XP superbezpečná

50 nejlepších bezpečnostních nástrojů

Použijte Supermanovu sílu a zlikvidujte hackery jejich vlastními zbraněmi. Skenováním portů a zadními vrátky se jim zaručeně dostanete na kobylku.

Text: Markus Hermannsdorfer, Vratislav Klega, *vratislav.klega@chip.cz*

V TOMTO ČLÁNKU NAJDETE

Pozor! Lex Luthor pronikl do systému. Copak by asi v tomto případě udělal Superman? Nejdříve by zůstal nesmělým Clarkem Kentem, zrekonstruoval by průběh trestného činu a nakonec by pátral po stopách. Kterou bezpečnostní mezeru mohl Luthor zneužít? Přes který port mohl do systému propašovat svůj virus?

Postup nejen pro Supermany

Teď přijde čas na prozkoumání vašeho PC rentgenovým zrakem Supermana: Aha! Rootkit od Sony – odpusťte, samozřejmě z planety Krypton. Všechna hesla a přístupy k účtům se Lutherovi podařilo ukrást. My to však tak daleko zajít nenecháme.

Až bude nebezpečí zažehnáno, pustíme se do protiútoku. Budeme zpětně sledovat Luthorovu stopu a nástrojem Traceroute vypátráme jeho skrýš. Nebudeme sice zachraňovat celou zemi, ale i záchrana vlastního počítače stojí za námahu. Také nainstalujeme alarm, který bude upozorňovat na útoky na počítač.

WEBOVÉ STRÁNKY, SKRIPTY, PORTY

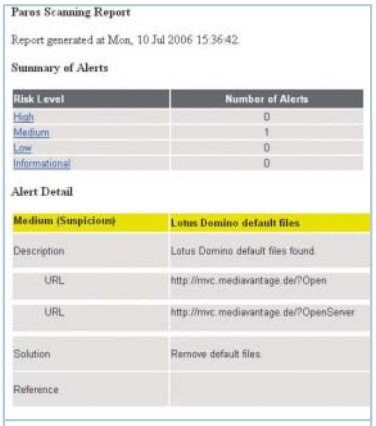
Jak nalézt bezpečnostní mezery

Skrz otevřené porty, přes nezašifrované spojení W-LAN, zmanipulovanou webovou stránkou, internetovým serverem – jsou desítky možností, jak může Luthor proniknout do vašeho PC. Odhalte tyto díry raději sami.

1) TESTOVÁNÍ WEBOVÉ STRÁNKY

Nástroj: Parosproxy

Webové stránky bývají od hackerů tak dobře připravené, že se na váš počítač zcela automaticky přenese škodlivý kód. To je snadné „díky“ bezpečnostním mezerám v prohlížeči nebo za „pomoci“ služeb ve Windows, které běží na pozadí. Proxy skener, který je mezi vaším PC a webovým serverem, analyzuje příchozí data z internetu a ihned rozpozná, zda obsahují škodlivý kód. Kvalitním skenerem je například opensourcový Parosproxy. Tento nástroj je naprogramován v Javě, proto potřebujete mít nainstalovaný „Java Runti-→



Paros Scanning Report

Report generated at Mon, 10 Jul 2006 15:36:42.

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	1
Low	0
Informational	0

Alert Detail

Medium (Suspicious)	Lotus Domino default files
Description	Lotus Domino default files found.
URL	http://mvc.mediavantage.de/?Open
URL	http://mvc.mediavantage.de/?OpenServer
Solution	Remove default files.
Reference	

Reklama odhalena: Stránka „mediavantage.de“ představuje z hlediska bezpečnosti střední riziko.

me Environment“. Po nainstalování programu Parosproxy spusťte svůj webový browser, například Internet Explorer. Zvolte *Nástroje | Možnosti Internetu*. Vyberte záložku *Připojení* a klikněte na *Nastavení místní sítě*... Ve spodní části okna povolte Proxy a do řádku Adresa zadejte „localhost“. Do řádku Port napište „8080“. Po potvrzení poběží váš internet přes proxy skener. Nyní otevřete webovou stránku, kterou chcete prověřit. Jakmile se stránka načte, otevřete okno Parosproxy. Pod „Sites“ uvidíte URL zvolené stránky a také podstránky, pokud se zde nacházejí. Zvolte *Analyse | Scan All* a prohlédněte webové stránky. Pokud je něco v nepořádku, zobrazí se to v okně „Alter“.

