linux. Ten je v tomto prípade iba nástrojom, ktorý nám umožní efektívne vyriešiť náš problém. Zapísať obraz diskety na fyzické médium zvládne zaiste každý, kto sa chce do niečoho takého pustiť. V tom prípade nebude na škodu upozorniť na obsiahlejšie bootovacie CD, ktoré okrem tohto nástroja obsahuje množstvo užitočných nástrojov. Ide o projekt Ultimate Boot CD, ktorý nájdete na www.ultimatebootcd.com, ten využijeme v dnešnom príklade my.

Začíname
Pred uskutočnením tejto operácie je vhodné uistiť sa, že pevný disk, na ktorom je postihnutý Windows nainštalovaný, neobsahuje žiadne logické chyby. Pri štarte operačného systému sa zväčša o vyriešenie problému postará automatické spustenie scandisku. Budeme teda predpokladať, že všetko je v najlepšom poriadku.

Zapísané Ultimate Boot CD vložíme do mechaniky a v BIOSe počítača zvolíme bootovaciu sekvenciu tak, aby sa systém zaviedol z CD mechaniky ešte predtým, ako bude spustené zavedenie z pevného disku. Túto voľbu nájdeme najčastejšie v sekcii „Advanced settings“ alebo „Boot“, kde zvolíme na prvú pozíciu CDROM mechaniku. Po uložení nastavení by mal počítač automaticky nabootovať z CD nosiča, kde sa nám CD prihlási nasledovne:

Stlačením klávesy „2“ zvolíme voľbu „Filesystem Utilities“, čo naznačuje, že sa pôjdeme zahrať so súbormi uloženými na pevnom disku.

Z druhej ponuky zvolíme zo sekcie NTFS nástrojov prvého zástupcu stlačením tlačidla „b“. Tí, ktorí sa rozhodli pre využitie bootovacej diskety, dosiahnu rovnaký efekt jej zasunutím do mechaniky a nabootovaním systému. Od tohto kroku sa budú činnosti v oboch prípadoch zhodovať.

Po natiahnutí kernelu sa spustí inicializačný skript, ktorý nás na úvod poinformuje o možnostiach poskytovaných týmto projektom. Ako je na prvý pohľad zrejmé, možnosti nesiahajú iba po zrušenie administrátorského hesla, ale i na zmenu hesla ľubovoľného účtu, odomknutie uzamknutého konta či možnosť editovania systémových registrov. Samozrejme, vo všetkých prípadoch bez akejkoľvek znalosti ľubovoľného z hesiel.

Po potvrdení privítania klávesou „Enter“ nám systém umožní zavedenie ovládačov pre SCSI zariadenia. Nie je to žiadnym prekvapením. Serverové systémy neraz používajú SCSI disky alebo polia, takže táto možnosť je na mieste. My sa pre jednoduchosť zaobídeme bez nich, takže pokračujeme potvrdením enterom.

V ďalšom kroku sú zobrazené všetky diskové oddiely. Našou úlohou je zvoliť ten, na ktorom sa nachádza inštalácia MS Windows. Tí, ktorí nemajú disk rozdelený, nemajú čo riešiť. Tí, ktorí tak urobili, zaiste nebudú mať problém so zvolením správneho diskového oddielu. Tým, ktorí sa doposiaľ s GNU/Linuxom nestretli, poradíme, že jednotkou na konci s najnižším abecedným písmenom, pri existencii výhradne FAT/NTFS partícií, bude typicky C:, rozšírené oddiely sa začínajú v oddieli končiacim päťkou (D: atď...) Nástroj však zväčša sám rozozná, kam sa treba pozrieť.

Po zvolení diskového oddielu nasleduje automatické namountovanie, či už ide o FAT alebo NTFS filesystém. Na rade je voľba systémového adresára. I v tomto prípade dokáže systém automaticky zvoliť ten správny, ak ste nainštalovali systém do implicitného adresára /windows. Ak nie, budete musieť zadať cestu ručne.

