WIFI-PINEAPPLE

Langattoman lähiverkon penetraatiotestaus

HAMK
HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Ammattikorkeakoulututkinnon opinnäytetyö

Tietojenkäsittelyn koulutus

syksy 2022

Jon von Denffer

HAMK
HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Tietojenkäsittelyn koulutus Tiivistelmä
Tekijä Jon von Denffer Vuosi 2022
Työn nimi Wifi Pineapple – langattoman lähiverkon penetraatiotestaus
Ohjaaja Ismo Turve

Opinnäytetyön tavoitteena oli tutustua langattomien lähiverkkojen tietoturvaan ja penetraatiotestaamiseen kuluttajatason laitteilla. Opinnäytetyö rajautuu tietoturvan osalta verkon murtamiseen, opinnäytetyö ei myöskään ota kantaa millaiset verkkorikolliset näitä tekniikoita käyttäisivät tai mikä heidän mahdollinen motiivinsa käytölle olisi.

Yrityskäyttöön tarkoitetut laitteet on rajattu opinnäytetyöstä pois. Lisäksi on poisrajattu WPA3-suojauksen käsittely, koska se on toistaiseksi vähän käytetty.

Työssä perehdyttiin langattomien verkkojen testausta varten valmistettuun Wifi Pineapple -laitteeseen. Opinnäytetyöllä ei ollut toimeksiantajaa ja aihe pohjautui tekijän omaan kiinnostukseen langattomia lähiverkkoja sekä niiden tietoturvaa kohtaan.

Opinnäytetyön teoriaosuudessa perehdyttiin yleisesti langattomiin lähiverkkoihin sekä niiden suojaukseen. Tutkimuksen kohteena on Wifi Pineapple jota verrattiin tietoturvan testaamiseen käytettyyn Kali-Linux-käyttöjärjestelmään. Käytännön osuudessa toteutettiin testiympäristössä WPA-kättelyn kaappaaminen ja sen murtaminen. Opinnäytetyö oli tutkimuspohjainen ja tutkimus tehtiin avoimen lähdemateriaalin pohjalta. Käytännön testaaminen toteutettiin Wifi Pineapplella ja Kali-Linuxilla testausta varten tehdyssä testiympäristössä. Testiympäristö koostui kannettavasta tietokoneesta sekä älypuhelimesta.

Tietoturvan merkitys kasvaa tulevaisuudessa ja sen testaaminen on yksi oleellinen osa riittävän suojauksen varmistamiseksi. Myös käyttäjiltä tullaan vaatimaan tulevaisuudessa entistä enemmän oman tietoturvan huomioimista.

Avainsanat Wifi Pineapple, Kali-Linux, penetraatiotestaus, langaton lähiverkko, tietoturva
Sivut 36 sivua

HAMK
HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Degree Programme in Business Information Technology Abstract
Author Jon von Denffer Year 2022
Subject Wifi Pineapple – wireless network penetrationtesting
Supervisors Ismo Turve

The purpose of this thesis was to learn about wireless network security and about penetration testing of wireless networks with commercial grade hardware. Enterprise level hardware has been left out along with WPA3 protection due to its relatively low prevalence. In terms of information security, the thesis is limited to breaching a wireless network, the thesis also does not take any position on what kind of cybercriminals would use these technologies or what their motives are for using them. Wifi pineapple, a hardware device built for testing wireless networks is also studied. The thesis had no client, and the topic was based on authors interest in wireless networks and their security.

In the Theory part of the thesis wireless networks and their protection methods were introduced in general. One of the subjects of the study was also Wifi Pineapple which was compared to Kali-Linux an operating system, which is used for penetration testing.

In the practical part of the thesis an WPA handshake was captured and cracked. The thesis was research-based, and the research was done on the bases of open-source material. Practical testing was done with Wifi pineapple and Kali-Linux in a testing environment. The testing environment consisted of an windows laptop and smartphone.

The importance of information and cyber security will increase in the future and its testing is an essential part to ensure adequate protection. Individuals will also be required to pay even more attention to one’s own information security.

Keywords Wifi Pineapple, Kali-Linux, penetration testing, wireless network, cybersecurity
Pages 36 pages

Sanasto

WLAN	Langaton lähiverkko (Wireless local area network) tekniikka, jolla päätelaitteet voidaan kytkeä langattomasti verkkoon
LAN	Lähiverkko (Local area network) kiinteä kaapeleilla toteutettava verkko
WI-FI	WLAN tekniikasta käytettävä kuluttajatermi
WEP	Wired Equivalent privacy 802.11-standardin ensimmäinen langatonta tietoliikennettä suojaamaan kehitetty salausmenetelmä
WPA	Wi-fi protected access on WLAN-verkkojen salausprotokolla
WPA2	Wi-fi protected access 2 on WLAN-verkkojen salausprotokollan uudempi versio joka käyttää TKIP sijaan AES salausta
TKIP	Temporal Key Integrity Protocol langattomien lähiverkkojen tietoturvaprotokolla, vanhentunut vuonna 2012
AES	Advanced Encryption standard lohkosalausmenetelmä tietojen salaamiseen
SSID	Service set identifier eli langattoman lähiverkon verkkotunnus
MAC osoite	Media Access Control verkkosovittimen yksilöivä osoite
Kali-Linux	Penetraatiotestaamiseen tehty linux distribuutio
HTTP	Hypertext transfer protocol on protokolla, jota selaimet ja WWW-palvelimet käyttävät tiedonsiirtoon
HTTPS	Hypertext transfer protocol secure on HTTP-protokollan ja TSL/SSL-protokollan yhdistelmä, jota käytetään suojattuun tiedonsiirtoon
Live CD	On CD/DVD-levy jolle asennettu ohjelma käynnistyy koneen keskusmuistissa ja mahdollistaa vaikkapa käyttöjärjestelmän ajamisen
BSS	Basic service set tukiasemallisen verkon liityntäpiste
Raspberry Pi	Suosittu yksipiiritietokone (Englanniksi single board computer)

Sisällys

Kuva- ja komentoluettelo

1 Johdanto

Tietoturvan merkitys korostuu entisestään tulevaisuudessa ja on kiinnostava sekä monipuolinen aihe tutkia. Erilaisten tietoturvahyökkäysten sekä kyberrikollisuuden määrä kasvaa mikä korostaa tarvetta tutkia laitteiden, verkkojen ja järjestelmien tietoturvaa.