Během našeho testování jsme narazili na stránky reklamního „mediavantage“, které se zobrazují jako neškodné „podstránky“. V menu *Report | Last Scan Report* jsme zjistili, že tato reklama používá nástroj „Lotus Domino“, který překrývá stránky reklamou a ještě představuje pro náš počítač středně velké bezpečnostní riziko. Krátká internetová rešerše na internetu prokázala, že programy Lotus komunikují přes port 1352. Pokud tedy chcete zablokovat všechny „mediavantage“, stačí na firewallu zablokovat tento port.

NA CHIP DVD

CO NALEZNETE NA CHIP DVD

Hledání bezpečnostních mezer
- Paros Proxy 3.2
- Netcat 0.7.1
- Network Scanner 2.5
- Angry IP scanner 2.21
- Nmap 4.11
- Advanced Port Scanner 1.2
- Secure Eraser 1.2
- AIO SECRETMAKER 5.0.7
- Airsnort 0.2.7
- Libwhisker 2.2.3
- Amap 5.2
- Wikto 1.63
- HTTrack 3.40
- Httprint 301
- Nikto 1.34
- Kismet 0.04
- NetStumbler 0.4
- Cain & Abel 2.9
- John the Ripper 1.7.0
- THC Hydra 5.3
- PWDUMP2
- RainbowCrack 1.2

Eliminace škůdců
- Atack Tool Kit 4.1
- Metasploit Framework 2.6
- a-squared Free 1.6
- BlackLight 2.2
- Rootkit Revealer 1.7
- HijackThis 1.99
- SpyBot S&D 1.4
- AntiVir 6.32
- SpywareBlaster 3.5
- TrojanCheck 6
- BitDefender Antispyware 9

Zpětné vyhledání hackerů
- WhoisAssistant 1.1
- 3d Traceroute 2.1

Zabezpečení počítače
- Snort 2.6.1b
- IDSCenter 1.1
- OSSEC HIDS 0.9.2
- Base 1.2.6
- Sguil 0.6.1
- PGP4WIN 1.0.6
- OpenSSL 0.9.8
- Tor 0.1.1
- Armor2Net 3.1
- Stunnel 4.18
- OpenVPN 2.0.8
- TrueCrypt 4.2
- Krypter2002 2.02
- ArchiCrypt Stealth 3.3.2
- SpyBlocker 8.7

VLOUPÁNÍ

Aby byl váš PC sabotován, musí do něj Lex Luthor alespoň jednou vniknout. To se mu povede jen za předpokladu, že máte otevřené porty. Těmi hledá tajnou chodbu do vašeho počítače. Pokud používáte bezdrátové připojení, může prolomit šifrování WEP/WPA.

Nástroje:
Netcat, SuperScan4, Angry IP-Scaner, Nmap, Netstat, X-Scan, Nessus, CoSara, Aircrack, Airsnort.

Co to může znamenat?
Krádež dat, sabotáže, špionáž.

Jak se bránit?
- Aktivujte automatické aktualizace Windows.
- Zavřete co nejvíce portů ve firewallu.
- Měňte zabezpečení W-LAN.
- Nainstalujte Intrusion Detection System.
- Neotvírejte maily od neznámých odesílatelů nebo z podezřelých adres.

KRÁDEŽ

Pokud se Luthor úspěšně vloupal do vašeho počítače, již mu nic nestojí v cestě. Má přístup k pevnému disku, uloženým pinům, heslům, osobním fotografiím... prostě ke všemu. Největším škodám však lze zabránit.

Nástroje:
Netstumbler, Kismet, Cain & Abel, John the Ripper, THC Hydra, Pwdump, RainbowCrack.

Co to může znamenat?
Krádež identity, rabování bankovních kont, surfování na vaše náklady.

Jak se bránit?
- Pravidelně aktualizujte antivir.
- Neukládejte hesla a informace o účtech na PC.
- Používejte hesla se zvláštními znaky.
- Neodpovídejte na maily, které požadují osobní informace, natož čísla účtů.

Alternativní řešení:

Whisker: Prověří server a HTTP spojení z hlediska bezpečnostních mezer (požaduje prostředí Perl).

WebInspect: Odhalí typické webové útoky a nebezpečné či nedůvěryhodné obsahy. Rovněž rozpozná ilegálně přidělené parametry URL.

