Platit za přístup na některé placené internetové stránky? Proč, když například profesionální hackeři se dostanou všude zdarma! Tato exkluzivní zpráva vám na následujících stránkách odkryje nejčastější finty hackerů a vysvětlí jejich technické pozadí.

Exkluzivní zpráva o hackerech

Způsob práce hackerů a triky, jak se nabourávají do cizích serverů

DAVID ČEPIČKA, ARNE ARNOLD,
DANIEL BEHRENS A TOBIAS WEIDEMANN

Není hacker jako hacker – alespoň pokud se zeptáte někoho, kdo se pohybuje v jejich vodách. Dozvíte se totiž minimálně to, že existují dobří a zlí. Ti dobří se nazývají *hackeři*. Jejich zálibou je vyhledávání slabých míst na internetových serverech, mají na paměti blaho veřejnosti a nestojí o to, aby se touto činností třeba nezákonně obohatili. Zachovávají jakousi hackerskou etiku, jejíž principy si mohou zájemci přečíst například na internetové adrese **webzone.k3.mah.se/k3jolo/HackerCultures/tradethics.htm**. Existují však i zlí hackeři, kterým se jejich hantýrkou říká *crackeři*. Při své často nekalé činnosti sledují výlučně svůj zájem. V našem článku se od této chvíle budeme zabývat právě těmi zlými.

Rozdělení na hackery a crackery však nalezněte pouze v prostředí, kde se pohybují. Mimo něj nazýváme hackerem každého, kdo neoprávněně pronikne do obsahu internetových stránek.

Nabourání internetové stránky je daleko častější, než by se mohlo zdát. Proto jsme si pohovořili s řadou administrátorů, ale i s mnoha hackery a prolamovači hesel o tom, co se dá na internetových serverech objevit tajného.

Placené internetové stránky

Každý, kdo na internetu nabízí nějaké informace, za něž chce zaplatit, musí vybudovat nějaký způsob ochrany před neoprávněným přístupem. Až po přihlášení pomocí uživatelského jména a hesla může uživatel vidět placený obsah WWW stránek. Ale i přesto se tyto ochranné metody jeví jako krajně nevyhovující. Přečtěte si, jak hackeři takovou ochranu obcházejí!

Deep Links: jednoduchá metoda hackerů, jak se dostat na špatně chráněné placené WWW stránky

Řada odborníků se shoduje na skutečnosti, že při ochraně obsahu placených WWW stránek se jejich provozovatelé chovají přinejmenším naivně. U řady z nich vypadá ochrana proti neoprávněnému přístupu tak, že na svých neplacených stránkách neuvedou přímé odkazy k placenému obsahu a doufají, že na adresu placených stránek nikdo nepřijde.

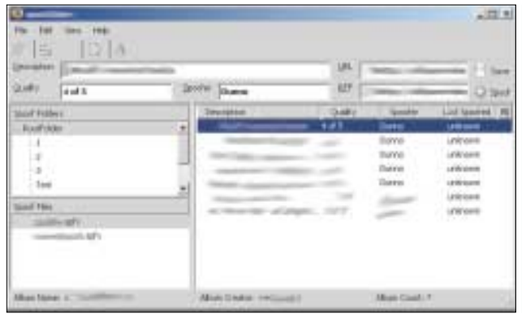
Takoví provozovatelé např. volně zpřístupní uvítací stránku na adrese **www.<hlavnistranka>.cz**. Po přihlášení se platící uživatel dostane na stránky s placeným obsahem. Tyto stránky leží kupříkladu na adrese **www.<hlavnistranka>.cz/placene/**. Přímý odkaz na tuto adresu chybí, ale to je zároveň veškerá ochrana proti neoprávněnému přístupu. Jakmile si zákazník adresy placené stránky všimne, může ji zdarma rozšířit dále. Takové odkazy, které vedou přímo k placenému obsahu, se nazývají *Deep Links*. V našem příkladu by mezi Deep Links patřila např. adresa **www.<hlavnistranka>.cz/placene/obsah1.htm**. Popisovaná ochrana je asi na takové úrovni, jako když si představíte malé dítě, které zavře oči a věří, že teď nikdo nemůže nic vidět, protože ono samo nic nevidí. Tímto primitivním způsobem ochrany operují zejména malí poskytovatelé placených služeb, jelikož nevlastní potřebné know-how pro nasazení pokročilejších technik ochrany WWW stránek.