Opinnäytetyö rajautuu tietoturvan osalta verkon murtamiseen. Opinnäytetyö ei myöskään ota kantaa millaiset verkkorikolliset, näitä tekniikoita käyttäisivät tai mikä heidän motiivinsa käytölle on. Langattomat lähiverkot ovat yleistyneet sekä yritys- että kuluttajatasolla ja niitä on käytössä miltei kaikkialla. Langattomien verkkojen käytössä piilee kuitenkin riskejä. Esimerkiksi kahvilat, hotellit ja kirjastot tarjoavat asiakkaileen avoimia wifi-yhteyksiä. Kuinka moni kuitenkaan osaa edes ajatella ettei se hotellin nimeä käyttävä verkko ollutkaan hotellin ylläpitämä. Langattomat verkot ovat yleisin tapa jolla kotitalouksien laitteet saatetaan verkkoon. Monissa kotitalouksissa ei välttämättä ole lainkaan laitteita kiinteässä langallisessa verkossa. Lisäksi erilaiset verkkoon kytketyt langattomat älylaitteet yleistyvät, jolloin verkkoon tunkeutuminen voi pahimmassa tapauksessa tarkoittaa esimerkiksi asunnon ”avainten” haltuun saamista. Opinnäytetyön aihe valikoitui omasta kiinnostuksesta tietoturvaan yleisesti ja ennen kaikkea langattomiin verkkoihin.

Opinnäytetyön teoriaosuudessa perehdytään langattomiin lähiverkkoihin yleisesti sekä niiden tietoturvaan. Lisäksi tutustutaan penetraatiotestaamiseen ja sen työkaluihin samalla tutkien ja hyödyntäen laitetta nimeltä Wifi Pineapple. Käytännön osuudessa hyödynnetään Wifi Pineapplea testiympäristöön kohdistettavassa hyökkäyksessä. Osa hyökkäyksistä toteutetaan lisäksi vertailutarkoituksessa perinteisempää työkalua Kali-Linuxia ja sen eri sovelluksia käyttämällä. Testien tarkoitus on osoittaa verkon suojauksen tärkeys sekä painottamaan hyvän salasanan merkitystä.

Tavoitteena on käytännön ja teorian kautta saada hyvä peruskäsitys siitä mitä on langattoman verkon tietoturva. Työssä tavoitteena on lisäksi kuvata langattomien verkkojen penetraatiotestaus menetelmänä sekä millaisia testaustyökaluja on olemassa ja miten niitä käytetään. Tutkimuskysymykset tässä opinnäytetyössä ovat: Mikä on langaton lähiverkko? Mitkä ovat langattoman lähiverkon yleisimmät penetraatiotestausmenetelmät? Mitä Wifi-Pineapple Mark VII:lla tehdään?

2 Langaton lähiverkko ja sen tietoturva

Puhuttaessa langattomasta lähiverkosta tarkoitetaan WLAN-standardiin pohjautuvaa langatonta tiedonsiirtoa. WLAN-arkkitehtuuri koostuu kolmesta peruselementistä. Nämä elementit ovat langallinen lähiverkko (LAN) sekä langattomaan tiedonsiirtoon kykenevät laitteet, kuten kannettavat tietokoneet, älypuhelimet ja tabletit sekä langaton tukiasema. Tukiasema mahdollistaa kannettavien laitteiden liittymisen langattomasti langalliseen lähiverkkoon (LAN). (EUI, 2022)

2.1 WLAN Standardi

Standardi IEEE 802.11 on maailmanlaajuinen standardi, jossa laitteet kommunikoivat käyttäen hyväkseen 2.4 GHz:n sekä 5 GHz:n taajuuksia. Taajuudet jakautuvat kanaviin, joiden käyttö vaihtelee riippuen alueesta, jossa laite on käytössä. Standardin kehittäjänä tunnetaan Institute of Electrical and Electronics Engineers (IEEE). (Kyberturvallisuuskeskus, 2014) Standardia kehitetään työryhmissä. Jokainen standardin versio ilmaistaan pienellä kirjaimella standardin perässä, pois lukien ensimmäinen versio, joka julkaistiin kesäkuussa 1997 ja on 802.11 (Wikipedia, 2022)

WLAN yhteydestä puhutaan myös usein nimellä Wi-Fi. Wi-Fi-sanan luullaan usein tarkoittavan lyhennettä sanaparista Wireless Fidelity. Todellisuudessa sellaista ei ole olemassa eikä Wi-Fi sanana tarkoita mitään. Lyhenne on markkinointitoimiston käsialaa ja muodostui tarpeesta löytää käyttäjäystävällisempi termi markkinoida langattomia laitteita kuin IEEE 802.11. Nimi on sittemmin vakiintunut käytettäväksi langattomista verkoista puhuttaessa. Euroopassa yleisimmin käytössä on standardi 802.11 b/g/n laitteita, jotka toimivat 2.4 GHz:n taajuudella (EUI, 2022; Verizon, 2022)

2.2 Wi-Fi-verkon hyötyjä

Langaton lähiverkko, josta käytetään myös nimitystä Wi-Fi, on ennen kaikkea helppokäyttöinen. Se mahdollistaa useamman käyttäjän samanaikaisen liittymisen verkkoon ilman johtoja ja aikaa vievää konfigurointia. Verkko mahdollistaa myös liikkuvuuden sillä tukiaseman voi ottaa mukaan tai jakaa verkon hotspottekniikalla mobiililaitteelta kuten älypuhelimesta. Käyttöönotto on myös langallisiin verkkoihin verrattuna helpompaa.