2) NEBEZPEČNÉ SKRIPTY NA SERVERECH

Nástroje: Wikto, HTTPrint, WinHTTrack

Pokud firewall a antivirový štít spustí poplach, leží nalezený škůdce již na pevném disku. Se supersilou se můžete napřáhnout k preventivnímu úderu – a škůdce odhalíte hned na webovém serveru.

Abyste vypátrali škodlivé programy, potřebujete nástroj „Wikto“. Kromě toho se vám budou hodit ještě další dva programy: HTTPrint a WinHTTrac. K provozu programu Wikto je nutné mít nainstalovaný .NET Framework.

Je-li vše nainstalované, přejděte v programu Wikto k položce „systemconfig“. Zadejte cestu k HTTPrint a WinHTTrack. Klikněte na *UpdateNiktoDB* a *Update GHDB*. V obou případech se objeví další dialog, který stažení obou databází potvrdí. Nyní je Wikto připraven k použití. Klikněte na *LoadDB*. Databáze webového skeneru obsahuje asi 3200 jmen nebezpečných souborů a CGI skriptů. Teď je třeba zjistit, zda se některý z uvedených škůdců nenachází na serveru. Proto zadejte v „Target selection“ URL, případně i port. Klikněte na *Start Wikto*. Pokud obdržíte chybové hlášení, že nelze nalézt žádné „@CGDir skripty“, pak nástroj potřebné informace ještě nenačetl. V tom případě přejděte na „Back End“ a sledujte „Start Mining“. To zabere trochu času. V položce „Wikto“ zatrhněte „Use AI“ a „Optimized“. Vyhledávání spusťte znovu pomocí *Update* a přes *Show all* si nechte zobrazit všechna hlášení.

Při jednom testu jsme narazili na podezřelý skript „Gozila.cgi“. Vysvětlení od programu Wikto po kliknutí na *Desciption* však nic nového nezobrazilo. Zapátrali jsme na Googlu a zjistili, že tento skript dokáže zhroutit routery značky Linksys. To představuje střední riziko...

Alternativní řešení:

Nikto: Pro hardcore uživatele, kteří odmítají jakoukoliv uživatelskou plochu. Program se ovládá z příkazové řádky.

Libwhisker: Nejedná se vlastně o program, ale o knihovnu, jejíž pomocí lze rozšířit schopnosti nástrojů Nikto a Whisker.

3) HLEDÁNÍ OTEVŘENÝCH PORTŮ

Nástroj: SuperScan 4

Nyní víte, na kterých webových stránkách vám Luthor připraví překvapení v podobě nepříjemného dárečku. Položme si ale další otázku: Jak skript pronikne do počítače? Je to zcela prosté – dostane se tam přes porty, které zůstávají bez povšimnutí většinou otevřené a každému programu tak umožňují přístup.

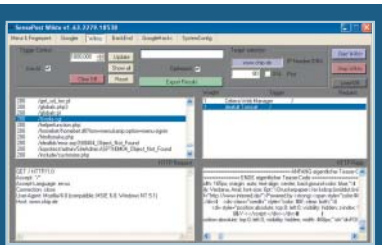
Abychom našli tyto otevřené porty, potřebujeme portskener – např. „SuperScan4“. K tomu potřebujete znát svou IP adresu. Do příkazového řádku zadejte příkaz „ipconfig –all“, v dlouhém výpisu naleznete i vlastní IP adresu. Teď spusťte SuperScan a zjištěnou IP adresu zadejte do řádku „Hostname/IP“. Potvrďte kliknutím na šipku doprava a spusťte test kliknutím na tlačítko *Play* vlevo dole. Po spuštění testu by se měl ozvat firewall s varovnou hláškou. Povolte provedení skenu a počkejte, dokud se nezobrazí konečný výsledek. Nalezne-li nástroj na vašem počítači otevřený port, měli byste ho ve firewallu zablokovat.

Alternativní řešení:

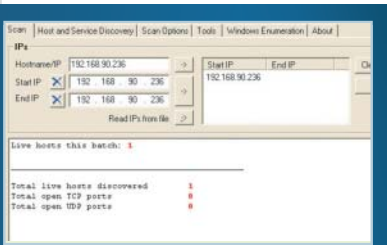
Angry IP-Scanner: Tento nástroj potřebuje méně místa na uložení a jeho možnosti lze rozšiřovat plug-iny.