WWW Spoofing: i lépe chráněné WWW stránky se dají prolomit

Řada poskytovatelů placeného obsahu WWW stránek se proti Deep Links chrání. Jestliže nějaký nepřihlášený uživatel zadá do internetového prohlížeče adresu odkazu typu Deep Link, je automaticky přesměrován buď na uvítací stránku nebo je vyzván k zadání přihlašovacího jména a hesla. Ale i tato technika má svoje slabiny. Skutečnost, zda je uživatel již přihlášen nebo zda se ještě nepřihlásil, pozná webový server podle toho, ze které stránky se uživatel na stránku s placeným obsahem dostal. Tuto informaci mu prohlížeč prozradí prostřednictvím tzv. *referreru*. Více informací k tomuto tématu vám poskytne rámeček s názvem **Triky prohlížeče: trocha teorie z oblasti internetových prohlížečů**.

A co se za tím vším skrývá? Dejme tomu, že se uživatel úspěšně přihlásí do placené zóny, dostane se tedy například na **www.<hlavnistranka>.cz/placene/obsah1.htm**. Odtud smí brouzdat na ostatní stránky s placeným obsahem, které vždy nejprve prověří, zda se na ně dostal rovněž z placené stránky. Jedině tak je zajištěno, že se uživatel pro přístup k placeným stránkám minimálně jednou (a to na začátku) úspěšně přihlásil. Pokud měla poslední stránka, z níž se uživatel na placené stránky dostal, úplně jinou adresu, například **www.<jinaadresa>.cz**, bude uživatelův požadavek na zobrazení obsahu placených WWW stránek odmítnut.

Tento způsob ochrany proti Deep Links je hojně rozšířen, ale je ho rovněž možné obejít. Jenom je nutné WWW server přesvědčit, že poslední stránka, z níž přecházíme na placené stránky, byla rovněž součástí placené oblasti. Pro tento účel existují speciální utility, s nimiž je to hračka.



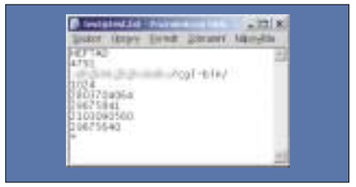
◀ Prolomení prostřednictvím plug-inu: dokonce i ti, kdo se v počítačích tolik nevyznají, mohou pomocích speciálních programů pro spoofing proniknout do chráněných placených internetových stránek.

Takovému „přesvědčování“ WWW serveru se rovněž říká *spoofing*. V angličtině sloveso *„to spoof“* znamená švindlovat nebo podvádět. Podvod spočívá v hlavičce HTTP protokolu, který internetový prohlížeč používá pro zobrazování WWW stránek. Právě v této hlavičce se upraví informace o tom, ze které WWW stránky uživatel na placené stránky přichází.

Aby ani počítačoví laici nezůstávali v hackerských technikách příliš pozadu, hackeři vyvinuli a umístili na internet malé utilitky, kupříkladu plug-in pro prohlížeč Firefox. Začátečník se zájmem o proniknutí do technik hackerů nemusí dlouho hledat vhodné internetové stránky, neboť plug-in jej automaticky přesměruje na nejvhodnější internetové fórum. Tam nalezne spoustu konfiguračních souborů, v nichž najde jak Deep Links, tak vhodné adresy pro nasazení spoofingu. Po jejich instalaci se takovým zájemcům, kteří hackerství berou jako svátečního koníčka, otevřou dokořán a bez jakýchkoliv poplatků k ilegálnímu použití stránky s názvy jako „Bobs' Videos“ či „Yvon's s Training“.

Cookies: jednoduchá ochrana, která se dá stejně jednoduše obejít

Správci serverů nasazují v boji proti krádežím a ztrátám plynoucím z nelegálních průniků do placených stránek stále nové technologie. Ty by měly být pokud možno co nejjednodušší a současně co nejúčinnější, což bohužel nejde vždy dohromady. Jedním z horkých favoritů bývaly *cookies*. Pokud nějaký uživatel zaplatil a následně se přihlásil, obdržel od vás soubor cookie, který obsahoval všechny potřebné informace a který se uložil na jeho počítači na pevný disk.



