UNIVERZITA PARDUBICE

FAKULTA ELEKTROTECHNIKY A INFORMATIKY

BAKALÁŘSKÁ PRÁCE

2017 Jiří Danielka

Univerzita Pardubice

Fakulta elektrotechniky a informatiky

Penetrační testování bezdrátových sítí

Jiří Danielka

Bakalářská práce

2017

Univerzita Pardubice
Fakulta elektrotechniky a informatiky
Akademický rok: **2016/2017**

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Jiří Danielka**
Osobní číslo:	**I14081**
Studijní program:	**B2646 Informační technologie**
Studijní obor:	**Informační technologie**
Název tématu:	**Penetrační testování bezdrátových sítí**
Zadávající katedra:	**Katedra informačních technologií**

Zásady pro vypracování:

Cílem bakalářské práce je ukázat a otestovat útoky používané pro získání přístupu do bezdrátové sítě s využitím nástroje KaLi Linux. V teoretické části práce budou popsány:
bezpečnostní standardy IEEE 802.11,
softwarové, hardwarové prostředky a terminologii používanou v penetračním testování,
skenovací nástroje.
Praktická část se zaměří na možnosti prolomení zabezpečení WEP, WPA, WPA 2 a WPS a Man-in-the-Middle útoků. Pro každé testování bude vypracován podrobný testovací scénář.

Rozsah grafických prací:

Rozsah pracovní zprávy: **40**

Forma zpracování bakalářské práce: **tištěná**

Seznam odborné literatury:

SAK, Brian a Jilumudi Raghu RAM. Mastering Kali Linux Wireless Pentesting. 1. BIRMINGHAM - MUMBAI: Packt Publishing, 2016. ISBN 978-1-78528-556-1.
Wi-Fi Alliance. Wi-Fi CERTIFIEDTM for Wi-Fi Protected Setup: Easing the User Experience for Home and Small Office Wi-Fi R Networks (2014) [online]. 2014 [cit. 2016-10-29]. Dostupné z URL: <http://www.wi-fi.org/downloads-registered/wp_Wi-Fi_CERTIFIED_Wi-Fi_Protected_Setup_20140409_0.pdf/Wi-Fi+CERTIFIED+Wi-Fi+Protected+Setup>

Vedoucí bakalářské práce: **Ing. Soňa Neradová, Ph.D.**
Katedra informačních technologií

Datum zadání bakalářské práce: **31. října 2016**

Termín odevzdání bakalářské práce: **12. května 2017**

Univerzita Pardubice Česká republika

L.S.

Ing. Zdeněk Němec, Ph.D.
děkan

Mgr. Josef Horálek, Ph.D.
vedoucí katedry

V Pardubicích dne 31. března 2017

Prohlášení autora

Prohlašuji, že jsem tuto práci vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny v seznamu použité literatury.

Byl jsem seznámen s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorský zákon, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Souhlasím s prezenčním zpřístupněním své práce v Univerzitní knihovně.

V Pardubicích dne 10. 04. 2017

Jiří Danielka

PODĚKOVÁNÍ

Rád bych poděkoval své vedoucí práce, Ing. Soně Neradové, za vstřícnost, ochotu a cenné rady, které mi poskytla v průběhu zpracování bakalářské práce. Dále bych chtěl poděkovat rodině a přátelům za podporu v průběhu studia.

ANOTACE

Bakalářská práce se zaměřuje na slabiny současných standardů zabezpečení bezdrátových sítí. V práci jsou popsány bezpečnostní standardy IEEE 802.11, pojmy používané při penetračním testování a potřebné hardwarové a softwarové prostředky. Jednotlivé bezpečnostní standardy jsou následně podrobeny sadám testů, které poukazují na jejich slabiny.

KLÍČOVÁ SLOVA

penetrační testování, WEP, WPA, WPS, Aircrack-ng

TITLE

Penetration testing wireless networks

ANNOTATION

Bachelor thesis focuses on the weaknesses of the current security standards for wireless networks. The paper describes the safety IEEE 802.11 standards, terms used in penetration testing and the necessary hardware and software resources. The security standards are then subjected to a test suites that highlight their weaknesses.

KEYWORDS

penetration testing, WEP, WPA, WPS, Aircrack-ng

OBSAH

SEZNAM ILUSTRACÍ A TABULEK

SEZNAM ZKRATEK A ZNAČEK

AES	Advanced Encryption Standard
ARP	Address Resolution Protocol
ASCII	American Standard Code for Information Interchange
BSSID	Basic service set identifier
CBC-MAC	Cipher Block Chaining Message Authentication Code
CCMP	Counter Mode CBC-MAC Protocol
CRC	Cyclic Redundancy Check
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DVD	Digital Versatile Disc
FCS	Frame Check Sequence
FMS	útok Fluhrera, Mantina a Šamira
FTP	File Transfer Protocol
GUI	Graphical User Interface
HMAC	Keyed-hash Message Authentication Code
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IEEE	Institute of Electrical and Electronics Engineers
IMAP	Internet Message Access Protocol
IP	Internet protocol
IV	Inicializační vektor
MAC	Media Access Control
MIC	Message Integrity Code

MTU	Maximum transmission unit
NFC	Near Field Communication
NIST	Národní institut pro standardy a technologie
PCI	Peripheral Component Interconnect
PID	Process Identifier
PIN	Personal Identification Number
POP	Post Office Protocol
PPP	Point-to-Point Protocol
PSK	Pre-Shared Key
QoS	Quality of Service
RADIUS	Remote Authentication Dial In User Service
RAM	Random Access Memory
RC4	Rivest Cipher 4
SHA-1	Secure Hash Algorithm 1
SSID	Service Set Identifier
TELNET	Teletype network
TKIP	Temporal Key Integrity Protocol
USB	Universal Serial Bus
WEP	Wired Equivalent Privacy
WPA	Wi-Fi Protected Access
WPS	Wi-Fi Protected Setup
XOR	eXclusive OR

ÚVOD

Bezdrátové sítě se těší stále větší popularitě. V posledních deseti letech si našly cestu do domácností, rozšiřují konektivitu ve firemním prostředí a jsou využívány ve veřejných prostranstvích. S jejich rozšířením se stále častěji skloňuje problematika jejich bezpečnosti, která hraje velmi důležitou roli. Uživatelé přenáší pomocí bezdrátových sítí velké objemy dat, které obsahují velké množství citlivých informací, které je možné zneužít pro páchání trestné činnosti. Nárůst objemu přenášených dat je dán způsoben vlastnictvím několika různých typů IT zařízení (notebook, tablet, pevný počítač, mobil). Většina uživatelů IT zařízení upřednostňuje vlastnosti, jako je mobilita a uživatelské pohodlí. V současnosti uživatelé vlastní několik počítačů, chytrých mobilních telefonů nebo tabletů umožňující velmi pohodlný způsob, jak tato zařízení připojit do sítě. Bezdrátový způsob komunikace přináší i četná rizika, která se nesmí přehlížet, a proto je nutné síť zabezpečit tak, aby do ní měli přístup jen oprávnění uživatelé.

Vhodným způsobem zabezpečení je použití bezpečnostních mechanismů, například WPA2, které zajistí, že se do sítě dostanou oprávnění uživatelé. Bohužel velké množství sítí je zabezpečeno velmi nevhodně, ať už se jedná o nepoužití žádných bezpečnostních mechanismů, nebo použití zastaralých standardů, jejichž prolomení je v dnešní době otázkou minut.

Podcenění bezpečnosti může mít za následek ztrátu soukromí nebo například v případě firemního prostředí újmu na zisku. Těmto situacím je dobré předcházet.

Tato práce se v první kapitole zaměřuje na základní pojmy, které se používají v rámci penetračního testování. Odborně provedené penetrační testování je schopno odhalit největší slabiny informačních systému, a proto jsou zde popsány jednotlivé fáze penetračního testování.

Druhá kapitole se práce zaměřuje na používané bezpečnostní standardy bezdrátových sítí. Jsou zde popsány jejich principy a slabá místa.

Třetí kapitola je zaměřena na použité hardwarové a softwarové vybavení.

Čtvrtá kapitola představuje základní skenovací nástroje, které se používají při provádění penetračních testů.

Praktická část práce se zaměřuje na prolomení zabezpečení bezdrátových sítí. Je zde představena sada postupů a nástrojů umožňující využít slabiny použitých bezpečnostních mechanismů.

1 PENETRAČNÍ TESTOVÁNÍ

Penetrační testy, zkráceně někdy nazývané pentesty, se používají k hodnocení zabezpečení informačních systémů. V rámci testování se tester snaží úmyslně pronikat do testovaného systému za účelem určení současného stavu zabezpečení daného informačního systému. (Weber, 2007)

Z této definice vyplývá, že penetrační testování je možné zařadit do skupiny tzv. etického hackingu. Etický hacking si klade za cíl zvýšit bezpečnost napadaného systému, protože jeho cílem není škodit, či krást, ale hledat potenciální slabá místa, která mohou být napravena. Etický hacker je tedy člověk, který disponuje potřebnými znalostmi, ale stojí na naší straně a pomáhám svým klientům udržovat systémy v bezpečí. (CENGAGE Learning, 2010)

V rámci penetračního testování se testuje nejenom technická stránka informačního systému, mezi kterou patří například nastavení systému nebo aktuálnost softwarového vybavení, ale také organizační opatření. Mezi organizační opatření se řadí například odolnost systém proti napadení od interního uživatele, který se může v rámci své pracovní pozice pokusit třeba o podvod.

Důležité je také zmínit, že mechanismus, který je v rámci provedených penetračních testů považován na bezpečný a neexistuje pro něj způsob, jak ho prolomit, tak není bezpečný navždy. Příkladem je symetrická šifra DES, která byla vyvinutá v 70. letech a byla později zvolena jako standard, který se používal k šifrování dat v civilních organizacích USA. Dnes je považována za silně neperspektivní a její 64bitový klíč je možné prolomit hrubou silou za méně než 24 hodin. Tato doba se s pokrokem v oblasti informačních technologií bude i nadále zkracovat, a proto je vhodné penetrační testy opakovat pravidelně a zahrnout je například do bezpečnostního auditu. Opakování by se také mělo provést po zásadní změně testovaného systému. (Selecký, 2012, s. 11-38; Weber, 2007; Piper, Murphy, 2006, s. 93-95)

Výstupem penetračního testování je závěrečná zpráva, která nám určuje, do jaké míry fungují současná bezpečnostní opatření, případně poukazuje na možné slabiny. Z této zprávy může vlastník systému určit, jaké škody by mu případné napadení mohlo způsobit a současně zpráva říká, jaká protiopatření můžeme aplikovat, aby rizika vzniku škod minimalizoval. (Selecký, 2012, s. 11-38)

1.1 Druhy testů

V rámci penetračního testování se rozlišuje několik druhů testů, které se liší podle způsobu provedení nebo podle úrovně znalostí, které o systému máme. V následujících odstavcích si představíme postupně:

- manuální testy,
- automatizované testy,
- semioautomatické testy,
- black-box testy,
- white-box testy,
- grey-box testy.

1.1.1 Manuální testy

Manuální testy, jak již název napovídá, vykonává tester na testovaném systému manuálně. To přináší velkou řadu výhod, ale i nevýhod.

Mezi výhody se řadí skutečnost, že člověk dokáže přistupovat k testovanému systému sofistikovaněji než automatické testy. Tím dojde k lepšímu prověření testovaného systému. Mezi další výhody můžeme zařadit i například fakt, že konkrétní osoba, která systém testovala, zná lépe podrobnosti testů a může i sobám, které se v oboru bezpečnosti neorientují, lépe vysvětlit, jaké nedostatky se v testovaném systému nachází a lépe prezentovat možné důsledky, které z těchto nedostatků plynou. (Selecký, 2012, s. 11-38)

K nevýhodám se řadí hlavně časová náročnost, protože je potřeba mít dokonalé znalosti o použitých technologiích nebo programovacích jazycích. Samotnou časovou náročnost podtrhuje fakt, že testy jsou vykonávané manuálně. (Selecký, 2012, s. 11-38)

1.1.2 Automatizované testy

Penetrační testy, které se provádějí automaticky, mají celou řadu výhod. Oproti manuálním testům, je zde výhodná časová náročnost, kterou testy spotřebují, protože je časově méně náročné se test naučit ovládat, než chápat důležité principy a ty následně umět aplikovat na testovaný systém. Mezi další výhody se řadí relativně snadná verifikovatelnost a reprodukovatelnost testů. (Selecký, 2012, s. 11-38)

Automatické testy mají celou řadu nevýhod. Obzvláště v porovnání s manuálními testy není možné dokonale pokrýt testované systémy. Důležité je poznamenat, že žádný z testovacích postupů nedokáže 100% pokrýt testované systémy, můžeme se maximálně dokonalému pokrytí přiblížit. Dále se výsledky testů hůře obhajují před zadavatelem, protože v některých případech

nemusí tester přesně vědět, jak testy fungují nebo chápat důležité principy, které využívají. (Selecký, 2012, s. 11-38)

1.1.3 Semioautomatické testy

Tato kategorie testů kombinuje předešlé dva způsoby provedení testů. Cílem této kategorie je minimalizace nevýhod použitých testů a maximalizace výhod. (Selecký, 2012, s. 11-38)

1.1.4 Black-box testy

Mezi nejpoužívanější způsob testování patří black-box testy. Tyto testy popisují útočníka, který zná pouze vstupy a výstupy do systému, vnitřní struktura systému je mu skryta. Pro určení vstupů a výstupů testů je často potřebný velmi rozsáhlý průzkum, jehož časová náročnost je závislá na rozsáhlosti systému. (Selecký, 2012, s. 11-38)

