JIHOČESKÁ UNIVERZITA V ČESKÝCH BUDĚJOVICÍCH

Ekonomická fakulta

Katedra aplikované matematiky a informatiky

Studijní program: **B1103 Aplikovaná matematika**

Studijní obor: **Finanční a pojistná matematika**

Audit zabezpečení bezdrátových sítí

Bakalářská práce

Autor práce:

Jan Vrátný

Vedoucí práce:

Ing. Ladislav Beránek, Csc., MBA

2012

Prohlášení

Prohlašuji, že svoji bakalářskou práci jsem vypracoval samostatně pouze s použitím pramenů a literatury uvedených v seznamu citované literatury. Dále prohlašuji, že v souladu s § 47b zákona č. 111/1998 Sb. v platném znění souhlasím se zveřejněním své bakalářské práce, a to v nezkrácené podobě elektronickou cestou ve veřejně přístupné části databáze STAG provozované Jihočeskou univerzitou v Českých Budějovicích na jejích internetových stránkách.

V Českých Budějovicích dne 25. dubna 2012 Jan Vrátný

Poděkování

Na tomto místě bych rád velmi poděkoval panu Ing. Ladislavu Beránkovi, Csc., MBA za poskytnutí odborných rad a profesionálnímu přístupu při vedení mé bakalářské práce. Kromě toho bych také chtěl poděkovat panu Jiřímu Kašparovi, IT správci počítačové sítě v Bertiných lázních Třeboň, s. r. o. a lázních Aurora, pod jehož dohledem jsem prováděl průzkum a testoval zranitelnost bezdrátové sítě v těchto dvou objektech.

Anotace

Tato bakalářská práce se zabývá problematikou zabezpečení bezdrátových sítí známých také pod názvem Wi-Fi. Úkolem bakalářské práce bude vysvětlit pojem Wi-Fi síť, z jakých komponent je složena, seznámit s použitými bezpečnostními prvky u bezdrátových sítí, provedení průzkumu ve vybraném městě v lokalitách s největší koncentrací lidí zda jsou bezdrátové sítě zabezpečeny a pokud ano, tak jaký typ zabezpečení je použitý. V domácích podmínkách bude proveden názorný útok na Wi-Fi síť zabezpečenou 128 bitovým WEP klíčem. Také názorně popíši novou bezpečnostní chybu, která byla objevena u funkce WPS. Dále se bakalářská práce podrobněji zaměří na jednu místní firmu, která ve větší míře kromě klasické LAN používá právě Wi-Fi síť. Bude provedena analýza zabezpečení této Wi-Fi sítě a z výsledků se vyhodnotí ekonomické dopady pro tuto firmu pokud by se stala terčem útoku a došlo by k úniku citlivých dat.

Abstract

This bachelor thesis deals with security problems of wireless networks, also known as Wi-Fi. The purpose of the thesis is to explain the concept of Wi-Fi network, from what components it is composed, introduce safety devices used in wireless networks, and perform a research in a selected city in a specific location with the largest concentration of people if the wireless networks are secured and if they are what type of security is used. In a domestic environment an illustrative attack will be made on a Wi-Fi network secured by 128-bit WEP key. Also I will describe a new security bug that was discovered at the WPS function. Furthermore, this bachelor thesis will focus in detail on a local business, which in addition to conventional LAN extensively uses Wi-Fi network. An analysis of the security of the Wi-Fi network will be performed and the results will be evaluated to show the economic impact on the company if it were to be subjected to an attack in which sensitive data are leaked.

Klíčová slova

Bezdrátová síť, Wi-Fi, zabezpečení bezdrátových sítí, Wi-Fi protokoly, IEEE 802.11, BackTrack 5 R1, Gerix wifi cracker, Reaver

Keywords

Wireless Network, Wi-Fi, wireless network security, Wi-Fi protocols, IEEE 802.11, BackTrack 5 R1 Gerix wifi cracker, Reaver

Obsah

1 Úvod

Téma této bakalářské práce jsem si vybral z toho důvodu, že se již od útlého dětství zajímám o všechny věci, které mají něco společného s výpočetní technikou a právě počítačové sítě jsou toho nedílnou součástí. Velký podíl na volbě tohoto tématu měl také předmět Počítačové sítě, který jsem úspěšně absolvoval s hodnocením výborně v zimním semestru ve druhém ročníku na Jihočeské univerzitě v Českých Budějovicích, kde vyučujícím byl právě pan Ing. Ladislav Beránek, Csc., MBA, kterého jsem si zároveň vybral i jako vedoucího mé bakalářské práce. A dalším důvodem co mě k výběru tohoto tématu vedlo je jeho aktuálnost, neboť v dnešní době je slovo bezpečnost často skloňovaným pojmem v počítačové terminologii.

Každý z nás jistě zaslechl výraz hacker nebo dnes stále častější pojem kyberzločin. V současné době je vlna kyberzločinu na vzestupu a počítačoví experti varují, že v následujících letech bude ještě hůř. V době rozmachu internetu se hackeři obzvláště zaměřovali na vykrádání dat z osobních počítačů v domácnostech a firmách pomocí virů a trojských koních šířených právě pomocí internetu. Internet byl dříve jedinou cestou jak se dostat do cizího počítače. Dnes, kdy se masově používají bezdrátové sítě v mnoha podnicích a domácnostech, se hackerům otevřela další cesta jak se dostat k citlivým a soukromým datům. Značné finanční škody a ztráty způsobí hackeři velkým nadnárodním firmám. Pokud se dokážou nabourat do jejich počítačové sítě, tak si odnesou daleko více hodnotnějších dat než od běžného počítačového uživatele v domácnosti. Tyto ukradená data, ať jsou to osobní informace o zaměstnancích či různé technologické a marketingové plány dané firmy, jsou na černém trhu velmi výnosným artiklem. Toto je jenom malý výčet všeho toho, čeho jsou hackeři schopní. Jsou známy i případy, kdy se hackeři s úspěchem nabourali do rozvodné sítě a sabotovali rozvod elektrické energie. Určitě si každý z nás dokáže domyslet co by se stalo, kdyby se například dostali k ovládání zbraní pro hromadné ničení.

Proto musíme na prvním místě dbát na zabezpečení počítačové sítě, které začíná už dobře zvoleným uživatelským nastavením na osobním počítači a pokračuje přes vhodnou volbu antivirového programu, firewallu a dalšími různými bezpečnostními prvky, aby do ní měli přístup jen oprávnění lidé. U bezdrátových sítí je zabezpečení

mnohem obtížnější, protože se na rozdíl od metalického vedení počítačové sítě šíří pomocí rádiových vln vysílaných do okolí a tyto rádiové vlny jsou snadno zachytitelné s potřebným vybavením

2 Cíl práce

Cílem této bakalářské práce bude charakterizování Wi-Fi sítí a pojmů, které s nimi souvisejí. Bude vysvětleno na jakém principu bezdrátové sítě fungují a bude proveden obecný průzkum bezdrátových sítí ve městě Třeboni, který poslouží jako statistické zhodnocení použité míry zabezpečení u Wi-Fi sítí. Měření bude prováděno v oblasti s největší koncentrací obyvatelstva. Po provedení obecného průzkumu se pokusím nabourat do mé vlastní bezdrátové sítě a popíši postup a prostředky, které k tomu budou potřeba. Potom se podrobněji zaměřím na jednu z největších firem v daném městě a to jsou Bertiny lázně Třeboň, s. r. o. spolu s lázněmi Aurora, s. r. o. a provedu rozbor zabezpečení jejich bezdrátové sítě. Tuto firmu jsem si vybral proto, že využívá pro svoji vnitřní komunikaci právě i Wi-Fi síť a zároveň mi vyšla vstříc a poskytne mi potřebné informace, které budu k mému výzkumu potřebovat.

3 Bezdrátová síť

Bezdrátová síť je mnohým uživatelům známá také pod názvem Wi-Fi z anglického Wireless Fidelity (bezdrátová věrnost). Toto označení bezdrátové sítě vzniklo

analogicky k termínu Hi-Fi neboli High Fidelity (vysoká věrnost) což je označení pro reprodukci zvukového signálu. Wi-Fi je registrovaná ochranná známka neziskové organizace Wi-Fi Aliance. Do této organizace spadá asociace stovek výrobců a vývojářů Wi-Fi technologií. Úkolem Wi-Fi Aliance je vydávat certifikace pro zařízení různých výrobců Wi-Fi komponent, aby mezi sebou mohla tato zařízení vzájemně spolupracovat. Takto certifikovaná zařízení nesou označení "Wi-Fi certified". Technologie Wi-Fi využívá bezlicenčního frekvenčního pásma tzv. pásmo ISM (Industrial Scientific and Medical), které je vyhrazené pro vědecké, lékařské a průmyslové účely a potřeby. To znamená, že provozovatel nemusí mít patřičnou licenci pro vysílání v této frekvenci. Pro Wi-Fi se používá pásmo o frekvenci 2,4 GHz a 5 GHz. V posledních letech zažívají bezdrátové sítě neuvěřitelný vzestup nejenom ze strany domácích uživatelů, ale především i firem. Člověk už totiž není závislý na kabelech a může se svobodně s počítačem pohybovat z jedné místnosti do druhé a nemusí řešit nutnost kabeláže, aby se mohl připojit ke své počítačové síti. Bezdrátová síť představuje rozšíření klasické pevné sítě LAN.

Obrázek 1: Zařízení s podporou Wi-Fi technologie

Zdroj: www.google.com; sekce obrázky

Obrázek 2: Certifikační logo společnosti Wi-Fi Aliance

Zdroj: www.google.com; sekce obrázky

3.1 Zařízení pro provoz Wi-Fi sítě

Pro úspěšné vytvoření bezdrátové sítě je potřeba několik komponent. Stěžejní prvek pro fungování Wi-Fi sítě je přístupový bod (AP), který dokáže vysílat a přijímat data. Jde o samostatné zařízení s vlastním napájením, které ve Wi-Fi síti zastává funkci ethernetového switche. Všechny dnes prodávané přístupové body mají minimálně jeden a více konektorů RJ45 pro propojení se stávající LAN sítí. Dražší zařízení obsahují i konektory USB díky nimž se dají například připojit do sítě tiskárny a přenosné disky. Pro bezproblémový příjem je nutná anténa. Jsou tři typy antén a to směrová, všesměrová a sektorová anténa. Směrová anténa slouží k přenášení signálu do jednoho bodu na delší vzdálenosti až v řádech několika kilometrů. Všesměrová anténa šíří signál do všech stran pod úhlem 360 stupňů. Slouží k pokrytí menších prostorů souvislým signálem a je nejčastěji používanou anténou. Sektorová anténa se používá tam, kde je potřeba pokrýt signálem větší souvislý prostor, ale přitom je zbytečné použít všesměrovou anténu. Šíří signál do určitého úhlu (například 180, 90 nebo jen 60 stupňů). Jedním z nejdůležitějších parametrů u antén je jejich ziskovost. Zisk antény se udává v dBi (decibel na isotrop). Laicky řečeno čím vyšší máme ziskovost u antény, tím vzdálenější signál je anténa schopná zachytit (Tabulka 1). V praxi musíme brát ještě v potaz jaký je použitý čip ve Wi-Fi kartě, protože právě čip nám zpracovává zachycený

signál z antény. Čím je čip citlivější, tím lépe si dokáže poradit se signálem z delší vzdálenosti. Další nezbytnou komponentou je Wi-Fi karta (tzv. klientský adaptér), která funguje na stejném principu jako síťová karta jen s tím rozdílem, že se k ní nemusí připojovat síťový kabel a vše funguje bezdrátově.

Tabulka 1: Nutný zisk antény klienta při přímé viditelnosti

Vzdálenost	Zisk antény
0,8 km - 3 km	7-9 dBi
3 km - 8 km	9-15 dBi
8 km - 11 km	15-20 dBi

3.2 Druhy Wi-Fi zařízení

Obrázek 3: Všesměrová anténa pro příjem Wi-Fi signálu

Obrázek 4: Směrová anténa

Obrázek 5: Přístupový bod se zabudovanou anténou

Obrázek 6: Stožár se sektorovými a směrovými anténami

Klientské adaptéry jsou nejčastěji vyráběny v provedení PCI, PCI Express, USB, miniPCI, CardBus (PCMCIA) a ExpressCard. Tyto adaptéry slouží k připojení klientských PC k přístupovému bodu. Nejčastějším zařízením pro vytvoření bezdrátové sítě je Wi-Fi router (Obrázek 5), který je kombinací klasického routeru a přístupového bodu.

Obrázek 7: Wi-Fi adaptér s rozhraním CardBus

Zdroj: www.google.com; sekce obrázky

Obrázek 8: Wi-Fi adaptér s rozhraním USB

Zdroj: www.google.com; sekce obrázky

Obrázek 9: Wi-Fi adaptér s rozhraním PCI Express

Zdroj: www.google.com; sekce obrázky

3.3 Použité kanály a frekvence

Frekvenční spektrum u pásma 2,4 GHz je rozděleno na 39 kanálů od 2312 MHz do 2732 MHz. [5] Různí regulátoři povolují jiný počet kanálů. V Americe je povoleno 11 kanálů od 2412 MHz do 2462 MHz. V Evropě je navíc povolen 12. a 13. kanál tj. 2467 MHz a 2472 MHz. V Japonsku dokonce i 14. kanál.

Tabulka 2: Povolené kanály ve vybraných státech a kontinentech [2]

Země	Kanály
USA a Kanada	1 - 11 (2,412 GHz - 2,462 GHz)
Evropa kromě Francie a Španělska	1 - 13 (2,412 GHz - 2,472 GHz)
Francie	10 - 13 (2,457 GHz - 2,472 GHz)
Španělsko	10 - 11 (2,457 GHz - 2,462 GHz)
Japonsko	14 (2,484 GHz)

Tabulka 3: Frekvenční spektrum v pásmu 2,4 GHz [3]

Kanál	Frekvence (GHz)
1	2,412
2	2,417
3	2,422
4	2,427
5	2,432
6	2,437
7	2,442
8	2,447
9	2,452
10	2,457
11	2,462
12	2,467
13	2,472
14	2,484

3.4 Výhody a nevýhody Wi-Fi

Výhoda Wi-Fi spočívá v tom, že jde o bezdrátové připojení a tím pádem není potřeba optických a metalických kabelů. Přednost bezdrátové síti se dává i z toho důvodu, že je ekonomičtější a levnější vybudovat Wi-Fi síť než klasickou síť vedenou po kabelech. Tímto si Wi-Fi sítě získaly velkou oblibu ve firmách, na letištích, v hotelech, vysokých školách aj. Odpovídá tomu i počet zařízení vybavených Wi-Fi rozhraním. Notebooky, tablety, mobilní telefony a mnohé další zařízení jsou dnes již standardně vybaveny Wi-Fi modulem. Wi-Fi je zároveň globálním standardem, takže zařízení koupené třeba v Anglii bude bez problémů fungovat v České republice. K hlavním nevýhodám patří především to, že Wi-Fi síť využívá bezlicenční pásmo ve kterém pracují i jiné přístroje a tím dochází k rušení signálu. Obecně platí pravidlo, že mezi Wi-Fi anténami by měla být přímá viditelnost. To ve většině případů není ani fyzicky možné. Pokud je signál šířen na delší vzdálenosti, tak zde hrají roli především povětrnostní vlivy a různé překážky při šíření signálu jakou jsou třeba stromy a různé zástavby. Také hraje roli počet připojených klientů. Klienti se dělí o dostupnou šířku pásma tj. s jejich zvyšujícím se počtem klesá přenosová rychlost. Další nejvíce diskutovanou nevýhodou je zabezpečení bezdrátových sítí, které je u některých použitých zabezpečení s potřebným vybavením celkem snadno prolomitelné.

3.5 Standard IEEE 802.11

Standardem pro bezdrátové sítě Wi-Fi se stalo označení IEEE 802.11. [4] Označení IEEE vyplývá z anglického spojení Institute of Electrical and Electronics Engineers (Institut pro elektrotechnické a elektronické inženýrství.). Tento institut je mezinárodní neziskovou organizací usilující o vzestup technologií, které souvisejí s elektrotechnikou. IEEE působí od roku 1992 také u nás v České republice. Termín 802.11 je původním standardem bez dalších doplňků. Postupem času začal tento standard zahrnovat několik doplňků tzv. modulací u rádiového signálu. Tyto doplňky se začaly značit malými písmeny a připisovaly se na konec standardu. Jak je patrné, tak použité standardy se

mezi sebou liší především v přenosové rychlosti a použitém frekvenčním pásmu. Dnes se můžeme setkat se zařízeními, které kombinují tyto použité modulace dohromady. Převážně se tak vyskytují Wi-Fi zařízení u kterých převažuje označení 802.11b/g/n. Ale není problém narazit na zařízení s označením 802.11a/b/g, 802.11a/n nebo čistě jen 802.11g. Výčet těch nejdůležitějších doplňků ke standardu 802.11 je uveden níže v tabulce.

Tabulka 4: Přehled nejpoužívanějších standardů [4]

Standard	Rok vydání	Maximální přenosová rychlost (Mbit/s)	Frekvenční pásmo (GHz)
IEEE 802.11	1997	2	2,4
IEEE 802.11a	1999	54	5
IEEE 802.11b	1999	11	2,4
IEEE 802.11g	2003	54	2,4
IEEE 802.11n	2009	600	2,4 nebo 5
IEEE 802.11y	2008	54	3,7
IEEE 802.11ac	2012	1000	2,4 a zároveň 5

3.5.1 Doplňky k standardu 802.11

IEEE 802.11a

Na rozdíl od standardu 802.11 pracuje ve frekvenčním pásmu 5 GHz a nabízí vyšší přenosovou rychlost a to 54 Mbit/s. [4] Výhodou je nejenom vyšší přenosová rychlost,

ale také zvolené frekvenční pásmo, které je méně vytížené než frekvenční pásmo 2,4 GHz a dovoluje šířit signál na delší vzdálenosti. Standard 802.11a je hojně využíván převážně internetovými poskytovali, kteří tak mohou například šířit internet z měst na vesnice.

