Bezplatné surfování v cizí síti

Internet na letišti, v kavárně nebo na koupališti je příjemný, ale drahý. Díky našemu návodu a programům z Chip DVD budete i zde moci **SURFOVAT ZCELA ZADARMO**. Zabezpečení totiž není v těchto případech tak silné, abyste je nepřekonali.

VRATISLAV KLEGA

Chat, ICQ, e-maily, zprávy, surfování – nic z toho nefunguje, jestliže nemáte připojení k internetu. Podle nejnovějších informací Českého statistického úřadu má připojení k internetu 42 % domácností, 33 % domácností je připojeno k vysokorychlostnímu internetu. Není se čemu divit, vždyť nejlevnější připojení lze často pořídit od 200 Kč měsíčně. Co ale dělat, vydáte-li se mimo dosah svého access pointu? Zde se cena dramaticky zvyšuje. Ani připojení přes mobilní síť není žádnou výhrou. 3G internet je dostupný jen na vybraných místech a rychlost je oproti připojení přes Wi-Fi řádově nižší.

O mnoho lepší není ani situace na veřejných místech, jako jsou třeba letiště. Připojení je předražené, a navíc se často prodává po celých hodinách. Přečtení jednoho e-mailu se tak může pořádně prodražit. Proto vám ukážeme, jak se připojit k hotspotu a nezaplatit ani haléř. A jak je to s právní problematikou takového jednání? Podrobnosti najdete v boxu na straně 45. Na závěr vám pak ještě poradíme, jak byste si měli zabezpečit svoji vlastní Wi-Fi síť, aby se do ní nikdo nedostal.

DNS trik: Neprůchodný firewall

Hotspot je vlastně takovou informační dálnicí. Abyste mohli po dálnici jezdit, je třeba zaplatit mýto. Jenže obyčejná cesta, která vede hned vedle dálnice, je zcela zadarmo. A právě této cesty využijeme. Nebudeme připojeni k běžnému proxy serveru poskytovatele internetu, ale využijeme DNS (Domain Name System) serveru. DNS server slouží standardně k tomu, aby převáděl názvy serverů na IP adresy. Pokud do svého internetového prohlížeče zadáte **www.chip.cz**, DNS server prozradí, že se jedná o server s IP adresou 217.31.59.53, ke kterému se pak prohlížeč připojuje. Servery jsou totiž na internetu identifikovatelné právě podle IP adres a uživatel by si nikdy nezapamatoval desítky čísel svých oblíbených serverů. DNS servery vlastně fungují jako telefonní seznam – vy zadáte jméno a DNS najde správné číslo.

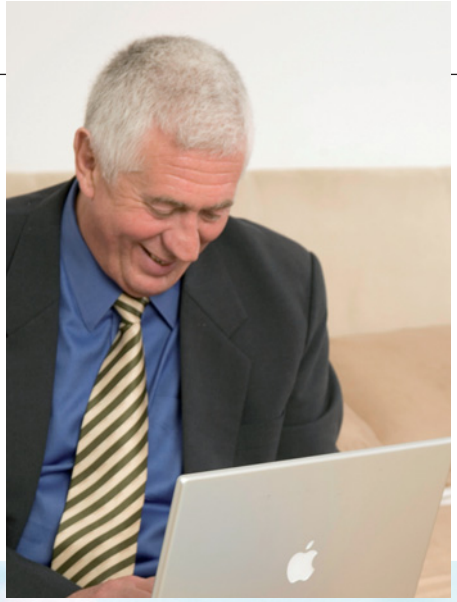
DNS server je naší první cestou k bezplatnému surfování. Provozovatel hotspotu totiž může zakázat přístup do domén, ale ne k DNS serverům. Pokud by zakázal přístup k DNS serveru, nemohla by se zobrazit ani úvodní obrazovka, která vás nabádá k zaplacení internetu a přihlášení se ke službě.