Aplikace těchto testů poskytuje celou řadu výhod. Základní výhoda vyplývá ze skryté vnitřní struktury samotného testovaného systému, protože tester nepotřebuje znalosti daného programovacího jazyka, ve kterém je systém napsán. Při využití tohoto způsobu odpadá také nutnost poskytnutí zdrojového kódu aplikace jiným osobám, než jsou jeho majitelé. Poslední výhodou je i vysoká variabilita testů, protože může dojít k otestování například jen některých vstupů nebo výstupů v systému. (Selecký, 2012, s. 11-38)

Black-box testy mají i několik nevýhod. V rámci testování není otestována efektivnost kódu. Další nevýhodou je, že tester nemusí objevit chyby, které vyžadují sofistikovanější přístup k systému, protože podmínkou pro úspěšnou aplikaci tohoto druhu testů jsou široké znalosti testera, které musí mít, aby dokázal podchytit veškeré variace vstupů a výstupů v testovaném systému. (Selecký, 2012, s. 11-38)

1.1.5 White-box testy

Tyto testy jsou pravý opak testům předcházejícím. V tomto případě zná tester kompletní kód aplikace a její architekturu, v případě testů kompletních systému, zná jejich architekturu a nastavení politik. Součástí testování je analýza zdrojového kódu, ve kterém se hledají chyby a kontroluje se i jeho efektivnost. (Selecký, 2012, s. 11-38)

Mezi výhody lze zařadit, že tester zkoumá kompletní aplikaci a její zdrojový kód. Při tomto výzkumu jsou opravovány chyby a současně může docházet k optimalizacím kódu. Současně, při kompletní znalosti systému probíhá hledání chyb rychleji a efektivněji, navíc dokážeme lépe pokrýt testovaný systém. (Selecký, 2012, s. 11-38)

K nevýhodám se řadí například vyšší cenová náročnost, protože v rozsáhlejších testovaných systémech může průzkum zdrojových kódů a architektury zabrat velké množství času. Současně cenovou náročnost zvyšují vyšší kvalifikační požadavky na testera, který musí znát použité programovací jazyky či technologie, ze kterých je systém postaven. (Selecký, 2012, s. 11-38)

1.1.6 Grey-box testy

Posledním typem testů jsou grey-box testy. Ty kombinují výhody white-box a black-box testů. V těchto testech se využívají znalosti architektury systému, které se pak dále aplikují při testech, které se provádí z hlediska potencionálního uživatele nebo útočníka. Někdy tyto testy obsahují prvky reverzního inženýrství, které se používá pro hodnocení míry informací, které jsou obsažené v chybových hláškách. (Selecký, 2012, s. 11-38)

1.2 Fáze penetračního testování

V problematice penetračního testování se můžeme setkat s nejrůznějším členěním průběhu testů. Nejčastěji se však uvádí následující čtyři fáze, které jsou uvedeny na obrázku 1:

Obrázek 1 − Fáze penetračního testování

Zdroj: vlastní

1.2.1 Stanovení cílů a rozsahu testování

Prvotní fáze penetračního testování zahrnuje stanovení cílů a rozsahu testů, které bude tester provádět. V prvé řadě je nutné stanovení hlavních cílů, které určují, který systém či aplikace bude testovaná, ale hlavně, na které části testovaného systému se zaměříme. Penetrační testy je možné například u aplikací zaměřit třeba jen na přihlašovací formulář či na data, která se vyměňují mezi klientem a serverem. (Selecký, 2012, s. 11-38)

1.2.2 Sběr dat

Po absolvování prvotní fáze, kdy určíme cíle, je potřeba získat maximum informací o testovaném systému. Množství informací bude závislé na zvoleném způsobu testování, protože v případě black-box testů budeme zjišťovat jiné podrobnosti o systému, než v případě white-box testů. Do sběru informací řadíme také například verze softwaru, který se používá na klientských stanicích či jiných informací, které souvisí s testovaným systémem. (Selecký, 2012, s. 11-38)

1.2.3 Skenování a exploitace

Třetí fáze obsahuje již samotné testování systému. Zde testujeme míru zabezpečení, snažíme se na základě prolamování bezpečnostních mechanismů získávat přístupy do testovaného systému, například do bezdrátových sítí, což bude nastíněné v dalších kapitolách této práce.

V oblasti informačních technologií nelze zaručit, že je aplikace či systém dokonale bezpečný. S postupem času, kdy se zvyšuje výpočetní výkon současných počítačů, je snazší prolamovat zabezpečení útoky hrubou silou. K nalezení nových potencionálně slabých míst používaných aplikací či technologií pomáhají také otevřené standardy, které jsou snadno dohledatelné. Každý tak do nich může nahlédnout a hledat slabá místa, které je možno využít. Většina těchto nálezu je následně zveřejněna a je možné jejich využití i v rámci této fáze penetračního testování. (Selecký, 2012, s. 11-38; Weber, 2007)

1.2.4 Vyhotovení závěrečné zprávy

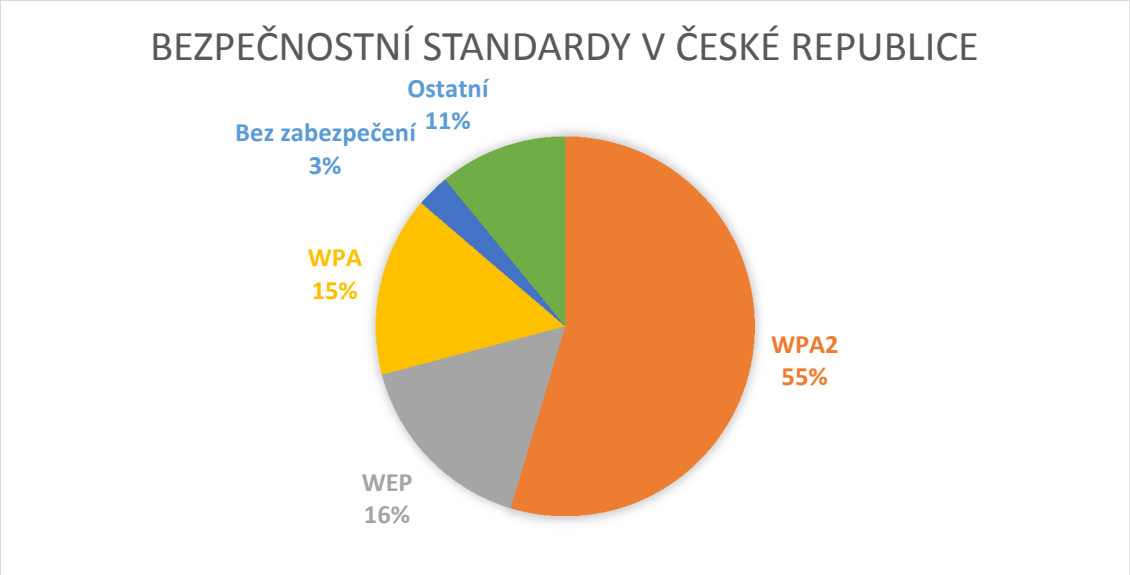
Poslední fází penetračního testování je sumarizace výsledků. Do závěrečné zprávy poznamená tester výsledky testů, poukáže na možná místa, která ohrožují testovaný systém. V závěrečné zprávě se také mohou objevit vysvětlivky, které slouží pro objasnění uvedených informací a použitých postupů. (Selecký, 2012, s. 11-38)

2 BEZPEČNOSTNÍ STANDARDY IEEE 802.11

Bezpečnostní standardy bezdrátových sítí jsou velmi důležité. Jelikož rádiové vlny se šíří i za přirozené hranice, například za zdi domů nebo hranice pozemků, je důležité je zabezpečit a chránit tak přenášená data před útočníky, kteří by je chtěli zneužít.

Existuje celá řada způsobu, jak bezdrátovou síť zabezpečit. Mezi poměrně slabá zabezpečení jako je skrytí SSID, jehož prolomení je otázkou vteřin až po poměrně robustní zabezpečení, které zajišťuje dodatek k IEEE 802.11i standardu, který je také známý pod zkratkou WPA2.

Současné rozložení zabezpečení bezdrátových sítí můžeme vidět na následujícím grafu. Z něho vyplývá, že více než polovina bezdrátových sítí využívá nejmodernější zabezpečení WPA2, ale je stále velké množství sítí, které používají prolomená zabezpečení WEP.



Obrázek 2 – Graf rozložení standardů zabezpečení

Zdroj: zpracováno dle (Čížek, 2017)

2.1 WEP

Zkratka WEP (Wired Equivalent Privacy) znamená v českém překladu: soukromí ekvivalentní drátovým sítím. Cílem tohoto bezpečnostního standardu bylo přinést do bezdrátových sítí zabezpečení, které je srovnatelné drátovým sítím. Bylo součástí původního standardu IEEE 802.11, který vyšel již v roce 1997. Bohužel, jelikož zabezpečení bylo šito na míru tehdejším zařízením, není moc složité a bylo již v roce 2001 prolomeno. Od této doby se objevují další typy útoků, které ho umí prolomit rychleji a efektivněji. (Šustr, 2009)

2.1.1 Charakteristika

Šifrování pomocí WEP probíhá na linkové vrstvě. K šifrování se používá proudová šifra RC4 a pro kontrolu integrity kontrolní součet CRC 32. Samotný šifrovací klíč může být použit v různých délkách. WEP64 používá 64bitový klíč, který se skládá z 40bitového klíče a 24bitového inicializačního vektoru. Analogická je situace u WEP128, kde se 128bitový klíč skládá z 104bitového klíče a 24bitového inicializačního vektoru. Existují ještě další varianty WEP zabezpečení, ale ty nejsou rozšířené. Mezi nimi můžeme jmenovat například WEPplus nebo WEP2. Za oficiálního nástupce lze považovat zabezpečení WPA, které odstraňuje řadu neduhů. (Šustr, 2009)

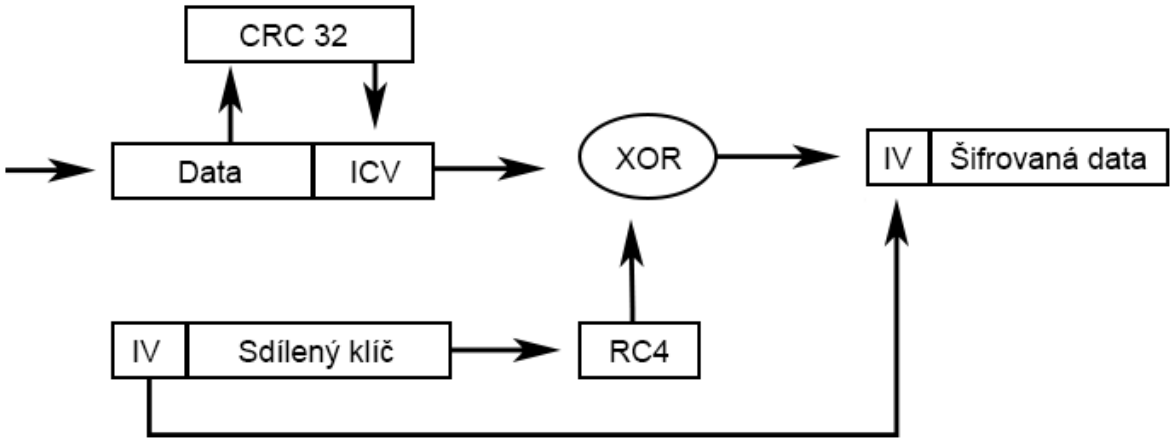
Samotný postup šifrování je velmi jednoduchý. Na vstupu se nachází data, ze kterých je nejdříve spočítán kontrolní součet pomocí hašovací funkce CRC 32, který slouží po dešifrování ke kontrole integrity dat. Hodnota kontrolního součtu je přiložena k datům, která jsou následně poslána na jeden vstup operace XOR. Druhým vstupem této operace je šifrovací klíč, který vznikne jako výstup algoritmu RC4. Do tohoto algoritmu přivádíme sdílený klíč, ke kterému přidáme inicializační vektor, který nám zajišťuje obměnu šifrovacího klíče v nezávislosti na ostatních datech. (Šustr, 2009)

Operace XOR nebo také exkluzivní disjunkce, je logická operace, při které je pravdivých hodnot dosahováno v případě, že jsou vstupy unikátní mezi sebou. Pro upřesnění tohoto tvrzení poslouží následující příklad. Na dvou vstupech, kdy na jednom je hodnota jedna a na druhém nula, je výstupem operace XOR pravda. V případě stejných hodnot na vstupech je hodnota nepravda. Více v následující tabulce:

Tabulka 1 − Operace XOR

A	B	Výstup
0	0	0
0	1	1
1	0	1
1	1	0

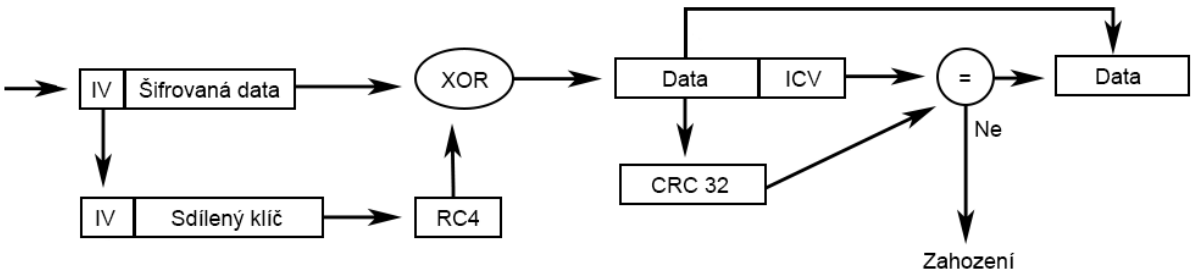
Výsledkem operace XOR jsou již šifrovaná data, která doplňuje inicializační vektor, který je přenášen bez šifrování. Vektor není šifrován, protože druhá strana, která bude provádět dešifrování dat, musí znát jeho hodnotu. (Šustr, 2009)