Kaapeleita ei tarvitse vetää jokaiselle työpisteelle tai koneelle, ainoastaan Wi-Fi-tukiasemalle. Uuden tukiaseman lisääminen onnistuu yhtä helposti, mikä tekee langattomasta verkosta myös helposti laajennettavan. Sopivalla tunnistautumisella myös käyttäjien lisääminen on helppoa. Langattomat verkot ovat lisäksi langallisia verkkoja kustannustehokkaampi toteutustapa, sillä kaapeloinnin määrä vähenee huomattavasti. (Roomi, 2020)

Tuoreimpana lisäyksenä Wi-Fi-verkkoihin on käyttää kutsuttua Mesh-verkkoa, jolla voidaan luoda isompaankin kohteeseen luotettava ja nopea yhteys. Mesh-verkolla tarkoitetaan järjestelmää, jossa on kaksi tai useampi Mesh WLAN -tukiasemaa, jotka muodostavat yhden saumattoman verkon. Näin saadaan koko asunnon tai toimiston kattava verkko, jossa ei ole katveita. Perinteinen Wi-Fi-tukiasema muodostaa yhden liityntäpisteen. Yhden pisteen kantama on hyvin rajallinen ja parhaan signaalin saaminen on paikkasidonnaista. Mesh-verkossa yksi tukiasema toimii reitittimenä tai tukiasema on kytketty reitittimeen ja muut Mesh-tukiasemat toimivat sen satelliitteina. Nämä satelliitit uudelleen lähettävät verkkoa lähellä oleville asiakaslaitteille. Mesh-verkko on myös perinteistä Wi-Fi-verkkoa helpommin skaalattavissa. (Bayley & Halliday, 2022; Spadafora, 2022)

2.3 Wi-Fi-verkon heikkouksia

Useammasta salaustekniikasta huolimatta langattomien lähiverkkojen suurimpia heikkouksia on sen turvallisuus. Erityisesti tämä korostuu avoimissa julkisissa Wi-Fi-verkoissa, kuten kahviloiden ja hotellien tarjoamissa verkkoyhteyksissä. Lisäksi Wi-Fi-verkon kantama on rajallinen. Signaali heikkenee mitä kauempana käyttäjä kulloinkin on tukiasemasta, millä on vaikutusta verkon nopeuteen. Verkon nopeus on monesti myös heikkous, johon vaikuttaa esimerkiksi langattomaan verkkoon kytkettyjen laitteiden määrä. Normaalissa kotikäytössä nämä kuitenkin usein riittävät, sillä laitemäärät ja etäisyydet eivät ole liian suuria. 2.4 GHz:n taajuus on myös altis erilaisille häiriöille kuten esteille tukiaseman ja laitteen välissä, joka taas heikentää yhteyden laatua. (Roomi, 2020)

5 Ghz:n taajuudella toimiva Wi-Fi-verkko tuo käyttäjälleen nopeamman yhteyden, mutta langattoman verkon kantama laskee entisestään. 5 Ghz:n taajuudella on myös vieläkin huonompi kiinteiden esteiden kuten seinien läpäisykyky. (CenturyLink, 2022)

Osa päätelaitteista lähettää aktiivisesti kyselyitä, jotka hakevat laitteen muistamia langattomia verkkoja. Tämä ominaisuus voi johtaa siihen, että laite voi yhdistää samannimiseen verkkoon, eikä käyttäjän omaan verkkoon. Automaattinen yhdistäminen lisää riskiä sille, että laite tosiasiassa yhdistää ei toivottuun, mahdollisen hyökkääjän verkkoon, jolloin verkkoliikenteen kaappaaminen on mahdollista. (Kyberturvallisuuskeskus, 2014)

Langattomat verkot ovat alttiita myös erilaiselle häirinnälle, tahattomalle tai tahalliselle. Etenkin 2.4 GHz:n taajuudella toimii myös muita laitteita, jotka saattavat häiritä tahattomasti verkon toimintaa kuten tutkat ja mikroaaltouuni. On olemassa tahallisiakin tapoja häiritä langatonta verkkoliikennettä. Yksi tapa on Autentikointi- ja Assosiaatiotulvitus (Authentication / Assosiation flooding), jossa tukiasemaan kohdistetaan jatkuvalla syötöllä autentikointi- ja assosiaatiokehyksiä vaihtaen välissä MAC-osoitetta. Häirinnän tarkoitus on ylikuormittaa tukiaseman muisti ja prosessointi kyky niin, että se ei pysty enää palvelemaan oikeita asiakaslaitteita. (Armitage, 2011)

Myös Deautentikointitulvitus (De-authentication flooding) on verkon häirintää. Siinä hyödynnetään yhtä langattoman verkon heikkoutta. Tässä tavassa lähetetään kaikille tukiasemaan

yhdistäneille asiakaslaitteille deautentikointikehyksiä ja näin asiakaslaitteet jotka vastaanottavat kehykset katkaisevat välittömästi yhteytensä tukiasemaan. (Armitage, 2011)

Langattomien verkkojen salakuuntelu tai nuuskiminen (Wireless sniffing) on langattomuudesta johtuen helppoa. Langattomilla verkkosovittimilla voidaan kuunnella ympärillä olevaa liikennettä jota muut langattomat verkkolaitteet lähettävät. Kaikki tapahtuu ilman, että kuunteleva laite lähettää itse mitään signaalia. Tämä tekee sen havaitsemisesta miltei mahdotonta. (Grimmick, 2022)

2.4 WEP, WPA ja WPA2 (langattoman verkon suojaus)

Langattomien verkkojen suojauksen tarkoituksena on estää luvaton pääsy langattomaan verkkoon sekä estää verkossa liikkuvan tiedon varastaminen. Suojaus salaa verkkoliikenteen, tiedon sekä tiedostot, joita langattoman verkon yli lähetetään. (Toktabek, 2021)

Vanhin langattomien verkkojen suojaksi kehitetty protokolla on WEP (Wired Equivalent Privacy), joka ratifioitiin tietoturvastandardiksi vuonna 1999. Protokollan tarkoituksena oli tuoda langattomalle lähiverkolle langalliseen verkkoon verrattavissa oleva suojaustaso. WEPin tarkoituksena oli luoda hyvä tietoturva, mutta se kärsi monista tietoturvapuutteista, joita on yritetty parannella kuitenkaan tässä onnistumatta. WEP siirtyi virallisesti pois käytöstä vuonna 2004. WEP-suojauksen murtaminen on hyvinkin helppoa sen turvaprotokollaan liittyvien heikkouksien takia. Tapoja on monia kuten WEP-suojattujen pakettien murtaminen tai WEP-avaimen haltuun ottaminen.