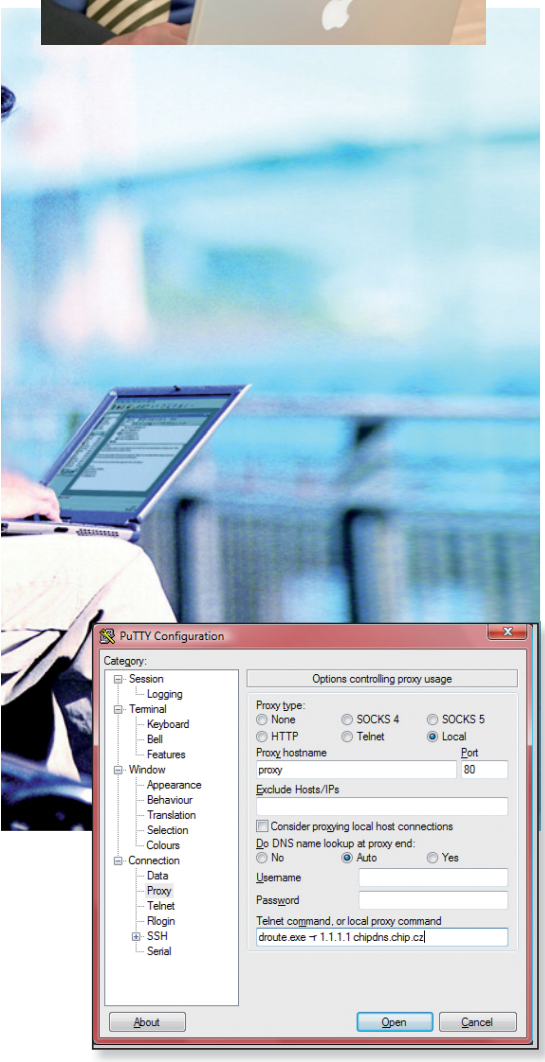
Toho můžeme využít. Svoje pakety přidružíme k DNS paketům a oklikou je pošleme, kam budeme chtít. Tak se dostaneme na běžné webové stránky. Příchozí pakety se pak navíc správně pošlou na náš počítač.

Jednoduchý princip, který ale vyžaduje pečlivou přípravu: aby DNS server převáděl jména na IP adresy, musíme vytvořit objížďku. Je třeba vytvořit speciální server, který provede DNS převod. Tím vytvoříme kódované spojení, přes které je možné posílat data.

Příprava serveru: Datový převáděč

Pro přípravu vlastního DNS serveru neboli převáděče budete potřebovat počítač při-





Vlastní přenos: Pomocí nástroje PuTTY bude obsah webu zabalený v DNS paketech, které vám hotspot rád předá.

NAJDETE NA CHIP DVD

Prolomení Wi-Fi

OzymanDNS ► server pro DNS

PuTTY ► telnet klient

Backtrack ► linuxová distribuce pro hackery

► **NA DVD:** Programy k tomuto článku najdete na DVD pod indexem **PROLOMENÍ WI-FI**.

pojený k internetu. Tento počítač musí mít vlastní doménové jméno, aby jej bylo možné po zadání dotazu vyhledat v DNS databázi.

DYNDNS POMŮŽE: Aby bylo možné váš vlastní DNS server v internetu najít, je třeba, aby měl veřejnou statickou IP adresu. Jen tak budete mít jistotu, že se ke svému serveru budete moci kdykoliv dostat. Používáte-li k připojení k internetu ADSL od O2, dostanete sice veřejnou adresu, ale ne statickou. Adresa se tedy kdykoliv může změnit. Pokud byste chtěli statickou adresu, je třeba za ni připlatit.

Řešením je služba DynDNS (**www.dyndns.com**). Je-li vaše IP adresa přidělována dynamicky, DynDNS problém vyřeší. Otevřete si uvedenou webovou stránku a klikněte na »Create Account«. Zaregistrujte si službu – bude po vás vyžadován jen login a e-mail. Pro dokončení registrace je třeba otevřít e-mail, který přijde vzápětí po registraci, a dále kliknout na uvedený odkaz. Poté se ke službě znovu přihlaste. V části »My Services« klikněte na »Add Host Services«. Do řádku »Hostname« zadejte libovolné jméno své subdomény a vpravo si pak vyberte doménu. Do řádku »IP Address« zadejte současnou IP adresu svého připojení, případně můžete využít funkci pro automatickou detekci. Tu můžete použít v případě, že jste právě na internetovém připojení, na kterém bude v provozu také váš DNS server. Kliknutím na »Create Host« je dynamický DNS záznam vytvořen.