Obrázek 3 − Šifrování pomocí WEP

Zdroj: vlastní

Dešifrování později probíhá stejně jednoduše jako šifrování. Ze šifrovaných dat je nejdříve oddělen inicializační vektor, který je spolu se sdíleným klíčem přiveden na vstup šifrovacího algoritmu RC4. Výsledek tohoto algoritmu je přiveden na jeden vstup operace XOR. Druhým vstupem jsou samotná zašifrovaná data. Výstupem z operace XOR jsou již dešifrovaná data, u kterých je znovu spočítán kontrolní součet pomocí hašovací funkce CRC 32, který je porovnán s hodnotou, která byla přenesena spolu s daty. Pokud tyto hodnoty odpovídají, data jsou označena jako platná a jsou použita dále. V opačném případě došlo cestou mezi zařízením, která je šifrovala a zařízením, která jej dešifrovala, ke změně, a proto budou zahozena. Ke změně dat může dojít vícero způsoby, od prostého vlivu prostředí až po pokus o úmyslnou změnu, kterou by mohl někdo využít pro svůj prospěch. (Šustr, 2009)



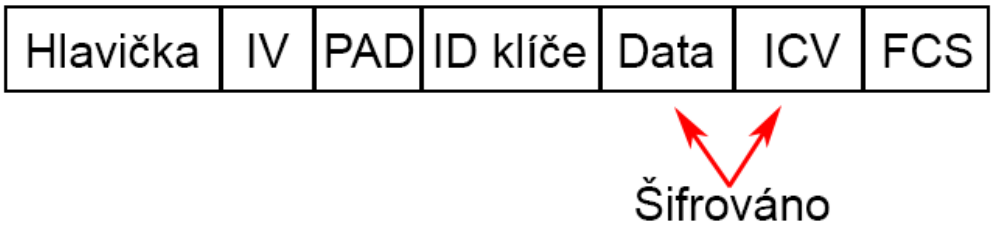
Obrázek 4 − Dešifrování WEP

Zdroj: vlastní

Data do rámce jsou poskládána velice jednoduše. Součástí hlavičky rámce jsou, jak úvodní informace, tak zdrojová a cílová adresa. Za úvodní části následuje konkrétní hodnota

o inicializačním vektoru. Tato hodnota má délku 3 bajty a není šifrována. Následuje část, která se stará o výběr klíče. Oblast PAD značí část, která je závislá na výběru klíče, je velká 6 bitů a na ní plynule navazuje ID klíče, které určuje konkrétní klíč. Tato hodnota je velká 2 bity, protože klíče mohou být maximálně čtyři. Tato část také není šifrována. (Šustr, 2009)

Následuje šifrovaná oblast, kde jsou přenášena samotná data. U nich je přiložen také kontrolní součet ICV, který je čtyři bajty velký. Součet je stejně jako data přenášen v zašifrované podobě. Na konci rámce se nachází kontrolní součet celého rámce, konkrétně zde označený jako FCS. (Šustr, 2009)



Obrázek 5 – Struktura rámce s WEP

Zdroj: vlastní

2.1.2 Slabá místa

Zabezpečení WEP obsahuje celou řadu chyb a nedostatků. Mez základní nedostatek můžeme označit použití statický klíčů, které se nemění. Použít je možné až 4 klíče, ale jediná proměnná část je inicializační vektor, který se velmi často opakuje, protože nabývá pouze 224 unikátních hodnot. Slabinu v nízkém počtu unikátních hodnot podtrhuje fakt, že vektor je přenášen v nezašifrované podobě spolu s šifrovanými daty. Současně je nedostatečné, že se používá stejný algoritmus na šifrování i autentifikaci. (Šustr, 2009)

Jako další nevýhodu můžeme označit i linearitu hašhovací funkce CRC 32, kterou lze obejít vhodnou záměnou bitů nebo skutečnost, že k šifrování kontrolního součtu dochází společně s daty. (Šustr, 2009)

Mezi další slabé místo můžeme zařadit použití šifrovacího algoritmu RC4, který zde byl použit hlavně pro svoji nenáročnost a snadnou implementaci. Dnes je tento algoritmus již zastaralý a neperspektivní, protože existuje celá řada mechanismů, jak ho prolomit. V současnosti je již na ústupu. (Piper, Murphy, 2006; Šustr, 2009)

2.1.3 Útok hrubou silou

Jedním z nejprimitivnějších útoku na WEP je útok hrubou silou. Tento útok využívá skutečnosti, že WEP64 má velmi krátkou délku klíče. Při délce klíče 40 bitů, tvoří klíč buď 5 znaků ASCII, nebo 10 hexadecimálních číslic. Tyto podmínky velmi zjednodušují útok hrubou silou, protože množství klíčů není velké a vyhledání klíče netrvá příliš dlouho. Obranou proti tomuto druhu útoku je použití delšího klíče, například WEP128, který má délku klíče 104 bitů, což znamená použití 13 znaků ASCII nebo 26 hexadecimálních číslic. (Šustr, 2009)

2.1.4 Injektace rámců

Injektace rámců nám sama o sobě šifrovací klíč neposkytne, ale může nám pomoci zlepšit podmínky pro jiné typy útoků. Každý zachycený rámec je možno poslat znovu, protože klíč je statický a inicializační vektor se může opakovat. Těchto podmínek se dá využít, protože jediné co je potřeba udělat, je změnit pořadové číslo rámce tzv. Sequence number v rámci. Po této úpravě může být rámec odeslán znovu, čímž můžeme zpomalovat tok dat v síti nebo naopak můžeme zvyšovat provoz, který následně zachytíme a využijeme ho k provedení jiných útoků, například FMS. (Šustr, 2009)

Obrana proti injektaci rámců v rámci standardu IEEE, který obsahuje část o zabezpečení WEP, není. Některá zařízení proti tomuto útoku bojují malou vyrovnávací pamětí, do které si ukládají poslední rámce a v případě, že se opakuje velké množství inicializačních vektorů, tak rámce ignorují. (Šustr, 2009)

2.1.5 Fragmentační útok

Princip tohoto útoku spočívá ve spojování rámců přístupovým bodem. V případě, kdy je tento princip využit, zvolíme vlastní proud dat, která jsou šifrována pomocí RC4 šifry a inicializační vektor. Tento proud je rozdělen na několik fragmentů a vyslán spolu s inicializačním vektorem k přístupovému bodu. Ten využije vlastnosti, že fragmentované rámce poskládá do jednoho, maximálně však do délky MTU, znovu zašifruje, v tomto případě využije znovu inicializační vektor, a odešle složený rámec zpět. Útočník takto získá výhodu, protože text, který odeslal na přístupový bod v rámci fragmentů, sám určil a stejně tak zná inicializační vektor a díky tomu získá nový a delší proud dat, který je zašifrován pomocí RC4. (Bittau, 2005)

2.1.6 FMS útok

Útok FMS, který byl představen v roce 2001, využívá vlastnosti algoritmu RC4, která v určitém případě přenese první bajt vstupního proudu do prvého bajtu výstupního proudu. Jelikož na vstupu bývají jako první bajty inicializační vektory, tak vektory, které trpí touto vlastností,

nazýváme slabé inicializační vektory. Na základě vytvořených dvojic slabých vektorů a prvních bajtů, které vytvoří algoritmus RC4, je možné statisticky dohledat šifrovací klíč. (Fluhrer, Mantin, Shamir, 2001)

Tato metoda je velmi populární, a proto ji využívá řada nástrojů jako Aircrack-ng nebo Airsnort. Obranou proti tomuto útoku je například vynechání slabých inicializačních vektorů. Tuto techniku používá vylepšené zabezpečení WEPplus. Další možností je změna zabezpečení na WPA, které používá techniku TKIP, která využívá tzv. silné inicializační vektory. (Šustr, 2009; Fluhrer, Mantin, Shamir, 2001)

2.1.7 Kleinův útok

Tento typ útoku potřebuje pro získání šifrovacího klíče znát prvních 16 bajtů nešifrovaného textu. Tyto data je možné získat například u ARP rámců, které jsou až do 16 bajtu stejné, na 16 pozici se liší pouze podle toho, jestli se jedná o dotaz či o odpověď. Tento 16 bajt je možné snadno odhadnout podle MAC adres. Když je tato podmínka prvních 16 bajtů splněna, je možné získat šifrovací klíč ze 40 000 nasbíraných ARP rámců s pravděpodobností 50% a při nasbírání 85 000 ARP rámců je možné získat klíč s pravděpodobností 95%. Obrana proti Klenovu útoku je pouze přechod na WPA a WPA2, které Kleinův útok neumožnují. (Šustr, 2009)

2.2 WPA

Zabezpečení WPA je nástupce zabezpečení WEP, které bylo prolomeno. V reakci na tuto událost vydala Wi-Fi Alliance v roce 2002 zabezpečení WPA, které bylo součástí tehdy připravovaného standardu IEEE 802.11i. (Sak, Raghu, 2014, s. 83-87)

2.2.1 Charakteristika

WPA používá protokol TKIP, který byl navržen tak, aby ho bylo možné provozovat na starých zařízeních, která podporovala WEP. Tento protokol na rozdíl od svého předchůdce obsahuje celou řadu vylepšení, která ho činní bezpečnějším. Protokol stále pracuje s šifrovacím algoritmem RC4, ale použitý klíč se zde pravidelně každých 10 000 paketů mění. Současně je zde použit delší inicializační vektor, který má délku 48 bitů. Vylepšená byla také kontrola integrity rámce, kterou vedle lineární funkce CRC 32 zajišťuje také funkce MIC. Tento algoritmus obsahuje přímo v sobě počítadlo rámců, takže je znemožněna injektace rámců, kterou známe z WEP. (Sak, Raghu, 2014, s. 83-91; Held, 2003, s. 220-222)

Tabulka 2 − Porovnání zabezpečení

Vlastnost	WEP	WPA
Klíč	40 bit, 104 bit	128 bit
Inicializační vektor	24 bit	48 bit
Druh klíče	Statický	Dynamický
Šifrovací algoritmus	RC4	RC4

Zdroj: zpracováno dle (Rackley, 2007, s. 213)

Ovšem i TKIP má své slabiny, hlavně v použitém RC4 algoritmu, a proto není doporučeno ho dnes používat. Jsou známé útoky, které dokáží ve specifických případech zabezpečení prolomit, a proto je vhodné použít vylepšenou variantu WPA s algoritmem AES, která není příliš rozšířená, nebo nástupce WPA2, které používá AES ve výchozím stavu. (Held, 2003, s. 220-222; RACKLEY, 2007, s. 212-216)

Autentizace klienta může být zabezpečena buď pomocí předsdíleného klíče, zkráceně PSK, nebo pomocí autentizačního serveru podle protokolu IEEE 802.1x. Tímto serverem bývá typicky RADIUS. PSK je vhodné použít v domácnostech nebo v malých kancelářích, protože nevyžaduje dodatečnou infrastrukturu jako standard IEEE 802.1X. Délka hesla je v rámci PSK 8 až 63 ASCII znaků nebo 64 hexadecimálních číslic. (Held, 2003, s. 220-222)

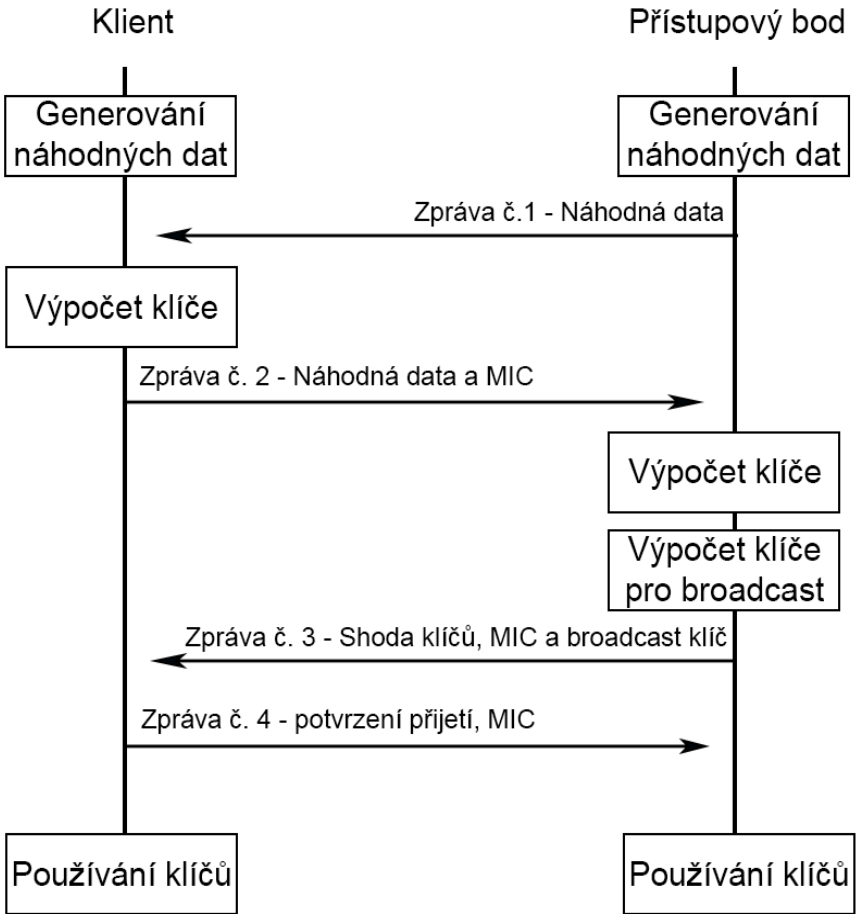
Výměna šifrovacích klíčů je při použití WPA zajištěna za pomocí výměny čtyř zpráv, tzv. čtyřcestného handshaku. Během tohoto procesu se přístupový bod a klient domluví na šifrovacích klíčích a hlavně ověří, že obě strany používají stejné klíče. (Novák, 2017)

