Ministrování s Ferdou Kuliferdou

napsal Jan Lukeš
nakreslil Jiří Vančura

PRESBYTÁŘ
OPAKOVÁNÍ

Zdar kolegáčku,
doufám, že jsi s rodinou prožil pěkné Vánoce. Snad Ti Silvestr nezpůsobil ztrátu paměti a doufám, že si pamatuješ, že jsme si minulý měsíc povídali o presbytáři :-)!
Teď si vezmi propisku a do prázdných okének napiš, jak se nazývají tyto nejdůležitější věci. Když si nebudeš vědět rady, podívej se do minulého čísla.

Poradím Ti, že někde tady je **SEDES, OLTÁŘ – OBĚTNÍ STŮL, AMBON, VĚČNÉ SVĚTLO** a **STARÝ OLTÁŘ**, a na ostatní už přijdeš jistě sám.
Navíc pro Tebe mám další zajímavý úkol. Najdi **DVACET** rozdílů oproti obrázku z minulého čísla. Jestli jsi vše dobře našel, to se dozvíš v příštím čísle.

Kamarádi v sukních, přeji vám krásný rok 2012 a hodně krásných zážitků při sloužení Pánu Ježíši u oltáře.
Ferda Kuliferda

BEZPEČNÉ HESLO

Foto: wikipedia.org

HESLA ZASTÁVAJÍ V OBLASTI POČÍTAČŮ ÚLOHU KLÍČŮ. POKUD CHCETE OCHRÁNIT SVÁ DATA, MUSÍTE VOLIT KVALITNÍ KLÍČE A NENECHÁVAT JE POD ROHOŽKOU.

JAKÉ HESLO JE BEZPEČNÉ?

Bezpečnost hesla vychází ze způsobů, kterými se ho útočník může pokusit prolomit (totiž zjistit). V zásadě existují tři typy útoku: použitím síly, slovníku nebo znalosti napadeného.

ÚTOK HRUBOU SILOU

Myšlenka útoku hrubou silou (v angličtině brute force) je prostá: budeme zkoušet všechny možné kombinace znaků tak dlouho, až se trefíme. Bezpečnost hesla je tudíž závislá na tom, kolik možností bude muset útočící program vyzkoušet, než se dostane k té správné.

V podstatě je to otázka matematiky: útočník musí otestovat přibližně (počet znaků abecedy) na (počet znaků hesla) kombinací. Kdo neumí umocňovat, tomu poradím, že například 10^4 (čte se to „deset na čtvrtou“) znamená vynásobení desítky čtyřikrát sama sebou, tj. 10 × 10 × 10 × 10 = 10 000.

Základní abeceda bez háčků a čárek má 26 znaků. To znamená, že když budete používat jen malá písmenka, bude vaše heslo s každým znakem navíc 26× silnější a například z deseti malých písmenek už lze sestavit přes 140 bilionů hesel, což je velké sousto i pro počítač, který se pro tyto útoky silou v dnešní době používá.

SLOVNÍKOVÝ ÚTOK

Málokdo si za hesla volí nesmyslné kombinace písmen a čísel, čehož využívá slovníkový útok. Útočník prostě zkouší slova ze slovníku (což nemusí být slovník spisovné češtiny, ale třeba všechna slova, která najde na internetu). A protože běžně používaných slov zas tak moc není, stačí vyzkoušet třeba milion hesel s dobrou nadějí na úspěch.

Pokud se chcete ubránit slovníkovému útoku, používejte neobvyklé kombinace slov, u kterých se dá předpokládat, že nikdy nikoho ani nenapadly. Když přidáte nějaké to číslo, bude heslo ještě silnější.

ÚTOK SE ZNALOSTÍ NAPADENÉHO

Útočník může také zkoušet, jestli si jeho oběť nezvolila za heslo něco, co se jí osobně týká. Třeba jméno, bydliště, název oblíbené kapely a podobně. Používání podobných hesel je proto vysoce nebezpečné, zvlášť když dnes mnoho lidí tyto informace veřejně uvádí na sociálních sítích.

SHRNUTÍ

Za bezpečná hesla, která odolají všem třem popsaným typům útoku, lze považovat například řetězce 7smutnychokurek, bavlnenypuding nebo kaprabolizuby. Zbývá dodat, jak bylo nastíněno v úvodu, že heslo byste měli nosit v hlavě a nikde jinde. Pokud je někdo nepovolaný najde na papírku vedle počítače, poděkuje vám a použije vaše heslo k nekalým praktikám. Jestli se bojíte, že vás zradí paměť, doporučuji poznamenat si někam pouze začátek hesla; na zbytek si člověk už obvykle vzpomene.

POZNÁMKA O ZVLÁŠTNÍCH ZNACÍCH

Na mnoha místech se dočtete, že správné heslo musí obsahovat velká i malá písmena, čísla, zvláštní znaky, jako vykřičník, a nejlíp asi ještě japonštinu. Nic takového ale nutné není, protože heslo o deseti malých písmenech je prakticky stejně bezpečné jako osmiznakové složené z velkých i malých písmen a číslic. Navíc, i když je to první delší, napíšete ho asi rychleji.

Proti používání zvláštních znaků hovoří také problémy s kompatibilitou: když se dostanete k počítači s anglickou klávesnicí, můžou vám zvláštní znaky a diakritika (háčky a čárky) pěkně zavařit.

Ze stejného důvodu doporučuji také nepoužívat Z a Y, protože tyto klávesy bývají někdy prohozené.

Autor: Josef Plch

Chytne hajný lovce.
„Člověče, jak tu můžete lovit, když máte povolení z loňského roku?“
„Vždyť já lovím jen to, co jsem loni netrefil!“
Michal Strašil