Většina domácích routerů již dnes podporuje službu DynDNS. Stačí se připojit k webovému rozhraní routeru. Pod položkou Advanced zde nejčastěji bývá Dynamic DNS nebo přímo DynDNS. Do rozhraní pak stačí vyplnit své uživatelské jméno a heslo, které jste zadávali při registraci, a doménu, kterou jste registrovali, v našem případě to bylo »chipdns«.

POUŽITÍ DOMÉNOVÉHO JMÉNA: Aby mohl DNS server na straně poskytovatele hotspotu přistupovat k vašemu převáděcímu DNS serveru, potřebujete mít doménové jméno, které bude přesměrováno na váš server. Máte dvě možnosti: Buď máte zakoupenu vlastní doménu, a pak si sami můžete upravit DNS záznam na odpovídající hodnotu (IP adresu). Ve většině případů stačí poslat vašemu správci e-mail s novými údaji, a tím je vše zařízeno.

Pokud doménu nevlastníte, je zde služba **www.dnstunnel.de**. Na uvedené stránce je vysvětleno, co musíte udělat. Celá stránka je bohužel v angličtině, proto přinášíme stručný popis. Poté, co máte vytvořen DynDNS záznam nebo máte pevnou IP adresu, pošle-

INFO

Zbavte se spolusurfařů

Náš trik se zneužitím DNS funguje jen u hotspotů, za které chce pronajímatel zaplatit. U domácích access pointů a routerů je třeba na několika frontách provést opatření, aby se k nim nikdo nepřipojil.

ZABEZPEČENÍ ROUTERU

Když vybalíte router z krabice a připojíte kabely, většinou už funguje. I notebook se sám připojí k otevřené Wi-Fi a vše se zdá v pořádku. Většina uživatelů se proto ani nesnaží nic měnit a nechá Wi-Fi tak, jak je. To je ovšem ten nejhorší případ – Wi-Fi síť je nezabezpečená, kdokoliv se k ní může přihlásit a změnit nastavení routeru. Je proto třeba provést potřebná zabezpečení.
Jak zabezpečení provést, to si ukážeme na routeru AirLive WN-300R. Spusťte internetový prohlížeč a zadejte adresu http://192.168.1.254. Výchozí adresu svého routeru najdete v návodu, někdy bývá adresa napsaná na spodní části routeru. Router bude požadovat uživatelské jméno a heslo. Jméno zadejte »admin«, heslo »airlive«.
V menu poté zvolte »Password«. Router bude vyžadovat napsání starého hesla (airlive) a dvakrát budete muset zadat nové heslo. Doporučujeme zvolit délku aspoň osm znaků.

SKRYTÁ SÍŤ

V části »Wireless« nastavte parametry sítě. Pod položkou »Mode« zadejte název sítě. Zrušte také zatržení u položky »Broadcast SSID«. Díky tomu nebude síť standardním způsobem viditelná, což řadu čmuchalů odradí. Pokračujte kliknutím na »Configure SSID1«.

