

OTESTOVÁNÍ BEZPEČNOSTI WIFI SÍTĚ

Semestrální práce

Filip Šebesta

ČVUT – FEL 2008

Sít'



- Wifi sít' pro sdílené připojení k Internetu
- AP + Switch +ADSL modem
- Primitivní zabezpečení pomocí WEP se 128b délkou klíče

Příprava



- Nejvíce času zabralo shánění vhodného SW + HW
- Většina notebooků neobsahuje přípojku pro externí anténu ale dá se poměrně jednoduše vyrobit
- Anténu jsem si vyrobil vlastní podle návodu z plechovky
- Jako OS se nehodí Windows, nejlépe Back Track případně WiFiSlax

Wifislax 3.0



- Wifislax je specialni pentest distribuce (BackTrack derivát) kterou vyvíjí španelská skupina Seguridad Wireless.
- Primárně vyplňuje díru vzniklou vývojem a prodejem nových Wifi chipsetů

Podporované chipsety

- ❑ 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)

Důležité pojmy

- **Promiskuita vs. Monitor Mode** - Karta v promiskuitním režimu neignoruje pakety, které v hlavičce neobsahují její MAC adresu. Po překonání této bariéry získává uživatel veškeré informace v síti. Monitor Mode je obdobná technika aplikovatelná v bezdrátových sítích.
- **Promiskuita**
ifconfig eth0 promisc
- **Mode Monitor**
iwconfig eth0 mode Monitor

Důležité pojmy 2

- **Packet Injection** - Injekce paketu 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 aplikace plně automatizované (aireplay-ng, Wireshark)

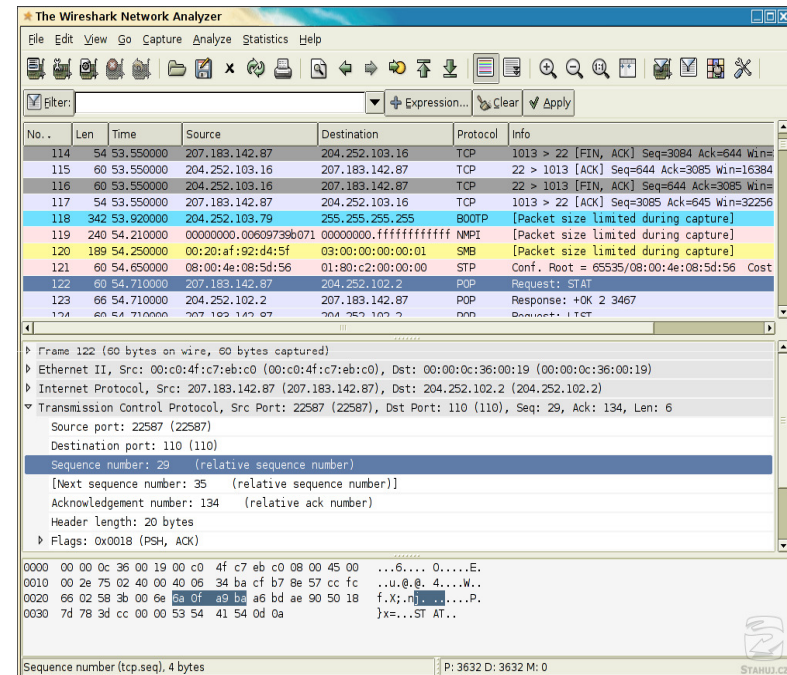
Postup pentestu zranitelnosti WEP

- 1. boot OS z live cd
- Zavedení ovladačů pro WiFi kartu
- Zapnutí packet injection (nastavení MAC, rate a kanálu) a raw skoketu
- V systému se objeví 2 nové rozhraní - wifi0 a rtap0
- Spuštění Airodump-ng (wufi0) a Aireplay-ng(rtap0)
- Případně vyšla vylepšená verze Aircarck-ptw

