Ze života hackera

Hackeři získávají zdarma **FILMY, HUDBU I PLNÉ VERZE PROGRAMŮ** a také útočí na cizí webové stránky. Chip se podíval na softwarové piráty při jejich práci.

MARKUS HERMANNSDORFER

Všechno, co obsahuje elektroniku nebo je tvořeno z jedniček a nul, může být „hacknuto“ – ať už jde o iPod, poslední CD Madonny nebo testovací počítač atomové elektrárny. My jsme vyzpovídali Toma, jednoho z crackerů „scény“ – a zjistili jsme vše o jeho názorech na firewally, šifrování a snahy směřující k ochraně proti kopírování.

První, co vás na Tomovi zaujme, je jeho komunikace. Používá neobvyklé termíny, protože lidé, kteří se potulují na hackerských konferencích typu DefCon či na méně známém ShmooCon, žijí ve svém vlastním světě se svými pravidly a se svým vlastním jazykem. Tom by se sám nikdy neidentifikoval jako cracker. Sám sebe nazývá freak (šílenec), což v jazyce hackerů vypadá takto: „ph34|<“.

Možnost vyzkoušet si „hackerský žargon“ a přeložit si své vlastní jméno máte i vy – vyzkoušejte to na adrese **www.catb.org/jargon/html/index.html**.

A proč se o tom zmiňujeme? Je to velmi jednoduché: ti, kterým nejsou známy praktiky světa hackerů, vyčnívají při komunikaci s nimi jako bolavý palec. Ten, kdo neví, je označen jako „|oo53r“ (looser nebo newbie), ztrácí přístup k „//4r3z“ (warez) pirátským kopiím a za žádných okolností se nemůže nazývat „<|OO<|3“ (dude – elitní hacker, profesionál).

Přístup povolen: Cracknutí webových stránek

Abychom porozuměli postupu těchto lidí, pozorovali jsme Toma při práci. Důležité upozornění: Všechno, co zde uvádíme, patří ve většině evropských zemí k trestně postižitelnému chování a v žádném případě by nemělo být napodobováno.

Nejprve Tom „crackne“ webovou stránku – přesněji řečeno obejde ochranu heslem, používanou majitelem internetových stránek k blokování přístupu na interní místa nebo k administraci webu. Tom obejde tuto ochranu pomocí scanneru „intelitamper“, což je nástroj z kategorie „web spider“. Odkryje adresáře a soubory umístěné na webovém serveru, který je atakován. Útočník může podobně jako ve Windows Exploreru brouzdat po struktuře a prohlížet si obsah souborů – stahovat jinak nepřístupné obrázky nebo číst dokumenty.

Tom na Googlu pomocí vyhledávacího termínu „intitle: login“ (nebo ještě lépe „intitle:admin intitle:login“) nachází spoustu stránek, které přicházejí v úvahu pro útok. A protože si nepřeje být identifikován majiteli stránek, jeho volba padla na web univerzity, jejíž jméno zmiňovat nebudeme. Pracují zde desítky profesorů a IT odborníků, proto je možné při pokusu o útok předpokládat „silné protihráče“. Po spuštění aplikace intelitamper vyžaduje chvilku na přečtení celkové adresářové struktury stránky. My se poté kvůli různorodosti dokumentů a velkého počtu složek omezujeme jen na určité vzorky. Tom nakonec kopíruje několik dokumentů, které podle našeho odhadu nejsou určeny „pro cizí oči“.

INFO

Pirate Bay – konec pirátského ráje?

Na internetu existuje jen málo adres, které patří k opravdovým pirátským legendám a zároveň nikdo z jejich provozovatelů nesedí ve vězení.

Jednou z nich je švédský server The Pirate Bay (TPB) (**http://thepiratebay.org/**), známý torrent tracker a vyhledávač. Tento server byl sice mnohokrát pod palbou mezinárodních právníků, vždy však vyšel ze soudního sporu vítězně, a nejednou naopak odcházela s ostudou žalující strana. Padla celá řada obvinění, byl zabavován majetek serveru, docházelo k blokování jeho IP adresy (v Dánsku a Itálii) a jeho poštovní schránky jsou plné výhružných dopisů od gigantů softwarového a multimediálního průmyslu. Reakce z „pirátské zátoky“ si můžete sami přečíst na adrese **http://thepiratebay.org/legal**.