Seuraavana suojausversiona kehitettiin WPA (Wi-Fi Protected access), jonka tarkoitus oli korvata WEP ja sen haavoittuvuudet. WPA julkaistiin vuonna 2003. Edeltäjäänsä verrattuna tämä versio on turvallisempi, sillä WPA käyttää 128-bittistä salausavainta, kun taas WPE käyttää 64- ja 128-bittistä salausavainta. WPA käyttää TKIP-protokollaa (Temporary Key Intergrity Protocol), jossa jokaiselle paketille tai tietoyksikölle luodaan oma uusi avain. TKIP-protokollan vaihtuva salausavain on WEP:n käyttämää kiinteää avainta turvallisempi.

WPA2 on WPA suojauksen seuraava versio, joka tuli käyttöön vuonna 2006. WPA verrattuna se on parempi, suurimpana erona on TKIP-protokollan sijaan 256-bittisen AES (Advanced Encryption Standard) -salauksen käyttö. (Armitage, 2011; Ghimiray, 2022; Hoffman, 2017; Panda Security, 2020)

WPA- ja WPA2-suojaukset ovat kuitenkin alttiita hyökkäyksille. Vaikka molemmat tekevät verkosta turvallisemman heikoin lenkki on kuitenkin salasana. Käyttäjien asettamat salasanat ovat usein liian lyhyitä tai suoraan yksittäisiä sanoja. Koska WPA ja WPA2 muodostavat salatun yhteyden avoimen nelivaiheisen kättelyn kautta on se mahdollista kaapata. Kaapattu kättely on taas mahdollista huonon salasanan takia murtaa esimerkiksi sanakirjahyökkäyksellä. (Armitage, 2011; Ghimiray, 2022)

2.5 WPA ja WPA2 nelivaiheinen kättely

WPA/WPA2 (4-way handshake) -kättelyllä tarkoitetaan ensimmäisiä neljää viestiä, jotka asiakaslaite ja tukiasema vaihtavat keskenään. Kättely tapahtuu asiakaslaitteen yrittäessä yhdistää tukiasemaan ja sen tarkoituksena on luoda salausavaimet, joilla langaton liikenne asiakaslaitteen ja tukiaseman välillä salataan. Kättelyn neljässä viestissä vaihdetaan prosessin aikana generoituja avaimia. Onnistuneen kättelyprosessin jälkeen virtuaalinen hallintaportti tukiaseman päässä avautuu ja liikennöinti voi alkaa salattuna. (Ronder, 2020; Wifi-professionals, 2019)

2.6 WLAN-verkon hallintakehykset

Hallintakehykset ovat yksi kolmesta 802.11 kehystyypistä. Kehystyypit liittyvät hallintaan, ohjaukseen sekä dataan. Hallintakehyksiä käytetään basic service set (BSS) -hallintaan, ohjauskehyksiä tietovälineisiin sisäänpääsyyn, kun taas datakehykset sisältävät erilaisia hyötykuormia eli käytännössä lähes kaiken liikenteen. Hallintakehykset mahdollistavat Wi-Fi-verkon ylläpidon, ja ne esimerkiksi kertovat tukiaseman läsnäolon sekä hallitsevat tukiasemaan liittymisen ja yhteyden katkaisun. Hallintakehyksillä on eri alatyyppejä, joita ovat beacon, probe, association, authentication sekä deauthentication.

Beacon-kehys kertoo ympäristöön tukiaseman läsnäolosta sekä pitää sisällään kaiken asiakaslaitteelle oleellisen tiedon kyseisestä verkosta. Näitä ovat verkon nimi (Service set identifier eli SSID), verkon nopeus, protokolla sekä muut tukiaseman modulaatioon liittyvät parametrit. Beacon-kehykset ovat oleellisia verkkojen löytymisen kannalta sillä ne ovat niitä, joita asiakaslaitteet kuuntelevat haettaessa lähiympäristön langattomia verkkoja.

Probe-kehykset edesauttavat verkon löytymistä. Ne jakautuvat kahteen osaan, pyyntöihin (probe request) sekä vastauksiin (probe response). Kun asiakaslaitteet etsivät verkkoja, ne lähettävät probe-pyyntöjä. Probe-vastaukset ovat tukiaseman vastine pyynnöille.

Association-kehyksiä on viisi tyyppiä, ja ne käsittävät myös pyyntöjä ja vastauksia. Yksi näistä tyypeistä on disassociation, jolla asiakaslaite kertoo haluavansa päättää tukiasemaan liittymisen.

Authentication-kehykset vuorostaan huolehtivat siitä, että asiakaslaite sekä tukiasema voivat ylipäätään olla yhteydessä toisiinsa. Alkujaan turvatasoja oli vain kaksi, avoin tai WEP-suojattu verkko, joista jälkimmäinen on sittemmin vanhentunut. Nykyään käytössä on WPA2-suojaus.