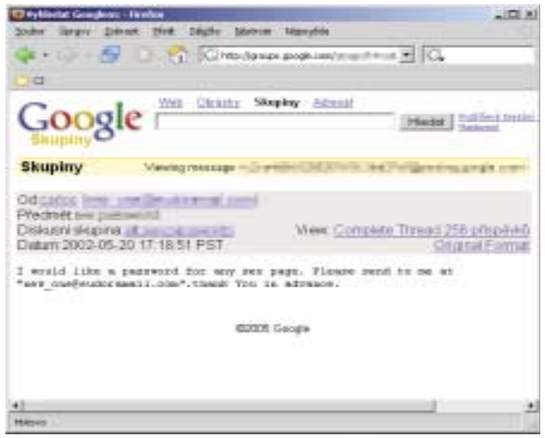
▲ Bez dalších dotazů: ten, kdo jednou dostal cookie z placené stránky, si je může prohlížet zdarma, i když už neplatí.

Pak si takový uživatel mohl prohlížet obsah placených stránek, aniž by se musel vždy přihlašovat.

Přesto i u cookies se brzy objevil jeden háček. Mazanější uživatelé si službu přihlásili, zaplatili, ale jakmile jim však došlo cookie, tak si ho zazálohovali a službu si okamžitě odhlásili. Poté si cookie nahráli zpět na stejné místo na pevném disku a s minimální námahou a výdaji surfovali po placených stránkách dále. Na tuto chybu přišel jeden administrátor v okamžiku, kdy se mu na stránky přihlásilo současně 300 uživatelů, ačkoliv službu zaplatilo pouze 250. Proto se dnes používají spíše zabezpečená cookies.

Zdroje informací

Deep Links, *cookies*, *spoofing* – i ten, kdo všechny tyto techniky ovládá, potřebuje spoustu dalších informací: prostřednictvím jaké URL adresy může spoofing provozovat nebo u které internetové služby funguje trik s cookies? Takové informace hackeři hledají v Usenetu nebo na internetu, popřípadě v různých diskusních fórech.



◀ **Diskusní skupiny: na internetu panuje velmi čilá výměna uživatelských jmen a hesel – zdvořilost je přitom takřka povinností.**

Bezostyšná výměna hesel: v Usenetu se dá získat skoro vše

Hlavně se zdvořile zeptejte! Tak nějak zní základní rada, pokud člověk shání hacknutá data pro přihlášení k nějaké internetové službě. Jaké tedy vlastně jsou informační zdroje pro nezákonné přístupy na internetové stránky? Je fakt, že nejčastěji se prolamují stránky s tématikou sexu. Potřebné Deep Links či zfalšované přihlašovací údaje zjistíte v Usenetu. Tam se přesuňte do vyhledávání diskusních skupin a jako podmínky pro hledání zadejte, možná trochu překvapivě, výrazy „sex" a „password". Tyto výrazy se musí vyskytovat v titulku diskusních skupin. V nich najdete stovky dotazů na poskytnutí vhodných uživatelských jmen a hesel. Po krátkém hledání pak určitě narazíte na FAQ s řadou návodů, jak má zájemce o informace pro hacknutí nějaké stránky či služby požádat.

Poněkud překvapivý je fakt, jak lidé, kteří sami jednoznačně pravidla porušují, sami velmi přísná pravidla stanovují. Například o informace pro hacknutí nějaké stránky smíte žádat maximálně dvakrát týdně, pro poskytnutí správných informací musíte zadat přesnou adresu odkazu a svoji e-mailovou adresu. Na tuto adresu vám totiž bude zaslán návod na prolomení nějaké stránky, popřípadě sem přijdou přihlašovací informace pro využívání nějaké internetové služby. V samotných diskusních příspěvcích tato data většinou zveřejněna nebývají.

„To se mě netýká": hackeři beze strachu z trestu

Lidé, kteří na Usenetu shánějí informace pro hacknutí nějakých stránek, beze strachu poskytují svoji e-mailovou adresu. Učinili jsme pokus, kdy jsme desítkám z nich odepsali a zeptali jsme se jich, zda nemají právní či morální pochyby o svém jednání. Jednalo se navíc o ilegální používání stránek, za něž nebyly poplatky tak vysoké.