IEEE 802.11b

Tento standard poskytuje vyšší přenosovou rychlost (11Mbit/s) ve frekvenčním pásmu 2,4 GHz a umožňuje dynamicky měnit přenosovou rychlost v závislosti na aktuálním rušení z okolí na 11Mbit/s, 5,5Mbit/s, 2Mbit/s a 1Mbit/s. [6] Rušení z okolí vzniká pokud se v blízkosti vyskytuje více zařízení, která pracují na stejné frekvenci. Tím může být třeba několik desítek Wi-Fi sítí pracujících ve stejném frekvenčním pásmu a kanálu.

IEEE 802.11g

Podobný standardu 802.11a jen s tím rozdílem, že namísto v pásmu 5 GHZ pracuje pouze v pásmu 2,4 GHz. Přenosová rychlost je 54Mbit/s a zároveň také obsahuje dynamicky měnitelnou rychlost v závislosti na rušení z okolí. Rychlosti jsou pak následující (jednotky jsou uvedeny v Mbit/s): 54, 48, 36, 24, 18, 12, 11, 9, 6, 5,5, 2, 1. [8]

IEEE 802.11n

Vylepšený standard typu IEEE 802.11g. Liší se v maximální možné přenosové rychlosti a větším dosahem signálu a odolností proti rušení. [4] U tohoto standardu je novinkou použití více směrových antén najednou u jednoho zařízení.

IEEE 802.11y

Stejné parametry jako u standardu IEEE 802.11g jen s tím rozdílem, že tento standard pracuje ve frekvenčním pásmu 3,7 GHz což je veřejné frekvenční pásmo v USA. U nás se tedy s tímto standardem nesetkáme. [4]

IEEE 802.11ac

Nástupce standardu IEEE 802.11n s teoretickou maximální rychlostí až 1000 Mbit/s.[7] První zařízení by se měla začít objevovat na trhu během roku 2012 a od roku 2015 se předpokládá masové nasazení do mobilních zařízení, televizorů apod.

4 Bezpečnost bezdrátových sítí

Nezabezpečená bezdrátová sít představuje pro majitele této sítě velké bezpečnostní riziko, jelikož signál bezdrátových sítí ve většině případů přesahuje prostor, který jsme schopni fyzicky ohlídat. Tím může být byt v panelovém domě nebo firma v rušné zástavbě, kde může signál zachytit někdo z vedlejšího bytu, budovy nebo z ulice. Do této sítě se může připojit kdokoliv, kdo disponuje zařízením s podporou Wi-Fi. Pomineme-li fakt, že Wi-Fi karta je dnes již standardem v každém notebooku a případně není problém se Wi-Fi kartou dovybavit. Ceny těchto zařízení se na trhu pohybují od 200 korun a výše. Ve většině případů jsou nezabezpečené bezdrátové sítě hojně využívány cizími návštěvníky k připojení k internetu. Pokud je v takové síti nevhodně nastaveno sdílení dat, tak dotyčný člověk může získat snadno přístup k našim soukromým dokumentům jako jsou multimediální soubory nebo ve firemní síti získat přístup k interním věcem a citlivým informacím jako jsou třeba údaje o zaměstnancích. Nebezpečí hrozí také i člověku, který se například připojí k nezabezpečené Wi-Fi síti někde ve městě nebo na dovolené a začne brouzdat po internetu. Síť může být odposlouchávána neznámým útočníkem, který může zneužít případné přihlašovací údaje k e-mailu a dalším internetovým službám, které dokáže s příslušnými programy bez problémů zachytit. Jako dalším bezpečnostním rizikem je využívání nezabezpečených bezdrátových sítí k páchání trestné činnosti. Tím může být nahrávání nelegálně pořízených kopií filmů, her, programů a hudby na internet. Touto činností vznikají mnohamilionové škody firmám a společnostem, které vlastní autorská práva k těmto kopiím. Pokud se o tuto činnost začne zabývat orgán činný v trestním řízení, tak není problém zjistit IP adresu přidělenou vaším ISP (Internet service provider) a na základě tohoto údaje se od internetového poskytovatele připojení zjistí informace o uživateli jako je jméno a adresa bydliště. Tím pádem policejní vyšetřovatelé logicky zabouchají na vaše dveře a nebude je zajímat, že tuto nelegální činnost prováděl zřejmě někdo úplně cizí, kdo se připojil přes vaši nezabezpečenou bezdrátovou síť, protože za aktivity na internetu je zodpovědný vlastník internetového připojení. Proto tou nejlepší ochranou bezdrátové sítě je využít šifrování veškeré datové komunikace, což by znemožnilo případné odposlouchávání takto zabezpečené sítě a dávalo by nám jen samá

nesmyslná data. Není to tak složité vytvořit zabezpečenou bezdrátovou síť, stačí jen vhodně nakonfigurovat bezdrátový router podle manuálu, který je ke každému zařízení dodáván, a máme po starostech a nikdo cizí se nám do sítě nedostane. To bohužel v dnešní době už tolik neplatí.

Při úspěšném proniknutí do firemní počítačové sítě za využití bezdrátové sítě mají útočníci převážně přístup k [9]:

- **Serverům** => Po nabourání se do serveru získá útočník do rukou mocný nástroj. Buď může server vyřadit z provozu a tím dané firmě znemožnit síťovou komunikaci a nebo může využít výpočetní sílu serveru ve svůj prospěch k nekalým praktikám jako je například rozesílání spamu.

- **Pevným diskům s informacemi** => Tím dostane útočník přístup k soukromým informacím jako můžou být osobní údaje zaměstnanců, know-how a jiné informace, které si každá firma pečlivě tají. Poskytnutí těchto údajů většinou za úplatu třetí straně může firmě způsobit nevyčíslitelnou škodu, ztrátu prestiže či nedůvěru zaměstnanců k firmě.

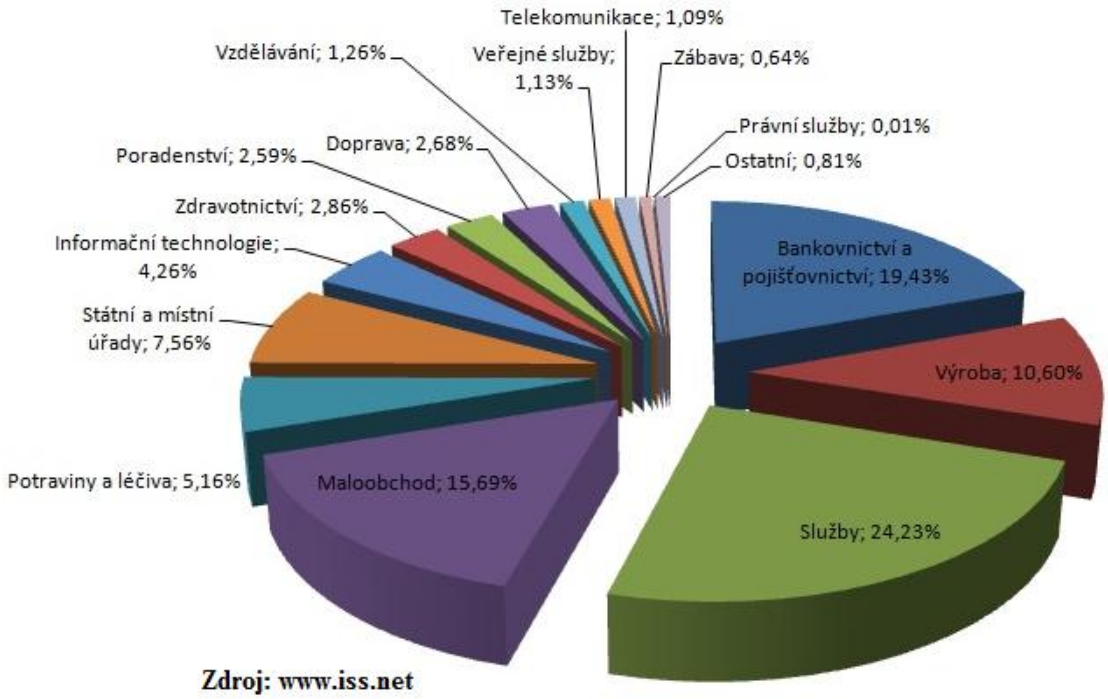
- **Připojení k internetu** => Firemní připojení k internetu poskytne útočníkovi patřičnou anonymitu a může být využito jako prostředek k vedení dalšího útoku na jiný důležitější cíl a nebo může přes toto připojení nahrávat na internet nelegální obsah.

- **Odposlouchávání komunikace** => Za použití patřičných nástrojů je schopen útočník odposlouchávat síťovou komunikaci probíhající ve firmě a může se dostat k dalším citlivým údajům jako jsou hesla k e-mailu, internetbankingu atd.

a zneužít je ve svůj prospěch a to i v případě pokud používáme bezpečnostní protokol SSL (Secure Sockets Layer).

Všechny tyto hackerské aktivity můžou pro danou firmu znamenat hrozbu právního a kriminálního postihu! Pro představu v grafu z roku 2003 (Graf 1) uvádím na jaký sektor se nejvíce útočníci soustřeďují. Tyto čísla dnes berme pouze orientačně, jelikož každoročně hackerské aktivity narůstají. V počítačové terminologii se stále častěji vyskytuje pojem hacktivismus. [10] Jde o spojení hackingu a aktivismu, politiky a technologie. Hacktivismus je popisován jako hacking k politickým účelům. Nejčastěji používanou metodou hacktivistů je blokování a narušování obsahu webových stránek.

Graf 1: Cíle útoků podle oboru podnikání



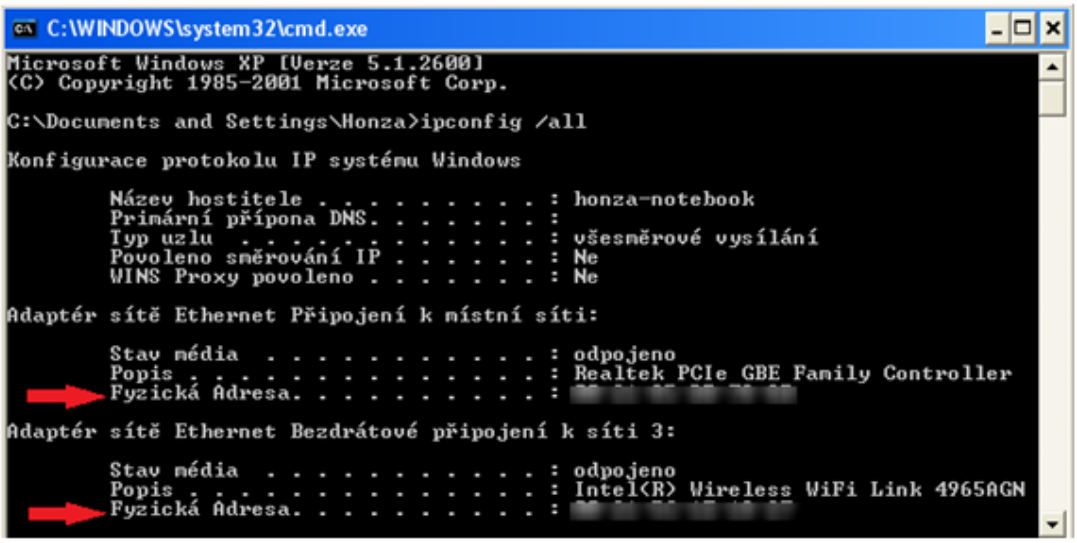
Zdroj: www.iss.net

4.1 Druhy použitých zabezpečení u Wi-Fi sítí

4.1.1 Filtrace MAC adres (Media Access Control)

MAC adresou rozumíme jedinečný identifikátor síťového zařízení v hexadecimálním tvaru. Také se jí říká fyzická adresa, protože je síťovému zařízení přidělena bezprostředně při výrobě. [11] MAC adresa je nejčastěji uváděna jako šestice dvojciferných hexadecimálních čísel oddělených dvojtečkami (např. 11:22:33:44:55:66). V operačním systému Windows XP zjistíme MAC adresu přes tento postup: Start→Spustit→napsat příkaz "cmd" a do otevřeného dialogového okna napsat "ipconfig /all" (Obrázek 10). V novějších verzích operačního systému Windows (Windows Vista a Windows 7) je postup obdobný jen s tím rozdílem, že příkaz "cmd" napíšeme do políčka pro vyhledávání souborů v počítači, které je úplně dole, když si rozklikneme nabídku Start. Tato adresa je pro každé síťové zařízení celosvětově jedinečná a tudíž by neměly existovat dvě a více síťových zařízení se stejnou MAC adresou. Paradoxem je, že MAC adresu lze celkem snadno změnit, jelikož řada bezdrátových karet mívá ovladač, který tuto změnu umožňuje. Filtrace MAC adres je jednou z doplňkových možností k dalším použitým zabezpečením u bezdrátových sítí, která budou popsána v dalších kapitolách. Filtrování MAC adres se nastavuje v konfiguračním rozhraní přístupového bodu. Většina běžných počítačových uživatelů nemá ani tušení, že lze takovou MAC adresu změnit. Proto pokud si takové zabezpečení nastaví ve své bezdrátové síti, tak podstupují značné bezpečnostní riziko. Pro zkušeného útočníka není obtížné filtraci MAC adres obejít. Stačí když bude odposlouchávat datový provoz na Wi-Fi síti a bez problémů si zjistí, kterým MAC adresám je dovoleno komunikovat s přístupovým bodem. Pak už jen stačí změnit hodnotu MAC adresy na jednu z připojených k přístupovému bodu a rázem máme povolen přístup do sítě.

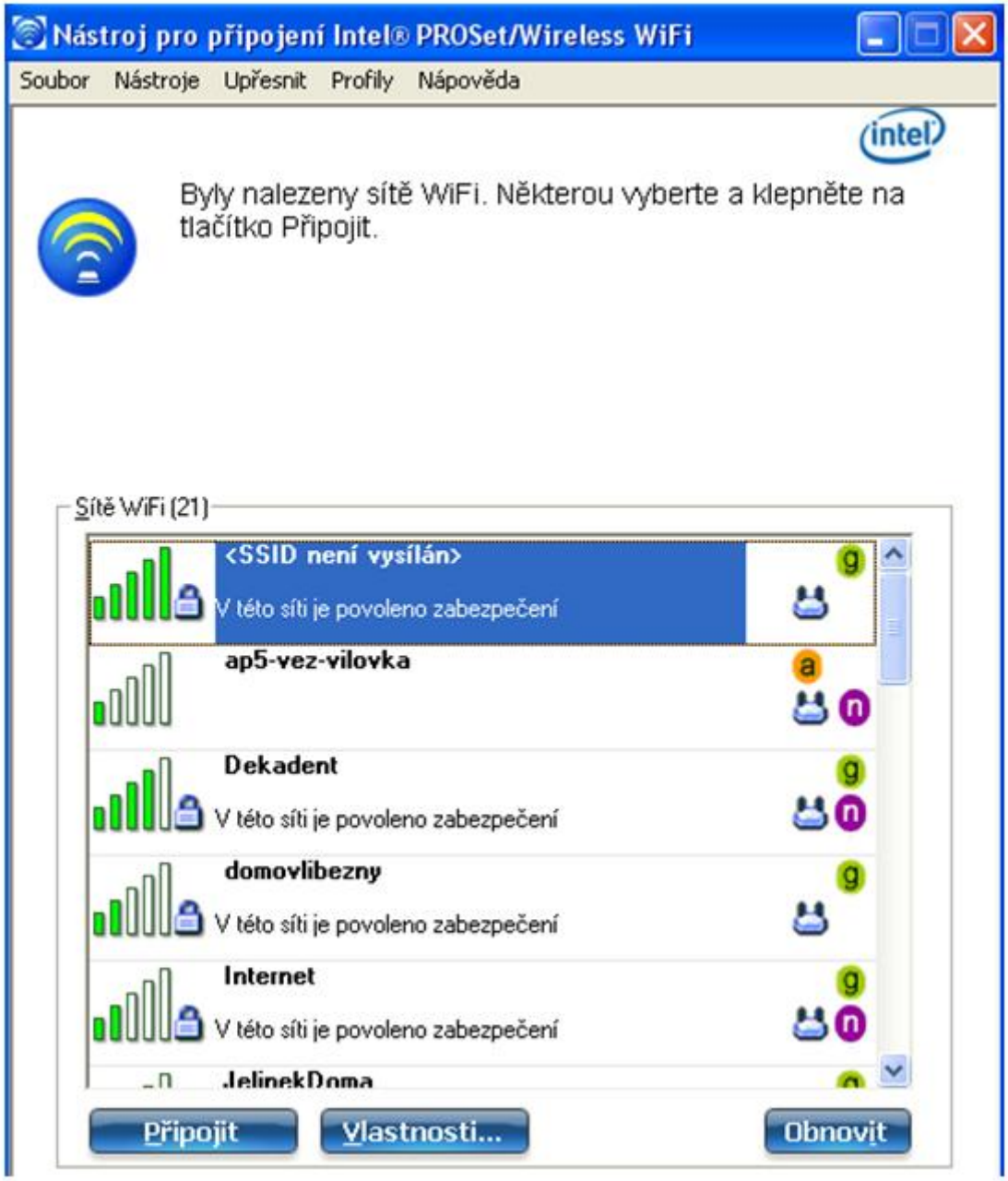
Obrázek 10: Dialogové okno s vypsanými MAC adresami



4.1.2 Skrytí SSID (Service Set IDentifier)

Pod SSID se skrývá název bezdrátové sítě, který je vysílán do okolí. [1] Slouží k tomu, aby případní klienti věděli, že je v dosahu nějaká bezdrátová síť a dále k tomu, že zároveň brání bezdrátové stanici, aby se omylem připojila k jinému přístupovému bodu. Přístupový bod vysílá každých několik sekund tento jedinečný identifikátor ve zprávě, které se říká beacon a ve které jsou uvedeny další informace o AP jako podporované rychlosti a síla signálu. [12] SSID je složeno z řetězce ASCII znaků o maximální délce 32 znaků. Pokročilejší přístupové body dokážou vysílat i více SSID najednou, kde každému SSID můžeme přiřadit individuální síťové nastavení a zabezpečení. Skrytím SSID zabráníme tomu, aby bezdrátovou síť nemohl vyhledat někdo cizí, který do ní nemá mít přístup. Útočník může poměrně snadno skryté SSID zjistit. Pošle falešný požadavek na odpojení aktivní stanice připojené ke skrytému SSID, která se ihned pokusí připojit znovu. Při opětovném připojování je vysílán název bezdrátové sítě a tímto způsobem tedy může útočník odposlechnout název skrytého SSID a nic mu nebrání se připojit do Wi-Fi sítě s takto skrytým SSID.