Ovšem páky a lobbing nadnárodních firem mají sílu i v jinak normálním Švédsku, a tak se zdá, že idylka „pirátské zátoky“ pomalu končí. Prvním krokem bylo schválení tzv. Wiretapping Law, o kterém se některá „severní“ média vyjadřují jako o „sledování horším než od tajné východoněmecké služby Stasi“. Server TPB na to hodlá reagovat nasazením SSL, snížením cen za VPN tunely, které se otevřou i pro zahraniční uživatele.

Poslední ranou P2P sítím je nově připravovaný zákon, ve kterém švédští legislativci připravují celou řadu opatření namířených přímo proti výměnným sítím. Server The Pirate Bay začal s taktikou automatického vkládání náhodných IP adres do databáze, což má ztížit práci pozdějším čmuchalům. Na pořádnou odpověď na připravovaný zákon si však budeme muset ještě chvíli počkat…

Tyto dokumenty další den poskytneme člověku zodpovědnému za ochranu univerzitních dat, který pochopitelně reaguje nervózně. Ihned zavede opatření pro lepší ochranu portálu a intelitamper je „vědecky otestován“.

Princip: Nástroj přijme „index.html“, který je dostupný pro většinu přístupů na web. Na této stránce bývají často kromě přihlašovacího dialogu i skryté linky na ostatní stránky. A i ty používá intelitamper při svém čmuchání po webové struktuře…

CHRAŇTE SE: U citlivých dat lze za bezpečné označit pouze jejich šifrování. Pro tento účel musí webový hostitel nabídnout podporu pro SSL šifrování. Takto chráněné webové stránky (identifikovatelné podle „https://“) nemohou být prozkoumány pomocí aplikací typu intelitamper.

Bez omezení: Odemkněte demo provždy

Mnoho známých výrobců softwaru nabízí demoverze svých produktů. Pokud chce Tom použít programy bez omezení, použije program „Date Cracker 2000“ a vrátí čas systémových hodin. Namátkou jsme vybrali demoverzi programu „Diskeeper 2008 Professional“.

Nejprve Tom tento program naprosto normálně nainstaluje. Pak spustí Datecracker a klikne na »Add«. Jako popis programu zadá „diskeeper“ a přidá spouštěcí soubor demoverze kliknutím na tlačítko označené »...«.. V tomto případě je to soubor „AppLauncher.exe“. Nyní je datum, kdy byla aplikace nainstalována, zobrazeno pod „Simulated Run Date“. K otestování posuneme systémový čas vpřed o dva měsíce. Diskeeper funguje bez problémů, i když povolené testovací období skončilo…

Další malý „pracovní“ úkol: Tom deaktivuje hlášení, které vyzývá ke koupi při každém spuštění Diskeeperu. Jak? Prohrabáváním se v registru a přesnou analýzou služby „dk.exe“. Tom zjišťuje, že tato „výzva k zakoupení“ je spouštěna souborem nazvaným „DKServiceMsg.exe“ – poté jednoduše nahradí originál prázdným textovým souborem se stejným jménem. Nyní se zpráva již neobjevuje…

Odemykání komerčního softwaru také není příliš obtížné. K tomuto účelu stačí jen sériové číslo. Pokud ho Tom nenajde na internetu, stáhne si již cracknutou verzi.

Plné verze: Použij cokoliv, neplať nic…

Sériová čísla a generátory klíčů jsou nástroje, které vám nabídnou platný licenční klíč. Není těžké je najít. Zadání příslušného termínu, jako například „serialz“ nebo „crackz“, do Googlu zvládne i malé dítě. Nicméně Tom ví, že v této „temné části

internetu“ není nic zadarmo: většina stránek „serialz“ propašuje do vašeho počítače malware. Výsledkem je, že i obyčejná prohlídka těchto stránek představuje velmi vysoké riziko nákazy.