Princip čtyřcestného handshaku je velmi jednoduchý. V první fázi si klient a přístupový bod vygenerují 32 bajtů náhodných dat. Obsahem první zprávy jsou náhodná data, která vygeneroval přístupový bod. Tato zpráva je odeslána klientovy, který tímto má všech pět složek pro výpočet šifrovacího klíče. Tento klíč se skládá z PSK, které je spočítané pomocí SSID a hesla, které zadal uživatel. Další složkou klíče jsou náhodná data, která přístupový bod odeslal klientovi spolu s daty, která vygeneroval sám klient. Poslední dvě složky jsou fyzické adresy, jak klientova bezdrátového adaptéru, tak přístupového bodu. (Novák, 2017)

Výpočet klíče proběhne jednoduše, všechny výše jmenované složky jsou vložené do pseudonáhodné funkce, která využívá HMAC-SHA1. Výsledkem této funkce je 48 bajtů dlouhý šifrovací klíč. (Novák, 2017)

Ve druhé zprávě probíhá vše analogicky, jediným rozdílem je, že příjemcem dat je přístupový bod. Ten následně vygeneruje totožným postupem šifrovací klíč. Současně s náhodnými daty posílá klient hodnotu funkce MIC, pomocí které přístupový bod ověří, že vygenerované šifrovací klíče se rovnají na obou stranách. (Novák, 2017)

Obsahem třetí zprávy je následně jiný šifrovací klíč, který se používá pro šifrování skupinového a všesměrového provozu. K tomuto klíči je opět přiložena hodnota MIC, která slouží pro ověření na straně klienta, že přístupový bod používá stejný šifrovací klíč. Po přijetí této zprávy následně klient zasílá jen potvrzení zpět, které je zase doprovázeno hodnotou MIC. Tímto celý proces výměny zpráv končí. (Novák, 2017)



Obrázek 6 − Proces výměny zpráv

Zdroj: vlastní

V průběhu celého čtyřcestného handshaku nedochází k přenosu hesla k bezdrátové síti ani vygenerovaného šifrovacího klíče. To zvyšuje bezpečnost, ovšem má to i nevýhody, přístupový bod si musí pamatovat více šifrovacích klíčů, protože jsou unikátní pro každého klienta. (Novák, 2017)

2.2.2 Útoky

V současné době jsou známé dva druhy útoků na WPA. Jedním z nich je klasický slovníkový útok, kdy po zachycení handshaku se útočník snaží získat heslo pomocí slovníků, pomocí kterých zkouší určité kombinace. Tento útok je bohužel časově náročný a v případě použití silného hesla, které může být například složeno z více slov nebo používá speciální znaky, je téměř nemožné ho odhalit. (Sak, Raghu, 2014, s. 83-87)

Mezi další typ útoku patří tkiptun, který nám neumožní získat přístupový klíč, ale umožní nám injektaci několika rámců. Bohužel jeho použití je velmi obtížné, protože je zapotřebí splnění specifických podmínek, mezi které patří podpora QoS a nebo změna klíče pomocí TKIP musí probíhat alespoň 20 minut. (airdump.cz, 2009)

2.3 WPA2

WPA2 se od svého předchůdce příliš neliší. Jedná se o plnohodnotnou implementaci standardu IEEE 802.11i. Od roku 2006 je toto zabezpečení povinné pro všechny zařízení, která chtějí být certifikována jako Wi-Fi. (Sak, Raghu, 2014, s. 83-91)

2.3.1 Charakteristika

WPA2 používá vylepšený protokol CCMP, jehož hlavní silnou stránkou je použití symetrického šifrovacího algoritmu AES, který zde nahrazuje zastaralý algoritmus RC4 známý z protokolu TKIP. (Sak, Raghu, 2014, s. 83-91)

Algoritmus AES vzešel z výběrového řízení, které nařídil NIST v roce 2001. Jeho cílem bylo najít vhodný šifrovací symetrický algoritmus, který by měl minimální délku klíče 128 bitů, ale podporoval by i delší, například 192 či 256 bitů. Požadavek na minimální délku klíče zaručuje odolnost algoritmu proti útokům hrubou silou. V současnosti je tento algoritmus považovaný za bezpečný a již téměř vytlačil předchozí standardní algoritmus DES nebo jeho dočasnou bezpečnější variantu 3DES. (Piper, Murphy, 2006, s. 94)

2.3.2 Útoky

Zabezpečení WPA2 je v současné době považované za nejbezpečnější způsob, jak ochránit bezdrátovou síť. Je totiž znám jen jeden druh útoků a to jen slovníkový útok, který je velmi časově náročný. Opakuje se zde situace známá ze zabezpečení WPA, kde je také minimální délka klíče 8 znaků ASCII a maximální až 63 znaků ASCII. Za této situace by útok hrubou silou trval příliš dlouho a jediná možnost je použít vhodný slovník, který by mohl dané heslo

obsahovat. Bohužel i tak se nemusí v případě silného hesla podařit hledaný klíč najít a útok skončí neúspěchem. (Sak, Raghu, 2014, s. 83-91)

2.4 WPS

WPS je bezpečnostní standard, který byl navržen Wi-Fi aliancí v roce 2003. Jeho hlavním přínosem mělo být zjednodušení připojení klientů do bezdrátové sítě. Myšlenkou tohoto standardu je, že si uživatel přinese domů zařízení, který má nastavené silné heslo a vhodné zabezpečení, například WPA2. Toto zařízení následně připojí k elektrické síti a internetu a je nastaveno. Ostatní zařízení připojí do sítě pomocí WPS. (Hruška, 2012; Wi-Fi Alliance, 2014)

2.4.1 Charakteristika

Zařízení se do sítě připojují několika způsoby. Nejjednodušší je stisk WPS tlačítka přímo na přístupovém bodě, které aktivuje speciální režim, který připojí po omezenou dobu (typicky tři minuty) všechna zařízení, která o připojení zažádají. Druhým způsobem je zadání osmimístného PIN kódu, který se musí shodovat s tím, který je v zařízení nastaven. Mezi další způsoby můžeme zařadit přiblížení zařízení a následný přenos potřebných údajů pomocí technologie NFC nebo pomocí USB zařízení. V praxi se ovšem nejčastěji setkáme s prvními dvěma způsoby. (Hruška, 2012; Wi-Fi Alliance, 2014)

Ve chvíli, kdy klient zažádá o připojení pomocí WPS například pomocí PIN kódu, tak dojde k ověření tohoto kódu, a pokud je PIN kód přijat, tak se ke klientovy přenese klíč a potřebné údaje o síti, mezi které patří například typ zabezpečení. (Sak, Raghu, 2014, s. 96-99; Hruška, 2012)

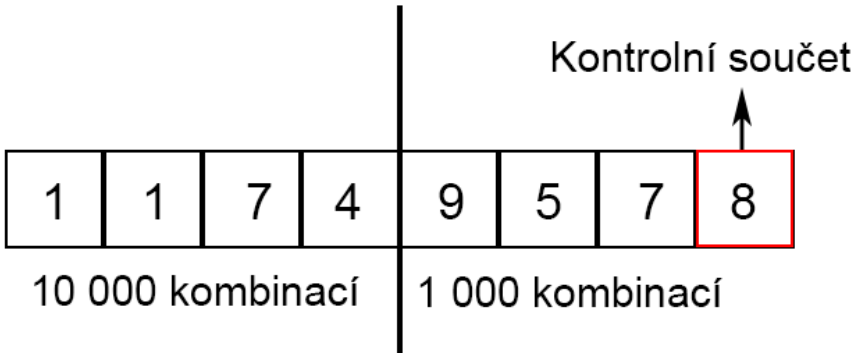
2.4.2 Útoky

Hlavní slabina technologie WPS se skrývá v procesu připojování pomocí PIN kódu. První vážnou chybou je, že některé domácí routery dovolují zkoušet PIN s neomezeně pokusy. Tento stav vede k možnosti prolomení pomocí útoku hrubou silou. V současné době se tento problém týká pouze starších zařízení. Pro nová zařízení a některá starší výrobci zjednali nápravu pomocí nových firmwarů, které nedovolí například více než tři pokusy za minutu. Druhou možností je technologii WPS na zařízení vypnout a nepoužívat ji. (Hruška, 2012)

Problémem je, že i tento počet může stačit. WPS sice používá osmimístné číslo, které znamená 10^8 kombinací, ale současně při pokusu o připojení zašle zpět informaci, jestli útočník trefil, buď první čtyři čísla pinu, nebo druhá čtyři čísla. To počet kombinací snižuje. V útoku dále

pomáhá i fakt, že poslední číslo z osmimístného pinu tvoří kontrolní součet. To dále snižuje počet kombinací, a proto je použití technologie WPS velmi nebezpečné. (Hruška, 2012)

V celkovém součtu tedy potřebujeme až 10^4 pokusů pro uhodnutí první části pinu a následně 10^3 pokusů k uhodnutí části druhé. Celkem je tedy potřeba 11 000 pokusů na projití a nalezení PINu, což u routeru, který nemá omezený počet pokusů, znamená při frekvenci jeden pin za tři sekundy maximálně 9 hodin. Po tomto čase má útočník heslo do sítě, která je zabezpečená nejmodernějším zabezpečením WPA2, ale doplatila na slabinu WPS. (Hruška, 2012)



Obrázek 7 – Možné kombinace WPS PINu

Zdroj: vlastní

V případě, že zařízení disponuje omezením na počet PINů, dostává se útočník přibližně na maximální čas 60 hodin.

3 POUŽITÉ PROSTŘEDKY

3.1 Hardwarové prostředky

K provádění penetračních testů bezdrátových sítí je potřeba mít odpovídající hardwarové vybavení. U sítové Wi-Fi karty je nutné, aby její firmware podporovala monitorovací režim a nejlépe, aby uměla injektaci paketů. Pro účely této práce byla vybrána USB Wi-Fi karta TP-Link TL-WN722, která výše uvedené splňuje.[1] Wi-Fi adaptér podporuje standardy 802.11bgn a pro lepší příjem disponuje odnímatelnou 4 dBi anténou. S cenou okolo 300Kč se jedná o levné a snadno dostupné zařízení. (TP-Link, 2017)

Obrázek 8 − USB Wi-Fi adaptér TP-Link

Zdroj: zpracováno dle (TP-Link, 2017)

Wi-Fi adaptér byl následně použit na dnes již spíše starším notebooku Lenovo ThinkPad T61, který disponuje 4GB RAM paměti, procesorem Intel Core2 Duo T7700 o taktu 2.4 GHz klasickým plotnovým diskem o kapacitě 500GB. Současně s USB Wi-fi adaptérem byl používán integrovaný PCI Express Wi-Fi adaptér Intel PRO/Wireless 4965agn, který sloužil ke generování provozu při pokusech o prolomení testovaných bezpečnostních standardů. Pro tento účel sloužil střídavě i mobilní telefon BlackBerry Passport. Na tomto notebooku bylo nainstalované také potřebné softwarové vybavení, které bude rozebráno v následujících kapitolách.

Poslední součástí hardwarového vybavení byl bezdrátový router ASUS RT-N10U, který disponuje podporou standardů IEEE 802.1bgn, což znamená podporu zabezpečení od WEP

[1] https://www.aircrack-ng.org/doku.php?id=compatibility_drivers

po WPA2, včetně WPS. Tento router současně se svoji pořizovací cenou okolo 600Kč reprezentuje standardní vybavení průměrné domácnosti.

3.2 Softwarové prostředky

Jako softwarové vybavení notebooku byla zvolena speciální linuxová distribuce Kali Linux, která vychází z Debianu. Kali Linux se zaměřuje na bezpečnost, penetrační testování a forenzní analýzy. Díky tomu obsahuje vše potřebné pro penetrační testování bezdrátových sítí. V současnosti nahrazuje svého předchůdce, distribuci BackTrack, která již není dále aktivně vyvíjena. (Kali, 2017)

Mezi minimální požadavky této distribuce se řadí 10GB volného místa na disku a minimálně 512MB RAM jak pro verzi i386, tak pro verzi AMD64. Samotnou distribuci ani nemusíme instalovat. Je možné ji spustit pomocí spustitelného DVD nebo USB flash disku. (Kali, 2017)

Obrázek 9 – Prostředí GNOME Kali Linux 2016.2

Zdroj: vlastní

Pro potřeby této práce byla použita v té době poslední verze 2016.2, která vyšla 31. srpna 2016 a je volně ke stažení.[2]

[2] https://www.kali.org/downloads/

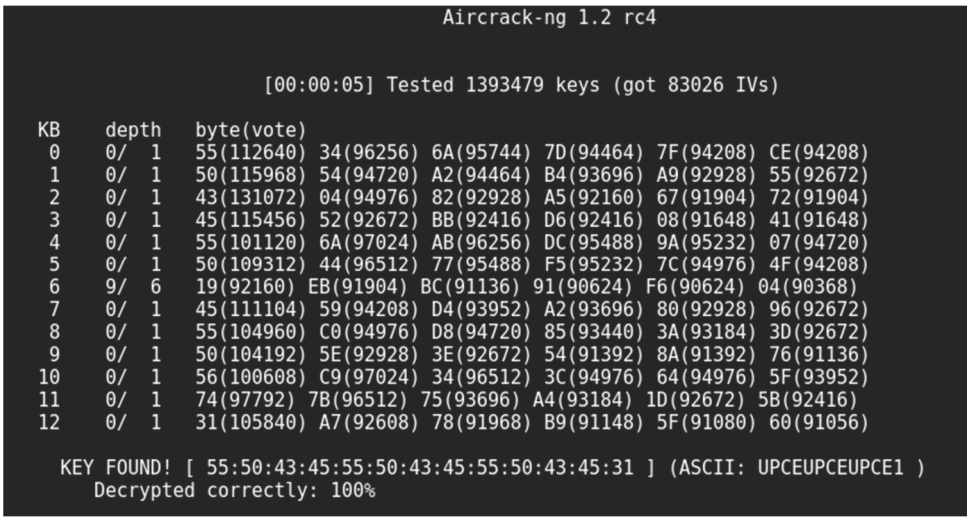
4 SKENOVACÍ NÁSTROJE

4.1 Aircrack-ng

Balíček nástrojů Aircrack-ng obsahuje nástroje, které se soustředí na testování Wi-Fi sítí, převážně se zabezpečením WEP a WPA. V současnosti existuje ve verzi 1.2-rc4, která vyšla v únoru 2016. Samotný balík existuje v předkompilovaných verzích pro Windows a Linux nebo je součástí distribuce, jako je tomu v případě Kali Linuxu. (Aircrack-ng, 2017)