Kehykset ovat lähes aina avoimia huolimatta suojauksen tasosta ja varsinaisen autentikoinnin hoitaa myöhemmät kehykset, kunhan asema on jo autentikoitu sekä assosioitu. Deautentikointikehykset toimivat samankaltaisesti kuin disassosiationkehykset ja ne lähetetään asemalta toiselle yhteyden katkaisemiseksi. Esimerkiksi tukiasema voi lähettää deautentikointikehyksen sellaiselle asiakaslaitteelle, joka ei ole enää valtuutettu yhdistämään sen verkkoon. (Darchis, 2010; Hak5, 2022; Sharp, 2020)

3 Penetraatiotestaaminen

Penetraatiotestaaminen on tapa arvioida IT-infastruktuurin turvallisuutta, hyödyntäen turvallisesti ja luvallisesti mahdollisia haavoittuvaisuuksia eri palveluissa kuten käyttöjärjestelmissä, sovelluksissa, palveluissa ja verkkoyhteyksissä. Haavoittuvuudet voivat olla esimerkiksi virheelliset määrittelyt.

Penetraatiotestauksia tekevät erilaiset tietoturvayhtiöt asiakastöinä sekä yritysten omat asiantuntijat. Testaajat suorittavat hyökkäyksiä järjestelmiä vastaan tarkoituksena tunnistaa ja hyödyntää niiden haavoittuvaisuuksia. Tyypillisesti penetraatiotestaus toteutetaan käyttämällä manuaalisia tai automatisoituja tekniikoita, joilla järjestelmällisesti vaarannetaan kohteen palvelimia, verkkosovelluksia, langattomia verkkoja sekä muita mahdollisia kohteita. Usein yksikin onnistunut haavoittuvuuden hyödyntäminen avaa mahdollisuuden hyödyntää järjestelmää laajemman pääsyn mahdollistamiseksi.

Testaaminen koostuu useammasta vaiheesta. Ensimmäisessä vaiheessa määritellään tavoitteet sekä yleiset testaamisen aloittamiseen liittyvät asiat. Seuraavassa vaiheessa kerätään testattavasta kohteesta mahdollisimman paljon tietoa jota voidaan hyödyntää. Näitä tietoja ovat esimerkiksi IP-osoitteet, työntekijöiden nimet ja sähköpostiosoitteet sekä kohteen verkot. Kun tarvittava määrä tietoa on koottu, voidaan aloittaa penetraatiotestausten tekeminen, joiden tarkoituksena on näyttää miten syvälle verkkoon tai järjestelmään on mahdollista päästä.

Testaamisen lopputuloksena kootaan yhteen raportti, jossa kuvataan mitä on tehty sekä mihin järjestelmiin, sovelluksiin tai niiden osiin on päästy käsiksi sekä muut mahdolliset havaitut heikkoudet ja puutteet tietoturvassa. Raportin tarkoitus on olla työkalu, jolla voidaan tehdä tarvittavia korjaustoimia ja muutoksia turvallisemman IT-infrastruktuurin luomiseksi.

Lopuksi testaaja siivoaa jälkensä eli poistaa kaikki lisätyt asiat ja palauttaa muutokset, jotka voisi hyödyttää paikolleen jäädessään oikeita hyökkääjiä. Penetraatiotestauksen jälkeen asiakas voi aloittaa varsinaisten korjausten tekemisen ja paikkaamisen. (Core Security, 2022)

Myös langattomien lähiverkkojen penetraatiotestaus koostuu vaiheista, jotka ovat osittain samat kuin penetraatiotestaamisessa yleisesti. Tiedon kerääminen ja analysointi on erittäin tärkeä osa myös langattomien verkkojen testaamista. Tiedusteluvaiheessa on erittäin tärkeää tunnistaa kaikki kohdetaholle kuuluvat tai siihen mahdollisesti liittyvät langattomat verkot. Näistä on hyvä tunnistaa lisäksi mitkä verkot on tarkoitettu yrityksen oman laitteiston käyttöön ja mihin verkkoon henkilökohtaiset laitteet on kytketty. Seuraava vaihe on verkkojen tarkempi analysointi, jossa seulotaan tiedustelun tuloksena saadusta verkkolistauksesta verkkojen nimet sekä mitä laitteita verkkoon on yhdistetty. Analysointivaiheessa selvitetään verkkojen, yksittäisten laitteiden liikenne ja käyttömallit sekä käytössä olevat verkon kanavat, portit ja verkon osat. Kaikesta tehdystä selvityksestä on hyötyä seuraaviin vaiheisiin. Analyysien pohjalta tehty haavoittuvuuksien tunnistaminen auttaa määrittelemään mitä verkkoa tai verkkoja kohtaan lopulta hyökätään ja miten niihin päästään käsiksi. (”Bronze Hacker” Spinning Security, 2021)

3.1 WLAN penetraatiotestaamisen suosittuja työkaluja

Penetraatiotestaamisessa yleisesti käytettäviä työkaluja on useita ja riippuen hieman tahosta, suositut tai hyväksi havaitut työkalut vaihtelevat. Muutama nimi kuitenkin esiintyy erilaisilla ohjelmien listauksilla toistuvasti. Useimmilla listoilla esiintyviä ohjelmistoja ovat Metasploit, John the Ripper, Wireshark ja Aircrack-Ng.

Metasploit on arviolta näistä työkaluista tunnetuin sekä käytetyin testaustyökalu sen kattavien ominaisuuksien ansiosta. John the Ripper on salasanojen murtamiseen tehty työkalu. Wireshark on verkkoliikenteen analysointityökalu, joka ei itsessään ole penetraatiotestaamista varten, mutta on tähän kuitenkin erittäin hyödyllinen ja jopa tarpeellinen ohjelma. Aircrack-Ng on suosituin

erityisesti langattomien verkkojen testaamiseen tehty työkalu. (Fruhlinger & Prorup, 2021; Jevtic, 2019; Poston, 2021)

3.1.1 Brute-force

Brute-force-menetelmä perustuu salasanan tai muun tunnuksen arvaamiseen. Menetelmässä kokeillaan kaikkia mahdollisia numero- ja kirjainyhdistelmiä, kunnes oikea löytyy. Brute-forcing on aikaa vievää. Murrettavana olevan salasanan pituus vaikuttaa merkittävästi arvaamiseen käytetyn ajan määrään. Menetelmä murtaa helposti heikot, erityisesti lyhyet salasanat.