Obrázek 11: Případ, kdy Wi-Fi síť nevysílá svoje SSID



4.1.3 WEP (Wired Equivalent Privacy)

Účelem zabezpečení WEP je poskytnutí takové bezpečnosti v bezdrátové síti, které odpovídá bezpečnosti v LAN sítích. Odtud také anglické spojení Wired Equivalent Privacy, které v překladu do češtiny znamená "soukromí ekvivalentní drátovým sítím". Bohužel toto zabezpečení svá očekávání nesplnilo. V dnešní době je WEP považováno za zastaralé zabezpečení. Avšak v době uvedení standardu IEEE 802.11 (rok 1997) byl WEP základním zabezpečením bezdrátových sítí. V srpnu v roce 2011 ale přišel zlom, WEP bylo hackery prolomeno. [2] Odposlechem datové komunikace v bezdrátové síti, lze během několika minut zjistit takzvaný WEP klíč díky kterému získáme přístup do bezdrátové sítě. Tomuto zabezpečení se budu věnovat podrobněji v další části mé bakalářské práce.

4.1.4 WPA (Wi-Fi Protected Access)

Zabezpečení WPA bylo uvedeno necelý rok poté co se WEP zabezpečení stalo nevyhovující z důsledku jeho prolomení. [13] WPA je narychlo vylepšené zabezpečení WEP, ke kterému byl přidán šifrovací protokol TKIP (Temporal Key Integrity Protocol), který nabízí silné šifrování (dynamicky se měnící) a řeší hlavní nedostatky díky kterým se podařilo hackerům prolomit WEP. [1] Autentizace klienta s přístupovým bodem probíhá pomocí předsdíleného hesla PSK (Pre-shared key) nebo pomocí autentizačního serveru (většinou Radius). PSK bylo navrženo pro sítě v domácnostech a malých kancelářích, které si nemohou dovolit finančně nákladné autentizační servery. WPA klíč se skládá z 8 až 63 tisknutelných znaků z ASCII tabulky. Toto zabezpečení bylo navrženo jako dočasné než se pořádně vyřeší chyby v zabezpečení WEP. I toto zabezpečení (také značené jako WPA/PSK) je náchylné ke zjištění předsdíleného hesla za použití slovníkového nebo brute force útoku za předpokladu použití triviálního hesla. Takže čím složitější a delší bude heslo, tím delší dobu bude trvat útočníkovi proniknutí do bezdrátové sítě.

4.1.5 WPA2

Jde o vylepšený šifrovací a autentizační algoritmus WPA také jinak známý pod názvem 802.11i. [13] Do WPA2 bylo zabudováno šifrování AES (Advanced Encryption Standard) spolu s CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol), které nahradilo nedostačující šifrování RC4 použité u WEP a WPA. Tento standard je považován v dnešní době za nejbezpečnější, protože jeho prolomení vyžaduje obrovský výpočetní výkon se kterým by to i tak trvalo minimálně desítky let pokud je použito dostatečně silné heslo.

4.1.6 WPS (Wi-Fi Protected Setup)

Technologie která umožňuje snadnou konfiguraci zabezpečení WPA/WPA2 pro běžné uživatele, kteří jsou odrazeni složitým procesem nastavování u těchto zabezpečení. Touto technologií je dnes vybavena většina přístupových bodů. [14] Po zadání PIN kódu (osmimístný číselný kód, který je předprogramovaný v přístupovém bodu a bývá zároveň natištěn na štítku, který je nalepen na samotném AP) dojde k automatické konfiguraci zařízení bez manuálního nastavování. O této technologii se zmiňuji proto, že dne 27. 12. 2011 byla nalezena bezpečnostní chyba díky které můžou útočníci získat za zlomek času i heslo k zabezpečení WPA/WPA2. Jedinou podmínkou je, aby na přístupovém bodu byla technologie WPS zapnuta. U některých zařízení je tato technologie zapnutá neustále a nejde nijak vypnout a u některých dalších zařízení jde naštěstí manuálně vypnout/zapnout. Bezpečnostní chyba je v tom, že přístupový bod sděluje o PIN kódu příliš mnoho informací. Tím pomáhá v jeho odhalování. Když je zadán špatný kód, tak přístupový bod odešle nazpátek klientovi zprávu, ze které lze vyčíst jestli je správně uvedená první polovina kódu a zároveň poslední číslice PIN kódu je také známá. Udává kontrolní součet zbytku hesla. Tato bezpečnostní chyba redukuje počet pokusů při útoku hrubou silou (brute force). Bez této chyby by se podle kombinatorického pravidla muselo vyzkoušet 10^8 kombinací. Nyní jich tak stačí $10^4 + 10^3$ což je pouhých 11 000 pokusů. Navíc většina přístupových bodů nemá implementováno žádné pravidlo pro omezení počtu pokusů v čase, takže je možné hádat velmi rychle za sebou. Ověřování každého kódu trvá zhruba jednu sekundu. Byl napsán

skript, který toto hádání provádí automaticky a dokáže si případně poradit i s tím, že přístupový bod pozná, že je veden brute force útok na PIN kód. Tím pádem jsou ohroženy všechny přístupové body se zapnutou technologií WPS. Jedinou dostupnou ochranou před tímto útokem je prozatím vypnout funkci WPS.

Tabulka 4: Doporučení pro nasazení bezpečnostního řešení v sítích [1]

	autentizace	šifrování	použitelnost pro podnikové sítě	použitelnost pro domácí a malé sítě
WEP	nulová	WEP	nic moc	dobrá
WPA (PSK)	PSK	TKIP	nic moc	nejlepší
WPA2 (PSK)	PSK	AES-CCMP	nic moc	nejlepší
WPA (plná)	802.1x	TKIP	lepší	dobrá
WPA2 (plná)	802.1x	AES-CCMP	nejlepší	dobrá

Tabulka 5: Porovnání odolnosti WEP, WPA a WPA2 [1]

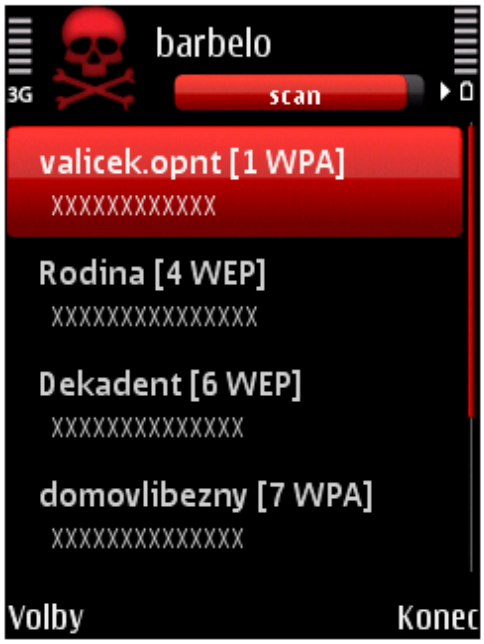
	WEP	WPA	WPA2
útok:	**odolnost:**		
na integritu, důvěrnost dat	dobrá	lepší	nejlepší
falešná autentizace	nic moc	nejlepší	nejlepší
na slabý klíč	nic moc	nejlepší	nejlepší
falšované pakety	minimální	nejlepší	nejlepší
falešný přístupový bod	minimální	lepší	lepší

5 Průzkum bezdrátových sítí

Průzkum Wi-Fi sítí za účelem zjištění jejich míry zabezpečení probíhal v místě mého trvalého bydliště a to ve městě Třeboni. Pro dosažení přesnějších výsledků bylo provedeno měření ve dvou dnech a sice v dopoledních hodinách (9:00 hod. - 11:00 hod.) a v pozdních odpoledních hodinách (17:00 hod. - 19:00 hod.) v nejvíce využívaném frekvenčním pásmu 2,4 GHz. Záměrně jsem vybral dva na sobě nezávislé dny a sice středu a sobotu tj. střed pracovního týdne a víkend, abych mezi sebou porovnal jestli se během dne mění množství aktivních bezdrátových sítí s ohledem na to jestli se jedná právě o pracovní den nebo o den volna. Osobně pokud nejsem doma, tak svou bezdrátovou síť vypínám z toho důvodu, že jsem si vědom různých bezpečnostních rizik. Trasa měření je vyznačena červenou čárou na přiložené mapce města Třeboně (Obrázek 12). Tato trasa byla optimálně navolena, tak aby procházela oblastí s největším počtem obyvatel. V mém případě tedy trasa začínala od mého bydliště a procházela centrem města a vedla přes panelová sídliště a vilové čtvrti. Měření bylo prováděno pěšky za pomocí mobilního telefonu Nokia N95 8GB, který disponuje zabudovaným Wi-Fi adaptérem a běží na operačním systému Symbian OS 9.2. Do telefonu jsem musel doinstalovat bezplatnou aplikaci s názvem Barbelo, jelikož telefon v základu nepodporuje logování naskenovaných Wi-Fi sítí do textového souboru. Program Barbelo je dostupný z webových stránek http://www.darkircop.org/barbelo, kde je k dispozici obrázkový návod a další funkce, kterými program disponuje. Velké plus má u mě tento program, že dokáže naskenovat i skryté bezdrátové sítě, které nevysílají své SSID. Za pomocí této aplikace byl již mobilní telefon schopen naskenované sítě průběžně ukládat do souboru xml, který pak lze bez problémů otevřít na stolním počítači v tabulkovém procesoru Excel a je možné snadno s pořízenými daty dále pracovat. Na levém obrázku (Obrázek 13) vidíme úvodní obrazovku, kde se nám ihned po spuštění programu zobrazí dostupné bezdrátové sítě v okolí. Před hranatou závorkou se nám zobrazuje název naskenované sítě. V hranaté závorce nám číslo udává kanál na kterém je daná Wi-Fi síť vysílána a značení WPA nebo WEP nám udává použité zabezpečení. Řádek s písmeny "X" nám udává sílu signálu. Čím více daných písmen, tím máme lepší signál. Na pravém obrázku (Obrázek 14) se nám ukazuje obrazovka, kterou vyvoláme pokud u červeně vyznačené Wi-Fi sítě

stiskneme tlačítko pro potvrzení. Zde se nám zobrazují údaje o názvu, síle signálu, použitém šifrování a číslo kanálu. Průměrně bylo naskenováno 726 bezdrátových sítí. Z toho největší podíl měly bezdrátové sítě se zabezpečením WPA1/2 a o něco menší podíl tvořily bezdrátové sítě využívající zabezpečení WEP. Nutno podotknout, že i v dnešní době se lze stále setkat s větším počtem nezabezpečených WI-FI sítí. Z průměrně naskenovaných 726 bezdrátových sítí bylo zhruba necelých 20% nezabezpečeno.

Obrázek 13

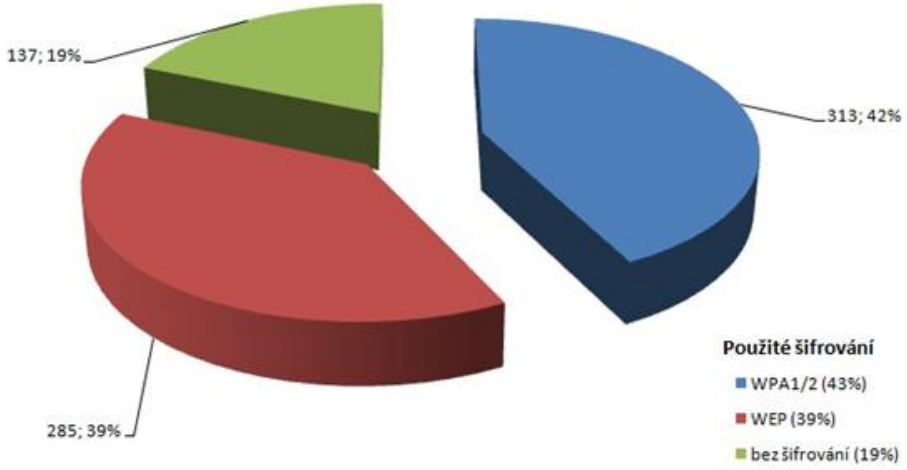


Obrázek 14

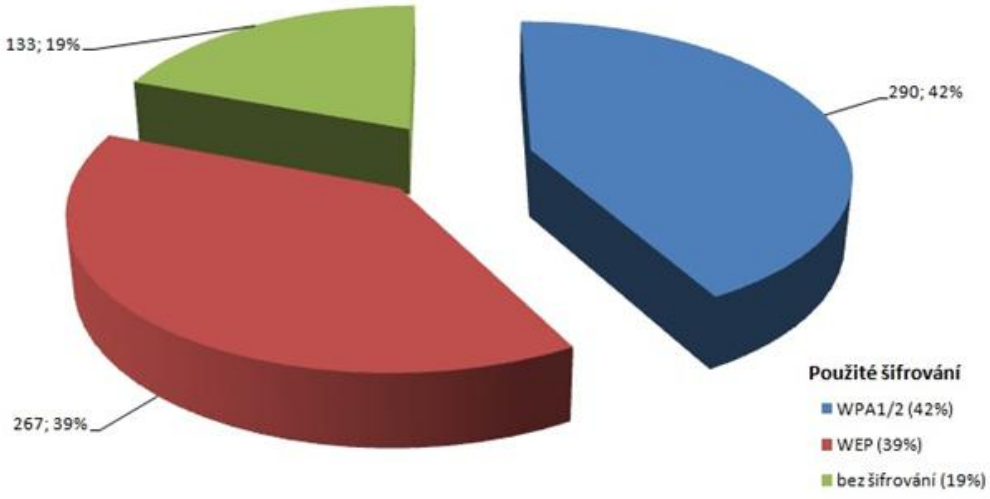
Obrázek 15: Mapa Třeboně s vyznačenou trasou průzkumu

Zdroj: www.mapy.cz

Graf 2: Naskenovaný počet Wi-Fi sítí v pracovním dnu v rozmezí 9:00 hod. - 11:00 hod.

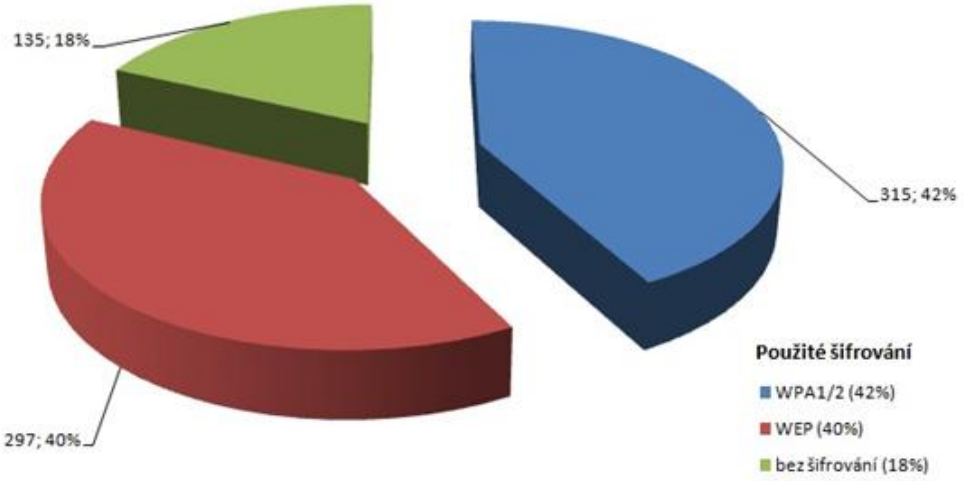


Graf 3: Naskenovaný počet Wi-Fi sítí v pracovním dnu v rozmezí 17:00 hod. - 19:00 hod.

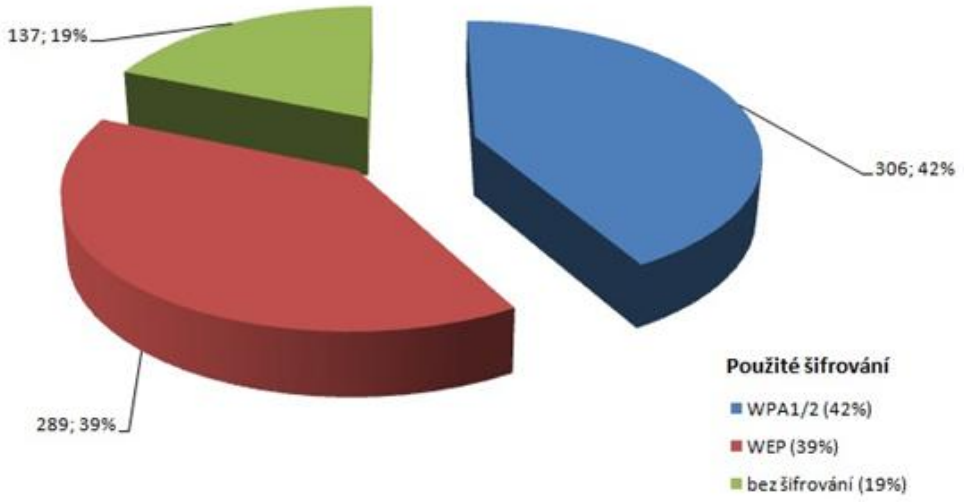


Jak je z grafů patrné, tak u obou dvou převažuje zabezpečení využívající protokol WPA. Druhý největší díl si v grafech ukously bezdrátové sítě zabezpečené protokolem WEP, který se skoro vyrovnává sítím se zabezpečením WPA. Nezanedbatelnou část tvoří i bezdrátové sítě, které nejsou chráněny žádným šifrováním. U nich může být použita maximálně filtrace MAC adres, která zkušeného útočníka ale nijak neodradí.