SILNÉ HESLO

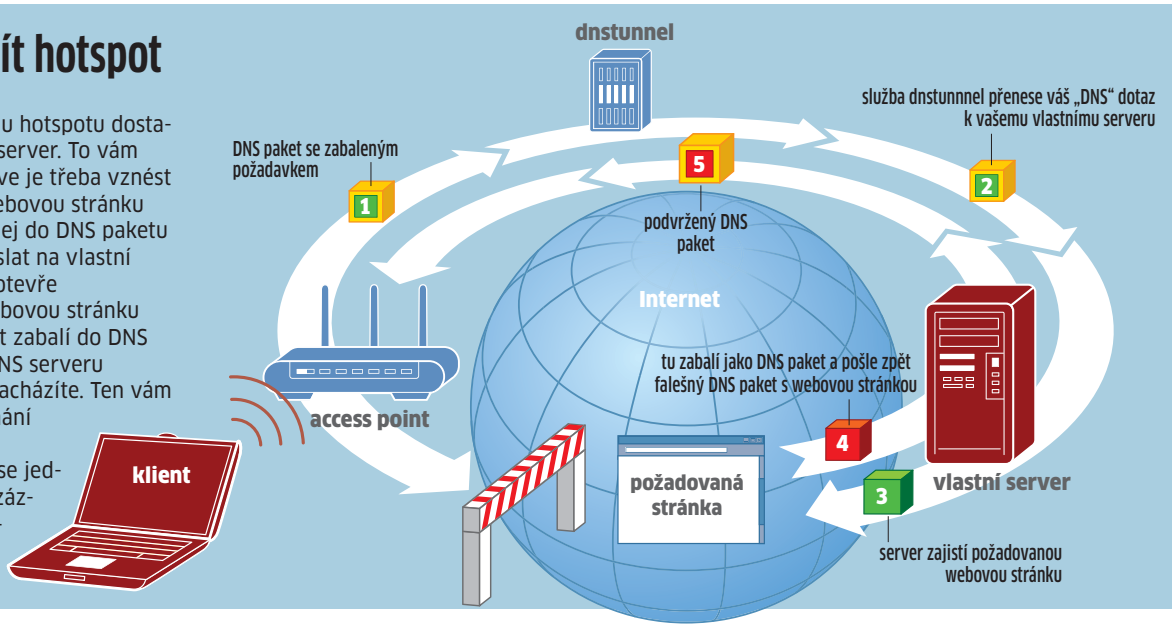
V části Security System vyberte »WPA2-PSK«. To je jediné šifrování, které lze považovat za dostatečně bezpečné. Do řádku PSK pak napište své heslo. Chcete-li mít jistotu neprůstřelnosti, zvolte heslo aspoň o délce 15 znaků. Kliknutím na »Save« změny uložíte.

JEN PRO VYVOLENÉ

Šifrování pomůže také k tomu, aby nikdo nerozkódoval vaši internetovou komunikaci. Pro dokonalou bezpečnost nastavte, aby se k síti nepřipojil nikdo cizí. Klikněte na »MAC Filter«. Dále zvolte »Trusted Wireless stations only«. Router nyní zobrazí seznam Wi-Fi klientů, kteří jsou nebo byli připojeni k routeru. Ta zařízení, kterým chcete dovolit přístup k Wi-Fi, označte a kliknutím na »<<« je přesuňte do důvěryhodné zóny. Budete-li chtít přidat nové zařízení, stačí vyplnit jeho jméno a MAC adresu. Ta je většinou zapsaná na zařízení; jedná-li se o počítač s Windows, zjistíte ji příkazem »ipconfig -all« v příkazovém řádku.
Máte-li síť skrytou, použito šifrování WPA2 a aktivován filtr MAC adres, do vaší Wi-Fi sítě se nedostane ani profesionální hacker.

Jak přelstít hotspot

Bez zaplacení se u hotspotu dostanete jen na DNS server. To vám však stačí. Nejprve je třeba vznést požadavek na webovou stránku (zelená), zabalit jej do DNS paketu (žlutý) a poté poslat na vlastní DNS server. Ten otevře požadovanou webovou stránku (červená), tu opět zabalí do DNS paketu a pošle DNS serveru v místě, kde se nacházíte. Ten vám pak data bez váhání předá, protože předpokládá, že se jedná o běžné DNS záznamy, a ne o placený web.



ILUSTRACE: HARALD FUCHSLOCH

te e-mail na adresu **request@dnstunnel.de**. Do e-mailu uveďte své jméno, IP adresu, případně DynDNS záznam a také jméno subdomény, kterou chcete používat – jakmile bude vaše žádost vyřízena, získáte záznam v podobě jméno.dnstunnel.de.

Nyní je ještě třeba doplnit CNAME záznam služby DynDNS. Ten je určen k přesměrování na subdoménu. Pokud je referenční záznam například »chipdns.chip.cz«, bude záznam ze služby DynDNS vypadat třeba jako »chipdns.gotdns.com«. Odpovídající CNAME záznam pak vypadá takto: Do »Alias Name« zadejte název subdomény, v našem případě »chipdns«. Jako »Host Name« zadejte jméno včetně adresy svého DynDNS serveru, v našem případě »chipdns.gotdns.com«. Do položky »TTL« se zadává, jak dlouho má mít server uloženo připojení – standardně se zadává jedna hodina.