Z tohoto důvodu Tom spouští virtuální PC s Windows XP, které mohou autoři stránek zamořit či „prozkoumat“. Z tohoto virtuálního počítače pak Tom prozkoumává jednotlivé generátory klíčů a přitom jeho pravý systémový disk zůstává nedotčený. Pokud nenajde žádné funkční sériové číslo, pak si jednoduše vyhledá cracknutou verzi požadované aplikace na stránce PirateBay. Aby si ji mohl stáhnout, potřebuje pouze Bittorrent klienta typu Azureus. Spustí ho na anonymní proxy kaskádě (například TOR network), tak aby ho agenti softwarového průmyslu nemohli vystopovat.

Multimédia: Vypnutí DRM ochrany

I Tom má rád co možná nejpohodlnější cestu. „Nikdo zbytečně nepracuje s chráněnými multimédii, pokud si může stáhnout nechráněnou hudbu či filmy z P2P sítí,“ vysvětluje Tom. Nouzovým řešením je odstranění ochranných mechanismů a DRM. Ale i zde má Tom dobrou radu: „Nevyhledávejte programy na pochybných serverech – je lepší použít nástroje ‚renomovaných firem‘.“ Držíme se rady a zkoušíme komerčně dostupné programy firmy Daniusoft – ty si dokáží poradit s DRM bez problémů. Při převádění chráněné hudby či filmového souboru pak není ochrana „cracknutá“ – jednoduše zmizela...

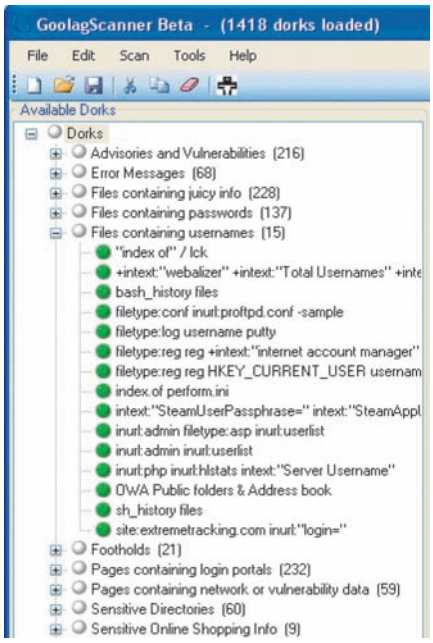
Pomocí tlačítka »Add« si nahrajeme hrstku chráněných hudebních souborů do programu Daniusoftu s názvem „WMA MP3 Converter“. Nastavíme jako výstupní formát MP3 a poté už jen klikneme na tlačítko »Start«. V závislosti na požadavcích (audio/video) a kodeku použitém ve vstupním souboru (WMA, WMV, VOB, M4V...) nabízí Daniusoft celou řadu převodníků, které stojí od 20 do 40 eur.

Poznámka: Existuje i další legální metoda. Něco podobného dělá i Tunebite (**http://tunebite.com**). Tato metoda však u crackerů příliš oblíbená není, protože jí chybí příslušná dávka vzrušení.

Zadní vrátka: Odblokování cizích PC

Napadání cizích počítačů patří k obzvlášť odsouzeníhodným aktivitám, přesto k činnosti hackerů patří. Před útokem je nutné na PC potenciální oběti buď vyhledat bezpečnostní mezery, nebo si je vlastnoručně vytvořit. Tom nám ukazuje obě možnosti útoku.

HLEDÁNÍ ZADNÍCH VRÁTEK: Tato metoda se provádí přes vyhledávač Googlu. Pomocí skeneru Goolag, který byl vyvinut známou skupinou hackerů „Cult of the Dead Cow“, Tom vyhledává hesla, uživatelská jména, zranitelné servery a podobné „užitečné“ materiály. Po spuštění skeneru vloží do položky »Hosts« adresu počítače, který má být cílem útoku. Pak si v sekci „Available Dorks“ zvolí vyhledávací metodu, jako například „Files containing password“, a kliknutím na tlačítko »Scan« zahájí hledání. Poté Goolag Scanner odešle mnohonásobné dotazy Googlu. V našem případě bylo aktivováno 137 různých možností.