Graf 4: Naskenovaný počet Wi-Fi sítí o víkendu v rozmezí 9:00 hod. - 11:00 hod.



Graf 5: Naskenovaný počet Wi-Fi sítí o víkendu v rozmezí 17:00 hod. - 19:00 hod.



Na těchto grafech můžeme sledovat podobný trend jako je tomu u předešlých grafů z pracovního dne. Prvenství si drží bezdrátové sítě šifrované protokolem WPA. Hned za nimi se o pár procent níže drží sítě se zabezpečením WEP. A se skoro 20% jsou zastoupeny bezdrátové sítě, které nevyužívají žádné šifrování.

5.1 Zajímavé poznatky při průzkumu Wi-Fi sítí

Většina z nezabezpečených bezdrátových sítí se řadila mezi free Wi-Fi hotspoty jenž slouží k přístupu k bezplatnému bezdrátovému internetu a které zřídilo buď samotné město Třeboň nebo internetoví poskytovatelé, kteří zde nabízejí internet pomocí technologie Wi-Fi. Tyto bezdrátové sítě může odposlouchávat prakticky kdokoliv, kdo má příslušné znalosti. Pokud se musí člověk k takovýmto sítím připojit, tak se nedoporučuje připojovat k webovým stránkám, které vyžadují naše důvěrné přihlašovací údaje (e-mail, internetové bankovnictví, Paypal, Facebook a mnohé další). U bezpečnostního protokolu WEP mě překvapilo, že i v dnešní době je to hojně využívané zabezpečení, které je už dávno mrtvé a nelze ho považovat za dostatečně dobré při ochraně bezdrátové sítě před nezvanými hosty. Prolomení je otázkou několika minut pro zkušeného útočníka. Na daleko zajímavější poznatky jsem přišel u bezdrátových sítích zabezpečených pomocí protokolu WPA. Docela hojně jsem se u těchto sítí setkal se zapnutou funkcí WPS čímž se toto téměř neprolomitelné zabezpečení WPA podaří v rozmezí maximálně několika hodin obejít a získat tak přístup do bezdrátové sítě, aniž by se musel provádět útok na samotné WPA zabezpečení. Funkce WPS, která se vyskytuje snad na všech novějších zařízení, se většinou automaticky zapíná, když se na přístupovém bodu nastaví režim zabezpečení WPA. Dle poznatků z internetových diskuzí nejde u některých zařízení dokonce tato funkce vypnout! Jako další slabinu v zabezpečení bych viděl možnost, že některé Wi-Fi routery podporují funkcí vysílání zároveň dvou SSID. S tímto se lze hlavně setkat v hojné míře u ADSL modemů, které v dnešní době zároveň plní i funkci Wi-Fi routeru. Druhé SSID bývá ve většině případů pod notoricky známým označením VOIP, které je z továrního nastavení zabezpečeno pouhým protokolem WEP a valná část uživatelů ani neví, že má něco takového na svém Wi-Fi routeru zapnuto, takže se neobtěžuje to vypnout nebo případně zvýšit zabezpečení . Při svém průzkumu jsem takto narazil na velké množství bezdrátových sítí, kdy jedno SSID bylo zabezpečeno pomocí WPA a druhé SSID pomocí WEP. Tím pádem se nám tu nabízí druhá možnost jak snadno během chvilky obejít protokol WPA a dostat se do Wi-Fi sítě. Pokud chce mít uživatel opravdu jistotu, že je jeho bezdrátová síť s protokolem WPA dobře zabezpečena, tak by se měl vyvarovat těchto dvou bezpečnostních chyb a to vypnout funkci WPS a prověřit

si jestli jeho přístupový bod vysílá jenom pod jedním SSID a jaké je u něj použito zabezpečení.

6 Prolomení 128 bitového WEP klíče

Zde se pokusím pomocí zachycených dialogových oken popsat jak se během několika minut dostat do bezdrátové sítě v nejvyužívanějším pásmu 2,4 GHz, která je zabezpečena pomocí 128 bitového WEP klíče. Předem bych chtěl upozornit, že to co zde budu popisovat slouží čistě jenom ke studijním účelům a nabourávat se do cizích bezdrátových sítí je trestné. Prolomení WEP klíče jsem prováděl u sebe doma na své bezdrátové síti. Útok byl proveden na VDSL modem Huawei HG622u, který zároveň slouží i jako Wi-Fi router. Ke zjištění WEP klíče jsem použil notebook ke kterému byl připojen Wi-Fi USB adaptér s čipem Atheros, který podporuje injekci paketů díky které dosáhneme větší rychlosti při zjišťování WEP klíče. K urychlení prolomení zabezpečení WEP jsem na daný modem připojil druhý notebook, na kterém jsem nechal puštěné internetové rádio (nebo stačí jakákoliv webová aplikace, která generuje datový provoz) a to z toho důvodu, aby po Wi-Fi síti neustále proudila data a tím se prolomení WEP klíče stalo opravdu chvilkovou záležitostí. Zároveň popíši jak postupovat, když na bezdrátové síti není žádný provoz a není připojeno žádné zařízení. Vše bylo prováděno na linuxové distribuci BackTrack 5 R1.

6.1 Co je potřeba?

• stolní nebo přenosný počítač (dnes snad v každé domácnosti)

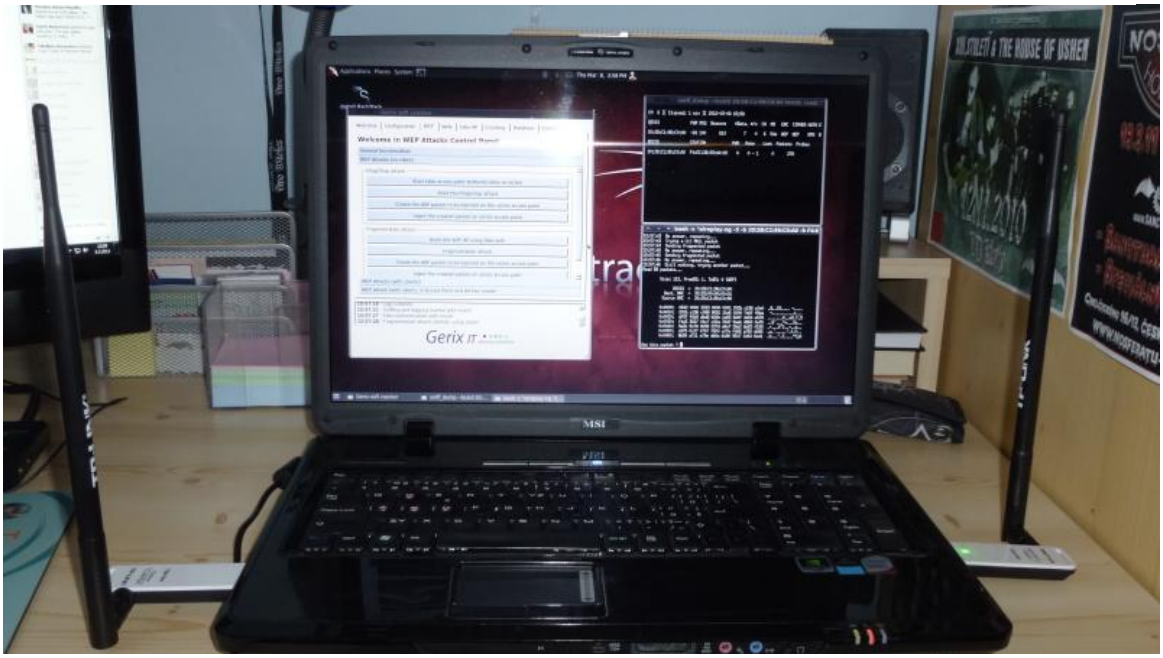
• pokud není počítač vybaven Wi-Fi kartou s čipem, který podporuje injekci paketů, tak takovou vhodnou kartu zakoupit - v mém případě to je USB Wi-Fi karta TP-LINK TL-WN722N (orientační cena 267 Kč)

• není vyžadováno, ale doporučuji k takové Wi-Fi kartě, u které je možnost odmontovat anténu, dokoupit silnější anténu pro zkvalitnění signálu a příjmu - v mém případě to je všesměrová anténa TP-LINK TL-ANT2408CL 8dBi (orientační cena 182 Kč)

• linuxová distribuce BackTrack 5 R1 (zdarma ke stažení na internetu)

Z požadavků můžeme vidět, že finanční náklady na prolomení WEP klíče nejsou žádné pokud již v počítači disponujeme patřičnou Wi-Fi kartou nebo jsou opravdu minimální v řádech stokorun a jsou dostupné opravdu každému. Dále je velkou výhodou, že operační systém na kterém se to všechno provádí je k dispozici zdarma na internetu.

Obrázek 16: Běžící operační systém BackTrack 5 R1 při odhalování WEP klíče



6.2 Jak postupovat při prolomení ochrany WEP

6.2.1 Na Wi-Fi síti je datový provoz

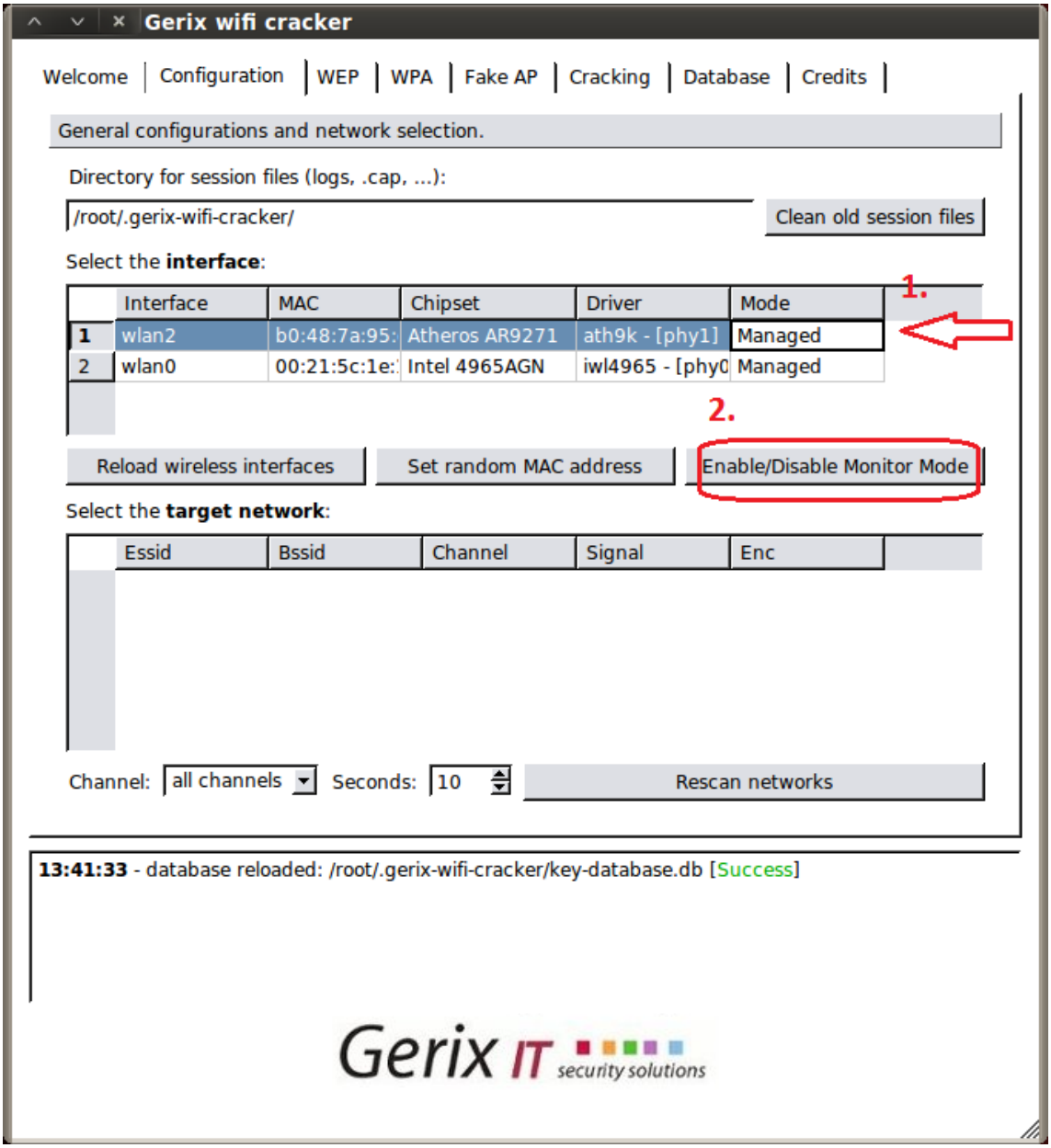
Obrázek 17

Po naběhnutí operačního systému BackTrack budeme potřebovat program s názvem Gerix wifi cracker, který pracuje v přehledném grafickém rozhraní a vyhneme se tím práci v linuxové systémové konzoli, se kterou mohou mít problémy především začátečníci, kteří s Linuxem doposud nepracovali. Práce s tímto programem je opravdu snadná a zvládne s ním pracovat téměř každý. Program nalezneme v nabídce podobné té, kterou známe z prostředí Windows. Na úvodní obrazovce systému BackTrack klikneme v levém horním rohu na tlačítko "Applications" a postupujeme podle cesty (Obrázek 17) tj. BackTrack → Exploitation Tools → Wireless Exploitation → WLAN Exploitation → gerix-wifi-cracker-ng.

Obrázek 18

Po spuštění daného programu nám vyskočí úvodní obrazovka s uvítáním a informací k čemu program slouží. V horní nabídce záložek vybereme tu s názvem "Configuration" a klikneme na ní (Obrázek 18).

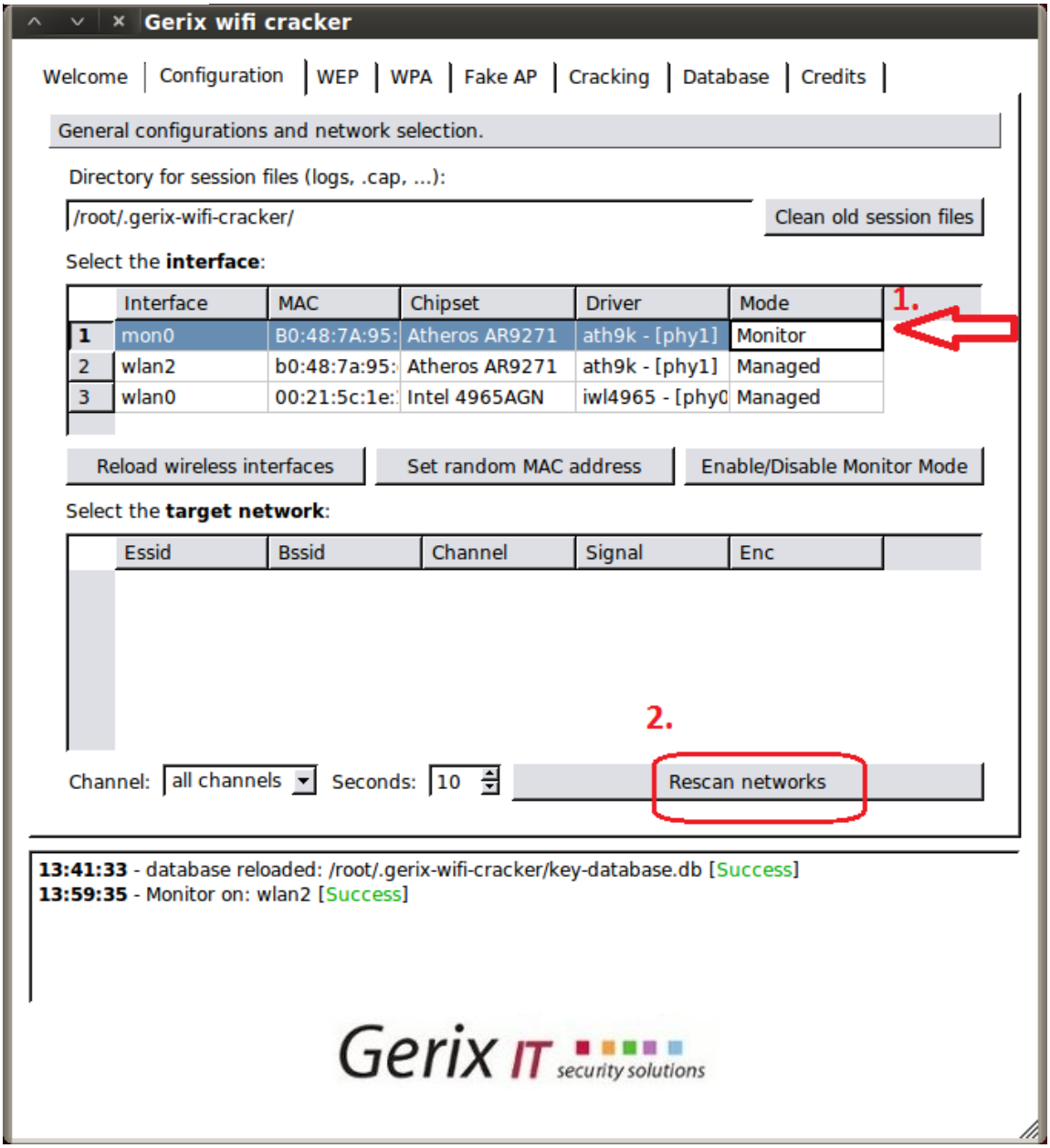
Obrázek 19



Na této kartě (Obrázek 19) se nám zobrazí dostupné Wi-Fi zařízení, které máme nainstalované na počítači. Kliknutím vybereme vhodné zařízení. V mém případě to je Wi-Fi karta s čipsetem Atheros AR9271 podporující injekci paketů (aktivní režim) a tudíž je to vhodné zařízení pro naše účely. Jako další krok klikneme na položku "Enable/Disable Monitor Mode". Tímto se nám karta přepne do monitorovacího módu

(pasivní režim), kdy je schopná sledovat datový provoz v bezdrátové síti a nepotřebuje k tomu platnou IP adresu ani být připojena na daný přístupový bod.

