

WiFi ruuteri seadistamise aruanne

Töö eesmärk

Lua turvaline alamvõrk ning selgitada välja turvapõhimõtted antud võrgu puhul. Samuti tutvuda ka ruuteri seadistamisega.

Algtingimused

Tööks oli 2 arvutit operatsioonisüsteemiga Windows Vista, LinkSys WiFi ruuter WRT54G ja WiFi-USB seade.

Töö käigu kirjeldus

Kuna seadmed ei olnud omavahel ühendatud siis kõigepealt oli tarvis need omavahel ühendada. Seadmed said omavahel ühendatud järgnevalt:



WiFi USB seadmega arvuti.

- Esmalt installeerimise ühte arvutisse WiFi USB seadme.
- Läbi ruuteriga kaabliga ühendatud arvuti logisime ruuteri konfiguratsiooni lehele

- Muutsime ära ruuteri administraatoriparooli. Kasutajanime jätsime samaks. (algelt kasutaja: root, parool: admin)
- Määrasime uueks ruuteri võrguaadressiks 192.168.4.1 ja võrgumaskiks 255.255.255.0 (Algselt oli 192.168.1.1, 255.255.255.0).
- Ruuteri DHCP server lubas algselt 50 erinevat aadressi. Vahemikus 192.168.4.2-192.168.4.52. Muutsime vastavalt juhisele selle vahemiku 192.168.4.20 – 192.168.4.43. Nüüd siis oli võimalik ruuteril välja jagada ainult 23 aadressi.
- Määrasime ruuteri uueks MAC aadressiks 00-2C-F1-51-38-18.
- Ruuteri seadistuse lehel määrasime võrgustandardiks, millega ruuteriga ühendada saab b-standardi kaartidega. Algselt olid lubatud kõik standardid, mida ruuter toetas.
- Kuna Windows Vista all Network Stumbler ei tööta, siis leidsime internetist otsides sarnase programmi nimega Vistumbler. Sellega saime vaadata olemasolevate võrkude infot. Kuna meie ruuteri nimi ja võrgukrüpteering olid hetkel veel muutmata, siis oli ruuteri SSID dd-wrt, ning Vistumbler näitas, et krüpteering puudub.
- Järgnevalt muutsime ära ruuteri SSID, panime selleks „ruuter“ ja krüpteeringuks määrasime WPA2-Personal, parooliks panime „arapraktikum1“.
- Muutime ruuteri seadistust nii, et ainult kaabliga ühendatud arvuti pääses konfiguratsiooni lehele ligi.
- Uurisime veel võimalusi kuidas oma võrku turvalisemaks muuta, näiteks lubada ruuteriga ühendada ainult teatud MAC aadressiga seadmeid (MAC filter), peita ruuteri SSID, nii et ainult need saaksid ühendada, kes teavad õiget SSID.
- Proovisime ka ruuteri sageduskanalite muutmist.

Tulemused ja järeldused

Ruuteri poolt jagatavate IP aadresside piiramine annab võimaluse lubada võrku ainult mõistlik arv arvuteid, et võrguliiklust liiga üle ei koormataks. Ruuteri MAC aadressi vahetamine võib vajalikuks osutuda kui näiteks ISP poolt on lubatud võrku ühendada ainult üks arvuti, ning tahetakse võrku ühendada läbi ruuteri rohkem arvuteid. Sel juhul saab ruuterile anda ISP poolt lubatud MAC aadressi.

Ruuter SSID muutmise on kasulik kuna siis on võimalik ruuterit teste seast üles leida. Algselt kui meie ruuteri SSID muutmata oli, oli suhteliselt tüütu sellesse võrku ühendada, kuna nagu selgus oli veel 2 ruuteril sama nimi.