Yleisesti brute-force-hyökkäystä käytetään henkilökohtaisten tietojen kuten salasanojen, salauslauseiden, käyttäjänimien tai PIN-koodien hankintaan. Menetelmässä hyödynnetään erilaisia komentosarjoja tai tähän tarkoitukseen varta vasten tehtyjä sovelluksia, jotka systemaattisesti käyvät läpi eri salasanayhdistelmiä, kunnes oikea yhdistelmä löytyy. Testaaminen useimmiten lähtee yhden merkin salasanasta ja kun kaikki vaihtoehdot on testattu, testataan läpi kahden merkin salasanat ja niin edelleen. Yksi suosittu tällainen työkalu on esimerkiksi Aircrack-Ng. (Forcepoint, 2018; Grigas, 2022; Hoffman, 2013)

Se kuinka kauan arvaaminen kestää brute-force-menetelmällä riippuu myös pitkälti käytössä olevista komponenteista. Kaikkein tehokkain komponentti tähän tarkoitukseen on näytönohjaimet. Näytönohjaimia voidaan myös ajaa rinnakkain, jolloin useamman salausavaimen testaaminen onnistuu samanaikaisesti. (Hoffman, 2013)

3.1.2 Sanakirjahyökkäys

Sanakirjahyökkäys on menetelmänä samankaltainen kuin brute-force-hyökkäys. Erona menetelmien välillä on satunnaisten merkkien sijaan sanakirjan käyttäminen. Sanakirjahyökkäyksessä käytössä on lista sanoista, esimerkiksi yleisimmistä käytössä olevista salasanoista, joita menetelmässä käydään yksittäisesti tai niiden yhdistelminä systemaattisesti lävitse. Varsinaiset salasanalistat voivat olla kerättyjä aikaisemmista tietomurroista tai hyödyntävät oikeaa sanakirjaa kaikkine sanoineen. Arvioiden mukaan sanakirjahyökkäyksellä on brute-force-hyökkäystä paremmat mahdollisuudet onnistua. Esimerkiksi englannin kielessä on

huomattavasti vähemmän yksittäisiä sanoja kuin yhdistelmien määriä, mitä saadaan, kun käytetään sattumanvaraisesti kaikkia aakkosia ja numeroita.

Tunnetuin sanakirjahyökkäyksissä käytetty sanalista on nimeltään rockyou.txt. Tiedosto sai alkunsa 2009 jolloin RockYou niminen yritys hakkeroitiin. RockYou ei ollut salannut käyttäjiensä tietoja. Hyökkääjä sai haltuunsa 32 miljoonan käyttäjätilin listan selkokielisenä ja julkaisi koko listan kaikkien saataville. Se sisältää lähes 15 miljoonaa uniikkia salasanaa. (Burns, 2018; Cubrilovic, 2009; Grigas, 2022; Hoffman, 2013; HYPR, ei pvm.; Sullivan, ei pvm.)

3.2 Kali-Linux

Kali-Linux on erityisesti tietoturvan testaamiseen ja forensiikkaan suunnattu Linux-distribuutio. Kali-Linuxin tarina alkoi vuonna 2006, jolloin Kalin edeltäjä BackTrack sai alkunsa. BackTrack sai vuosien varrella viisi versiota, joista viimeinen on vuonna 2011 julkaistu versio, joka pohjautui Linux Ubuntuun. Vuonna 2013 BackTrack koki täydellisen muodonmuutoksen vaihtuen samalla Ubuntusta Linux Debian pohjaiseksi ja siitä tuli Kali-Linux (Kuva 1). Kali-Linuxia ylläpitää ja rahoittaa Offensive Security -yhtiö. Käyttöjärjestelmä kehitettiin tarpeeseen, jossa testattaviin ympäristöihin ei voinut viedä omia koneita ja missä ei ollut pääsyä internettiin. Testaamista varten tarvittiin siis valmis paketti, jossa olisi mahdollisimman kattava määrä työkaluja ja jota voisi käyttää ilman omaa konetta. Ensimmäinen versio olikin Live CD -muodossa.

Kuva 1 Kali-Linux työpöytänäkymästä

Kali-Linuxia voidaan pitää yhtenä kehittyneimmistä penetraatiotestaamisen työkaluista. Erilaisia penetraatiotestaustyökaluja löytyy valmiiksi asennettuna noin 600 kappaletta ja se onkin sananmukaisesti penetraatiotestauksen sveitsiläinen linkkuveitsi. Kali-Linuxin sisältämät työkalut eivät rajoitu vain langattomien lähiverkkojen testaamiseen. Se voidaan asentaa joko suoraan koneen ainoaksi käyttöjärjestelmäksi tai virtuaalialustalle, myös boottaaminen USB-tikulta on mahdollista. Näiden asennustapojen lisäksi löytyy oma versio myös yhden piirin tietokoneille kuten Raspberry Pi. Langattoman lähiverkon testaamiseen Kali-Linuxista löytyy suoraan esimerkiksi, Aircrack-Ng ja Wireshark sekä kättelyiden murtamiseen hashcat.

Kalista löytyy kaikki tarvittavat sovellukset langattomien verkkojen testaamista varten. Kali-Linux tarvitsee lisäksi yhteensopivan USB-verkkoadapterin, joka tukee vaadittavia ominaisuuksia. Ilman tarkoitukseen sopivaa adapteria ei verkkojen testaaminen ole Kali-Linuxilla käytännössä mahdollista. Sopivia USB-verkkoadaptereita ovat sellaiset, joiden ohjauspiirit mahdollistavat toimintatapansa muuttamisen. (BackTrack, ei pvm.; Linux Shell Tips, 2022; OffSec Services Limited, 2022; Williams, 2020; WirelesSHack, 2022)

3.3 Lainsäädäntö

Penetraatiotestaaminen on sallittua järjestelmän omistajan luvalla. Testaaminen perustuu usein sopimukseen testaamisesta testejä tekevän yrityksen/henkilön välillä. Luvaton tunkeutuminen järjestelmiin on lailla kielletty.