Mezi většinou odpovědí zaznívaly názory typu: „To se mě netýká, já surfuji anonymně. Kromě toho by všechny informace na internetu měly být přístupné všem a zdarma." V menšině pak byly odpovědi typu: „Chtěl jsem si tuto službu jen krátce vyzkoušet, abych se mohl rozhodnout, zda si ji zaplatím, či ne. Teď už na tyto stránky vůbec nechodím." Co se týče anonymního surfování, podařilo se nám zjistit, že těch, kteří surfují anonymně, je minimálně. Mnozí z nich surfují s IP adresou, kterou jim přidělil poskytovatel připojení k internetu. Pro úřady státní správy by v těchto případech nebylo nic obtížného zjistit pravou identitu těchto lidí.

Lži

Ne vždy je nutné využívat pro neoprávněný přístup k internetovým stránkám různé technické triky. Někdy stačí zadat několik falešných údajů. Stránky, které povolují přístup například při pouhém zadání čísla občanského průkazu, se dají poměrně velmi snadno obejít.

Přístup prostřednictvím čísla občanského průkazu: správný věk stanoví generátory

Například v Německu obsahuje číslo v občanském průkazu šifrované datum narození majitele. Proto některé internetové stránky vyžadují jeho zadání, aby ověřily, že je uživatel kupříkladu starší 18 let. Algoritmus, podle něhož se generuje číslo v občanském průkazu, však není nijak zvlášť komplikovaný. Na internetu lze najít hromady generátorů, které vám vytvoří libovolná čísla. U některých se požaduje, abyste přesně zadali rok narození. Stačí pohled na příslušná internetová diskusní fóra, abyste pochopili, s jakou samozřejmostí se takové generátory používají. Kontrola přístupu k internetovým stránkám na bázi čísel občanských průkazů tedy bude účinná až v okamžiku, kdy se budou muset zadávat ještě další informace, například o bankovních účtech. Teprve potom bude anonymita internetu narušena.

▶ **V tomto příspěvku diskuzního fóra se nějaký nezletilec jen tak mimochodem zmiňuje o použití generátoru čísel občanských průkazů.**

Čísla kreditních karet: generátory se míjejí účinkem

Lži a podvody prostřednictvím generátorů čísel občanských průkazů většinou hladce projdou. Na internetu ovšem existují i utility, s jejichž pomocí se dají generovat dokonce i falešná čísla kreditních karet. Před několika lety se podařilo jednomu člověku předplatit internetové služby pomocí těchto falešných údajů. Poskytovatelé internetových služeb se ze škod způsobených těmito podvodníky velmi rychle poučili. Dnes většina internetových stránek provádí přesné ověření čísla kreditní karty. Falešná čísla už nemají žádnou šanci projít.

Krádež

Někteří hackeři se vůbec nenamáhají, aby na internetových stránkách hledali slabiny. Pro přístup k internetovému serveru jednoduše ukradnou přihlašovací údaje nějakému jinému uživateli.

Lovci přihlašovacích jmen a hesel

Jeden uživatel, říkejme mu třeba Martin, netušil nic zlého, když jednoho dne dostal od své banky e-mail s následujícím textem: „V rámci našich závazků poskytování těch nejlepších služeb…" V tomto e-mailu byl vyzván k tomu, aby minimálně jednou měsíčně on-line zkontroloval stav svého účtu. „Jsme si jisti, že toto bezpečnostní opatření povede k lepší ochraně vašeho bankovního účtu", stálo dále v e-mailu, jehož vzhled byl v designu WWW stránek banky. E-mail tedy bezpochyby pocházel z banky, vždyť obsahoval adresu odesílatele **security@<banka>.cz**, dále internetový odkaz na banku, na který měl klepnout, i certifikát zabezpečení a různá upozornění pro zvýšení bezpečnosti při manipulaci s účtem. Pan Martin byl další den přinejmenším zaskočen, kdy mu přišel prakticky totožný mail, tentokrát ale vyvedený v barvách konkurenční banky. Nejvíce podezřelé bylo to, že u této banky Martin žádný účet nikdy neměl. V tomto případě se jednalo o zvláště vyvedený tzv. *phishing mail*. Naštěstí Martin na první obdržený e-mail ještě nereagoval.