4.1.1 Aircrack-ng

Hlavním nástrojem v balíku je Aircrack-ng. Ten nám slouží k zjištění šifrovacího klíče u WEP pomocí slovníkového útoku nebo útoku FMS. U zabezpečení WPA a WPA2 je možné použít pouze slovníkový útok. Pomocí tohoto nástroje dostaneme v případě úspěšného útoku šifrovací klíč ve dvou podobách, hexadecimální a pomocí ASCII kódu. V některých případech není možné ASCII přepis zobrazit, a proto zobrazí Aircrack-ng jen hexadecimální variantu. (Aircrack-ng, 2017)



Obrázek 10 − Rozluštěný klíč WEP128 pomocí Aircrack-ng

Zdroj: vlastní

4.1.2 Airodump-ng

Dalším z nástrojů je Airodump-ng, který slouží k odchytávání provozu, který následně ukládá do souborů, které můžeme použít v jiných nástrojích balíků Aircrack-ng nebo třeba v programu Wireshark, kde následně po rozšifrování dat pomocí nástroje Airdecap-ng můžeme vidět proběhlou komunikaci a zjišťovat další informace, například hesla přenášená pomocí nezabezpečené varianty protokolu HTTP.(Aircrack-ng, 2017)

Dále zde najdeme podrobné informace o nalezených sítích:

```
CH  5 ][ Elapsed: 14 mins ][ 2017-02-03 22:49

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

C8:60:00:72:80:B4  -28 100     8582    83026    0   5  54e. WEP  WEP         Pokus2017

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

C8:60:00:72:80:B4  00:1F:3B:36:86:CB  -24   54e-48e     1    84412
```

Obrázek 11 − Podrobnosti o síti v Airodump-ng

Zdroj: vlastní

kde,

BSSID – je fyzická adresa přístupového bodu,

PWR – síla signálu, kterou získává program z ovladačů sítové karty,

RXQ – procentuální hodnota zachycených paketů,

Beacons - počet paketů, které přístupový bod odesílá o své existenci,

#Data – počet zachycených datových rámců, u WEP počet unikátních IV,

#/s – průměrný počet rámců, měřeno za posledních 10 sekund,

CH – číslo kanálu, kde přístupový bod vysílá,

MB – maximální rychlost, kterou přístupový bod podporuje,

ENC – použitý šifrovací algoritmus, například WEP, WPA nebo WPA2,

CIPHER – upřesnění šifrovacího algoritmu, například CCMP nebo TKIP,

AUTH – protokol, použitý pro ověření, například PSK,

ESSID – název bezdrátové sítě.

Ve spodní části výpisu najdeme informace o připojených stanicích, kde nalezneme informace o jejich fyzické adrese nebo například o počtu rámců odeslaných klientem. (Aircrack-ng, 2017; Selecký, 2012, s. 167-170)

4.1.3 Ostatní nástroje

Mezi další nástroje můžeme zařadit například Airmon-ng, který přepíná Wi-Fi adaptér do monitorovacího režimu nebo nástroj Aireplay-ng, který slouží k injektaci paketů. Dalším

zajímavým nástrojem je tkiptun-ng, který slouží k provedení stejnojmenného útoku na WPA. (Aircrack-ng, 2017)

4.2 Wifite

Wifite je utilita, který se snaží za pomoci programovacího jazyku Python zautomatizovat a zjednodušit lámání zabezpečení Wi-Fi sítí. Program sám přepne Wi-Fi adaptér do sledovacího módu, následně provede skenování okolí a zjistí podrobnosti o bezdrátových sítích. Dokáže současně detekovat zapnuté WPS nebo přítomnost klientů na přístupovém bodu.

Po zvolení cíle, na který se bude útočit, Wifite samo určí vhodné útoky a celý proces následně běží automaticky. Pokud je útok úspěšný, tak nakonec vypíše heslo. Programu tedy stačí pouhé dva vstupy od uživatele, a to výběr zařízení a cíle. Odpadá zdlouhavé zadávání příkazů či přepisovaní údajů z výstupů různých nástrojů.

Aktuálně je k dispozici verze 2 revize 87, která je součástí distribuce Kali Linux.

Obrázek 12 – Úvodní obrazovka Wifite

Zdroj: vlastní

4.3 Wireshark

Wireshark je analyzér sítových protokolů. Pomocí jeho funkcionalit můžeme vidět, jaká data proudí sítí nebo jaké verze protokolů se používají. Sběr těchto informací se využívá například při penetračním testování. Wireshark je v základní variante GUI aplikace, ale existuje i varianta TShark, která funguje v rámci terminálu. (Lamping, Sharpe, Warnicke, 2014)

Využití Wiresharku je velmi široké. Od verze 1.4 umí přepínat Wi-Fi adaptéry do monitorovacího módu, což ho předurčuje pro použití i pro penetrační testování bezdrátových sítí. Zachytávat ale může velké množství typů sítí jako například Ethernet, PPP nebo loopback. (Lamping, Sharpe, Warnicke, 2014)

Hlavní výhody Wiresharku spočívají v širokých možnostech filtrování zachycených paketů. Pomocí různých filtrů je možné soustředit pozornost na konkrétní protokoly, cílové adresy, porty nebo služby. Následně je možné zkoumat i obsah přenášených dat, a to i zpětně, protože se veškerý zachycený provoz může uložit do souboru. Díky tomu může Wireshark odhalit nežádoucí provoz na síti v podobě používání zastaralých nebo nezabezpečených protokolů.

V současnosti je program dostupný jak pro Windows, tak pro Linuxové systémy a je i součástí distribuce Kali Linux. (Lamping, Sharpe, Warnicke, 2014)

4.4 Wash

Program Wash je jednoduchý skenovací nástroj, který slouží k nalezení přístupových bodů, které mají aktivní WPS. Tento nástroj potřebuje pro svoji činnost aktivní monitorovací režim na Wi-Fi adaptéru. Součástí zobrazení je kromě názvu bezdrátové sítě a fyzické adresy přístupového bod, také informace o kanálu, kde přístupový bod vysílá a o verzi WPS, která je aktivní.

Nástroj Wash je součástí balíku Reaver, který slouží k prolamování sítí pomocí WPS. Je součástí distribuce Kali Linux.

```
root@Nikdo-PC:~# wash -i wlan1mon

Wash v1.5.2 WiFi Protected Setup Scan Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetsol.com>
mod by t6_x <t6_x@hotmail.com> & DataHead & Soxrok2212

BSSID                 Channel       RSSI       WPS Version       WPS Locked        ESSID
---------------------------------------------------------------------------------------------
[redacted]            1             00         1.0               No                D[redacted]
[redacted]            3             00         1.0               No                W[redacted]
C8:60:00:72:80:B4     5             00         1.0               No                Pokus2017
```

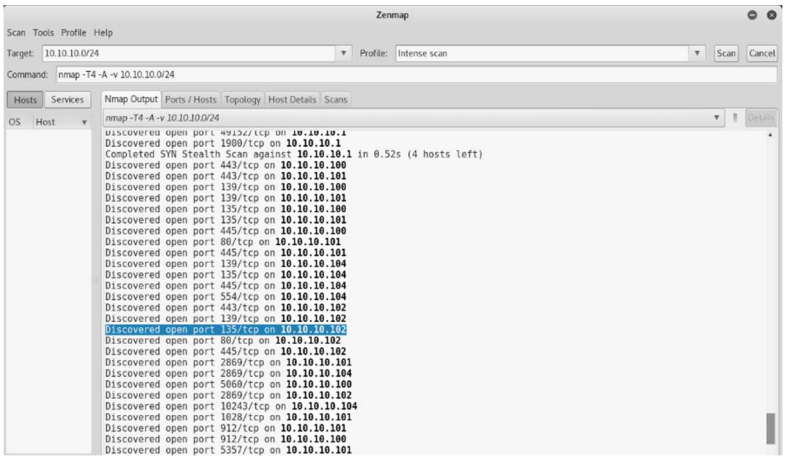
Obrázek 13 − Přehled aktivních zařízení s WPS

Zdroj: vlastní

4.5 Nmap

Nmap je skener portů, který dokáže zjistiti přítomnost hostitelských počítačů a služeb v počítačové síti. Hlavní funkce skeneru spočívá v odesílání upravených paketů, kde u jejich odpovědí následně dochází k analýzám, které je vyhodnotí. V současnosti jsou analýzy velmi rozsáhlé a je možné díky nim zjistit, jaké porty má hostitelský počítač otevřené porty nebo v případě rozsáhlejších analýz například získat informace o používaném operačním systému cílového zařízení, verze služeb, které poslouchají nebo například přítomnost firewallu. (Nmap, 2016)

Nmap má i grafické nástavby, například je možné jmenovat Zenmap, který usnadňuje použití a umí i lépe zobrazit výsledky než konzolová verze Nmapu.



Obrázek 14 – Zenmap

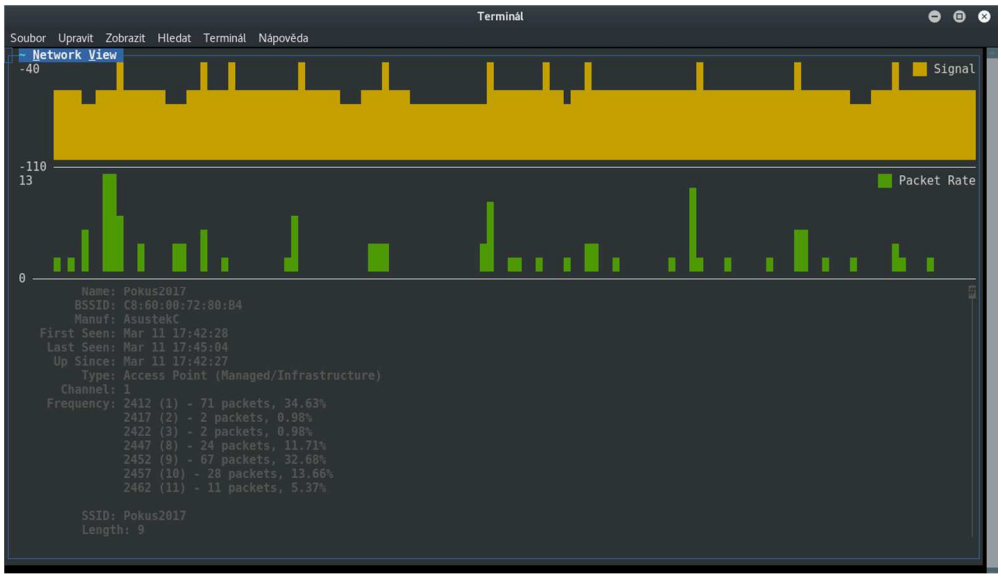
Zdroj: vlastní

Ve verzi 7.30 je součástí distribuce Kali Linux, včetně grafické nástavby Zenmap.

4.6 Kismet

Jedná se o detektor bezdrátových sítí, který pracuje v prostředí terminálu. Dokáže pracovat s Wi-Fi adaptéry, které mají podporu pro monitorovací mód. Zvládá zkoumat provoz ve standardech 802.11abgn, v závislosti na použitém adaptéru a jeho ovladačích. V současnosti podporuje i několik přídavných modulů, které umožňují pracovat i mimo standardy 802.11. (Kershaw, 2016)

Kismet pracuje pasivně. Pomocí sběru rámců dokáže detekovat sítě, u kterých následně zobrazí podrobnosti, podobně jako například Airodump-ng. Současně zvládá zobrazit skryté sítě a to i dokonce takové, které nevysílají beacon rámce. Tyto sítě odhalí pomocí provozu, který probíhá mezi přístupovým bodem a komunikujícím zařízením. (Kershaw, 2016)



Obrázek 15 – Kismet, údaje o přístupovém bodu

Zdroj: vlastní

4.7 Ettercap

Tento nástroj umí skenovat síť a následně zde provádět Man in the middle útoky, například ARP spoofing nebo DHCP spoofing. Jeho využití je široké, protože současně umí odposlouchávat speciální pakety, kde proudí hesla k jednotlivým službám jako je POP, IMAP, TELNET, FTP, HTTP a jiné. (Sak, Raghu, 2014, s. 114-115)

Jedná se o volně dostupný nástroj, který existuje v konzolové i grafické variantě. Je součástí Kali Linuxu, kde je přeinstalován s větším množstvím užitečných zásuvných modulů.

5 POSTUPY PENETRAČNÍHO TESTOVÁNÍ

5.1 WEP

První část práce je zaměřena na praktické prolomení zabezpečení bezdrátové sítě, která používá WEP. V současné době existující nástroje umožňující za specifických podmínek prolomit síť v řádu desítek sekund.

