Recenze časopisu Hakin9 5/2007

Vložil/a cm3l1k1 [1], 4 Září, 2007 - 21:11

- Hacking [2]
- Recenze [3]
- Security [4]

Hakin9 se věnuje otázkám, které jsou spojeny s bezpečností informačních systémů. Autoři článků nahlížejí na problematiku ze dvou úhlů – z pohledu osoby, která tuto bezpečnost ohrožuje a zároveň z pohledu toho, kdo bezpečnost brání. K časopisu je přidáno CD, které obsahuje Hakin9 live - bootovatelnou distribuci Linuxu. Tato příloha obsahuje pomůcky, tutoriály a dokumentaci, která je důležitá k procvičení technik, jež byly popsány v časopise.

Nabourávání WiFi sítí (Bartosz Kalinowski)
Tento článek je opravdu podrobným popisem fungování WiFi sítí. Dozvíte se z něj nejen jak WiFi sítě fungují, ale i jaké nástroje (a jak) používat. Popisuje teorii prolomení WEP i WPA ochrany, ale praxi si musí každý ověřit/vyzkoušet sám. Není to návod step-by-step (což je možná lepší), ale jde o pěkný souhrn metod a způsobů prolomení těchto všudypřítomných sítí.

SQL Injection (Jaromír Vaněk – aka Profik123)
Jedná se o pěkný úvod popisující nebezpečí, možnosti útoku (injection, blind injection) i s ukázkovými skripty. Navíc autor připravil i stránku http://hakin9.ic.cz [5] pro testování zneužití chyb ostatními čtenáři. Nyní se identická stránka nachází také na http://hakin9.security-portal.cz [6] kde mohou přibývat další vylepšení nebo (po dohodě) i jiné „cvičební“ programy českých přispěvovatelů toho časopisu.

Správa sítě na úrovni jádra (Konrád Malewski)
Autor zde opravdu velice podrobně popisuje síťovou komunikaci na úrovni jádra, jeho modulů a

ovladačů síťových karet. Z bezpečnostního pohledu dle mého názoru nic nepřináší, ale zaručeně je pro linuxové maniaky, které zajimá jak se zpracovávají síťová data již od prvního šumu na datovém kabelu, včetně zdrojových kódů a nákresů.

Restrikce v příkazovém interpretu – jak je obejít (Dawid Goluński)
Tento článek se mi opravdu líbil. Jde tu vlastně o restrikce interpretu (rbash, rsh, ..), které sebou nesou omezení pro uživatele, aby např. nemohli zjistit informace o systému, změnit adresář, či nějak napadnout systém. Autor zde popsal spoustu metod, jak tuto restrikci obejít a některé postupy jsou opravdu exotické. Spousta ukázkových příkladu mě opravdu překvapila (kolika způsoby lze obejít nastavení proměnných, kolika se dostat ke spuštění /bin/bash apod.) Doporučuji přečíst a restriktivní shelly raději nepoužívat :o)

Jak si zachovat soukromí při práci s Internetem (Petr Břehovský)
V tomto článku se seznámíme se základy a rychlým skokem přejdeme k tak sofistikovaným věcem jako je Tor (The Onion Router) [7], Mixminiom (zjednodušeně: Tor pro emaily). Autor vysvětlí jak fungují, jak se používají a na co si dát pozor, aby vaše identita nebyla odhalena.

MS SQL Server 2005 – bezpečné aplikace (Artur Żarski)
Tento článek je spíše pro programátory/administrátory MS SQL [8] serverů. Popisuje možnosti připojení DB (connection string), možnosti využití šifrování, používání uložených procedur a způsoby obrany před SQL Injection. Článek se na problematiků dívá z obou úhlů pohledu (programátor/admin) a doporučuje jak vyvíjet a spravovat aplikaci.

Spammeři se nevzdávají (Helena Nykodýmová)
SPAM... nevyžádaná pošta, která vám po desítkách denně příchazí do mailových schránek. Pojem SPAM původně znamená Spicy Meat And Ham, což bylo kořeněné maso a šunka poprvé vyrobeno firmou Hormel Foods v roce 1937. Velkou popularitu si získal během 2. světové války. Použití tohoto termínu ve smyslu nevyžádaného emailu je odvozeno od slavného skeče Monthy Pythonů, který byl poprvé vysílán v Británii 5. prosince 1970.
Ale to se ve článku nedozvíte :o) Článek pěkně rozebírá problematiku dnešních obrázkových spamů [9] a na spoustě příkladů ukazuje jak pokročilé metody spameři používají.

Přehled steganografie (Roman Cinkais)
Steganografie [10] je umění jak skrýt nebo utajit zprávu. Autor zde na odborné úrovni popisuje historii steganografie až do dnešních dnů. Doporučuji přečíst. V dnešním světě kompjůtrů a totalitních států bude zřejmě čím dál častěji k „vidění“. I na SP ji více jak 2 roky používám. Nevšimli jste si, že? :o)

Závěr
Tento díl byl rozhodně mnohem lepší než předchozí, o kterém jsem ani nepsal. Pořád se setkávám s chyby v překladu, s popletením slov z polského překladu (w místo v atd.) a pravopisné chyby. Každý, včetně mě, dělá chyby. Rozdíl je v tom, že Hakin9 je komerční časopis a na SP to lidi dělají pro lidi (ne, korektora opravu neplatím), takže by se to nemělo vyskytovat v tak velké míře jako doposud.

Snad budou další čísla stále tak dobrá a přinesou zajímavá témata. Můžeme jen doufat, že kvalita nebude upadat jako v minulosti.

Přeji hodně zdaru!

[11]

URL článku: https://security-portal.cz/clanky/recenze-%C4%8Dasopisu-hakin9-52007

Odkazy:
[1] https://security-portal.cz/users/cm3l1k1
[2] https://security-portal.cz/category/tagy/hacking
[3] https://security-portal.cz/category/tagy/recenze
[4] https://security-portal.cz/category/tagy/security

[5] http://hakin9.ic.cz
[6] http://hakin9.security-portal.cz
[7] http://www.security-portal.cz/clanky/tor-the-onion-router---system-pro-vysoce-anonymni-a-sifrovany-pristup-k-internetu.html
[8] http://www.security-portal.cz/clanky/metody-utoku-na-microsoft-sql-servery.html
[9] http://www.security-portal.cz/clanky/obrazkovy-spam---historie-a-budoucnost.html
[10] http://www.security-portal.cz/clanky/prakticke-zaklady-kryptologie-a-steganografie.html
[11] http://hakin9.org/cz