Po potvrdení názvu adresára nasleduje výpis súborov, ktoré sa v ňom nachádzajú. Nie je nutné zvoliť názov súboru, v ktorom sa definície hesiel nachádzajú. Typicky sú uložené v súbore s názvom sam, s čím systém automaticky počíta. Možnosť zmeny názvu bola možno ponechaná pre prípady budúcich verzií Windows.

Súbor hesiel máme zvolený, takže sa môžeme pustiť do odstraňovania hesla. Z ponuky zvolíme „jednotku“. Vhodné je všimnúť si, že pri predchádzajúcom zadaní názvu súboru registrov získavame prístup i k možnosti ich editovania. V našom prípade však nie je na túto činnosť žiadny dôvod. Postačí nám jednoduché vymazanie hesla.

Systém vypíše kompletný zoznam používateľov definovaných v systéme. V našom prípade je to základná inštalácia Windows XP, pri serveri ich však môžu byť stovky. Označenie používateľa, ktorého heslo chceme prekonať, automaticky predpokladá účet s názvom Administrator, v každom prípade však môžeme zadať priamo želaný názov, alebo identifikátor účtu. Nie každý zostáva pri prednastaveniach.

V rámci zobrazených informácií o zvolenom účte získavame prehľad o prítomnosti hesla a prípadnom uzamknutí účtu v prípade množstva neúspešných pokusov o prihlásenie. Pre vyššiu mieru istoty úspechu je lepšie heslo nie zmeniť, ale vymazať. Pre túto činnosť zapíšeme na výzvu pre heslo znak „*“ a voľbu potvrdíme.

Vždy je čas rozmyslieť si, či tak naozaj chceme spraviť. Zmazať na cudzom počítači heslo pre získanie

prístupu bez povolenia nie je tým, prečo sme tento článok napísali. Ak je však potrebné tento krok vykonať, nezostáva nič iné, iba prostredníctvom „y“ rozhodnutie potvrdiť.

Opäť sme sa vrátili do ponuky zoznamu používateľov, aby sme mohli činnosť opakovať pre každého z nich. Ak sme získali prístup k administrátorskému účtu, zvyšok môžeme spraviť priamo z prostredia OS. Výkričníkom teda ukončíme našu púť a pristúpime k ďalšiemu kroku.

V hlavnom menu zvolíme položku „q“ pre opustenie nástroja a ukončenie činnosti – lepšie povedané zavŕšenie riešenia systémového problému.

Na záver prichádza rekapitulácia zmenených súborov, ktoré sa zatiaľ nachádzajú v dočasnom adresári. Potrebné je teda prekopírovať ich späť na pôvodné miesto. Postačí jednoduchá odpoveď obligátnym stlačením ypsilonu nasledovaným Enterom.

Prichádza posledná možnosť pre odskočenie od prepísania pôvodných súborov. Zatiaľ sa nám v praxi nestalo, že by sa narušila konzistencia filesystému, alebo obsah súborov hesiel. Bolo by však nefér neupozorniť na to, že každý koná na vlastné riziko. Dvojité potvrdenie rozhodnutia je teda na mieste.

Prepísaním pôvodného súboru naša práca končí. Postačí opätovne nabootovať systém, tentokrát však priamo do Windows, kde sa môžeme presvedčiť o úspechu vykonanej práce.

I keď prekonanie administrátorského hesla nie je každodenným chlebíčkom, neraz sa dostávame do situácie, kedy si dokážeme ušetriť takýmto krokom nemálo času. Či už niekto úmyselne bez vedomia administrátora alebo vlastníka systému zmenil prístupové heslo, alebo je potrebné pristúpiť k údajom kolegu, ktorý si nechal rozpracovaný projekt na svojom disku, alebo nastala iná kuriózna situácia, riešenie je vždy na dosah ruky. Potrebné je iba vedieť, ako na to. Od dnes by to však už nemal byť žiadny problém.

Zdroj: www.zive.cz