5.1.1 WEP64

Postup prolomení sítě s WEP64 je velmi jednoduchý. V následující části se používá balík nástrojů Aircrack-ng a síťová karta TP-Link. Pro generování provozu byl použit chytrý mobilní telefon. Provoz byl generován v podobě načítání webových stránek na internetu ve vestavěném prohlížeči.

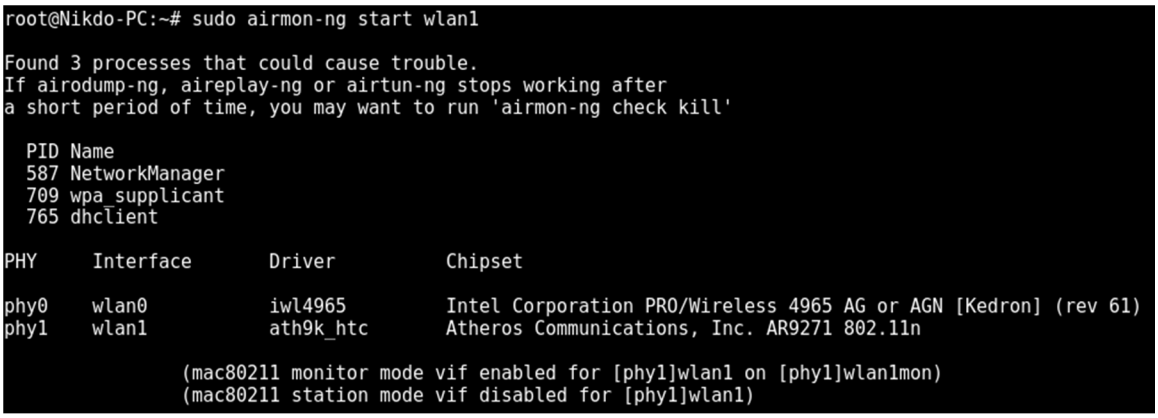
V prvním kroku došlo k nastavení použitého přístupového bodu na zabezpečení WEP, určen byl šifrovací klíč, který má v ASCII přepis *UPCE1* a SSID, které bylo nastaveno na *Pokus2017*. Současně došlo i k dalšímu nastavení bodu, tak aby na něm fungoval internet a aktivovaná byla služba DHCP, aby připojení klienti dostali potřebné adresy.

Následně bylo přistoupeno k přípravě notebooku, ke kterému byl připojen USB Wi-Fi adaptér. Po připojení byla zkontrolována přítomnost adaptéru v systému pomocí příkazu *ifconfig,* kde se ve výpisu objevil použitý adaptér pod aliasem *wlan0.* V případě, že adaptér ve výpisu *ifconfig* není vidět, je nutné zkontrolovat přítomnost firmware v operačním systému.

Například na systémech založených na Debianu, kam patří i Kali Linux, je nutné v případě použití Wi-Fi adaptéru od Intelu doinstalovat balíček *iwlwifi*. Toto je možné provést pomocí příkazu *apt-get install firmware-iwlwifi.* Před tímto příkazem je vhodné pomocí *apt-get update* obnovit repozitáře.

Po úspěšném nalezení adaptéru je nutné na něm aktivovat monitorovací režim. Ten aktivujeme pomocí příkazu *airmon-ng start wlan0.* Současně s touto aktivací se nám změní i název adaptéru, na který se budeme v dalších krocích odkazovat, v tomto případě se změnil na *wlan0mon*.

Občas se může stát, že se nepodaří nastartovat monitorovací režim na používaném adaptéru, protože ho blokuje jiný proces, který ho právě využívá. V takovém případě zvládá Airmon-ng vypsat konkrétní procesy, které adaptér využívají, včetně jejich PID. My musíme takové procesy ukončit ručně nebo pomocí příkazu *airmon-ng check kill* procesy nechat zabít samotným Airmonem-ng.



Obrázek 16 − Blokující procesy

Zdroj: vlastní

V dalším kroku nás již čeká výběr samotného cíle. Pomocí příkazu *airodump-ng wlan0mon* začneme skenovat okolí adaptéru a vyhledávat dostupné bezdrátové sítě. Při skenování okolí můžeme rozšířit získané informace ve výpisu programu Airodump-ng zajímavými přepínači:

- *--manufacturer,* který může ze získaných fyzických adres přístupových bodů odvodit výrobce zařízení,
- *--wps* zobrazí informace o použití WPS na daném zařízení,
- *--band*, který nastaví pásmo, buď 2,4GHz nebo 5GHz pásmo,
- *–c,* který omezí skenované kanály na jeden konkrétní.

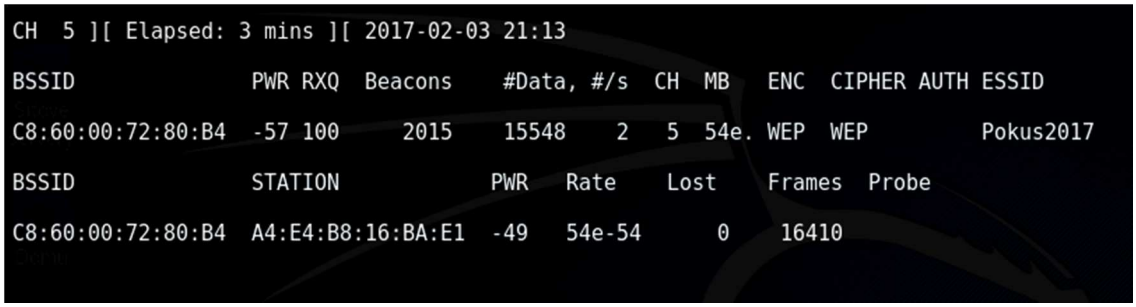
V základním nastavení tyto přepínače aktivní nejsou a Airodump-ng skenuje pouze v pásmu 2,4GHz. Důležité je zmínit, že pro skenování 5GHz pásma je zapotřebí patřičný adaptér, který toto pásmo podporuje, což zde uváděný TP-Link není.

Nyní je možno začít zachytávat data potřebná k rozluštění šifrovacího klíče. Po výběru cíle zastavíme Airodump-ng a upravíme příkaz, tak, aby nám zachytával rámce z konkrétního cíle.

V tomto případě budeme zachytávat provoz z přístupového bodu s názvem *Pokus2017.* Z výpisu je možné zjistit kanál, na kterém přístupový bod vysílá a jeho fyzickou adresu. Tyto informace stačí k zahájení sběru dat. Pomocí příkazu *airodump-ng --bssid C8:60:00:72:80:B4 –c 5 –w Pokus2017 wlan0mon,* kde:

- *--bssid* znační fyzickou adresu zařízení,
- *–c* filtruje číslo kanálu, na kterém vysílá přístupový bod,
- *–w*, který znační názvy souborů, do kterých se bude ukládat zachytávaný provoz na síti.

Po zadání tohoto příkazu průběžně sledujeme sloupec data, který říká počet zachycených unikátních inicializačních vektorů. Pokud jejich počet přesáhne určitý počet[3], je možno přistoupit k lámání hesla pomocí Aircracku-ng.



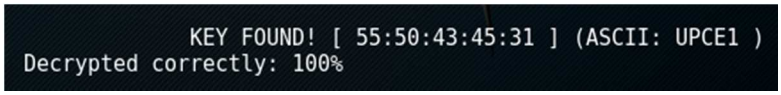
Obrázek 17 – Zachytávání provozu na síti

Zdroj: vlastní

Ve složce, kam Airodump-ng ukládá zachycená data, se nachází soubor s příponou .cap, který použijeme jako vstupní data pro Aircrack-ng. Spuštění je jednoduché, stačí zadat *aircrack-ng Pokus2017.cap* v tomto konkrétním případě. Výsledkem tohoto příkazu mohou být dva stavy.

V prvním případě se na výstupu objeví hláška „Failed. Next try with 5000 IVs.“. V takovém případě to znamená neúspěch, protože zatím není dostatečné množství inicializačních vektorů pro odhalení šifrovacího klíče. Pokud nastane tato situace, tak je důležité pokračovat ve sběru inicializačních vektorů a pokus s Aircrackem-ng opakovat s doporučeným dalším množstvím inicializačních vektorů.

V případě druhém se na výstupu objeví hláška „KEY FOUND!“ a v následujících závorkách se objeví hexadecimální varianta šifrovacího klíče. V případě, že je to možné, tak se vypíše i ASCII přepis.



Obrázek 18 – Úspěšně získaný šifrovací klíč WEP64

Zdroj: vlastní

Tento testovací scénář probíhal za ideálních podmínek, protože byl k bezdrátové síti připojen klient, v tomto případě mobilní telefon, který prohlížel webové stránky a tím napomáhal k rychlému odhalení šifrovacího klíče, protože generoval provoz, který mohl být zachycen.

[3] Program často doporučuje kroky po 5000 inicializačních vektorech.

Díky těmto podmínkám došlo k odhalení klíče přibližně po 75 vteřinách od zahájení zachytávání. Stačilo k tomu jen přibližně 16 000 inicializačních vektorů.

Ovšem v praxi nemusí nastat ideální podmínky, a proto je nutné si dopomoci například pomocí injektace rámců, kterou aktivujeme pomocí příkazu *aireplay-ng -3 –b C8:60:00:72:80:B4 –h B0:48:7A:92:FB:D5 wlan0mon,* kde:

- *-3* značí typ útoku,
- *-b* fyzickou adresu přístupového bodu,
- *–h* fyzickou adresu Wi-Fi adaptéru.

V takovém případě trvalo nasbírání potřebného množství rámců přibližně dvě hodiny.

Získaná data, která obsahuje soubor .cap, je následně možné dešifrovat pomocí Airdecap-ng. V takovém případě vypadá příkaz následovně: *airdecap-ng –w 55:50:43:45:31 Pokus2017.cap,* kde:

- *–w* značí šifrovací klíč v hexadecimální podobě.

Následně rozšifrovaná data je možné otevřít pomocí Wiresharku, kde je možné provádět další analýzy.

5.1.2 WEP128

V případě zabezpečení WEP128 je postup analogický, pouze se mění potřebné množství, které je nutné nasbírat, aby bylo možné odhalit šifrovací klíč. V případě, kdy byl generován provoz, došlo k nasbírání dostatečného množství inicializačních vektorů, přibližně 85 000, po sedmi minutách. V případě, že provoz na přístupovém bodu byl provoz minimální se při pokusu zastavily stopky po šesti hodinách.

5.1.3 WEP pomocí Wifite

Použití Wifite celý výše zmíněný proces zjednodušuje. V případě, kdy se budeme snažit proniknout do stejné sítě jako v přecházejícím případě s WEP64, tak nám stačí jen několik kroků.

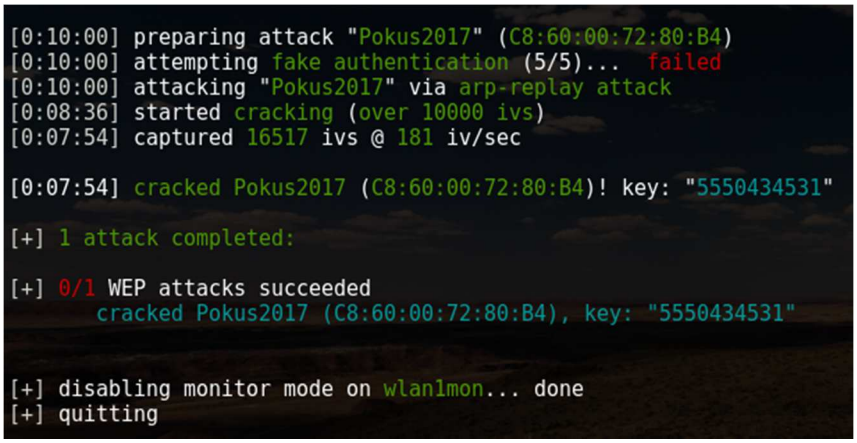
V prvním kroku došlo k nastavení použitého přístupového bodu na zabezpečení WEP, určen byl šifrovací klíč, který má v ASCII přepis *UPCE1* a SSID, které bylo nastaveno na *Pokus2017.* Současně došlo i k dalšímu nastavení bodu, tak aby na něm fungoval internet a aktivovaná byla služba DHCP, aby připojení klienti dostali potřebné adresy.

Po připojení adaptéru a spuštění samotného Wifite, program sám vyhledá dostupné Wi-Fi adaptéry a následně je přepne do monitorovacího režimu. V případě, že jich je nalezeno více,

nechá program uživatele vybrat, se kterým adaptérem se bude pracovat. Po vybrání adaptéru Wifite začne skenovat okolí a vypíše do konzole možné cíle.

Po přibližně dvou minutách skenovaní je možné zastavit proces vyhledávání pomocí control a c a Wifite nám seřadí možné cíle podle aktuálních podmínek, což znamená, že nejvýhodnější cíle budou na prvních pozicích. Následně číselně zvolíme cíl, na který bude Wifite útočit.

Po zvolení cíle dojde k výběru vhodných útoku a Wifite začne sbírat inicializační vektory a pravidelně automaticky testovat, zda jich nemá dostatečný počet pro získání hesla. Wifite současně dokáže poznat přítomnost klientů na zařízení a v případě, že není žádný klient asociován s přístupovým bodem, tak použije metody, jak generovat provoz bez klienta.



Obrázek 19 – Úspěšný útok na přístupový bod pomocí Wifite

Zdroj: vlastní

V testovaném případě nám Wifite zanechal pouze hexadecimální přepis šifrovacího klíče, což není velmi pohodlné. V takovém případě se může využít nepřeberné množství konvertorů, které jsou dostupné na internetu.[4]

Po ukončení útoku Wifite vypne automaticky monitorovací mód na adaptéru a uloží nalezené heslo do souboru s názvem cracked.csv.