Nmap: Skener s mnoha možnostmi nastavení, který ovšem předpokládá hlubší síťové znalosti.

Netstat: Součástí systému Windows je i jednoduchý portskener, který však běží jen v režimu příkazového řádku.



Škodlivý skript: Wikto vyhledává na webových serverech nebezpečné skripty jako „Gozila.cgi“, které dokáží shodit routery značky Linksys.



Absolutně bezpečný: Tak to má být. Na našem testovacím počítači nenašel SuperScan 4 žádný otevřený port, přes který by se mohl škůdce dostat do počítače.

ŠPIONÁŽ

Jak se vlastně Lex Luthor dozvěděl, kam jedete letos na dovolenou, zda jste muž, či žena nebo jakou hudbu posloucháte? Zcela jednoduše: na váš počítač nainstaloval trojského koně a zná všechna vaše data.

Nástroje:
Back Ocrifice, NSIS, Netcat, Ntop, Grep, Argus, Nemesis, Whusker, DRM, XCP.

Co to může znamenat?
Trapná odhalení, spam, obtěžování.

Jak se bránit?
- Používejte antispywarové nástroje.
- Deaktivujte nepotřebné služby.
- Šifrujte komunikaci.
- Zavřete otevřené porty.

4) JAK HLEDAT DÍRY V INTRANETU

Nástroj: X-Scan

Nikdy jste nebyli na internetu nebo nemáte žádný on-line účet? Pak je situace ještě horší. Vetřelec se totiž klidně prochází vaší firemní sítí. Dříve než se ho vydáte hledat, měli byste firemní síť prověřit, zda nemá nedostatky v zabezpečení. Nástroj X-Scan doslova simuluje rentgenový pohled Supermana. Jde o bezplatný program se skutečně luxusním uživatelským prostředím. V části *Config / Scan module* nastavte program podle toho, co vlastně budete chtít testovat a jaké nedostatky má program hledat. Nejlépe bude, pokud aktivujete úplně vše. Zvolte *Config | Scan parametr* a zadejte IP adresu, při větším počtu počítačů zadejte rozsah IP adres. Poté bude síť prověřena. Pokud X-Scan odhalí nějakou trhlinu v zabezpečení (např. „Finger Vulnerability"), získáte kliknutím na hlášení informaci o nebezpečnosti a o nedostatcích sítě. Nástroj disponuje i tipy, jak některé nedostatky vyřešit. Pokud nejste spokojeni, určitě poradí Google nebo Microsoft Knowledge Base.

Alternativní řešení:

Nessus: Bezplatný nástroj se skvělým uživatelským rozhraním. Výrobce vás ovšem bude neustále nutit ke koupi rozšířené komerční verze.

CoSara: Velice výkonný unixový nástroj, který malým trikem – propojením s Co-Linuxem – běží i pod Windows. Program předpokládá základní orientaci v systému Debian.

MSBA: Neboli Microsoft Baseline Security Analyzer. Nástroj, který se rovněž hodí pro skenování sítě.

5) PROKLEPNUTÍ W-LAN

Nástroj: Netstumbler, Aircrack

Vlastníte-li laptop a bezdrátovou síť, můžete si roli hackera vyzkoušet na vlastní kůži. Prověříte si, zda útočníci nemají přístup k vašemu access pointu, nebo zda už dokonce nerozluštili kódování WEP/WPA. Při tomto triku budete postupovat stejně jako hacker: Nejdříve vyhledejte existující sítě W-LAN. Pokud naleznete svou vlastní síť, přijde na řadu nástroj Aircrack. Pomocí tohoto programu zjistíte, je-li síť dostatečně chráněna.

Nainstalujte Netstumbler a Aircrack na laptop s podporou W-LAN. Spusťte Netstumbler a vyčkejte, než nástroj nalezne síť. Pokud se to nepodaří, podívejte se na „Device", zda software správně rozpoznal váš „W-LAN hardware". V opačném případě se podívejte na *www.netstumbler.org* do diskuse „Hardware", zda je váš hardware podporován. Pokud není, můžete vyzkoušet jiný program, například Kismet.

Pokud je W-LAN síť nalezena, Netstumbler vám graficky zobrazí, jak silný signál access point vyzařuje. To je dobrá příležitost k přezkoušení rozsahu antény vašeho access pointu.