Wireshark

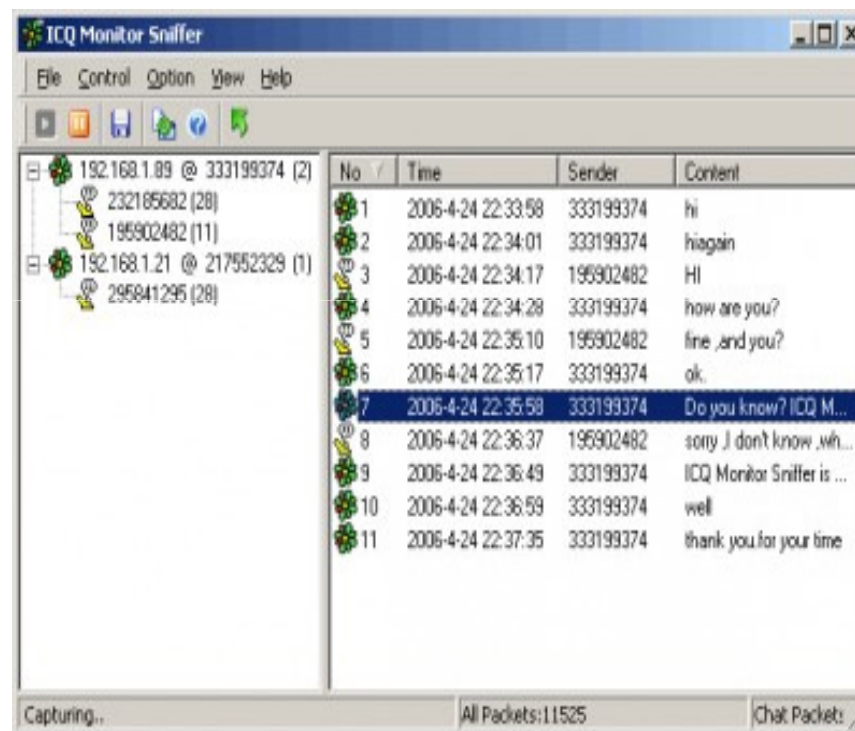
TI 6.9

- Následník Etherealu
- zachytává komunikaci procházející skrze síťová rozhraní vašeho počítače
- Po zadání WEP umí dešifrovat traffic



ICQ sniffer

- ICQ nepoužívá žádné šifrování!!
- Tato utilitka Vám krásně a přehledně zobrazuje veškerou komunikaci přes ICQ



The screenshot shows the 'ICQ Monitor Sniffer' application window. The window title is 'ICQ Monitor Sniffer'. The menu bar includes 'File', 'Control', 'Option', 'View', and 'Help'. Below the menu bar is a toolbar with several icons. The main area is divided into two panes. The left pane shows a tree view of captured connections, including '192.168.1.89 @ 333199374 (2)', '232185682 (28)', '195902482 (11)', '192.168.1.21 @ 217552329 (1)', and '295841295 (28)'. The right pane displays a table of captured chat messages.

No	Time	Sender	Content
1	2006-4-24 22:33:58	333199374	hi
2	2006-4-24 22:34:01	333199374	hiagain
3	2006-4-24 22:34:17	195902482	Hi
4	2006-4-24 22:34:28	333199374	how are you?
5	2006-4-24 22:35:10	195902482	fine ,and you?
6	2006-4-24 22:35:17	333199374	ok.
7	2006-4-24 22:35:58	333199374	Do you know? ICQ M...
8	2006-4-24 22:36:37	195902482	sorry I don't know ,wh...
9	2006-4-24 22:36:49	333199374	ICQ Monitor Sniffer is ...
10	2006-4-24 22:36:59	333199374	well
11	2006-4-24 22:37:35	333199374	thank you for your time

At the bottom of the window, there is a status bar with the text 'Capturing..', 'All Packets:11525', and 'Chat Packets:'.

Závěr



- WEP klíč je velmi chabá ochrana, dá se prolomit do 10 minut
- Velká část trafficu na síti není šifrována
- Sniffing sítě je velmi zajímavá a účinná metoda monitoringu sítě

Z čeho jsem čerpal

- [1] www.airdump.cz
- [2] <http://wizardsmag.ic.cz>
- [3] <http://www.security-portal.cz/>
- [4] <http://mozektevidi.net/clanek/wifi-hacking>



Děkuji za pozornost