5.2 WPA a WPA2

V následující kapitole bude popsán postup, jak prolomit zabezpečení WPA a WPA2 pomocí slovníkového útoku. Využito k tomu bude, stejně jako u zabezpečení WEP, balíku nástrojů Aircrack-ng a síťové karty TP-Link. Pro obě zabezpečení je postup analogický.

[4] https://www.branah.com/ascii-converter

Po nastavení testovaného přístupového bodu, kde bylo zvoleno zabezpečení WPA2 s protokolem CCMP, heslo *UPCEUPCE* a SSID *Pokus2017*. Současně došlo i k dalšímu nastavení bodu, tak aby na něm fungoval internet a aktivovaná byla služba DHCP, aby připojení klienti dostali potřebné adresy.

Následně začíná příprava notebooku s Wi-Fi adaptérem. Nejprve je nutné zjistit, zda je adaptér připojen pomocí příkazu *ifconfig*. Pokud ho ve výpisu nenalezneme, budeme řešit problémy podobně jako v kapitole o zabezpečení WEP. Následně na adaptéru aktivujeme monitorovací režim pomocí příkazu *airmon-ng start wlan0* a můžeme přejít k výběru cíle.

Pro výběr cíle byl využit nástroj Airodump-ng, který byl upraven tak, aby filtroval jen zabezpečení WPA a WPA2. Proces skenovaní byl spuštěn pomocí *airodump-ng --encrypt WPA wlan0mon.*

Po zvolení vhodného cíle bylo následně přistoupeno k zachytávání rámců pomocí Airodumpu-ng. Proces zachytávání musí probíhat do doby, než se mezi daty neobjeví handshake. Zachytávání provedeme pomocí příkazu *airodump-ng -c 3 -w PSKPokus2017 --bssid C8:60:00:72:80:B4 wlan0mon*, kde:

- *–c* znamená kanál, na kterém přístupový bod vysílá,
- *--bssid* fyzickou adresu přístupového bodu,
- *–w* název souboru, kam se budou rámce ukládat.

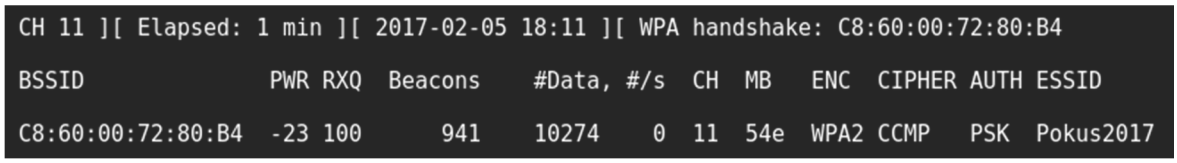
Vyslání handshaku můžeme i vynutit, stačí k tomu připojený klient na přístupovém bodu. V Airodumpu-ng uvidíme jeho fyzickou adresu, kterou použijeme jako jeden z argumentů pro nástroj Aireplay-ng, který ho násilně odpojí. Jelikož se většinou klient pokusí o připojení znovu, získáme tak handshake, který můžeme dále využít k útoku.

Příkaz pro násilné odpojení vypadá například následovně: *aireplay-ng -0 1 –a C8:60:00:72:80:B4 –c B0:48:7A:92:FB:D5 wlan0mon,* kde:

- *0* znamená, že se jedná o deautentizaci klienta,
- *1* značí jen jeden pokus o deautentizaci,
- *–a* je fyzická adresa přístupového bodu,
- *–c* fyzická adresa klienta, kterého chceme násilně odpojit.

Na konci příkazu nalezneme zařízení, přes které bude příkaz pro odpojení odeslán.

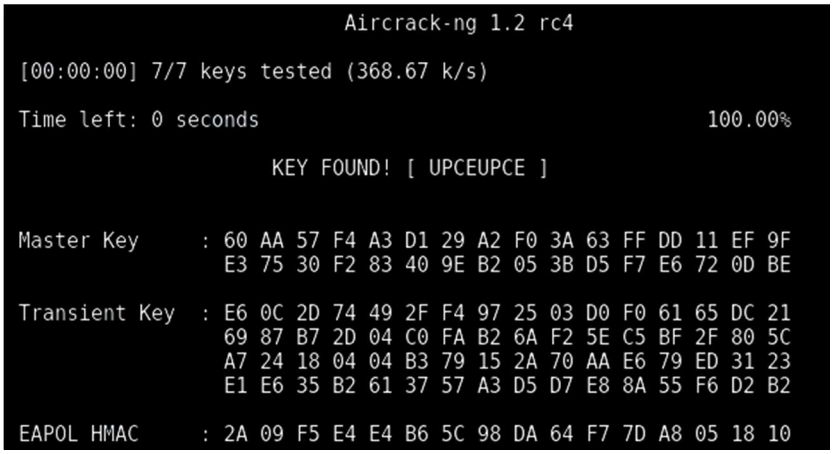
Po zachycení handshaku je možné přistoupit k samotnému slovníkovému útoku.



Obrázek 20 − Zachycený handshake

Zdroj: vlastní

Pokud vlastníme handshake, je možno přistoupit k pokusům o nalezení hesla. K tomu bylo využito nástroje Aircrack-ng. Příkaz *aircrack-ng -w worldlist.lst PSKPokus2017.cap* spustí vyhledávání v rámci .cap souboru, kde nalezne handshake, který následně porovnává s frázemi, které jsou uvedené ve slovníku. Pro účel testování byl použit vlastní slovník, který tvořilo pouze 7 frází z důvodu urychlení vyhledávání. Tvar slovníku je jednoduchý textový soubor, kde každý řádek představuje jeden testovací řetězec. Vytvořit ho je proto možné i pomocí běžného poznámkového bloku.



Obrázek 21 − Vyhledaný klíč ve slovníku

Zdroj: vlastní

Proces vyhledávání ve slovníku je velmi náročná úloha, která se může protáhnout na několik hodin. V rámci praktické části bylo uvažováno nejkratší WPA klíč, který má osm znaků, což při použití malých znaků anglické abecedy, kterých je dvacet šest, činní přibližně $2{,}08 \times 10^{11}$ kombinací. Toto množství je velmi velké a projití takového slovníku by trvalo velmi dlouho.

Pro představu došlo v praktické části k změření výkonu v aplikaci Aircrack-ng na dvou počítačích. V první případě byl otestován používaný notebook s procesorem, který disponuje dvěma jádry na taktu 2,4GHz. Naměřená rychlost byla okolo 1200 otestovaných klíčů za sekundu. Při tomto výkonu bychom otestovaly všechny osmimístné kombinace malé abecedy přibližně za pět a půl roku nepřetržitého běhu programu Aircrack-ng.

V druhém případě byla rychlost otestována na počítači s procesorem AMD FX-8320, který byl přetaktován na 4,3GHz. Tento procesor disponuje osmi jádry, a jelikož je úloha hledání klíče velmi dobře paralelizovatelná, tak došlo k navýšení rychlosti na hodnotu 6350 otestovaných klíčů za sekundu. V takovém případě by trvalo projití slovníku přibližně rok a patnáct dní.

Útok pomocí slovníku je tedy velmi časově náročný a s nejistým výsledkem, stačí použití silného a dlouhého hesla, u kterého by odhalení trvalo třeba i desítky let, což je vzhledem k možné délce až 63 znaků možné, a útočníkovy šance klesají na nulu.

5.3 WPS

Útok vedený na WPS je jednou z nejsnazších metod, jak získat přístupový klíč do sítě, která je zabezpečená pomocí WPA nebo WPA2.

V rámci praktického testování byl pokusný přístupový bod nastaven na zabezpečení WPA2 a použito bylo heslo *UPCEUPCE*. Následně bylo aktivováno WPS. Současně došlo i k dalšímu nastavení bodu, tak aby na něm fungoval internet a aktivovaná byla služba DHCP, aby připojení klienti dostali potřebné adresy.

Po připojení adaptéru a jeho nalezení ve výpisu programu *ifconfig*, je důležité nastartovat pomocí *airmon-ng start wlan0* monitorovací režim. Následně je možno přistoupit k vyhledání cílového přístupového bodu. Případné problémy se řeší stejně jako v kapitole o zabezpečení WEP.

K vyhledání cíle je možné použít dva nástroje, Airodump-ng z balíčku nástrojů Aircrack-ng nebo nástroj Wash. První jmenovaný se použije stejně jako v přechozích případech, jen se přidá přepínač *--wps*, který zajistí zobrazení verze aktivního WPS na přístupovém bodu. Celý příkaz tedy zní *airodump-ng --wps wlan0mon.* Druhou možností je použití nástroje Wash, který zobrazí méně informací než Airodump-ng, ale současně nezobrazí přístupové body, které nemají aktivní WPS. Aktivaci nástroje Wash je možno provést pomocí příkazu *wash –i wlan0mon,* kde:

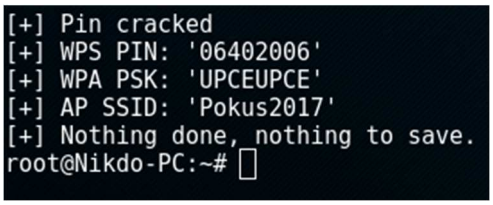
- *–i* značí používaný adaptér.

Po výběru cíle se následně přejde k samotnému útoku na WPS. Útok na WPS probíhá jednoduchým zkoušením všech možných kombinací PINů, což nám umožní nástroj Reaver, který je součástí Linuxové distribuce Kali Linux. Z výpisu, kde dojde k zvolení cíle, je důležité vybrat informace o fyzické adrese zařízení, na které se bude útočit a kanál, na které přístupový

bod vysílá. Použití programu vypadá následovně: *reaver -i wlan1mon -b C8:60:00:72:80:B4 -vv -c 11,* kde:

- *–i* značí použitý adaptér v monitorovacím režimu,
- *-b* fyzickou adresu přístupového bodu,
- *-c* kanál, kde přístupový bod vysílá,
- *–vv* zajistí rozšířený výpis v průběhu programu.

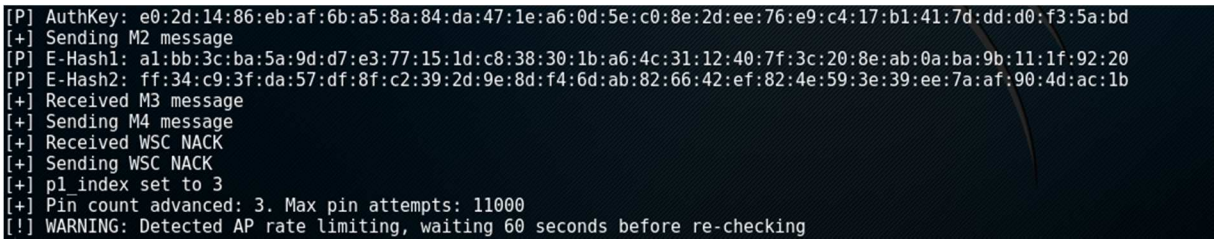
V případě úspěchu se nám po několika hodinách zobrazí jak fungující WPS PIN do sítě, tak heslo, které je potřeba pro přihlášení pomocí zabezpečení WPA2.



Obrázek 22 − Úspěšně získaný PIN a klíč k WPA2

Zdroj: vlastní

Proces získání klíče trval přibližně čtrnáct hodin, přičemž testovaný přístupový bod měl již ve svém firmware obsaženou ochranou technologii, která po několika špatně zadaných pokusech odložila další o určitý čas. Z pozorování, které bylo nabyto v průběhu testu, vyplývá, že po třech špatně zadaných kombinacích PINu přístupový bod zvolil náhodný čas z intervalu šedesáti až sto osmdesáti sekund, po které nedovolil další pokus o přihlášení.



Obrázek 23 − Obraná opatření před útokem na WPS

Zdroj: vlastní

Program Reaver je na takovéto opatření připraven, a proto zvládne čekat, když nedostává odpověď na testovaný PIN a vyzkouší ho vždy znovu po uplynutí 60 sekund.

I v případě WPS je možné celý postup zautomatizovat pomocí programu Wifite, který využívá mechanismy programu Reaver a Wash, díky kterým umí vyhledávat sítě, které mají zapnuté přihlašovaní pomocí WPS. Současně, při zapnutém WPS upřednostňuje tyto sítě v seznamu sítí a preferuje tento typ útoku před útoky pomocí slovníku, které se používají u WPA a WPA2.

5.4 Man in the middle

Tento typ útoků nám slouží k zachytávání dat oběti pomocí útočníkova zařízení. V následujícím textu bude konkrétně představen způsob zneužití protokolu ARP k provedení tzv. ARP spoofingu.

Protokol ARP má v počítačových sítích důležitou roli. Používá se pro překlad síťové IP adresy na adresu fyzickou. ARP spoofing je technika, kdy útočník podvrhne tyto adresy, konkrétně fyzickou adresu, kterou zvolí vlastní, například svého zařízení. To mu umožní stav, kdy veškerá komunikace mezi zařízenými proudí přes něj. (Sak, Raghu, 2014, s. 114-115)

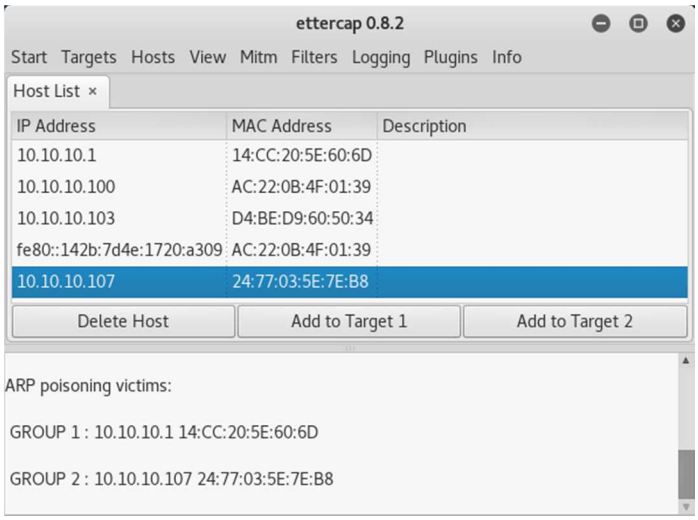
Pro tento typ útoky byl použit nástroj Ettercap, který díky svému jednoduchému grafickému rozhraní zjednodušuje provedení těchto útoků.