Útoky na weby: Goolag Scanner hledá hesla pomocí Googlu.

Výsledek: Google blokuje naši IP adresu, protože v této chvíli je nástroj hackera odhalen.

Je jasné, že opravdového „freaka“ taková „drobnost“ nezastaví. Pomocí dynamických IP adres je pro něj nový dotaz Googlu dětskou hračkou. Po restartu internetového připojení se otevře nová internetová session s novou IP adresou. Tentokrát Tom přistupuje k hledání

INFO

Ve Windows je to možné: Slídění v cizích počítačích

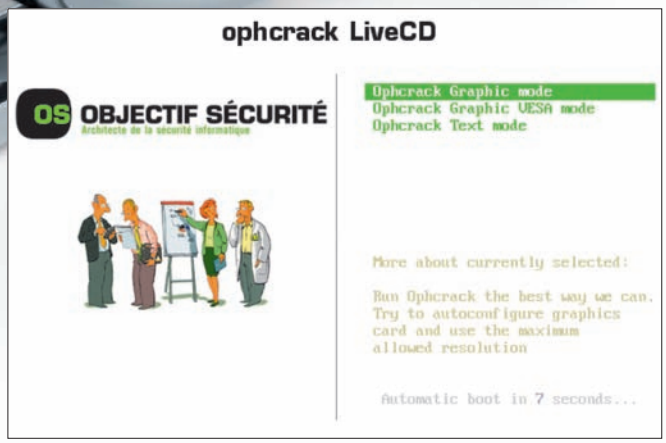
Jen aby nám demonstroval, že Windows může fungovat jako nástroj hackera, napadne Tom cizí počítač pomocí programů z Windows. Tento příklad vám ukáže, jak hacker postupuje.

SBĚR INFORMACÍ:
Nejdříve Tom zmíní důležitý termín: zajištění stop. Znamená to sběr co možná nejvíce informací o oběti. V současné době vám k tomu stačí služba typu **www.robtex.com**. Zde Tom získá informace o hostitelském PC, které má být cílem útoku: které porty jsou přesměrovány, jaké IP adresy sdílí s dalšími weby atd. Jestliže tyto informace nejsou dostatečné, podívá se na **www.dnswatch.info**, a pokud plánuje vloudit se pomocí SMTP (port 25), pak také na **www.mxtoolbox.com**. Zde se dozví důležité informace o poštovním serveru, včetně jeho „rychlosti“.

HACKING Z PŘÍKAZOVÉ ŘÁDKY
Nyní zjišťujeme důležitost informací, které Tom získal při „zajišťování stop“: nejmenovaný poskytovatel připojení nedávno nabízel routery, které se staly ve světě „hackerů“ terčem vtipů, a to i proto, že umožňují použití jednoho z nejstarších triků – použití telnetu. Tom vytváří dávkový soubor, který zjišťuje rozsah IP adres poskytovatele, a tak zjišťuje celou řadu obětí, které mají tento router. Avšak pro skutečný útok Tom potřebuje jiný dávkový soubor s příkazy. Ten obsahuje příkaz „telnet IP_adresa_routeru“ následovaný několika parametry, jmény a hesly. Obsahuje i standardní login tohoto routeru: uživatelské jméno „root“ a heslo „admin“. Poté Tom spouští dávkový soubor a tím i samotný útok.

ČMUCHÁNÍ NA CÍLOVÉM POČÍTAČI
Nyní se vloudí do cizího systému pomocí příkazu standardního portu pro telnet – 23. Je vytvořeno spojení, avšak hesla a uživatelská jména z dávkového souboru nejsou aktivní: oběť zřejmě změnila implicitní nastavení; samotný průnik do Windows už je nefunkční. Nyní budou potřeba metody typu brute force...

XP zdarma se zadními vrátky: Systém BlackXP byl nejen zdarma, ale také se zadními vrátky, pomocí kterých mohli hackeři navštěvovat i kontrolovat váš počítač.



