Otestování bezpečnosti Wi-Fi Sítě

Filip Šebesta

Cílem práce bylo otestovat zabezpečení jednoduché WiFi sítě. Prováděl jsem ho za pomocí sniffovacích nástrojů pod operačním systémem Wifislax. Práce se zabývá prolomením WEP klíče a čtením nezabezpečených dat na síti.

I. TESTOVACí SíŤ

Jako testovací síť jsem si zvolil malou domácí WiFi síť pro sdílené připojení k Internetu. Skládala se z jednoho přístupového bodu, switche a ADL modemu. Maximální počet uživatelů byl 8. Zabezpečení bylo primitivní pomocí WEP klíče o velikosti 128b.

II. TECHNICKÁ PŘÍPRAVA

Pro testování jsem musel obstarat potřebný software a hardware.
Jako testovací PC je ideální notebook s vývodem pro externí anténu. Ten jsem však bohužel neobstaral a proto jsem se rozhodl pro úpravu mého stávajícího notebooku. Postup byl následující: nejprve jsem odmontoval kryt displeje, pod kterým se schovává malá všesměrová anténa nevelkého výkonu. Tu jsem odpojil a připojil jsem zde vlastní pigtail pro výkonnější externí anténu. Tu jsem vyrobil z plechovky o průměru 7,5cm měděného drátu. Přesný návod se nachází na http://www.pcsvet.cz/art/article_print.php?id=4082

Dalším důležitým bodem je volba správné WiFi karty, jelikož zdaleka ne všechny umí potřebné funkce pro penetrační tesy. Můj notebook naštěstí obsahoval chipset Realtek rtl8180 jež při použití vhodných ovladačů tyto funkce umí.
Otázka volby operačního systému je klíčová. Jak jsem se dočetl, tak operační systém Windows je pro tyto účely nevhodný. Daleko lepší jsou speciální distribuce Linuxu, zejména Back Track nebo Wifislax. Já jsem se rozhodl pro Wifislax 3.0 což je specialní pentest distribuce (BackTrack derivát) kterou vyvíjí španělská skupina Seguridad Wireless. Primárně vyplňuje díru vzniklou vývojem a prodejem nových Wifi chipsetů.

obrázek 1:*ukázka použité antény*

III. CHIPSETY KTERÉ PODPORUJE WIFISLAX 3.0

- Prism54
- Madwifi-ng
- HostAP
- Ralink rt2570 , rt2500, rt73, rt61
- Zydas ZD1211rw
- Intel PRO Wireless ipw2100 / ipw2200 / Intel pro wireless ipw3945
- Realtek rtl8180, rtl8187
- Broadcom
- Texas Instruments (ACX)

IV. FUNKCE NEZBYTNÉ PRO SNIFFING

První a zcela bez pochyb nejnutnější funkcí každé WiFi katy používané pro sniffing je tzv. monitoring mód, což je obdobná funkce jako promiskuitní mód

akorát v bezdrátových sítích. Jednoduše řečeno karta v tomto režimu neignoruje pakety, které v hlavičce neobsahují její MAC adresu. Z toho vyplývá že jsme schopni číst i pakety které nejsou směrovány nám a jelikož se u WiFi používá sdílené médium, tak jsme schopni tyto pakety vcelku jednoduše odchytávat.
Na unixových systémech se monitor mód zapíná příkazem iwconfig eth0 mode Monitor.
Další důležitou funkcí je tzv. packet injection což je technika kterou se manipuluje provoz v síti, unáší spojení nebo upravuje samotný paket. Pro tento účel existují samostatné aplikace. Od těch kde lze napsat celý paket (Winject) přes ty co umí paket odchytnout a nabídnou jeho modifikaci (Ethereal) až po aplikce plně automatizované (aireplay-ng, Wireshark).