DNS PŘEVÁDĚČ: Nyní dojde k přípravě samotného serveru. Současné verze serverů jsou dostupné jen pro operační systém Linux. Bude tedy třeba spustit Linux. Ani jej nemusíte instalovat, zcela postačí vhodná live verze, kterou stačí nabootovat. Pro spuštění tak bude stačit starý počítač, případně si vystačíte i s virtuálním počítačem pod Windows. My jsme použili Slax, který je základem záchranného Chip DVD 5/09, stejně tak ale můžete použít jakýkoliv jiný Linux. Upozornění: Ve Slaxu se místo příkazu sudo používá sulogin.

Ke spuštění serveru použijeme aplikaci OzymanDNS, kterou naprogramoval v Perlu DNS guru Dan Kaminsky. Nástroj se skládá z pěti souborů – dva slouží pro upload/download za využití DNS. Hezké, ale pro nás nezajímavé. Skript nomde.pl je pak samotný server. Používá port UDP 53, který je privilegovaný, proto je třeba skript spustit jako root. Také se ujistěte, že port 53 je dostupný zvenku – aby jej neblokoval firewall. Poté spusťte server tímto příkazem:

```
sudo ./nomde.pl -i 0.0.0.0 vaše doména
```

Místo „vaše doména“ zadejte doménu, kterou jste registrovali jako CNAME-DNS záznam.

Server je hotový, teď je třeba přichystat klienta.

Klient: Vše ve Windows

I klient funguje standardně jen pod Linuxem, už se však objevily první verze, které klienta zprovozní i pod Windows. Vlastní spojení mezi klientem a vaším DNS serverem je chráněno a šifrováno pomocí SSH. Takto se vytvoří DNS tunel až k vašemu serveru.

Pro tunelování použijeme program PuTTY, který protokol SSH podporuje. Spusťte PuTTY – najdete jej na Chip DVD. Zvolte »Connection | Proxy« a »Proxy Type« nastavte na »Local«. Jako »Proxy hostname« zadejte »proxy« a port »80«. Poté aktivujte volbu »Consider proxying local host connections« a do »Telnet command« zadejte:

```
droute.exe -r 1.1.1.1 vaše doména
```

V menu »SSH« ještě zatrhněte položku »Enable compression«. To zrychlí komunikaci. Dále v menu »Session« jako »Host Name« zadejte libovolný název. Bez jména by PuTTY nefungovalo. Port ponechejte na hodnotě »22«. Kliknutím na tlačítko »Open« provedete připojení.

Nyní je vše nastaveno. Abyste se však mohli třeba z Internet Exploreru připojit do sítě, je ještě třeba provést úpravu v konfiguraci připojení. Spusťte Internet Explorer, zvolte »Nástroje | Možnosti Internetu | Připojení«, klikněte na »Nastavení místní sítě« a zatrhněte položku »Použít pro síť LAN server proxy«. Pokračujte kliknutím na »Upřesnit« a do řádku »Socks« zadejte »localhost« a port »5000«. Po kliknutí na »OK« můžete nyní surfovat ve všech placených hotspot sítích zcela zdarma.

Vloupejte se k sousedovi: Prolomení WEP

Hotspoty využívají poskytovatelé připojení k internetu. Co když se ale chcete podívat třeba do Wi-Fi sítě svého souseda? Pokud nečte Chip a neprovedl preventivní opatření před možným zneužitím, můžete se pomocí našeho postupu do jeho sítě dostat.

BACKTRACK: Abychom mohli síť rozlousknout, budeme potřebovat profesionální výzbroj, kterou používají hackeři po celém světě. Na Chip DVD najdete image bootovacího Linuxu Backtrack. Tím, čím je pro kuchaře vařečka, je pro hackera Backtrack. Je třeba, aby měl Linux plný přístup k hardwaru, proto nemá smysl jej pouštět ve virtuálním počítači. Pomocí vhodného vypalovacího programu vypalte image na CD a nabootujte z něj počítač. Zhruba po třech minutách vás přivítá grafické rozhraní systému.

Tip: Na webové stránce **http://backtrack.offensive-security.com/index.php/HCL:Wireless** je seznam podporovaných Wi-Fi karet. U některých je také poznámka, jak pomocí několika jednoduchých příkazů upravit ovladače, aby návod fungoval.