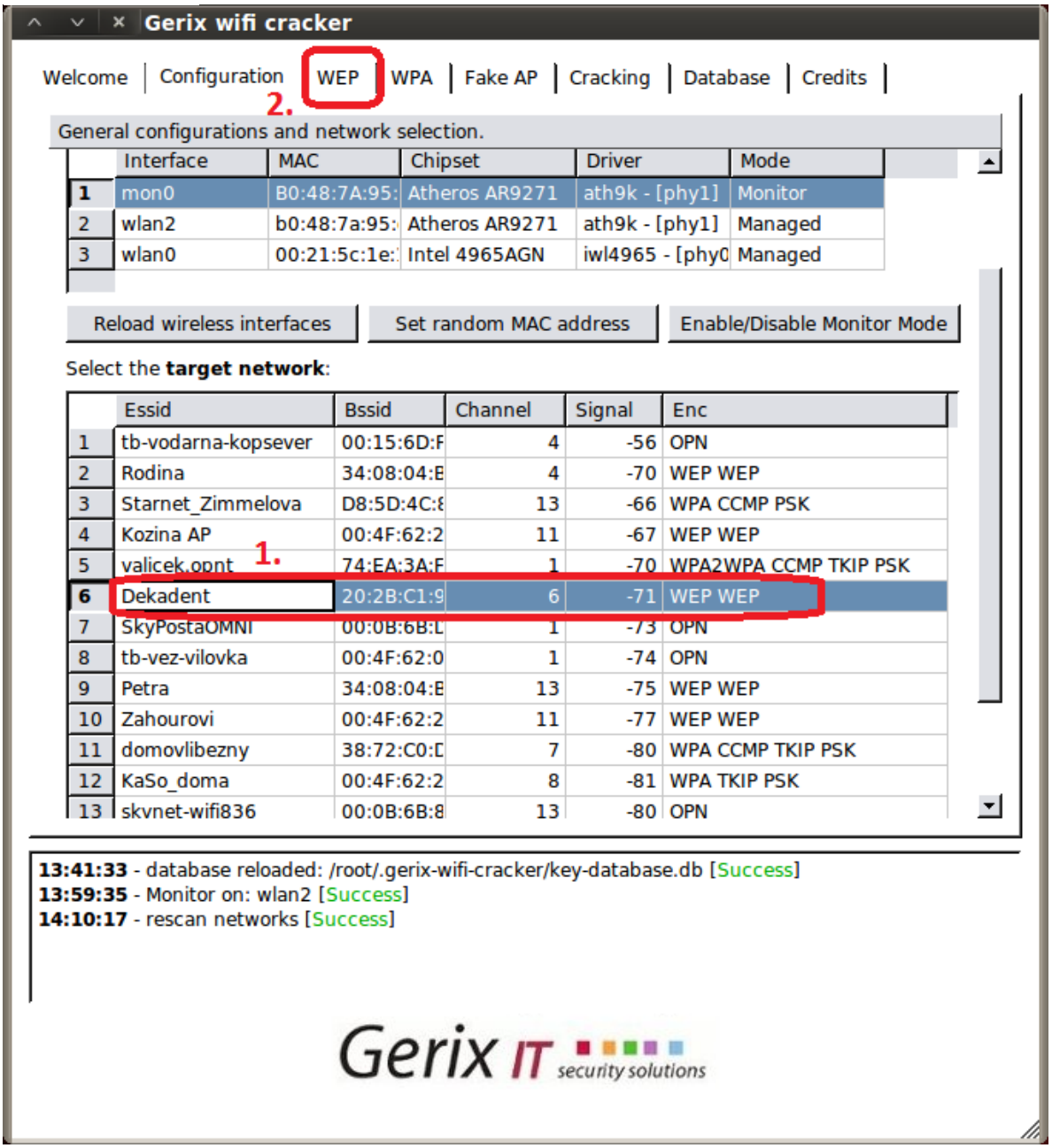
Obrázek 20



Nyní se nám v nabídce dostupných Wi-Fi karet objeví nová položka pod označení "mon0" (Obrázek 20). To nám signalizuje, že naše zvolená Wi-Fi karta byla přepnuta

do monitorovací módu. Kliknutím ji vybereme a pak klikneme na tlačítko "Rescan networks". To nám po chvilce zobrazí všechny dostupné bezdrátové sítě v okolí.

Obrázek 21



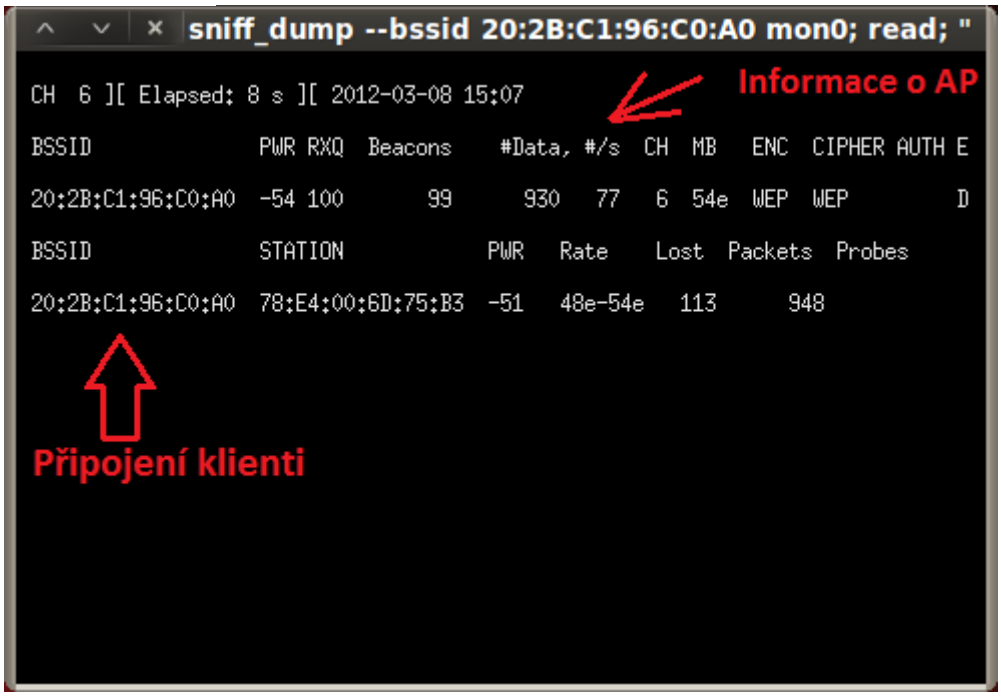
Zde můžeme vidět všechny dostupné bezdrátové sítě v okolí (Obrázek 21). Zobrazuje se nám tu i pár hlavních údajů jako je MAC adresa přístupového bodu, kanál na kterém

daná Wi-Fi síť vysílá, úroveň signálu a použité zabezpečení. Ze seznamu sítí vybereme námi zvolenou bezdrátovou síť se zabezpečením WEP a na horní liště klepneme na položku "WEP".

Obrázek 22

Jako první krok (Obrázek 22) klikneme na položku "Start sniffing and Logging". Vyskočí nám dialogové okno s údaji (Obrázek 23), které nebudeme zavírat. Poté klikneme podle druhého kroku na položku "WEP Attacks (no-client)". Jen upozorním, že žádné z dialogových oken s černým pozadím se nebude zavírat, aby se předešlo případným komplikacím, a nechá se puštěné na pozadí.

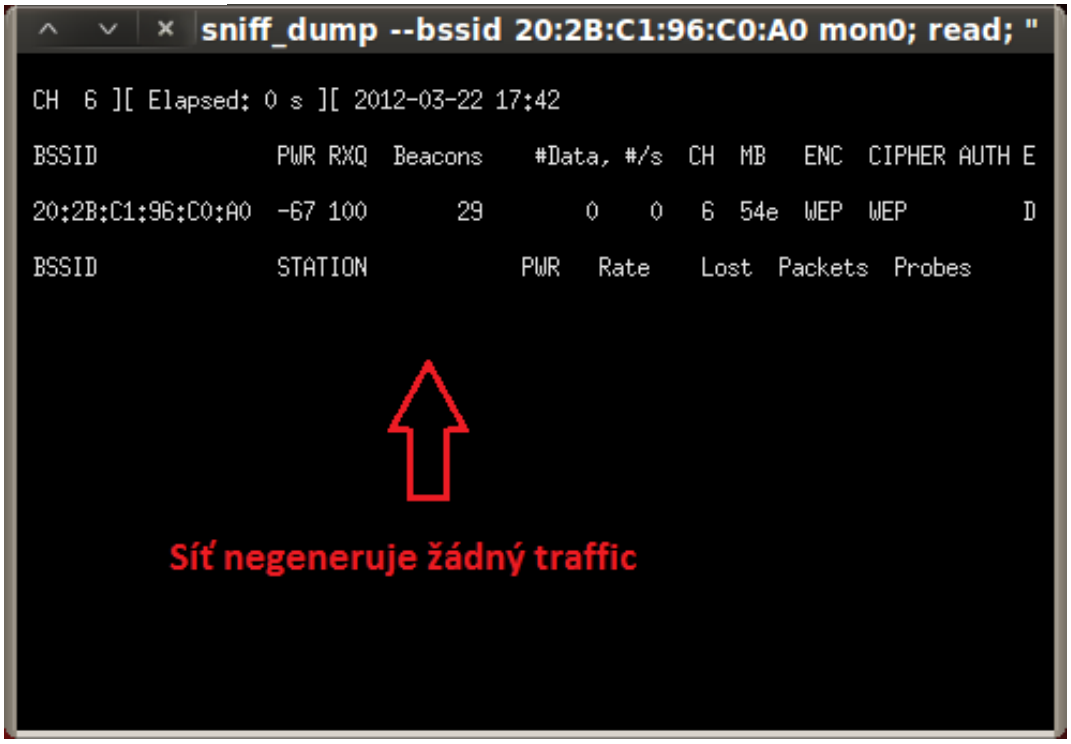
Obrázek 23



Toto dialogové okno (Obrázek 23) nám ukazuje podrobnější informace o přístupovém bodu. Zásadní je informace pod položkou PWR, RXQ a Beacons. PWR nám určuje sílu signálu. Čím menší číslo, tím lepší signál. Zde uvedená hodnota -54 znamená skoro plný signál. Číselná hodnota u Beacons by nám měla neustále bez přerušení vzrůstat. Jedná se o takzvané signální rámce obsahující informace o přístupovém bodu. RXQ nám označuje kvalitu přijímaných paketů. Tyto tři hodnoty jsou velmi důležité, protože potřebujeme opravdu silný a kvalitní signál bez výpadků, abychom mohli zjistit WEP klíč. V opačném případě se vůbec nemá cenu pouštět do prolamování zabezpečení,

poněvadž budeme mít problémy s příjmem signálu. Eventuálně pokud je to možné, tak si můžeme pomoci tím, že se přemístíme blíž k přístupovému bodu. V dialogovém okně můžeme také vidět případné připojené klienty. Na obrázku je vidět jedno připojené zařízení, které generuje datový provoz. Také nesmím ještě opomenout položku Data, která nám ukazuje počet zachycených dat, které slouží k výpočtu WEP klíče. Můžeme se hojně setkat i s tím, že na dané bezdrátové síti není připojen žádný klient a tím pádem se negeneruje žádný datový provoz (Obrázek 24).

Obrázek 24

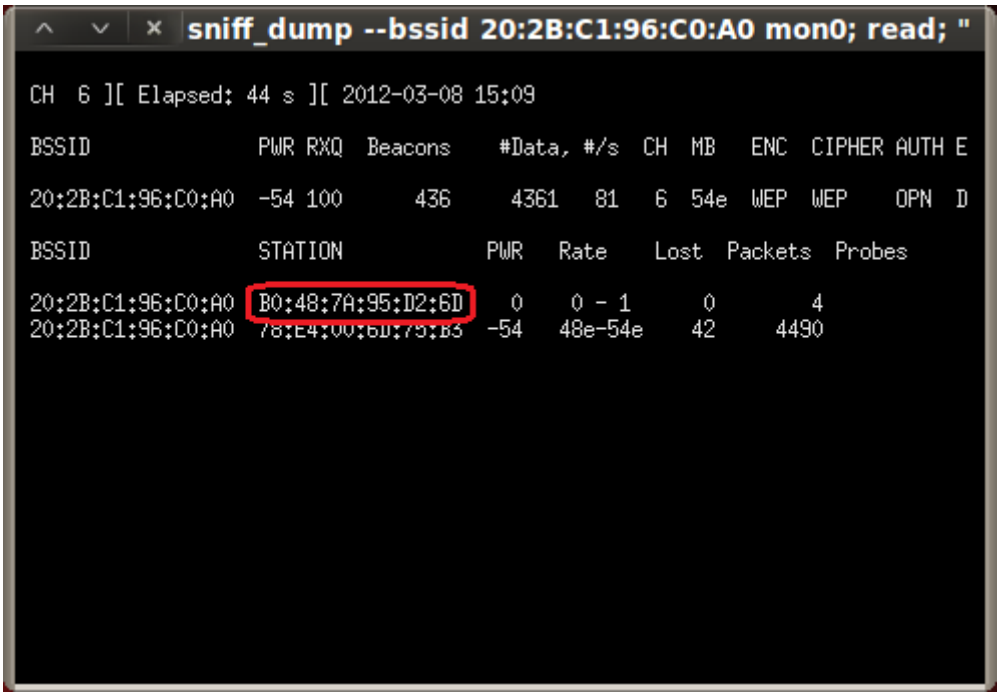


Obrázek 25

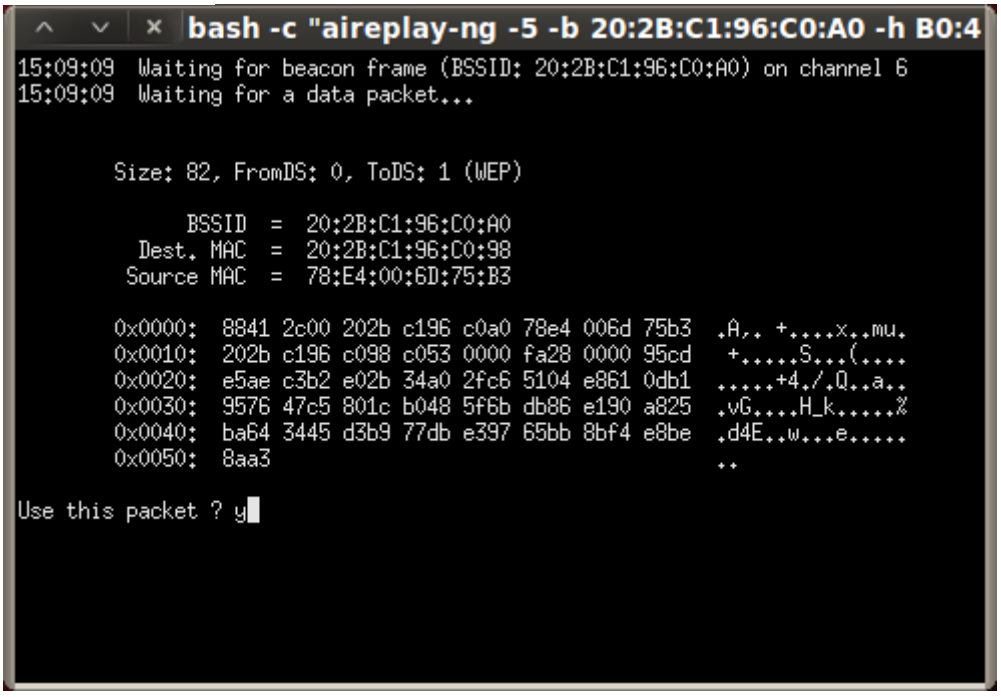
V této nabídce se nám nabízejí dvě formy útoku a tím je ChopChop útok a fragmentový útok (Obrázek 25). V našem případě vybereme fragmentový útok a klikneme na tlačítko "Associate with AP using fake auth". Můžeme si všimnout, že v druhém dialogovém okně (Obrázek 26) se nám objeví další připojený klient. Tím je náš počítač. Pokud se

tak nestane, tak je na vině většinou špatný signál a není dále možné pokračovat pokud se nám nějakým způsobem nepovede signál zlepšit, aby jsme se mohli na daný přístupový bod připojit. V další fázi klikneme na tlačítko "Fragmentation attack". Vyskočí dialogové okno (Obrázek 27) s otázkou "Use this packet ?". Pro potvrzení napíšeme "y" a stiskneme klávesu Enter.