Nyní dojde k simulaci pirátského testu. V adresáři s Aircrackem otevřete složku „bin". Spusťte „airodump". Nástroj začne ukládat odposlouchávaný signál rádiového spojení do souborů CAB nebo IVS, které lze vyhodnotit programem „aircrack-ng.exe". Pokud máte zařízení Fritz-Box a používáte kódování WEP, spusťte proces a zadejte do příkazového řádku „aircrack-ng –f –h {cesta k souboru CAB nebo IVS}". V tomto případě se Aircrack omezí na číselné řady od 0x30 po 0x39, které jsou pro Fritz-Box typické. Stane-li se, že program vyplivne vaše WEP už po několika málo minutách, měli byste s bezpečností něco neodkladně podniknout. Nejlepší bude, pokud použijete moderní router s kódováním WPA2.

Alternativní řešení:

Kismet: Na rozdíl od programu Netstumbler pracuje tento nástroj pasivně a v síti pozná vetřelce. Jeho konfigurace je však o poznání složitější.

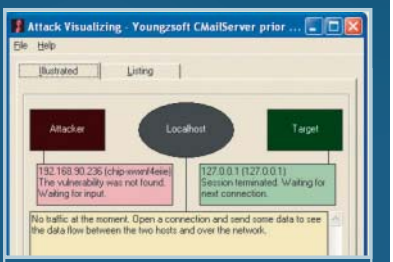
Airsnort: Pracuje podobně jako Aircrack, ovšem dokáže rozluštit pouze jednoduché kódování WEP.

EXPLOITS, ROOTKITS

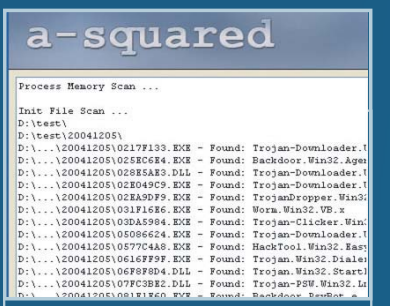
Eliminace škůdců

To, že se Lex Luthor dostal do vašeho PC, už víte. Co ovšem možná netušíte, je to, jak to ten chlápek vlastně udělal. Se speciálním

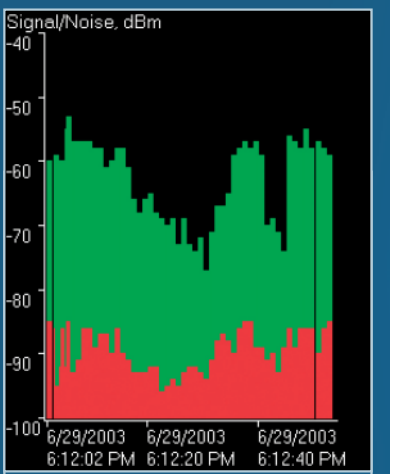
Prolomeno: Aircrack dokázal najít klíč k W-LAN, hacker má přímý přístup do sítě.



Útok odražen: Škodlivý exploit nemá šanci se do našeho počítače dostat.



Tajná zbraň: Nástroj „a-squared" odhalí a eliminuje velké množství trojských koňů.



Wi-Fi signál: Netstumbler ukazuje sílu signálu přicházejícího z access pointu.

Jako švýcarský sýr: Přes děravý protokol HTTP se může hacker pohybovat po firemním intranetu.

SABOTÁŽ

Je váš systém nestabilní? Zmizela záhadně vaše diplomová práce, na které jste pracovali již dva týdny? Možná je to práce sabotéra Lexe Luthera. Sabotáž bývá často spojena s vyděračskými maily typu „Zaplať za svoje data“.

Nástroje:
Metasploit Framework, Virus Datacrime II, Core Impact.

Co to může znamenat?
Ztrátu dat, programy se stanou nefunkčními, zmizí kontakty.

Jak se bránit?
- Pravidelně zálohovat data.
- Příležitostně otestovat počítač na výskyt exploitů.

softwarem budete simulovat útok a vysledujete záškodníky, kteří Luthorovi dodali vaše tajné informace.

6) SIMULACE ÚTOKU „EXPLOITEM“

Nástroj: ATK

Poté, co hacker odhalil bezpečnostní mezeru, propašuje skript rovnou do vašeho počítače. Tento skript se nazývá exploit. Pomocí nástroje Attack Tool Kit (ATK) prověříte, jaký typ exploitu může napadnout váš počítač. Nainstalujte program z Chip DVD a spusťte ho. Abyste mohli simulovat určité útoky, zvolte odpovídající plug-in a klikněte na *Start*. Útok si můžete nechat graficky znárodnit přes položku „Visualize“.