WI-FI OVLADAČE: Vedle tlačítka »K«, které je na stejném místě jako tlačítko »Start« ve Windows a které má i stejnou funkci, najde-

PRÁVO

Je to vlastně legální?

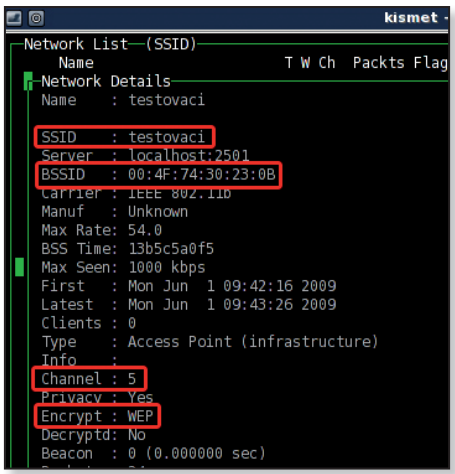
Je třeba se na letišti schovávat do temného koutku a neustále se dívat, nepřijde-li policejní kontrola? Nebo se není čeho bát?

PRÁVNÍ PROBLEMATIKU JEDNÁNÍ NÁM OBJASNIL ADVOKÁT.

Povolí-li provozovatel připojení omezený přístup na svůj hotspot, nedává tím sám o sobě najevo možnost jeho volného užívání. Pokud je dostupná jen některá neklíčová služba, využití takové služby k jinému účelu (např. služby tunelování HTTP pomocí DNS) v naprosté většině případů také není provozovatelem povoleno. Uživatel tak bude nejspíše porušovat obchodní podmínky provozovatele a způsobovat mu zejména neoprávněným vytížením přenosové kapacity škodu a dále ušlý zisk. Stejné je to s neoprávněným přístupem k cizí šifrované Wi-Fi síti. Navíc neoprávněné připojení k takové síti bude od příštího roku trestné.

Chip dodává: Ušlý zisk je v takovém případě v řádu desetikorun. Je tedy nepravděpodobné, že se v kavárně objeví zásahová skupina mužů v černém. Zkrátka: Kde není žalobce, tam není soudce.

Každopádně ale platí, že vás Chip nenabádá k tomu, abyste se takto prolomili do sítě, u které nemáte od jejího provozovatele svolení. Veškerou popsanou činnost **PROVÁDÍTE NA SVÉ VLASTNÍ RIZIKO**.



Informace o síti: Nástroj Kismet poskytne podrobné informace o síti, do které se chcete dostat.

te ikonu s černou obrazovkou – spuštění terminálu. Klikněte na ni, otevře se černé okno. Zadejte příkaz

```
iwconfig
```

a potvrďte klávesou [Enter]. Program vypíše, které síťové karty jsou v počítači dostupné. Distribuce Backtrack obsahuje ovladače pro množství Wi-Fi karet, takže je vysoká pravděpodobnost, že najde i tu vaši. Na našem počítači našel Backtrack dvě karty: eth0 a eth1. U eth0 je poznámka »no wireless extensions«, u eth1 je správně popsaná konfigurace. Víme tedy, že eth1 je správná karta, se kterou budeme laborovat. Pokud je u vašeho počítače Wi-Fi eth0, ve všech příkazech zadávejte eth0.

Dále zadejte příkaz

```
macchanger -s eth1
```

Tím se vypíše MAC adresa vaší síťové karty. Tu si poznamenejte, budete ji potřebovat.

OKOLNÍ SÍTĚ: Nyní je čas podívat se, jaké sítě jsou v okolí. Zvolte »K | Backtrack | Radio Network Analysis | 80211 | Analyser | Kismet«. Během několika sekund se spustí aplikace, která zobrazí dostupné Wi-Fi sítě. Na klávesnici stiskněte [s] a znovu [s]. Tím se sítě seřadí podle názvu. Šipkami si vyberte síť, do které se chcete nabourat, a stiskněte klávesu [Enter]. Zobrazí se podrobnosti o síti, tak jak vidíte na obrázku. Najděte řádek »Encrypt« a podívejte se, zda je v něm uvedeno »WEP«. Jedná se o typ šifrování. WEP lze relativně jednoduše prolomit, na rozdíl od WPA, kde je postup složitější. Pokud je nastaveno šifrování WEP a síť nemá omezený přístup podle MAC adres, máte téměř vyhráno. Ze zobrazeného okna si ještě poznamenejte hodnoty »SSID« (název Wi-Fi sítě), »BSSID« (MAC adresa přístupového bodu) a »Channel« (číslo kanálu). Stisknutím [q] a [Q] (velikost písmen hraje roli) aplikaci Kismet ukončíte.