Suomen rikos- sekä tietosuojalaissa on säädetty kyberrikoksista. Tarkemmin Rikoslaki 38 luku (21.4.1995/578) Tieto- ja viestintärikoksista. Tietojärjestelmiin luvatta tunkeutuminen tai tietojärjestelmien häirintä on Suomen laissa kielletty sekä rangaistava teko, josta voi seurata vankeustuomio.

Rikoslain 34 luku (21.4.1995/578) Yleisvaarallisista rikoksista pykälissä 9 a § (10.4.2015/368) Vaaran aiheuttaminen tietojenkäsittelylle sekä 9 b § (11.5.2007/540) Tietoverkkorikosvälineen hallussapito, määritellään erilaisten ohjelmistojen ja laitteiden hallussapidosta ja levittämisestä, kun niitä tehdään tai levitetään tarkoituksena aiheuttaa vaara tai haittaa. (FINLEX Rikoslaki, 2022)

Tietosuojalaki määrittelee, kuinka henkilötietoja tulee käsitellä ja suojata jotta niiden päätyminen vääriin käsiin esimerkiksi tietomurron seurauksena olisi minimoitu. (FINLEX Tietosuojalaki, 2022)

Yhdysvalloissa laki 1986 Computer Fraud and Abuse Act (CFAA) kattaa hakkeroinnin laillisuusnäkökulman Yhdysvalloissa. Yhdysvalloissa yksi merkittävä ero on tuomiot, niiden pituus voi vaihdella yhdestä vuodesta jopa kymmeneen vuoteen. (NACDL, 2022; Zuckerman, 2021)

4 WIFI Pineapple mark VII

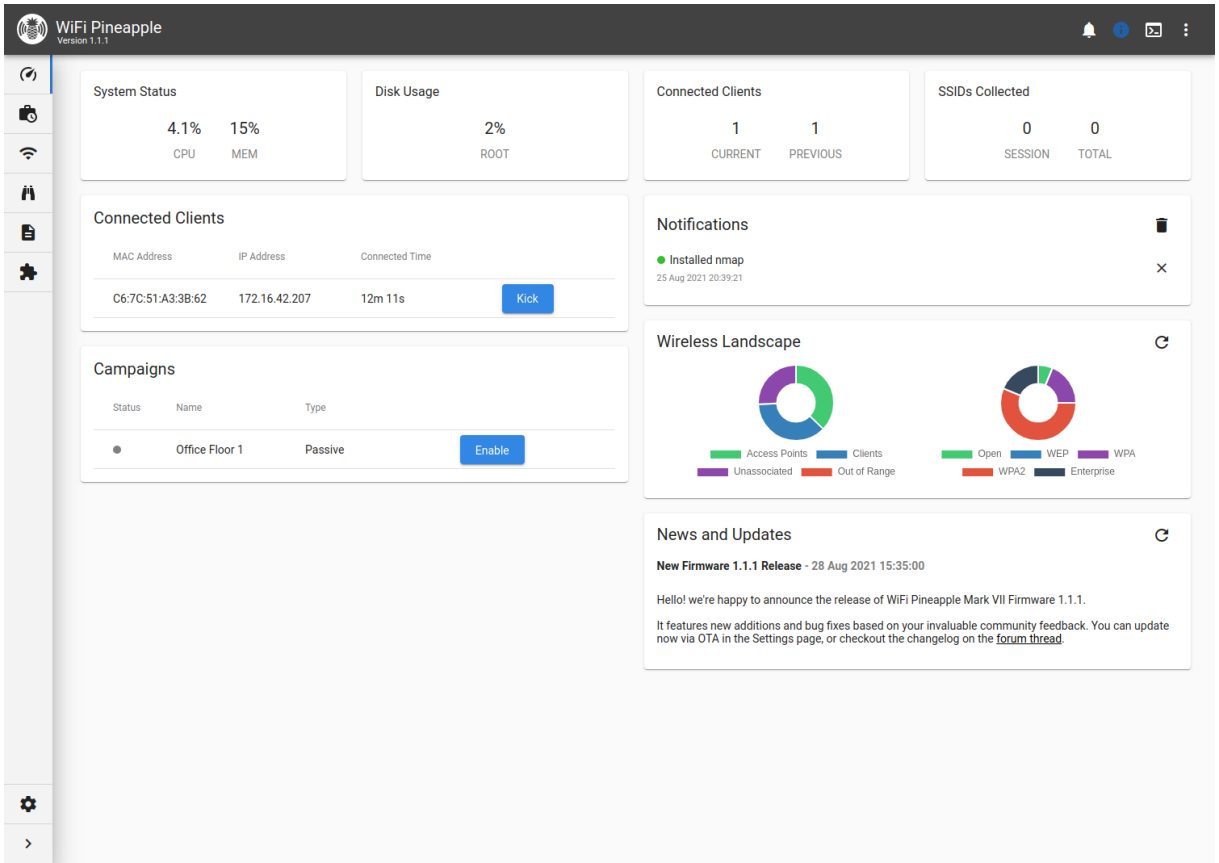
Wifi Pineapple eli tarkemmin Wifi Pineapple Mark VII (Kuva 2) on amerikkalaisen Hak5 LCC:n suunnittelema ja valmistama langattomien lähiverkkojen tietoturvan auditointiin ja testaamiseen kehitetty kannettava työkalu. Kyseessä on melko edullinen laite, joka avaa mahdollisuuksia omien verkkojen testaamiseen vaikkei omaisikaan kattavaa teknistä osaamista. Laite toimii 2.4.GHz:n taajuudella 802.11 b/g/n erillisen yhteensopivan verkkoadapterin avulla, sekä myös 5GHz:n taajuuksilla. Laitteessa on kolme Wi-Fi-radiota, jolle kullekin on annettu oma rooli. Sähkön syöttö ja ohjelmointi onnistuu USB-C-portin kautta. Laite sisältää sisäänrakennetun muistin, joka on kokoluokaltaan 256MB, RAM 2GB EMMC. (Hak5, 2022; Lutkevich, 2022)