Před započetím útoku proběhlo nastavení přístupového bodu, kde bylo zvoleno zabezpečení WPA2 s protokolem CCMP, heslo *UPCEUPCE* a SSID *Pokus2017*. Současně došlo i k dalšímu nastavení bodu, tak aby na něm fungoval internet a aktivovaná byla služba DHCP, aby připojení klienti dostali potřebné adresy. Následně byl útočící notebook připojen do sítě.

V prvním kroku k provedení ARP spoofingu je zapotřebí povolit přemostění komunikace a současně povolit odposlech komunikace na našem zařízení. K tomu v nástroji Ettercap slouží menu *Sniff*, kde se nachází položka *Unified sniffing*. Po aktivací se ve spodním stavovém okně objeví hláška *„Starting Unified sniffing“*.

Po tomto kroku následuje sken sítě, aby bylo možné zvolit žádaný cíl. V menu *Hosts* se použije položka *Host list*, po jejíž aktivaci se zobrazí seznam hostů, kteří jsou dostupní v síti.

V tomto se přistoupí k zvolení dvou cílů. Jeden bude klient v síti a druhý jeho výchozí brána. Mezi těmito dvěma zařízeními se nachází útočník, přes kterého proudí komunikace v obou směrech.

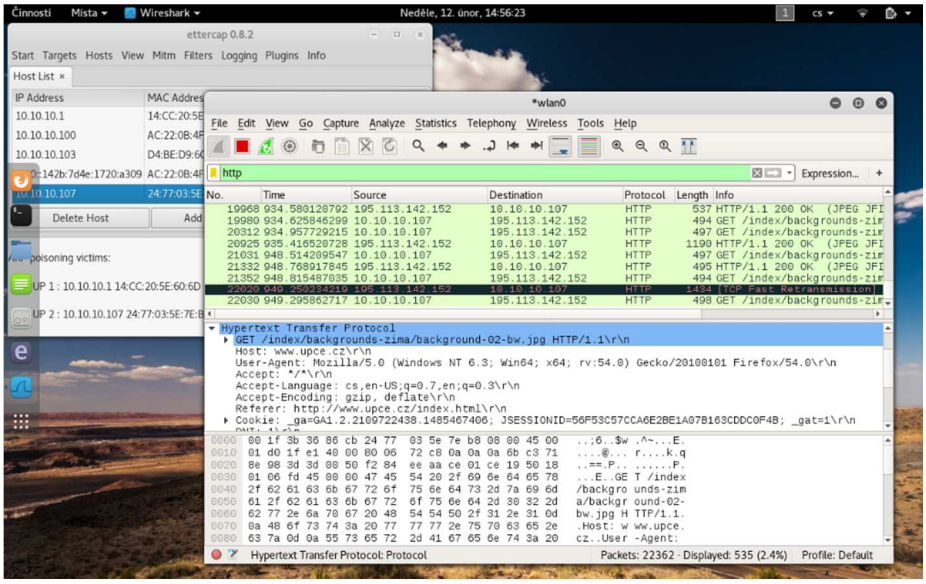


Obrázek 24 – Ettercap, volba cílů

Zdroj: vlastní

Jako cíl jedna byl v tomto případě zvoleno zařízení s adresou 10.10.10.1, které v této bezdrátové síti představuje výchozí bránu. Jako druhý cíl bylo zvoleno zařízení s adresou 10.10.10.107, které je v tomto konkrétním případě ztvárněno mobilním telefonem, na kterém klient prohlíží webové stránky.

Po volbě cílů je možné přikročit k spuštění útoku. To je možné provést v memu *Mitm*, kde zvolíme možnost *ARP poisoning*. Po zvolení se objeví okno, ve kterém je důležité zvolit možnost *Sniff remote connection*, která zajistí obousměrnou komunikaci přes útočníka. Po provedení tohoto kroku je nastavení kompletní.



Obrázek 25 – Wireshark a Ettercap

Zdroj: vlastní

Následně je možné, například pomocí Wiresharku, sledovat provoz na síti. Na Obrázku 25 je vidět průběh otevření univerzitních stránek. Veškerá komunikace, která směřovala do mobilního telefonu, tak proudí přes útočníkův notebook. Této situace se dá velmi snadno zneužít k zachycení přístupových údajů, které proudí po síti pomocí nezabezpečených protokolů. Jedním z řešení, jak například tomuto předcházet je použití zabezpečených protokolů pro komunikaci, například HTTPS.

ZÁVĚR

Cílem této práce bylo představení základních bezpečnostních mechanismů bezdrátových sítí, s důrazem na jejich slabé stránky. V prvních kapitolách práce byly představeny základní pojmy, které se používají v rámci penetračního testování a současně zde byly představeny jednotlivé fáze, kterými je charakteristický průběh penetračního testování.

V následující kapitole byly představeny základní bezpečnostní standardy, které se používají v rámci bezdrátových sítí. Byly zde popsány základní principy těchto zabezpečení, včetně popisu slabých míst a možných útoků. Součástí popisu každého slabého místa bylo i možné doporučení, jak útočníkovi ztížit možný útok nebo ho zcela vyloučit.

Další kapitoly práce mají návaznost na praktickou část práce. V rámci třetí kapitoly byly představeny potřebné hardwarové a softwarové prostředky, které byly použity při tvorbě této práce. Na tento úsek práce navazuje kapitola Skenovací nástroje, v niž jsou blíže rozepsány použité nástroje, včetně základního popisu jejich výstupů.

V praktické části práce jsou uvedeny konkrétní postupy, jak prolomit jednotlivá zabezpečení za pomoci prostředků, jež byly představeny v předchozích kapitolách. S podrobným popisem jsou v této části představeny i možnosti konfigurace pomocí přepínačů nebo také časové údaje, které ukazují, jak dlouho prolomení jednotlivých zabezpečení trvají.

Z pozorování v praktické části vyplývá, že zabezpečení WEP je v dnešní době zcela nedostatečné, protože jeho prolomení pomocí balíků nástrojů Aircrack-ng nebo Wifite je velmi snadné. Za ideálních podmínek je možné dosáhnout úspěchu v řádu desítek sekund.

Naopak zabezpečení WPA aWPA2 se jeví jako dostatečně bezpečné a je možné ho doporučit. Jeho prolomení je možné pouze za specifických podmínek, ale pokud je použito dostatečně silné heslo, tak je prolomení téměř nemožné. Jedinou bezpečnostní hrozbou je aktivní WPS na přístupovém bodu, které je možné prolomit v řádu hodin. V těchto situacích přístupový bod neochrání ani použití nejmodernějšího zabezpečení WPA2, a proto je dobré WPS vypnout.

Tato práce jasně poukazuje na fakt, že bezpečnost bezdrátových sítí není vhodné zanedbávat, a proto by se ji měla věnovat při návrhu sítě dostatečná pozornost. Bezpečnost sítě se nevyplatí podceňovat ani během jejího provozu, protože stejně jako se vyvíjí bezpečnostní mechanismy, tak se objevují nové postupy, jak tyto mechanismy obejít.

6 POUŽITÁ LITERATURA

Aircrack-ng [online]. 2017-03-10 [cit. 2017-03-11]. Dostupné z: https://www.aircrack-ng.org/doku.php.

Airdump.cz. TKIPtun-ng – První implementace útoku na WPA-TKIP šifrování [online]. 2009 [cit. 2017-02-28]. Dostupné z: http://airdump.cz/tkiptun-ng-prvni-implementace-utoku-na-wpa-tkip/.

BITTAU, Andrea. The Fragmentation Attack in Practice [online]. Stanford, 2005 [cit. 2017-03-15]. Dostupné z: https://www.offensive-security.com/wifu/Fragmentation-Attack-in-Practice.pdf. Stanford University.

CENGAGE Learning, 2010. Ethical hacking and countermeasures. Clifton Park, NY: Course Technology, ISBN 978-1-4354-8360-6.

ČÍŽEK, Jakub. Statistiky. Wifileaks [online]. 2017 [cit. 2017-02-19]. Dostupné z: http://www.wifileaks.cz/statistika/.

FLUHRER, Scott, Itsik MANTIN a Adi SHAMIR. *Weaknesses in the Key Scheduling Algorithm of RC4* [online]. 2001 [cit. 2017-02-26]. Dostupné z: http://wiki-files.aircrack-ng.org/doc/technique_papers/rc4_ksaproc.pdf . The Weizmann Institute

HELD, Gilbert. Securing wireless LANs: a practical guide for network managers, LAN administrators, and the home office user [online]. Hoboken, NJ: J. Wiley, c2003 [cit. 2017-03-01]. ISBN 04-708-5127-9. Dostupné z: https://books.google.cz/books?id=QsIALlyDDtsC&printsec=frontcover&hl=cs#v=onepage&q&f=false.

HRUŠKA, Pavel. Prolomení WPA/WPA2-PSK přes WPS snadno a rychle (teorie). Mrpear.net: osobní web jednoho ajťáka [online]. 2012-10-02 [cit. 2017-03-05]. Dostupné z: http://www.mrpear.net/cz/blog/386/prolomeni-wpa-wpa2-psk-pres-wps-snadno-a-rychle-teorie.

Kali. Kali by offensive security: Official Kali Linux Documentation [online]. Kali, 2017 [cit. 2017-03-11]. Dostupné z: https://www.kali.org/kali-linux-documentation/.

KERSHAW, Mike. Kismet Wireless: Documentation. Kismet Wireless [online]. 2016-01 [cit. 2017-03-11]. Dostupné z: https://www.kismetwireless.net/documentation.shtml.

LAMPING, Ulf, Richard SHARPE a Ed WARNICKE. Wireshark User's Guide: For Wireshark 2.1 [online]. 2014 [cit. 2017-03-11]. Dostupné z: https://www.wireshark.org/docs/wsug_html_chunked/.

Nmap. Nmap Network Scanning: Chapter 15. Nmap Reference Guide. Nmap [online]. 2016 [cit. 2017-03-11]. Dostupné z: https://nmap.org/book/man.html.

NOVÁK, Michal. Odposlouchávání a prolamování Wi-Fi sítí zabezpečených pomocí WPA2. INTERNET INFO. Root.cz [online]. 2017-01-04 [cit. 2017-03-18]. Dostupné z: https://www.root.cz/clanky/odposlouchavani-a-prolamovani-wi-fi-siti-zabezpecenych-pomoci-wpa2/.

PIPER, Fred, Sean MURPHY a Pavel MONDSCHEIN. Kryptografie. Praha: Dokořán, 2006, s. 93-95. Průvodce pro každého. ISBN 80-736-3074-5.

RACKLEY, Steve. *Wireless networking technology: from principles to successful implementation*. Boston: Elsevier, Newnes, 2007, s. 212-216. ISBN 978-0-7506-6788-3.

SAK, Brian a Jilumudi Raghu RAM. Mastering Kali Linux Wireless Pentesting. 1. BIRMINGHAM - MUMBAI: Packt Publishing, 2016. ISBN 978-1-78528-556-1.

SELECKÝ, Matúš. Penetrační testy a exploitace. Brno: Computer Press, 2012, s. 11-38, 167-170. ISBN 978-80-251-3752-9.

ŠUSTR, Matěj. Bezpečnost a Hacking WiFi (802.11) - 3. WEP. *Security-Portal.cz* [online]. Praha: Security-Portal.cz, 2009-12-22 [cit. 2017-02-25]. Dostupné z: http://www.security-portal.cz/clanky/bezpe%C4%8Dnost-hacking-wifi-80211-3-wep.

TP-LINK. Vysokovýkonný bezdrátový USB adaptér 150 Mbit/s: TL-WN722N [online]. TP-Link, 2017 [cit. 2017-03-05]. Dostupné z: http://cz.tp-link.com/products/details/cat-11_TL-WN722N.html.

WEBER, Filip. Penetrační testy v bezpečnostní analýze informačního systému. Svět sítí [online]. 2007-10-28 [cit. 2017-02-19]. Dostupné z: http://www.svetsiti.cz/clanek.asp?cid=Penetracni-testy-v-bezpecnostni-analyze-informacniho-systemu-28102007.

Wi-Fi Alliance. Wi-Fi CERTIFIEDTM for Wi-Fi Protected Setup: Easing the User Experience for Home and Small Office Wi-Fi R Networks (2014) [online]. 2014 [cit. 2016-10-29]. Dostupné z: http://www.wi-fi.org/downloads-registered/wp_Wi-Fi_CERTIFIED_Wi-Fi_Protected_Setup_20140409_0.pdf/Wi-Fi+CERTIFIED+Wi-Fi+Protected+Setup.

7 PŘÍLOHY

Příloha A - *Seznam použitého softwarového a hardwarového vybavení*

Hardwarové vybavení:

- Lenovo ThinkPad T61 7661 CTO
- TP-Link TL-WN722N
- Intel PRO/Wireless 4965agn
- ASUS RT-N10U
- BlackBerry Passport

Softwarové vybavení:

- Linuxová distribuce Kali Linux 2016.2
- Aircrack-ng 1.2-rc4
- Wifite 2 revize 87
- Wireshark 2.2.24
- Ettercap 0.8.2
- Reaver 1.5.2

Příloha B - *Seznam souborů na CD*

- soubor *Penetrační testování bezdrátových sítí – Jiří Danielka.pdf*