SBĚR DAT: Aby bylo možné heslo najít, je třeba nejprve začít sbírat data, která sviští vzduchem. Z nich se pak heslo rozkóduje. Spusťte Terminál a zadejte dva následující příkazy

```
cd Desktop
```

```
airodump-ng eth1 -w mojedata
--channel 5 --ivs
```

Za příkazem »channel« se zadává číslo (v našem případě 5), podle čísla kanálu sítě, do které se snažíte dostat. Toto číslo jste si zapsali v minulém kroku. Po potvrzení se spustí ukládání – nemusíte mu věnovat pozornost, do okna se vrátíme až na konci tohoto návodu.

PŘÍSTUP NA AP: Teď je třeba začít „oťukávat“ access point. K tomu poslouží utilita aireplay. Spusťte nové okno terminálu a zajdete následující příkaz:

```
aireplay-ng -1 0 -e testovaci -a
00:4F:74:30:23:0B -h 00:11:22:33:44:55 eth1
```

Tím přesně definujete, co je terčem vašeho útoku. Hodnota –1 říká, jaká je forma útoku, 0 je pak prodleva mezi útoky. Hodnotu »testovaci« zaměňte za SSID sítě, do které se chcete dostat, MAC adresu za parametrem –a zaměňte za MAC adresu AP. Oboje jste si zapsali v okně s příkazem kismet. MAC adresa za parametrem –h je MAC adresa vaší síťové karty. Také ji tedy změňte, je to první hodnota, kterou jste si poznamenali. Příkaz ještě nepotvrzujte a spusťte další okno terminálu.

INJEKCE PAKETŮ: Nyní začneme na access point posílat pakety a zjišťovat, co nám odpoví. Zadejte tedy příkaz

```
aireplay-ng -3 -b 00:4F:74:30:23:0B -h
00:11:22:33:44:55 eth1
```

První MAC adresa je opět vzdálený AP, druhá je opět vaše síťová karta.

Příkaz potvrďte, vraťte se do předchozího okna terminálu a příkaz také potvrďte. Nejlepší bude, když si okna dáte vedle sebe, abyste je mohli sledovat.

V prvním okně se budou posílat žádosti o autentizaci, ve druhém uvidíte, jak se injektují pakety. Zde je důležité sledovat hodnotu ARP, která se postupně zvyšuje. Čím větší je provoz na síti, tím rychleji hodnota roste. Aby bylo možné heslo určit, je třeba, aby ARP mělo aspoň hodnotu 1000. Někdy to trvá pět minut, jindy to může být hodina. Pokud se stane, že v prvním okně příkaz skončí, spusťte jej znovu. Již jej nemusíte celý opisovat, stačí na klávesnici stisknout šipku nahoru a potvrdit. Jakmile dosáhne ARP hodnoty 6000, můžete obě terminálová okna zavřít. Vraťte se do terminálového okna, které jste otevřeli v bodě „sběr dat“.

NALEZENÍ HESLA: Sběr dat ukončete klávesovou zkratkou [Ctrl]+[c]. Mezitím na ploše systému uvidíte nové soubory, které ukládaly informace potřebné k rozluštění hesla. Zadejte příkaz

```
aircrack-ng -s mojedata-01.ivs
```

Soubor mojedata-01.ivs vidíte na ploše systému. Pokud je název souboru odlišný, přizpůsobte jej. Po potvrzení se zobrazí tabulka s informacemi, co je v souboru uloženo. V prvním sloupci je číselný identifikátor sítí. Vyberte tu, do které jste se vlámali. Nyní dojde k hledání hesla – to může několik minut trvat. Nakonec vás přivítá hláška »KEY FOUND«.

VRATISLAV.KLEGA@CHIP.CZ