Windows cracker: Ophcrack lze spustit v grafickém nebo textovém modu. Dokáže odhalit heslo ve Windows XP i ve Vistě.

opatrněji a nejprve kliká na znaménko plus před položkou „Files containing password". Tímto způsobem otevře seznam všech možností vyhledávání. Vybere si prvních pět a spouští vyhledávání, aniž by vyvolal u Googlu podezření. Pak následuje dalších pět a poté dalších pět – do té doby, než vyčerpá všechny možnosti.

Bezpečné heslo prolomeno za tři minuty.

Atakovaná webová stránka však útok hackera přežila (byl to náš testovací web) – všechny útoky jsou neúspěšné.

VYTVOŘENÍ ZADNÍCH VRÁTEK: Cracknuté verze Windows XP kolující po internetu měly velice specifický účel. Operační systémy označované jako BlackXP vytvářejí v počítači zadní vrátka ihned po instalaci. Tom vybavený právy administrátora může těmito „vraty" vstupovat i odcházet. Podobně fungují i webové stránky nabízející „Crackz, Serialz a Warez". Zde můžete snadno získat trojského koně, pomocí kterého by mohli v budoucnu hackeři řídit váš počítač.

CHRAŇTE SE: Držte se z dosahu stránek, které se vám snaží „vnutit" sériová čísla a cracky nebo pirátské verze Windows. Tyto stránky nikdy nebudou bezpečné.

Duhové tabulky: Hacking Windows

„Nejbezpečnější operační systém světa" v podání Microsoftu obvykle donutí Toma k úšklebku. Důvod? Například Ophcrack je program pro prolamování hesel Windows, běžící jako malý linuxový systém, který dokáže cracknout heslo administrátora u Visty nebo XP během několika minut. Využívá metody útoku na heslo pomocí tzv. rainbow tables. Ophcrack získává všechna odpovídající hesla (respektive jejich hash hodnoty) z bezpečnostní oblasti registrů (SAM) a porovnává je s předdefinovanými „hash values", které má uložené v tabulkové formě (rainbow tables). Tímto způsobem může být heslo odhaleno rychleji než pomocí zastaralé metody „brute force". Podrobnější informace o tomto typu útoku můžete najít i v článku na serveru SOOM (**www.soom.cz/index.php?name=usertexts/show&aid=568**).

Abychom zkontrolovali, jak rychle Ophcrack funguje, spouštíme Windows Vista na virtuálním PC a pro konto administrátora volíme heslo, které Microsoft password checker (**https://www.microsoft.com/protect/yourself/password/checker.mspx**) označuje jako „vysoce bezpečné". Odhalení hesla by pomocí metody „brute force" trvalo několik tisíc roků, a to i v případě, že bychom měli k dispozici obrovské výpočetní centrum. Naopak Ophcrack si ve Windows XP vyžádá tři minuty a ve Windows Vista přibližně deset minut, aby „odhalil" naše heslo: „ftb5@alyx3z.com".

Postup je velice jednoduchý: Tom si na SourceForge vybere Ophcrack pro XP nebo Vistu. Vypálí si stažený ISO (přibližně 500 MB) na CD. Ihned po spuštění stiskne klávesu Enter, aby spustil Ophcrack v grafickém modu. Po několika minutách práce nástroj zobrazí jméno uživatele a heslo. Pokud to nefunguje, pak odpovídající „hash value" v rainbow table neexistuje. Ale ani to hackera nemusí trápit – autoři na svých stránkách nabízejí více tabulek...

NAŠE DOPORUČENÍ: Chraňte se a nikomu nepovolte přístup k vašemu PC bez dozoru. Může mít u sebe Ophcrack...

AUTOR@CHIP.CZ

ODKAZY NA DALŠÍ INFORMACE

www.hackingalert.com
Ukazuje nejen triky hackerů, ale také metody ochrany proti nim (pouze v angličtině).

www.computec.ch/download.php?cat=dokumente&index.html
Nabízí celou řadu informací souvisejících s hackingem a crackingem, a to ve formátu PDF.

www.shmoo.com/projects.html
Zde můžete získat poslední rainbow tables a jiné hackerské nástroje.

www.soom.cz
Web nabízející informace z oblasti IT bezpečnosti, zaměřující se na hacking, cracking a phreaking...