Lupiči loví, kde se dá: krádež prostřednictvím falešné internetové stránky

Phishing je trik, který se v poslední době používá stále více. Toto slovo je odvozeno z anglických výrazů „*password*" (heslo) a „*fishing*" (rybaření). Cílem *phishingu* je získat přihlašovací jména a hesla k různým internetovým službám a tyto nelegálním způsobem získané údaje pak zneužít kupříkladu pro převod peněz na svoje konto, pro nákupy na účet poškozeného apod. Takový e-mail se tváří, jako kdyby pocházel z banky nebo podobných institucí, jeho předmětem je většinou nějaká prosba o poskytnutí údajů či oznámení o vylepšení zabezpečení a cílem je, aby se uživatel musel přihlásit. Ve skutečnosti se však uživatel po zadání uživatelského jména a hesla dostane na úplně jiný server, který jeho přihlašovací informace přečte a uloží. Název odkazu v textu totiž vůbec nemusí odpovídat odkazu, na který má být přesměrován. V uvedeném případě sice e-mail z banky v textu obsahoval správnou adresu banky, ovšem zakrátko byl přesměrován na stránku s doménou **.info** a s velmi podobným, avšak ne totožným názvem.

Jak se proti takovým útokům bránit? Pokud dostanete nějaký e-mail v HTML formátu, který vás vyzývá k zadání nebo ověření nějakých informací, otevřete jej nejprve v internetovém prohlížeči a pohybujte kurzorem myši nad odkazem. Ve stavovém řádku prohlížeče se objeví odkaz, na který budete po klepnutí na odkaz přesměrováni. Rozhodně nedoporučujeme na odkaz klepnout a jednoduše čekat, co se stane. Mohli byste si do počítače nainstalovat nějakého trojského koně nebo jiného škůdce, nehledě k tomu, jak již bylo zmíněno, že adresa, která se objeví v adresním řádku prohlížeče, nebude vždy skutečně tou, která se zobrazí.

Hackeři profesionálové

Skutečný profesionál triky jako jsou Deep Links, spoofing nebo falešná cookies pohrdá. Na prolomení WWW stránek a internetových serverů totiž jde úplně jinak.

Profesionálové využívají bezpečnostních trhlin

Každý zkušený hacker vždy hledá zejména slabá místa systému. Často jsou jimi bezpečnostní trhliny v programech, které na serveru běží. Tyto trhliny se buď snaží odhalit sám, nebo se chytře podívá na internet na ty správné stránky. Mezi takové patří kupříkladu adresa **www.securityfocus.com** – zde najdete diskusní fórum věnované výlučně vyhledávání a utěsňování bezpečnostních trhlin.

Hacker je tedy tím úspěšnější, čím více bezpečnostních trhlin zná, čím je zkušenější. Záleží na tom, zda dokáže vhodně kombinovat i méně závažné trhliny v systému a je na tom samosebou lépe, pokud ovládá více operačních systémů a programovacích jazyků. Cílem hackera je získat k danému serveru všechna přístupová oprávnění. Pokud se mu to totiž podaří, dostane se ke všem na serveru uloženým datům.

Triky prohlížeče: trocha teorie z oblasti internetových prohlížečů

Pokud přistupujete k nějakému WWW serveru na internetu, přenáší váš internetový prohlížeč v hlavičce protokolu HTTP informace o konfiguraci vašeho systému, a to bez vašeho vědomí. Webový server se tak dozví, jaký používáte internetový prohlížeč, a jaký operační systém a v jaké jazykové mutaci. Kromě toho mu rovněž sděluje, zda jste se na stránku, kterou chcete zobrazit, dostali klepnutím na odkaz. Pokud ano, přenese se na webový server rovněž informace o internetové stránce, z níž jste se na aktuální stránku dostali – jedná se tedy o adresu stránky, na níž se odkaz na aktuální stránku nacházel (tzv. *referrer*). To ale stále ještě není vše. Webový server se dále dozví, které formáty obrázkových a jiných souborů váš prohlížeč podporuje (například JPG, DOC či XLS), zda podporuje formát XML a zda podporuje komprimování HTML stránek v reálném čase. Používáte-li nějaký proxy server, může se stát, že se do hlavičky protokolu HTTP zapíší ještě další informace, například vaše IP adresa. Zda tomu tak bude, závisí na konfiguraci proxy serveru. Jestliže se tam zmíněné informace zapíší, znamená to, že se jedná o tzv. *transparentní proxy server*, jenž se rozhodně nehodí k anonymnímu surfování po internetu.