Aby se Luthor nedostal do vašeho počítače s celou armádou exploitů, je potřeba být extrémně obezřetný. Proto otevřete nabídku *Configurations | Preferences*. V okně „Preferences“ zvolte *Full Audit*, abyste skutečně otestovali všechny útočné metody. Pod položkou „Altering“ zvolte funkci *Produce Alter when vulnerability is found*. Okno zavřete a klikněte na *Start*. Tento způsob sice zabere více času, zato ale zaručí, že neproklouzne žádný druh exploitu. Poté začne vyhledávání. Pokud ATK ohlásí, že v Internet Exploreru byla nalezena bezpečnostní mezera, neprodleně si z Microsoftu stáhněte záplatu.

Alternativní řešení:

Metasploit Framework: Umí rovněž simulovat útoky exploitu, ale nabízí také možnost si vlastní exploity vytvořit, což je z právního hlediska vskutku na pováženou. Vyvarujte se pokušení, ať neskončíte jako Lex Luthor!

7) PO STOPÁCH TROJSKÝCH KOŇŮ

Nástroj: a-squared

Trojské koně se podobně jako exploity zabydlují v cizích počítačích. Ovšem zatímco exploit má pouze jednu funkci, trojské koně toho dokáží víc. Svému majiteli pošlou například všechny znaky napsané na klávesnici, čísla bankovních účtů a jiné užitečné věci. Tomu je třeba zabránit. Běžné antivirové programy trojské koně zpravidla zachytí, ovšem ještě lepší je nástroj, který se přímo na tento druh škůdce specializuje. Jedná se o velmi výkonný nástroj a-squared, který detekuje a spolehlivě odstraní přes 90 000 škůdců. Jedinou nevýhodou bezplatné verze je to, že

nechrání počítač permanentně. Za trvalou ochranu v luxusním formátu budete muset zaplatit 40 eur. Samotná aplikace je velmi jednoduchá: stačí zvolit *Scan PC* a poté *Smart Scan*.

Alternativní řešení:

Trojan Defence Suite 3: Tento nástroj je velmi výkonný a spolehlivý. Nedávno však výrobce pozastavil podporu.

8) PROVĚTREJTE PLÁŠTĚNKU

Nástroj: Blacklight

Dalším rozšířením trojských koňů je rootkit. Tento škůdce má zabudovanou jakousi „pláštěnku“, a proto se umí schovat před běžnými antivirovými programy. Rootkit bohužel nelze odhalit ani žádným z výše uvedených softwarů. K odhalení rootkitů je potřeba použít speciální software. Nejlépe ovladatelný a bezplatný nástroj se nazývá Blacklight a pochází od známé společnosti F-Secure. Nástroj dokáže najít a automaticky odstranit nebezpečné rootkity, jako je např. Myfib či Berber. Bezplatná verze je ovšem časově omezená.

Tip: Majitelé balíku „F-Secure Internet Security Suite 2006“ nástroj nepotřebují, protože engine programu je již součástí balíku.

Alternativní řešení:

Rootkit Revealer: Nástroj najde všechny rootkity, které jsou v seznamu na *www.rootkit.com*. Dopředu ale počítá s některými znalostmi Windows API a lze ho doporučit pouze zkušeným uživatelům.

Rootkit Hook Analyzer: Dobrý nástroj, který se specializuje na kernelové rootkity. Rootkity, které se maskují jako DLL, v uživatelském modu nenajde.

IceSword: Nejnovější skener na rootkity, který odhalí všechny záškodníky, kteří k nám zatím ještě ani nedorazili.

WHOIS, TRACEROUTE

Pronásledování hackerů

Počítačový svět si může konečně oddychnout, protože Superman včas našel nebezpečnou bombu a zneškodnil ji. Ale pozor! To ještě není konec! Oblečte si svůj červeno-modrý úbor a vydejte se po stopách Lexe Luthora coby geniálního hackera a zneškodněte ho jednou provždy.

9) NALEZENÍ HACKERA

Nástroj: SmartWhois, Visual Route

Abyste Luthora vypátrali, potřebujete aspoň jednu malou stopu. Když jste kupříkladu v Nmap přišli na to, že program posílá data z vašeho počítače na nějakou neznámou IP adresu, můžete příjemce snadno najít pomocí sharewarového programu SmartWhois.