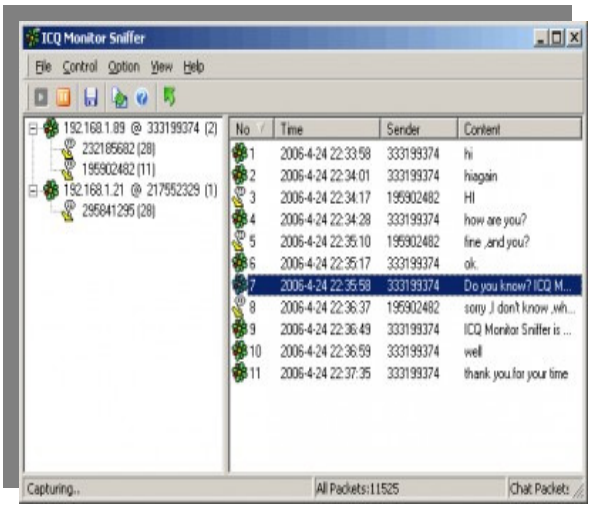
V. Penetrační test zranitelnosti WEP klíče

Postup penetračního testu byl následující. Nejprve jsem nabootoval Wifislax z live CD. Dále bylo potřeba zavést ovladače pro WiFi kartu. Pro spuštení karty obsahuje submenu volby injection a ipraw. Volba 1 zapne ipraw. Další volba zprovozní packet injection. U této volby je ale nutné přimo v konzoli, kterou kliknuti vyvolá, ručne zadat rate, kanál a platnou MAC adresu klienta kterého použijeme pro packet injection. Po této události se v systému se objeví 2 nove rozhraní - wifi0 a rtap0. Nyní již můžeme spustit Airodump-ng a Aireplay-ng, což jsou programy které slouží k prolomení samotného WEP klíče. Pro Airodump-ng pouzijeme rtap0 a pro Aireplay-ng wifi0. Také lze stáhnout poslední novinku Aircarck-ptw. Obsahuje nový algoritmus který je o poznání rychlejší. Implementovala ho a vypustila Technická Univerzita Darmstadt. Prolomení WEP klíčet trvá průměrnému pc maximálně 10 minut.

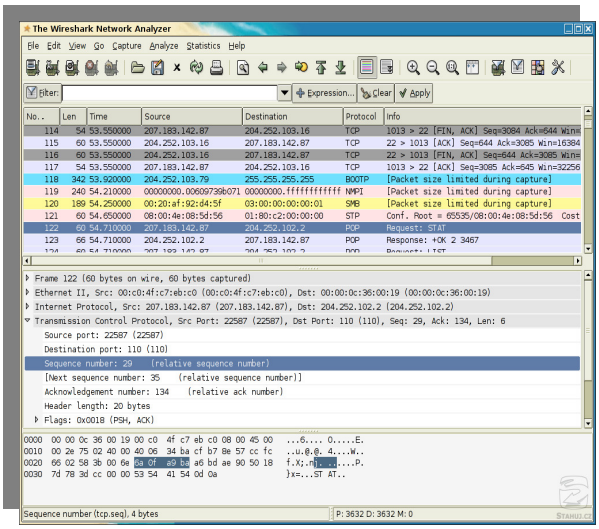
VI. Další programy

K testování bezpečnosti jsou vhodné takzvané sniffovací programy jež zachytávají komunikaci procházející skrze síťová rozhraní vašeho počítače. Asi nejznámější z nich je Wireshark (obrázek 3), což je následník již ukončeného Etherealu. Obsahuje různé filtrovací funkce a také například po zadání WEP klíče rozšifrovává komunikaci.

Dalším zajímavým programem jež jsem vyzkoušel byl ICQ Sniffer (obrázek 2) což je de facto program který umí filtrovat pakety s protokolem ICQ a zobrazovat v dobře čitelné podobě uživateli. Jelikož ICQ není nijak šifrováno, může si případný útočník lehce přečíst komunikaci mezi uživateli.



obrázek 2:*ICQ sniffer*



obrázek 3:*Wireshark*

VII Závěr

Na závěr bych chtěl dodat, že práce na tomto tématu mi přišla zajímavá a doufám že mi bude přínosem ať už při studiu, v zaměstnání či kdekoliv jinde. Osvojil jsem si základní postupy a uplatnil je v praxi. Ukázala mi nové obzory v oblasti síťových technologií a proto hodnotím její přínos velmi kladně.

VIII PRAMENY

[1] WWW.AIRDUMP.CZ

[2] HTTP://WIZARDSMAG.IC.CZ

[3] HTTP://WWW.SECURITY-PORTAL.CZ/

[4] HTTP://MOZEKTEVIDI.NET/CLANEK/WIFI-HACKING