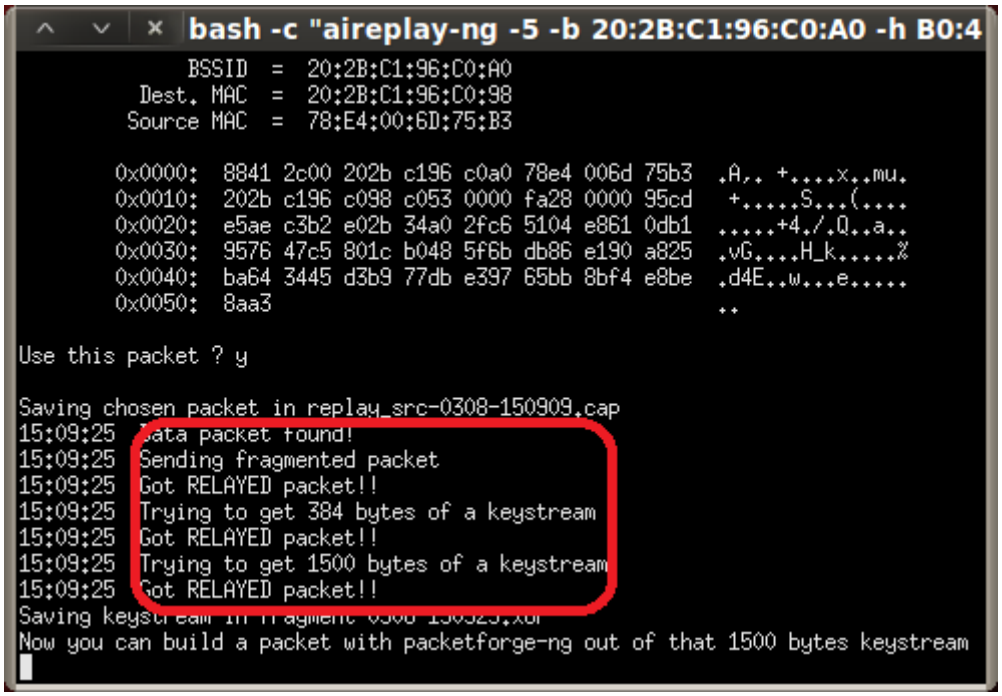
Obrázek 26



Obrázek 27



Obrázek 28

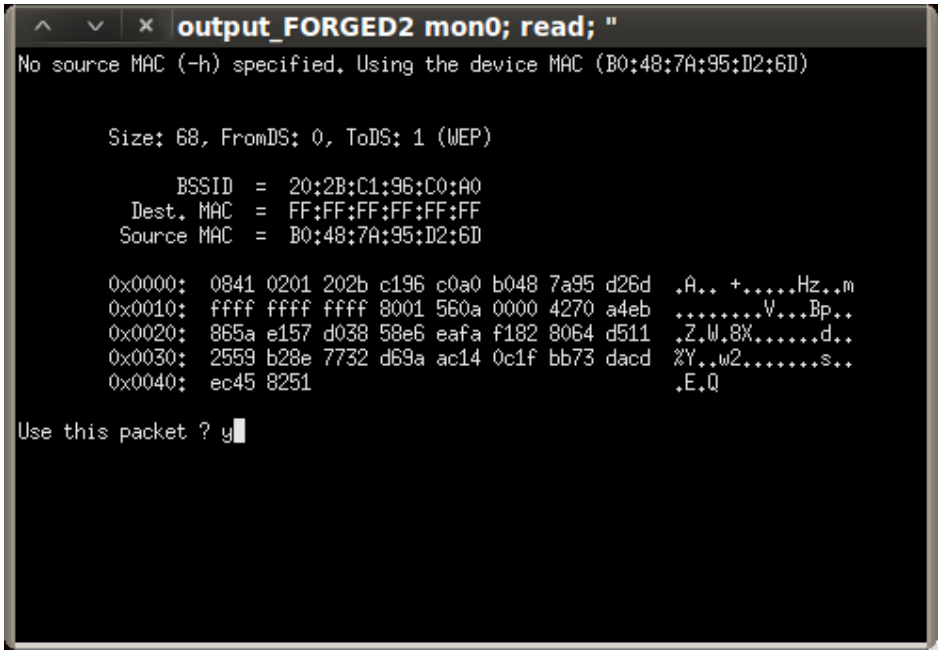


Po potvrzení klávesou Enter se nám vypíše informace, že jsme obdrželi potřebný paket ve kterém je obsažen tzv. keystream (Obrázek 28), který je potřebný k injekci paketu. Nyní se přepneme nazpět do okna hlavního ovládacího programu (Obrázek 29).

Obrázek 29

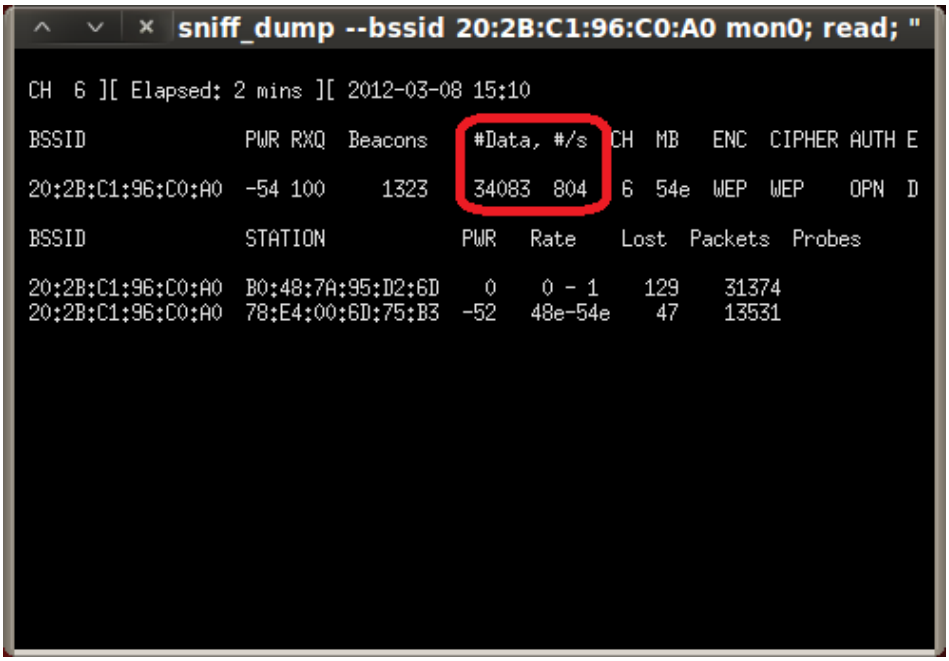
V části Fragmentation attack klikneme na tlačítko "Create the ARP packet to be injected on the victim access point" a hned poté na tlačítko "Inject the created packet on victim access point" (Obrázek 29).

Obrázek 30



Vyběhne dialogové okno s dotazem jestli chceme zvolený paket injektovat. Pro potvrzení napíšeme "y" a stiskneme klávesu Enter (Obrázek 30). Po potvrzení začne injekce paketů do přístupového bodu (Obrázek 31). Toto dialogové okno nezavíráme jinak by došlo k přerušení injektování. Tento krok nám zrychlí počet zachycených dat, která jsou potřebná pro výpočet WEP klíče pokud na bezdrátové síti není dost silný datový provoz.

Obrázek 31

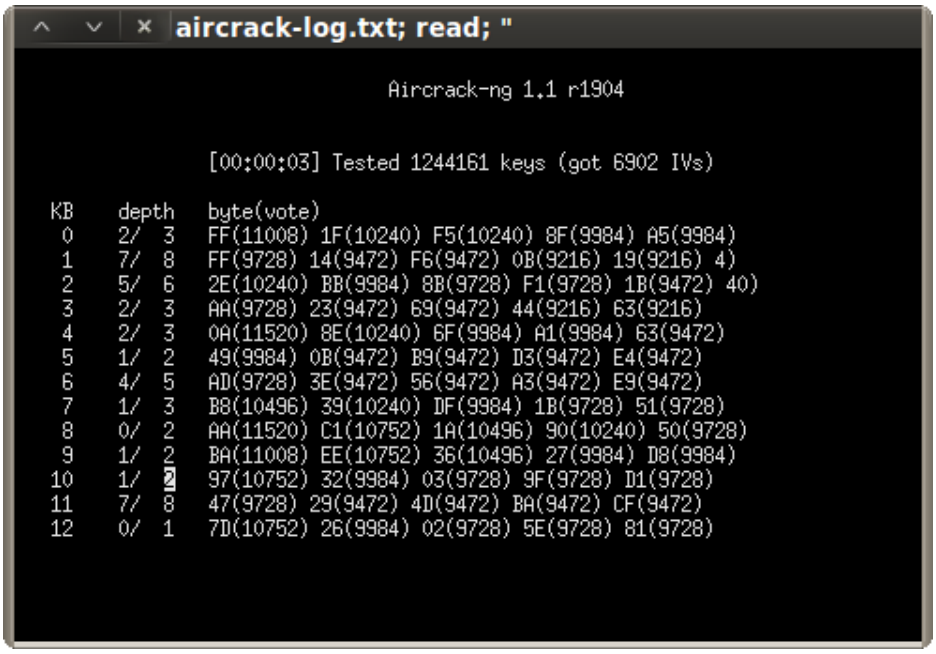


Obrázek 32

A nyní zbývá už jen poslední krok. V hlavním menu programu Gerix wifi cracker v horní liště záložek klikneme na položku "Cracking" a potom na tlačítko "Aircrack-ng -

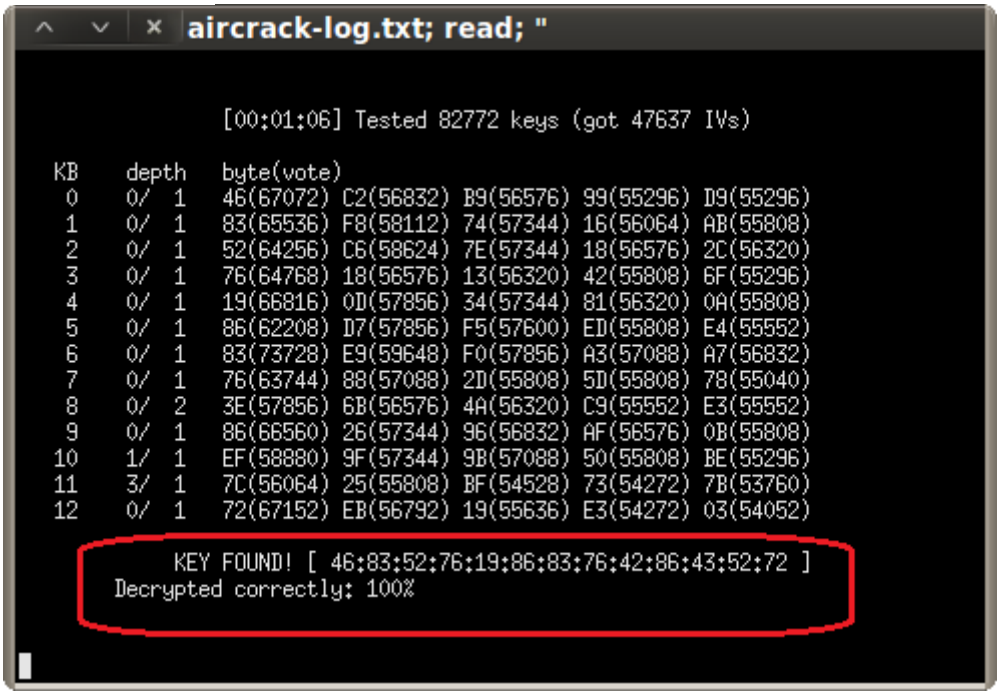
Decrypt WEP password"čímž započne luštění WEP klíče. Průběh se nám ukazuje v dialogovém okně (Obrázek 33).

Obrázek 33



Samotné dešifrování klíče trvá řádově několik sekund až minut a nezáleží na tom jak silný WEP klíč je použit (64bit, 128bit, 256bit). Zde můžeme vidět nalezený 128bitový WEP klíč vypsaný v hexadecimálním tvaru (Obrázek 34).

Obrázek 34

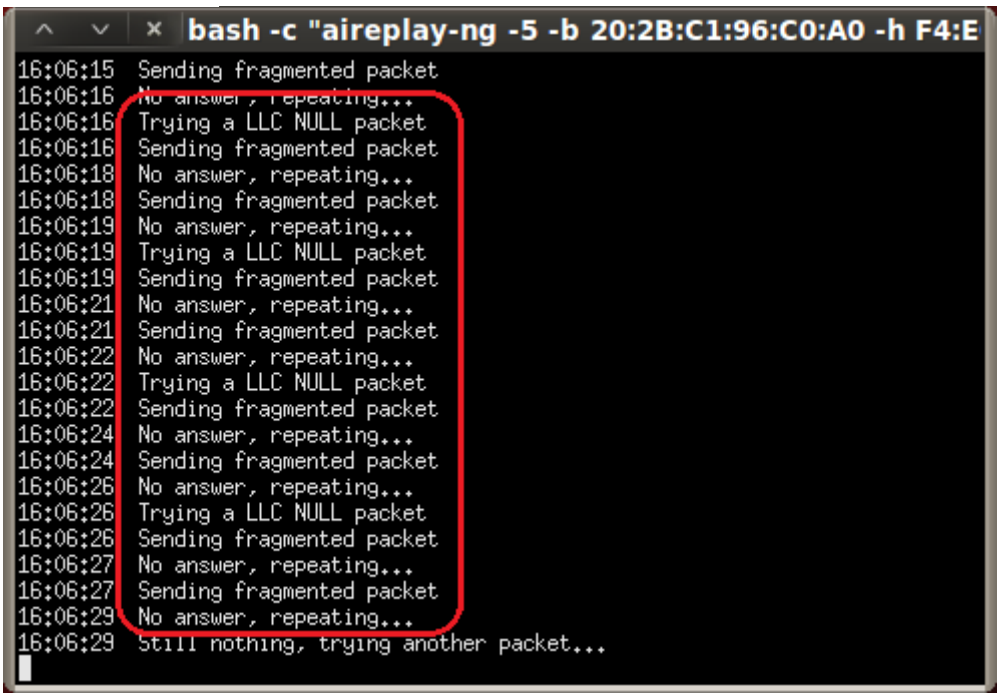


Tento popsaný postup ale neplatí pro bezdrátové sítě, ve kterých není žádný datový provoz. V tomto případě se musí postupovat trochu jinak.

6.2.2 Na Wi-Fi síti není žádný datový provoz

K tomuto postupu jsou potřeba dvě Wi-Fi karty. Pro každou kartu se spustí program Gerix wifi cracker a postup je stejný pro každou kartu až k obrázku 27. Při kliknutí na tlačítko "Fragmentation attack" nám bude po potvrzení, že chceme použít daný paket pořád dokolečka v dialogovém okně vypisováno, že není žádná odpověď (Obrázek 35). Je to způsobeno tím, že na dané bezdrátové síti není žádný datový provoz.

Obrázek 35

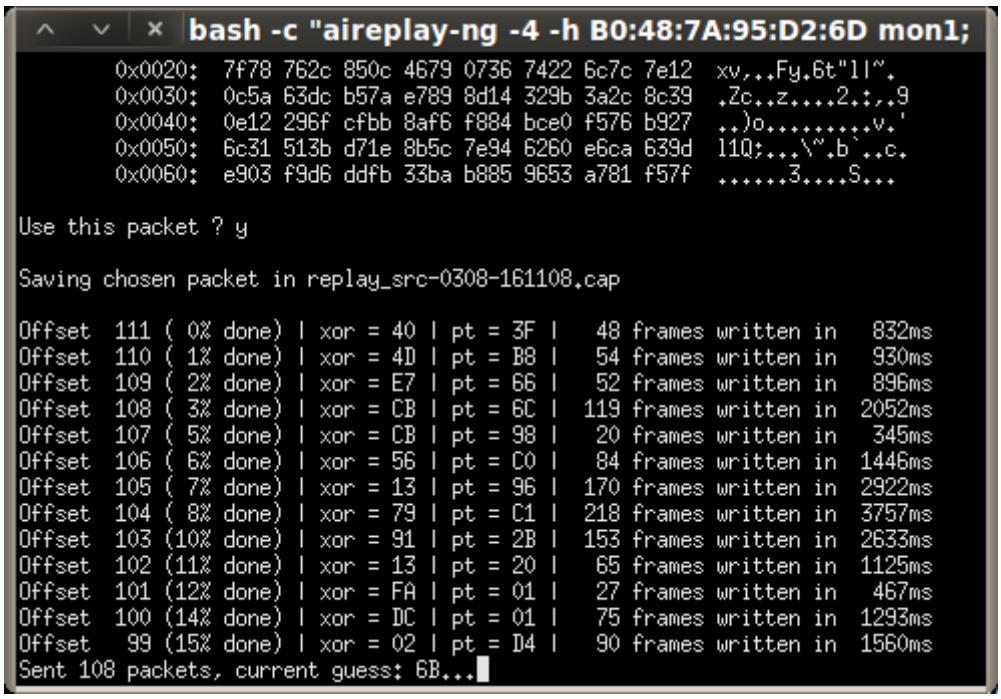


Proto budeme muset využít ChopChop útok, který dokáže dešifrovat pakety bez znalosti WEP klíče a vytvoří se nám něco na způsob keystreamu, který pak budeme moct injektovat nazpátek přístupovému bodu. U obrázku 25 tedy jako třetí bod klikneme na položku "Start the ChopChop attack" (Obrázek 36).

Obrázek 36

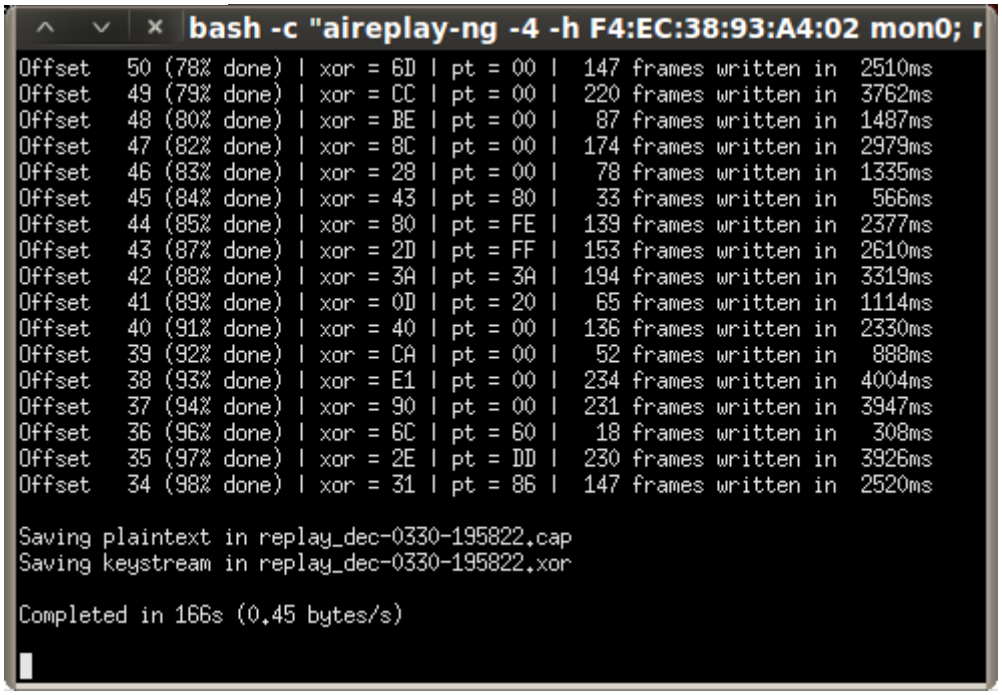
Po kliknutí na položku "Start the ChopChop attack" (je jedno u jaké Wi-Fi karty ChopChop útok spustíme) nám vyskočí podobné dialogové okno jako u fragmentového útoku. Až nám to nabídne jestli chceme použít zvolený paket, tak potvrdíme pomocí písmene "y" a klávesy Enter (Obrázek 37).