▲ **Co prozradí váš prohlížeč: tato testovací stránka ukazuje, jaké informace internetový prohlížeč bez vašeho vědomí odesílá.**

Mnohé webové servery potřebují zmiňovaná data z hlavičky protokolu HTTP pouze z technických důvodů, kupříkladu proto, aby rozhodly, kterou jazykovou verzi internetové stránky vám mají zaslat. Zadáte-li například adresu **www.mozilla-europe.org** z internetového prohlížeče v české jazykové mutaci, budete automaticky přesměrováni na českou verzi internetových stránek.

Podle tzv. referreru mnohé servery zjišťují, zda máte vůbec právo na zobrazení stránky, kterou požadujete. V každém případě jsou data v hlavičce protokolu HTTP přenášena z vašeho internetového prohlížeče vždy, bez ohledu na to, zda je server potřebuje nebo ne.

Chtěli byste vědět, která data v hlavičce protokolu HTTP najdete? Pak se přesuňte na internetovou adresu **www.ericgiguere.com/tools/http-header-viewer.html** a vyhledejte pojem *Your Headers*. Pro Firefox 1.0 existuje zdarma dostupný doplněk, který neustále zobrazuje všechny hlavičky protokolu HTTP – tedy jak ty, které odesíláte, tak ty, které přijímáte. V těchto hlavičkách tak kupříkladu můžete zjistit, na které aplikaci běží určitý internetový server. Popisovaný doplněk se nazývá **Live-HTTP-Headers 0.10** a najdete jej na internetové adrese **http://livehttpheaders.mozdev.org**, odkud si jej můžete přímo nainstalovat.

Neviditelní hackeři

Průnik do internetových stránek s placeným obsahem nepředstavuje pro zkušeného hackera žádný velký problém. Přesto: jsou hackeři tak rafinovaní, že dokáží ochránit sami sebe? Ve většině případů ano.

Hacker, který se pokouší získat přístup k nějakým internetovým serverům, činí všechna možná opatření, aby nebyl identifikován. Vždyť při každém pokusu o přístup k jinému počítači se tento počítač dozví minimálně IP adresu hackerova počítače. IP adresa je jednoznačným identifikátorem, který rozlišuje všechny počítače na internetu. Při síťové komunikaci se vkládá do každého paketu, aby WWW server a router na internetu věděl, kam má vyřízený požadavek zaslat.

Mnoho serverů ukládá z bezpečnostních a statistických důvodů všechny IP adresy počítačů, včetně času, kdy na server přistupovaly. Všimne-li si správce serveru neautorizovaného přístupu, podívá se do záznamového protokolu a z něj může odhalit identitu hackera podle jeho IP adresy.

IP adresa: nejdůležitější stopa, která vede k hackerovi

Pokud uživatel nemá trvalé připojení k internetu, zpravidla dostává při každém připojení k internetu přiřazenou jinou IP adresu. Pouze poskytovatel připojení může na základě souborů se záznamovými protokoly zjistit, který uživatel se připojil na internet, kdy to bylo a pod jakou IP adresou připojení probíhalo.

Z důvodu ochrany dat však tyto informace nesmí nikomu poskytnout – snad kromě orgánů činných v trestním řízení. Pouze na závažnosti trestného činu pak závisí, zda si správce serveru dá tu práci s porovnáním hledané IP adresy se seznamem neznámých, popřípadě anonymních vlastníků a jim přidělených IP adres. Pro hackery tudíž tato skutečnost nepředstavuje žádné riziko a spoléhají na to, že se IP adresy, které na serveru zanechali, nebudou nijak zvlášť zkoumat.

▶ **Findnot.com: tato služba nahrazuje IP adresu návštěvníka svou vlastní. Tímto způsobem mu umožňuje surfovat anonymně.**

Trik hackerů: používání zdarma poskytovaných internetových „přestupních stanic“

Pro větší zabezpečení anonymity používají hackeři jednu nebo i více jakýchsi „přestupních stanic“. Jedná se vlastně o proxy server nebo VPN (virtuální privátní síť). Data, která odesíláte a přijímáte, se umístí nejprve do této přestupní stanice, která se následně postará o jejich správné přesměrování. Server, na nějž se posílají vaše požadavky, se tedy prakticky dozví pouze IP adresu přestupní stanice. Na internetu existují stovky stanic, které lze používat zdarma. Pro hackery se hodí pouze některé z nich.