Do nástroje zadejte IP adresu nebo doménové jméno. V našem případě zvolíme samozřejmě modelové jméno – *www.luthor.com*. Stopa nás zavede do Los Angeles ve slunné Kalifornii.

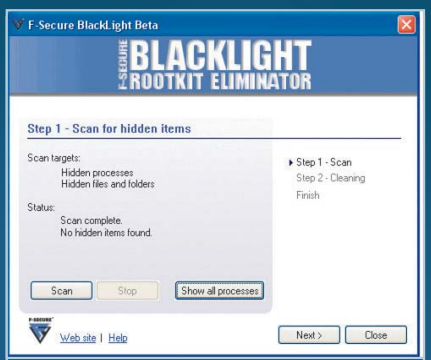
Abychom přišli na to, které cesty a které servery Luthor používal, potřebujeme trasovací nástroj. Velmi luxusní a spolehlivý je shareware „Visual Route 2006“.

Alternativní řešení:

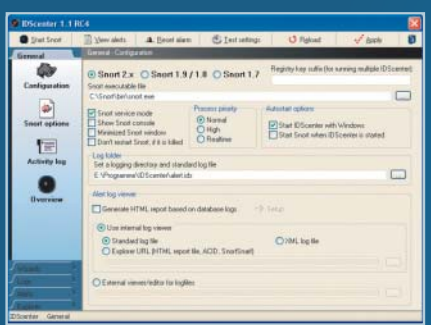
WhoisAssistant: Není tak obsáhlý jako SmartWhois, ale je zdarma.

Tracert: Nástroj, který je součástí Windows XP a který funguje jen přes příkazový řádek. Grafické rozhraní chybí.

3D Traceroute: Provede windowsovský příkaz „tracert“ a graficky ho znázorní. Je to užitečný nástroj, který je navíc zdarma.



Hledání rootkitů: Bezplatný nástroj „Blacklight“ najde neviditelné rootkity a odstraní je.



Poplašný systém: „Intrusion Detection System“ spustí alarm při každém útoku na počítač.

VNIKNUTÍ

Ochrana počítače

Lex Luthor byl polapen. Abychom však zabránili špatnému pokračování, jak je tomu u všech úspěšných filmů, zabudujeme do počítače alarm, který bude nepřátelské aktivity hlásit.

10) JAK VČAS POZNAT ZLODĚJE

Nástroj: Snort, IDSCenter, Winpcap.

„Intrusion Detection System“ spustí alarm okamžitě, když se někomu nepovolanému podaří vniknout do vašich dat. Nejlepší na tom všem je, že nebudete potřebovat hříšně drahé komerční řešení, ale vystačíte si s freewarovými programy.

Milovníci příkazové řádky si nainstalují opensourcový nástroj „Snort“. Pokud dáváte přednost grafické nadstavbě, nainstalujte si IDSCenter, což je grafické rozhraní pro Snort. Navíc budete potřebovat ještě síťovou knihovnu Winpcap.

Máte-li vše nainstalované, spusťte IDSCenter. V menu *Configuration | General* zadejte cestu k souboru „snort.exe“ (např. „C:\snort\bin\snort.exe“). Poté aktivujte „Snort Service Mode“. Nyní zvolte v „Snort options“ cestu k souboru „snort.config“, který se obvykle nachází v adresáři „snort/etc“. Pomocí jezdce „Wizard“ nastavte IDSCenter. Nastavení závisí na síťové kartě, na serveru SQL, na použití statické či dynamické IP adresy a na mnoha dalších faktorech. Podrobný návod naleznete v příručce k programu nebo na webových stránkách *www.engagesecurity.com* a *www.snort.org*.

Alternativní řešení:

Ossec-Hids: Funkčně je podobný nástroji Snort, je ovšem určený pro servery.

Base: Nejedná se o IDS, ale o rozšíření pro browser se stejným účinkem.

Sguil: IDS systém, který je založen na enginu Snortu.

Pokud jste udělali všechny postupy, můžete s klidem odložit převlek do skříně a odpočinout si. Virtuální svět vašeho PC je zabezpečený. Ovšem nikdy nezapomeňte na zlaté bezpečnostní pravidlo: Dnes bezpečný počítač může být za týden v ohrožení! ■ ■ ■