Obrázek 37



Zde je důležité neustále opakovat u obou Wi-Fi karet fragmentový útok, aby se nepřerušil ChopChop útok a zdárně doběhl do 100%. To znamená, že musíme u dialogových oken, kde nám běží fragmentový útok, stále potvrzovat že chceme použít daný paket (Obrázek 35). Slouží to k tomu, aby nás přístupový bod neodpojil, protože některé přístupové body jsou k tomuto útoku odolné a jakmile tento útok detekují, tak daného klienta odpojí.V dalším dialogovém okně můžeme vidět, že ChopChop útok byl úspěšně dokončen a zabralo to pouhých 166 sekund (Obrázek 38). Nyní se přepneme zpět do ovládání programu Gerix wifi cracker.

Obrázek 38



V nabídce ChopChop útoku jako první klikneme na položku "Create the ARP packet to be injected on the victim access point" (Obrázek 39). Tím se nám vytvoří paket, který se bude injektovat přístupovému bodu. A za druhé klikneme na položku "Inject the created packet on victim access point". Vyskočí nám dialogové okno ve kterém zase potvrdíme, že chceme použít zvolený paket. Pokud je vše funkční, tak už zbývá jen poslední krok, a to v horní liště programu Gerix wifi cracker kliknout na položku "Cracking" a v ní na text " Aircrack-ng - Decrypt WEP password" čímž se nám dešifruje WEP klíč podle postupu uvedeného výše.

Obrázek 39


Gerix wifi cracker
Welcome
Configuration
WEP
WPA
Fake AP
Cracking
Database
Credits
Welcome in WEP Attacks Control Panel
General functionalities
WEP Attacks (no-client)
ChopChop attack
Start false access point Authentication on victim
Start the ChopChop attack
1.
Create the ARP packet to be injected on the victim access point
2.
Inject the created packet on victim access point
Fragmentation attack
Associate with AP using fake auth
Fragmentation attack
Create the ARP packet to be injected on the victim access point
Inject the created packet on victim access point
WEP Attacks (with clients)
WEP Attack (with clients, in Access Point and Ad-Hoc mode)
15:04:30 - Logs cleaned
15:04:30 - Logs cleaned
15:06:18 - Monitor on: wlan2 [Success]
15:06:44 - rescan networks [Success]
15:07:39 - Sniffing and logging started with mon0
15:08:14 - Sniffing and logging started with mon0
Gerix IT security solutions

6.3 Zneužití bezpečnostní chyby u funkce WPS

Jelikož se jedná v době psaní mé bakalářské práce o čerstvou bezpečnostní chybu a tak jsem se rozhodl se jí v krátkosti věnovat a zaměřit se na to, že je opravdu snadné se dostat do zabezpečené bezdrátové sítě, když je na přístupovém bodu zapnuta funkce WPS. S touto zapnutou funkcí jsem se při svém průzkumu bezdrátových sítí setkal u skoro poloviny zařízení, které byly zabezpečeny pomocí protokolu WPA. Test jsem prováděl za pomocí programu Reaver na operačním systému BackTrack 5 R1.

Obrázek 40: Tímto logem jsou označena zařízení s funkcí WPS

Zdroj: www.google.com; sekce obrázky

Pro zjištění jestli je na dané bezdrátové síti vůbec zapnuta funkce WPS využijeme linuxový příkazový řádek, do kterého postupně zapíšeme následující příkazy:

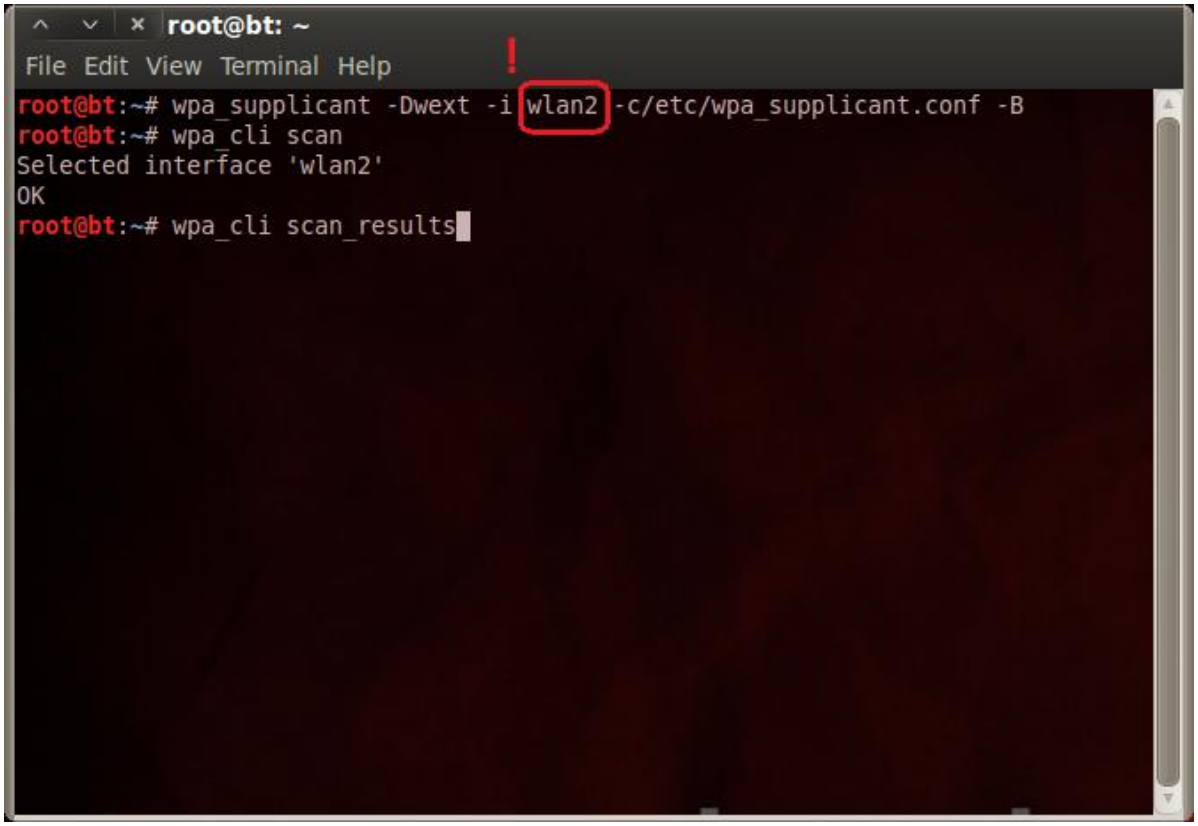
"wpa_supplicant -Dwext -i wlan1 -c/etc/wpa_supplicant.conf -B"

"wpa_cli scan"

"wpa_cli scan_results"

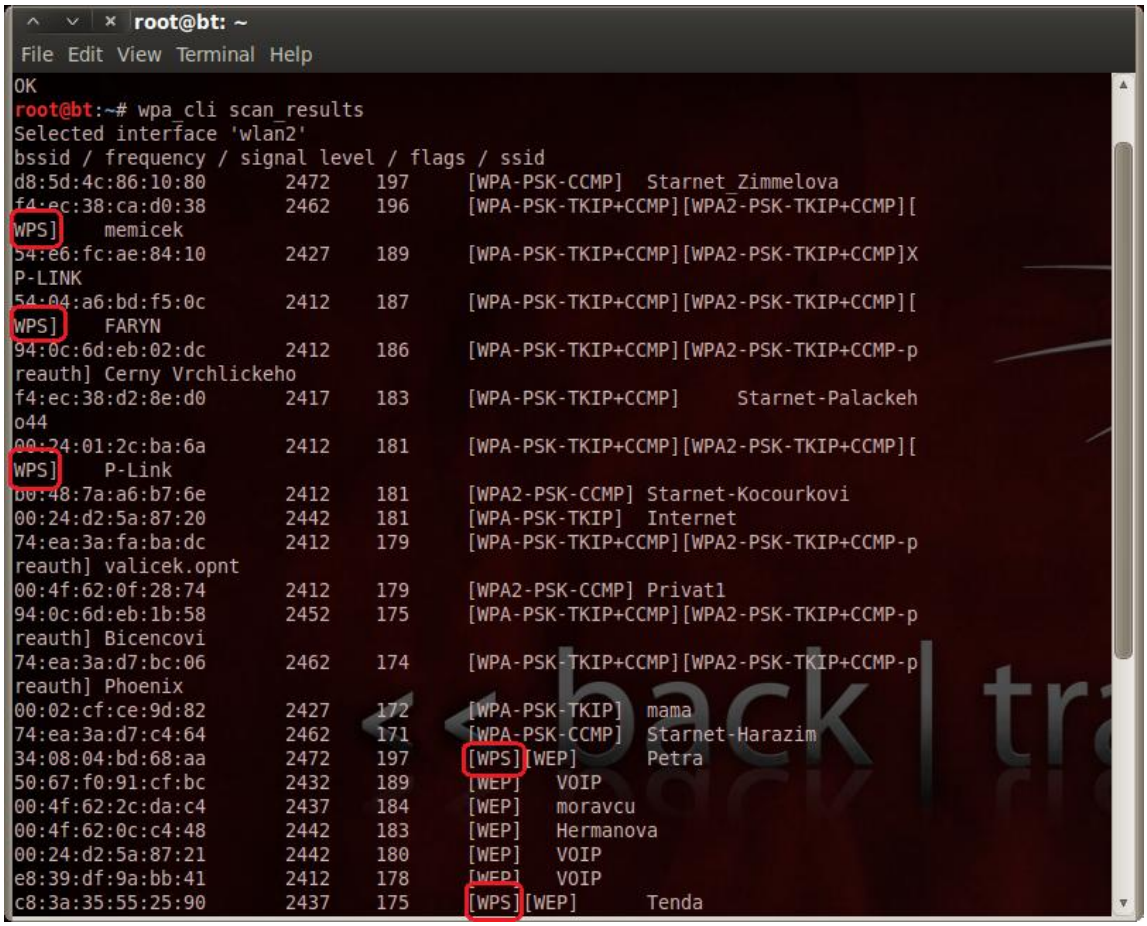
Každý z příkazů potvrdíme klávesou Enter (Obrázek 41). Jen pozor u parametru "-i", kde se musí zadat správný profil zvolené Wi-Fi karty. Většinou to bývá wlan0, wlan1 atd.

Obrázek 41



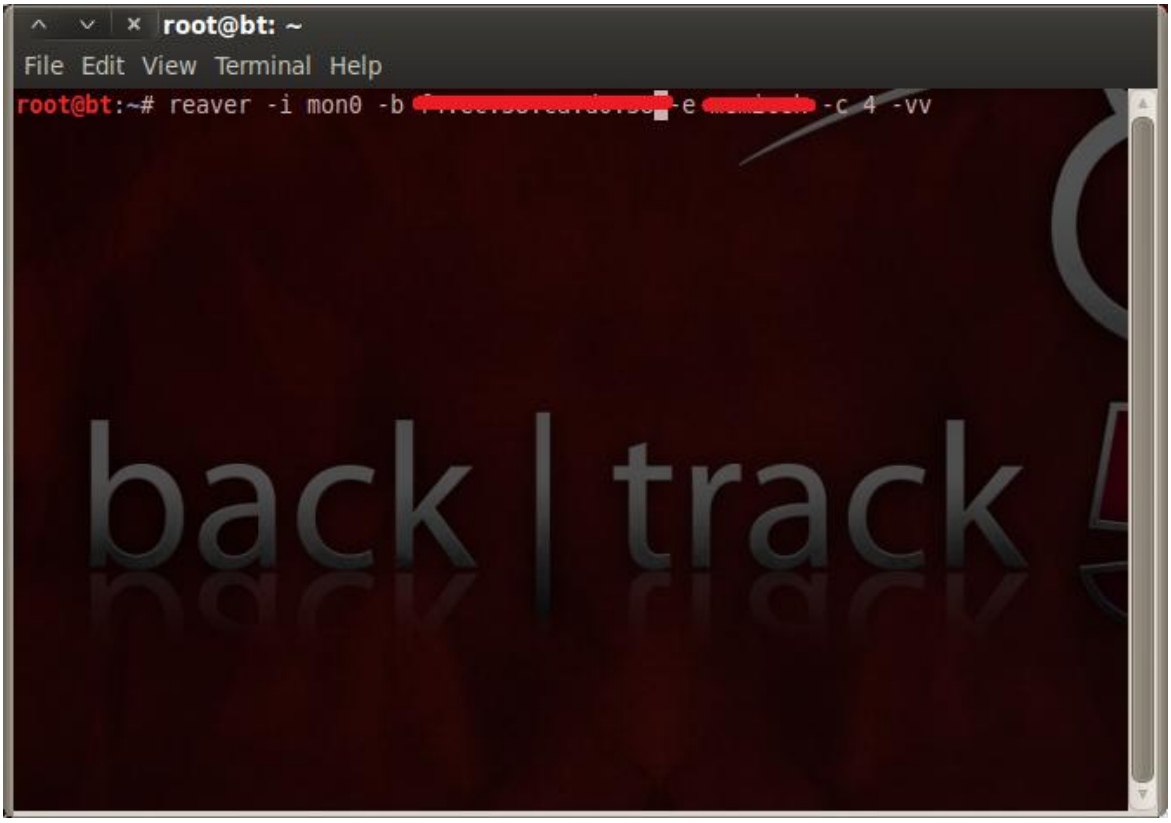
Po potvrzení posledního příkazu se nám zobrazí seznam dostupných Wi-Fi sítí (Obrázek 42). Nás bude zajímat jestli se někde nevyskytuje textová hodnota WPS (na obrázku je červeně orámovaná).

Obrázek 42

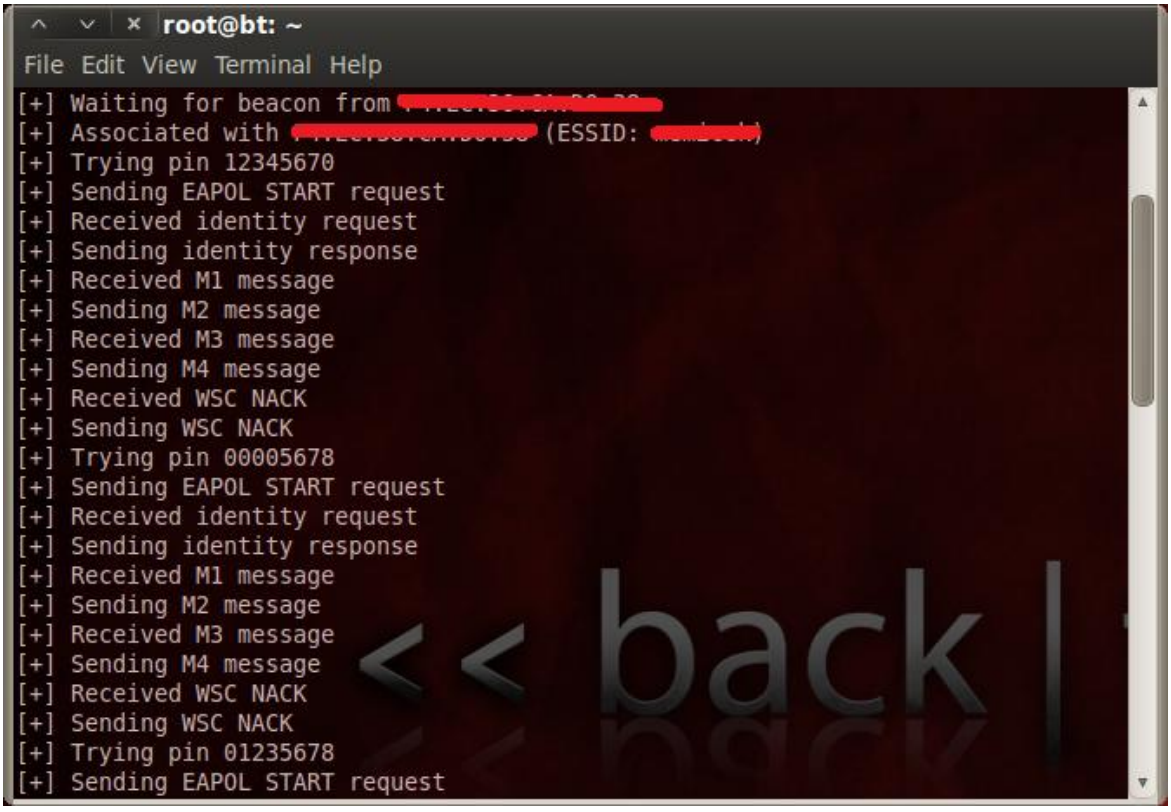


Teď už nám nebrání přejít k samotnému zjišťování PINu pomocí programu Reaver. Program se také spouští z příkazového řádku už rovnou s parametry bezdrátové sítě u které chceme PIN kód zjistit (Obrázek 43). Za parametrem "-b" napíšeme MAC adresu přístupového bodu, za "-e" napíšeme název bezdrátové sítě a za parametrem "-c" číslo kanálu na kterém Wi-Fi síť vysílá. Ostatní parametry pouze opíšeme. Po stisknutí klávesy Enter by mělo započít hledání PIN kódu (Obrázek 44).