1. Hacker musí na internetu ze všeho nejdříve vyhledat tzv. aktivní proxy server. Některé speciální služby, například **www.aliveproxy.com**, zvládnou vyhledávání aktivních proxy serverů samy a jejich seznam zveřejňují na webu.

2. Většinou není jasné, zda je takový proxy server zřízen na internetu záměrně k tomu, aby poskytoval svoje služby všem uživatelům internetu, nebo zda se jedná o chybu v jeho konfiguraci.

3. Vybraný proxy server by měl správně fungovat tak, že bude protokolovat všechny přístupy a tedy zaznamená i IP adresy hackerů.

4. Zdarma poskytované proxy servery jsou často přetížené a tudíž pomalé.

5. Proxy servery zpravidla fungují pouze pro surfování na internetu. Při pokusech o přístup na jiné porty než na standardní port 80 pro internetový prohlížeč takový požadavek neprochází přes proxy server, ale přímo. Koncový server se tak dozví IP adresu uživatele.

6. Mnohé proxy servery posílají skutečnou IP adresu hackera v hlavičce protokolu HTTP. Cílový server může tedy tuto informaci ve svém protokolu evidovat. V takových případech hovoříme o tzv. transparentních proxy serverech, které se v žádném případě k anonymnímu surfování nehodí.

Speciální služby poskytující skutečnou anonymitu při surfování na internetu

Hackeři, kterým stačí skutečně pouhý přístup na internet, například aby mohli používat Deep Links, používají pouze ty proxy servery, u nichž si jsou naprosto jisti, že nepořizují žádné záznamové protokoly. Zjišťuje se to však obtížně.

Pokud potřebují neomezený anonymní přístup ke všem portům, volí jinou cestu. Používají kupříkladu službu **www.findnot.com**. Pomocí Windows či prostřednictvím malé utility si na svoje připojení pořídí druhé virtuální připojení, přes VPN (virtuální privátní síť). VPN je něco jako tunel mezi dvěma počítači připojenými k internetu, jímž jsou přenášena data v zašifrované formě. Jakmile hacker vytvoří připojení prostřednictvím VPN, přiřadí se jeho počítači druhá IP adresa. Všechny odcházející a přicházející připojení od této chvíle probíhají přes druhou IP adresu. První IP adresa, která byla přidělena při připojení na internet, ustupuje do pozadí a je viditelná pouze pro provozovatele VPN.

Teoreticky by mohla i služba na **www.findnot.com** zaznamenávat všechny požadavky a být tak zdrojem informací pro orgány činné v trestním řízení. Provozovatelé této služby však slibují, že žádné protokoly se záznamy nevedou.

5 0199/FEL ❑

Internetové vyhledávače

Zjistěte přístupová hesla k WWW serverům přes Google

Mnozí hackeři naleznou ilegální cestu k internetovým serverům i pomocí vyhledávače Google. Ohroženy jsou minimálně ty servery, na nichž běží aplikace Apache. Za všechno může soubor HTACCESS, jenž řídí v programu Apache přidělování přístupových práv a ve většině případů se nachází na serveru ve stejnojmenné složce. Tento soubor zpravidla odkazuje na soubor, v němž jsou uložena hesla (většinou se jedná o soubor HTPASSWD). Když vyhledáte oba soubory pomocí Googlu, je pak možné na serveru chráněná data zpřístupnit.

TIP: Pokud používáte na svém internetovém serveru Apache, dejte pozor na to, aby soubor s hesly nebyl přístupný přímo z webu, a to ani prostřednictvím aliasu. Pokud vám poskytovatel prostoru na WWW serveru poskytuje pouze kořenový adresář, takže nemůžete vytvářet žádné podsložky, jimž byste mohli přidělovat různá přístupová práva, měli byste zvážit, zda celou složku nenastavit tak, aby se nedala Googlem vůbec najít. Dá se to zařídit tak, že na serveru vytvoříte soubor NOROBOT.TXT, do něhož zadáte název složky. Přesný postup najdete na internetu na stránce **Searchengineworld** na adrese**: www. searchengineworld.com/robots/robots_tutorial.htm**. Nezapomeňte ověřit funkčnost souboru NOROBOT.TXT! Při ověřování vám rovněž pomůže již zmiňovaná stránka **Searchengineworld**.