Ruuteri võrgu krüpteeringu lisamine on kõige lihtsam ning enimlevinud viis võrku turvalisemaks muuta, kuna sel juhul saavad ühendada ainult need kes võrgu parooli teavad. Ruuteri krüpteeringuks valisime WPA2, mis oli antud võimaluste puhul kõige turvalisem, kasutades krüpteerimiseks CCMP meetodit. Parooliks oli antud praktikumis „arapraktikum1“, kuid suurema turvalisuse huvides võiks parooliks kasutada suvalistest tähemärkidest koosnevat parooli, mis võib olla kuni 128 märki pikk WPA2 puhul.

Ruuteril MAC filtri kasutamine lisab oaksorda turvalisus, kuna siis on võimalik lubada võrku ainult neid seadmeid mille MAC on eelnevalt olemas. Samuti saab ka keelata teatud MAC aadressidega seadmete ühendamist.

Samuti on hea mõte ruuterist ära keelata traadita võrgu kasutajatel konfiguratsioonile ligi pääs, kuna parooli ja MAC aadressi on võimalik jäljendada nendel kes ikka väga võrku sisse tahavad pääseda. Sel juhul ei saa nad vähemalt omaniku määratud konfiguratsiooni muuta.

Ruuteri SSID peitmine annab võimaldab lihtsalt peita ruuterit nende kasutajate eest kellel ei peaks aimu olema, et antud ruuter WiFi võrku levitab.

Eelnevast järeldub, et WiFi võrk on turvalisem kui on olemas võrgukrüpteering, kasutatakse MAC filtrit ja WiFi kaudu ühendatud arvutitel pole lubatud ruuteri konfiguratsiooni muuta.

Samuti ei tee halba kui on piiratud võrguaadresside hulk ja ruuter ei *broadcasti* oma SSID.

Ruuteri sageduskanali muutmine on kasulik juhul kui läheduses on palju teis WiFi võrke, mis kasutavad sama sageduskanalit, sel juhul on parem valida kanal mida teised ei kasuta, et vältida seda, et ruuterid üksteist segama hakkavad.

Vistumbleriga oli võimalik ruuterit ka siis näha kui ruuter oma SSID ei avalikustanud, samuti oli võimalik näha mis kanalil läheduses olevad ruuteri töötasid, ruuteri MAC aadress, signaali tugevus, võrgu krüpteering, millist võrgustandardit ruuter toetas, ruuteri tootjat, võrgutüüpi, jne.

Vistumbleri tabeli on aruande lõpus ka olemas.

Lisaks

Praktikumis kasutatud ruuteri kohta leidsime infot Wikipediast (http://en.wikipedia.org/wiki/Linksys_WRT54G_series) ja ruuteri tarkvara kohta DD-WRT kodulehelt (<http://www.dd-wrt.com/wiki/index.php/Tutorials>) ning praktikumi materiale WiFi ruuteri konfigureerimisest.

SSID	BSSID	MANUFACTURER	Highest Signal w/GPS	Authentication	Encryption	Radio Type	Channel
eduroam	00:1F:CA:50:AA:C0	Unknown	0	WPA2-Enterprise	CCMP	802.11g	1
eduroam	00:17:DF:97:14:50	Cisco	0	WPA2-Enterprise	CCMP	802.11g	11
ut-public	00:1F:CA:50:AA:C1	Unknown	0	Open	None	802.11g	1
ut-public	00:17:DF:97:14:51	Cisco	0	Open	None	802.11g	11
tuit	00:1F:CA:50:AA:C2	Unknown	0	WPA2-Enterprise	CCMP	802.11g	1
utlib	00:1F:CA:50:AA:C3	Unknown	0	Open	None	802.11g	1
ruuter	00:14:BF:92:D4:43	Cisco-Linksys	0	WPA2-Personal	CCMP	802.11b	10
qwertyz	00:2C:F1:51:38:18	Unknown	0	Open	None	802.11g	6
	00:14:BF:92:D4:43	Cisco-Linksys	0	Open	None	Any Radio Type	10

[illegible]