Obrázek 43

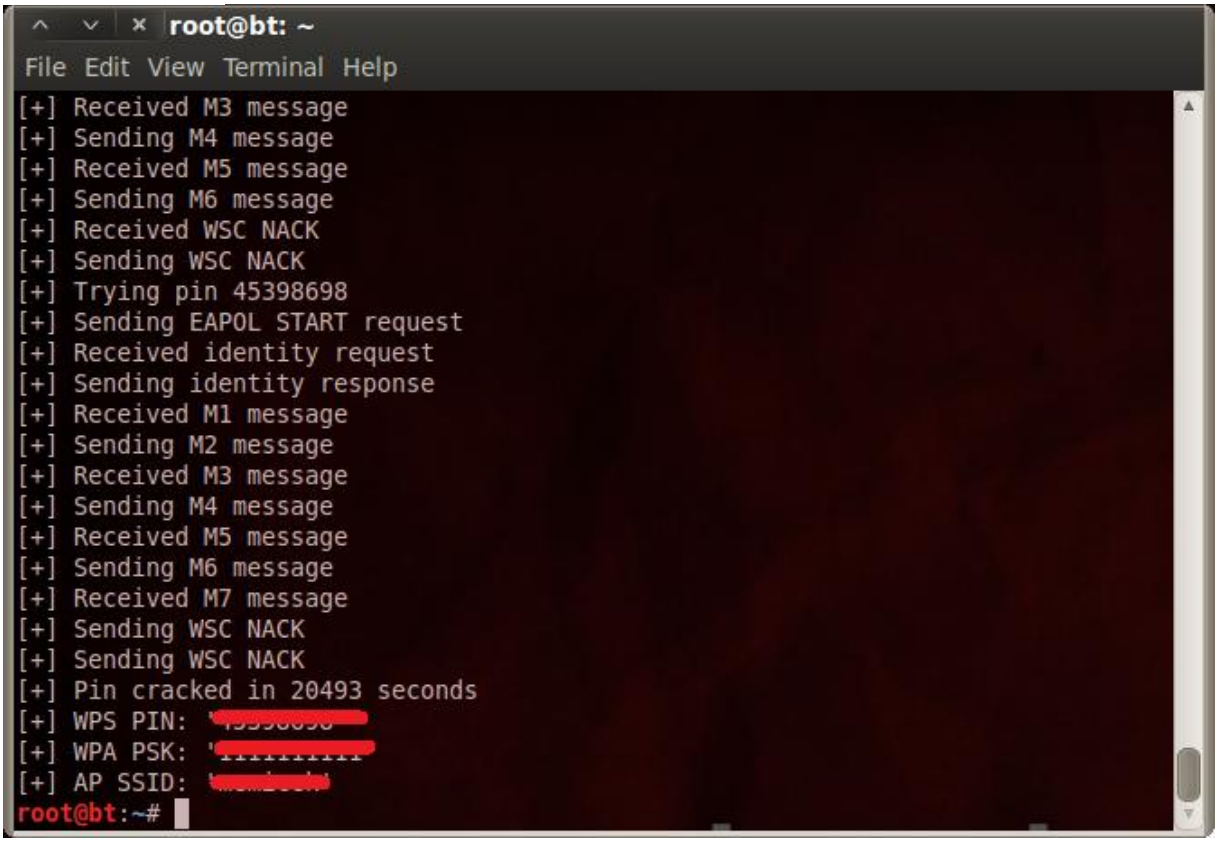


Obrázek 44



Hledání správného PIN kódu zabere maximálně až několik hodin. Záleží také na kvalitě a síle signálu u Wi-Fi sítě u které chceme PIN kód zjistit. Při dobrých podmínkách je rychlost hledání správného PIN kódu zhruba 2sec/pin. Naopak při špatném signálu se rychlost může prodloužit až na 5sec/pin a více. Pokud vezmeme v potaz, že dešifrování protokolu WPA/WPA2 při použití silného hesla může trvat desítky až tisíce let při současném výpočetním výkonu počítačů, tak útok vedený na PIN kód u funkce WPS zabere pouze několik hodin. To je značná úspora času a zabezpečení WPA/WPA2 se v tomto případě stává nedostatečným.

Obrázek 45



Na posledním dialogovém okně můžeme vidět úspěšné nalezení správného PIN kódu (Obrázek 45). Jeho hledání trvalo přes pět a půl hodiny a to hlavně díky tomu, že signál

nebyl moc kvalitní. Zároveň se nám tu rovnou zobrazí i použité heslo u zabezpečení WPA, kterým je přístupový bod chráněn.

Bezpečnostními experty je v současně době doporučeno následující:

- Vypnout bezdrátovou síť pokud je funkce WPS natrvalo zapnutá a nejde žádným způsobem vypnout.
- Nechat bezdrátovou síť zapnutou, ale vypnout funkci WPS.

7 Zabezpečení bezdrátové sítě v praxi ve firemním prostředí

7.1 Charakteristika podniku

Jak je patrné z provedeného průzkumu Wi-Fi sítí po městě Třeboni, tak stále valná většina bezdrátových sítí není dostatečně zabezpečena. Z mého měření se jedná především o Wi-Fi sítě v domácnostech. Proto jsem se rozhodl zaměřit i na firemní prostředí, kde případná odcizená data budou mnohem více lukrativnější a cennější než z nějaké domácnosti. Záměrně jsem si vybral ekonomicky nejsilnější podnik v Třeboni a tou jsou Bertiny lázně Třeboň, s. r. o. a lázně Aurora, s. r. o. tvořící dohromady jednu firmu. [15] Lázně jsou největším podnikatelským subjektem v Třeboni, který zaměstnává skoro 500 zaměstnanců. Třeboňské lázně jsou známé po celé České republice a řádí se k těm nejvýznamnějším v lázeňském sektoru, a to nejenom díky různým oceněním a certifikátům jakosti, ale především svou kvalitou a profesionálním přístupem k hostům. Je tedy možné, že by se mohly stát obětí cíleného počítačového útoku za účelem poškození lázní, ukradení citlivých dat, know-how atd.

Obrázek 47: Bertiny lázně Třeboň, s. r. o.

Zdroj: www.mapy.cz

Obrázek 46: Lázně Aurora, s. r. o.

Zdroj: www.mapy.cz

7.2 Využití bezdrátové sítě v prostorách firmy

Oba dva lázeňské objekty využívají kromě klasické LAN sítě také ve velké míře právě Wi-Fi síť. Slouží jednak lázeňským hostům k připojení na internet, ale hlavně slouží vedoucím pracovníkům a manažerům ke snadnému a bezbariérovému přístupu k firemní počítačové síti. Bezdrátová síť je dostupná v celém lázeňském komplexu a je realizována pomocí Wi-Fi roamingu s několika přístupovými body, kdy se připojený klient může pohybovat bez přerušení po celém objektu bez výpadku signálu a ztráty dat.

7.3 Zabezpečení Wi-Fi sítě

Každý přístupový bod vysílá více identifikátorů sítě (SSID), kde jeden slouží právě lázeňským hostům a ostatní klientele pro připojení k internetu. U tohoto přístupového bodu je autentizace prováděna přes webové rozhraní internetového prohlížeče, kde se jen vyplní přezdívka, kterou si člověk nechá zaregistrovat na recepci a může vesele surfovat na internetu. Další přístupové body slouží manažerům a vedení firmy pro připojení se k podnikové síti a k přístupu k citlivým informacím uložených na serveru. Tyto přístupové body využívají jako zabezpečení filtraci MAC adres, což je obrovské bezpečností riziko. MAC adresu lze poměrně snadno odposlechnutím datového provozu zjistit a pak si jí následně změnit na svém počítači. Tím pádem se bude útočníkovo notebook tvářit jako notebook některého ze zaměstnanců od kterého byla MAC adresa kompromitována. Případný útočník se ale naštěstí dál do firemní sítě nedostane, protože by dále musel zjistit topologii sítě, aby věděl kam se vůbec připojit. Topologii sítě lze zjistit například pomocí programu Wireshark. Ale je tu další háček - terminálové a fileservery jsou v doméně (Active Directory) a využívají její zabezpečení. Hesla mají určitou politiku a mimo jiné neumožňují použít jména, jeden znak a podobně. Pokud by se přeci jen někdo dostal do domény, musí namapovat disky, jestliže by tedy přímo nezneužil přihlašovacích údajů uživatele. Jako poslední krok se musí dostat do informačního systému, který je opět chráněn uživatelským jménem a heslem. Tyto přihlašovací údaje jsou rozdílné od přihlášení do domény.

7.4 Potencionální rizika zneužití slabého zabezpečení

Útočník může využít přístup k internetu k nelegálním činnostem díky kterým může podnik uvést do konfliktu se zákonem a nebo může jen čistě odposlouchávat datovou komunikaci a tím se může dostat k soukromým údajům vedoucích pracovníků jako jsou přihlašovací údaje k e-mailu a dalším internetovým službám, čímž může daného pracovníka zdiskreditovat či dokonce vydírat. Po mém upozornění a po projednání tohoto možného bezpečnostního rizika s vedením společnosti a správcem sítě bylo zabezpečení bezdrátové sítě zvýšeno a nyní je používáno zabezpečení WPA2 se silným heslem.

7.5 Následky pro podnik při kompromitování počítačové sítě

Kdyby se útočníkovi podařilo přes bezdrátovou síť získat přístup k serveru, tak by to mělo velké finanční následky pokud by se útočník rozhodl vyřadit z provozu server. Přes server běží recepční, pokladní, účetní a další jiné důležité systémy bez kterých by lázně byly úplně ochromené. Správcem počítačové sítě byla vyčíslena finanční ztráta zhruba 1 milion korun za jeden den pro oba dva lázeňské komplexy, jestliže by byl server útočníkem odstaven. Lázně by nemohli přijímat nové klienty, vést účetní a platební styk, nemohli by fungovat procedury a také by zůstaly zavřené lázeňské restaurace, které využívají pokladní systém, který také běží ze serveru. Pokud by ze serveru byla odcizena všechna důležitá data, tak vedení lázní se jednohlasně shoduje na tom, že by to pro lázně znamenalo finanční škodu nevyčíslitelných rozměrů v řádech několika milionů korun a ztrátu důvěryhodnosti a dobrého jména v očích široké veřejnosti a institucí se kterými lázně spolupracují a udržují dobré styky. Také by mohla následovat velmi tučná pokuta za ztrátu těchto dat v důsledku zanedbání bezpečnostních opatření, protože se zde nacházejí jednak osobní data zaměstnanců, interní informace o firmě a především údaje o klientech, kteří se jezdí do lázní léčit, jako je jejich zdravotní stav a další důvěrné informace, které se nesmějí díky zákonu o ochraně osobních údajů dostat na veřejnost.

Tabulka 6: Finanční újma v závislosti na formě zneužití počítačové sítě

Forma zneužití	Vyřazení serveru z provozu na 1 den	Odcizení dat ze serveru	Zneužití firemního internetového připojení a serveru k nelegálním činnostem (spam, hacking,...)
Finanční újma (v Kč)	cca 1 milion	několik milionů + pokuta až do výše 10 milionů	pokuta až 10 milionů + možné trestní stíhání

Z tabulky je patrné, že jakákoliv forma zneužití firemní počítačové sítě dosahuje vysokých finančních ztrát a proto se vyplatí investovat do lepšího zabezpečení počítačové sítě, a sice ať už se jedná o metalickou nebo bezdrátovou síť. Obětí hackera se může v dnešní době stát každý z nás.

8 Závěr

Bakalářská práce úspěšně splnila všechny předem stanovené cíle a měla i praktický dopad díky kterému byla ve firemním prostředí zjištěna bezpečnostní trhlina, na kterou jsem vedení firmy upozornil a byla následně obratem opravena. Čtenář je seznámen se základním principem fungování bezdrátové sítě, s jejími výhodami a nevýhodami a potřebným zařízením pro provoz takové bezdrátové sítě. Hlavní část této práce je věnována problematice bezpečnosti bezdrátových sítí. Jsou zde popsány dostupné druhy zabezpečovacích mechanismů a jejich bezpečnostní slabiny. Také je tu uvedeno porovnání odolnosti proti útoku vedeném na bezpečnostní protokoly WEP, WPA a WPA2 a doporučení, který z těchto protokolů použít v domácí a podnikové bezdrátové síti. Několikrát na sobě byl proveden nezávislý průzkum za účelem zjištění jak jsou dnes Wi-Fi sítě zabezpečené. Z vyvozených závěrů je patrné, že stále můžeme narazit na bezdrátové sítě, které jsou nedostatečně zabezpečeny nebo u nich dokonce není použit žádný bezpečnostní prvek. Pro názornou představu byl v domácích podmínkách proveden útok na dnes již nedostatečně zabezpečený protokol WEP o síle šifrování 128bit. Jak je patrné z výsledků, tak do Wi-Fi sítě s tímto použitým zabezpečením se lze dostat během několika minut. Zároveň je zde poukázáno na nově objevenou bezpečnostní trhlinu a tím je funkce WPS, která měla zjednodušit někdy až složité nastavování u bezpečnostního protokolu WPA. Zneužitím této funkce se stává bezdrátová síť s dosud nejsilnějším zabezpečením WPA/WPA2 také snadno zranitelnou. Rovněž jsem se zaměřil na jednu větší firmu, která kromě klasické metalické počítačové sítě ve velké míře využívá právě bezdrátovou síť, kde ochrana citlivých interních dat a informací je jednou z hlavních priorit. Pod dohledem správce sítě bylo zkoumáním zjištěno, že zabezpečení této bezdrátové sítě není 100% a za použití určitých nástrojů může docházet k odposlouchávání datového provozu. Na tuto bezpečnostní hrozbu byl podnik upozorněn a po vzájemné diskuzi bylo upuštěno od zabezpečení pomocí filtrace MAC adres a bezdrátová síť byla zabezpečena silnějším bezpečnostním prvkem využívajícím protokol WPA2. Nutno podotknout, že podnik mým průzkumem ušetřil značné finanční prostředky, jelikož kdyby tyto penetrační testy prováděla nějaká najatá externí společnost, která se specializuje na bezpečnost počítačových sítí, tak by provádění těchto testů stálo značné finanční prostředky. Na

úplný závěr bych rád připomněl, že valná většina lidí stále používá krátká a jednoduchá hesla například ve formě srozumitelných slov jako jsou třeba jména osob. Tím pádem se i to nejlepší zabezpečení založené na takovém primitivním heslu stává snadno zranitelným při použití slovníkového útoku nebo útoku hrubou silou při použití krátkého hesla.

9 Seznam použité literatury

[1] PUŽMANOVÁ, Rita. *Bezpečnost bezdrátové komunikace*: *jak zabezpečit wi-fi, bluetooth, GPRS či 3G*. Vyd. 1. Brno: Computer Press, 2005, 179 s. ISBN 80-251-0791-4.

[2] BARKEN, Lee. *Wi-Fi*: *jak zabezpečit bezdrátovou síť*. Vyd. 1. Brno: Computer Press, 2004, 174 s. ISBN 80-251-0346-3.

[3] ZANDL, Patrick. *Bezdrátové sítě WiFi*: *praktický průvodce*. Vyd. 1. Brno: Computer Press, 2003, 190 s. ISBN 80-722-6632-2.

[4] IEEE 802.11. In: *Wikipedia*: *the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2012-04-18]. Dostupné z: http://cs.wikipedia.org/wiki/IEEE_802.11

[5] Hardware: Srovnání vybraných wireless technologií 2/2. [online]. [cit. 2012-04-18]. Dostupné z: http://pctuning.tyden.cz/hardware/site-a-internet/11182-srovnani_vybranych_wireless_technologii_22?start=1

[6] Slovníček pojmů. *Slovníček pojmů o WiFi, IEEE, zkratky a jejich popis* [online]. [cit. 2012-04-18]. Dostupné z: http://802.11b.cz/pojmy.asp

[7] IEEE 802.11ac. In: *Wikipedia*: *the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2012-04-18]. Dostupné z: http://en.wikipedia.org/wiki/IEEE_802.11ac

[8] IEEE 802.11g-2003. In: *Wikipedia*: *the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2012-04-18]. Dostupné z: http://en.wikipedia.org/wiki/IEEE_802.11g

[9] THOMAS, Thomas M. *Zabezpečení počítačových sítí bez předchozích znalostí*. Vyd. 1. Brno: CP Books, 2005, 338 s. ISBN 80-251-0417-6.

[10] ALT, Jakub. Hacktivismus. In: [online]. [cit. 2012-04-19]. Dostupné z: http://kisk.phil.muni.cz/wiki/Hacktivismus

[11] MAC adresa. In: *Wikipedia*: *the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2012-04-19]. Dostupné z: http://cs.wikipedia.org/wiki/MAC_adresa

[12] SSID. In: *Wikipedia*: *the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2012-04-19]. Dostupné z: http://cs.wikipedia.org/wiki/SSID

[13] Wi-Fi Protected Access. In: *Wikipedia*: *the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2012-04-19]. Dostupné z: http://cs.wikipedia.org/wiki/Wi-Fi_Protected_Access

[14] KRČMÁŘ, Petr. WPS má bezpečnostní trhlinu, PIN lze odhadnout. In: *Root.cz* [online]. [cit. 2012-04-19]. Dostupné z: http://www.root.cz/zpravicky/wps-ma-bezpecnostni-trhlinu-pin-lze-odhadnout/

[15] Bertiny lázně: O lázních. [online]. [cit. 2012-04-19]. Dostupné z: http://www.berta.cz/cz/nase-lazne/filozofie-firmy