Kuva 2 Wifi Pineapple Mark VII -laite (Hak5 LCC)

4.1 Ominaisuuksia

Wifi Pineapplen hallintaan voi käyttää sen selainpohjaista käyttöliittymää (Kuva 3), johon yhdistäminen onnistuu syöttämällä selaimeen laitteen IP-osoite. Käyttöliittymä vaatii kirjautumisen. Kirjautumisen jälkeen ensimmäisenä on laitteen kojetaulunäkymä (dashboard), josta käyttäjä näkee eri toimintoja kuten järjestelmän käyttöstatistiikkaa, sekä siihen liittyneet laitteet. Käyttöliittymässä on myös ilmoituskenttä, josta selviää eri toimintojen onnistuminen sekä niihin liittyvät varoitukset ja virheet. Kojetaulun viestikenttä huomauttaa lisäksi tarvittaessa mahdollisista ristiriidoista laitteen konfiguroinnissa. Sivuvalikosta löytyvät kaikki laitteen toiminnot sekä pääsy laitteen asetuksiin. Käyttöliittymä ja käytön helppous on tunnistettu yhdeksi Wifi Pineapplen vahvuuksista. (Hak5, 2022; Lutkevich, 2022)

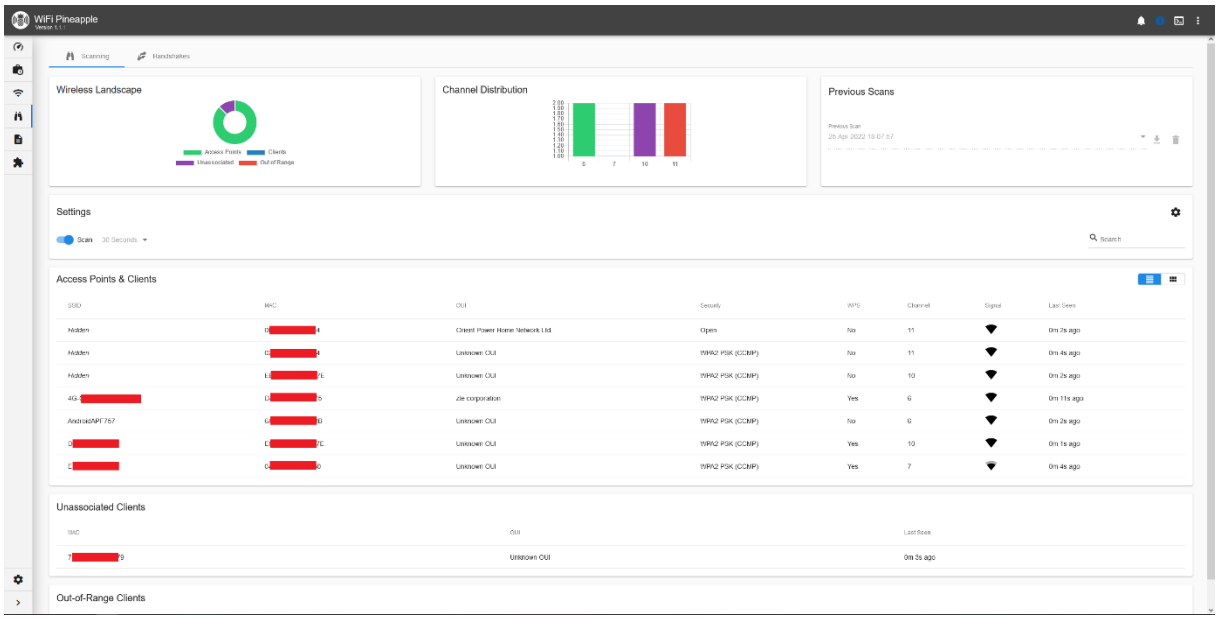
Kuva 3 Käyttöliittymän aloitusnäkymä kojelaudalla (Hak5 LCC)



4.1.1 Recon

Recon (Kuva 4) on Wifi Pineapplen päätyökalu, jolla kartoitetaan kohde verkot ja niiden ominaisuudet. Recon-näkymässä käyttäjä voi yhdellä silmäyksellä nähdä ympärillä olevat langattomat verkot. Näkymä kertoo suoraan verkon nimen, mac-osoitteen, laitevalmistajan, käytössä olevan salauksen tyypin, tukiaseman kanavan, signaalin voimakkuuden sekä sen onko WPS käytössä. Skannauksen jälkeen näkymään listautuu kaikki löydetyt tukiasemat sekä niihin liittyneet asiakaslaitteet (associated clients). Myös asiakaslaitteet, joiden verkkoassosiaatiota ei ole saatu selville (unassociates clients) näkyvät listalla.

Kuva 4 Recon-näkymä skannauksen jälkeen



Näkymästä voidaan valita mikä tahansa löydetty verkko ja kloonata se. Verkkojen nimiä voidaan myös kerätä varastoon myöhempää käyttöä varten. Asiakaslaitteita voidaan lisäksi lisätä suoraan pääsy- tai estolistalle. Deautentikointihyökkäyksen ja kättelyiden kaappaamisen aloitus ja kohdistaminen tiettyyn kohteeseen onnistuvat myös tästä näkymästä. (Hak5, 2022)

4.1.2 Kampanjat

Wifi Pineapplen kampanjat mahdollistavat automatisoitujen tehtävien luomisen testaamisen helpottamiseksi. Käyttöliittymä kertoo kunkin kampanjan tilan sekä tuottaa niistä raportin joko halutulla syklillä tai kun kampanja lopetetaan. (Hak5, 2022)

4.1.3 PineAP

PineAP-valikko pitää sisällään PineAP-prosessin asetukset sekä muita toimintoja. Aloitusvälilehdeltä löytyy varsinaiset asetukset kuten mitä ilmoituksia halutaan näytettävän. Sieltä voi myös asettaa laitteelle haluamansa MAC-osoitteen.

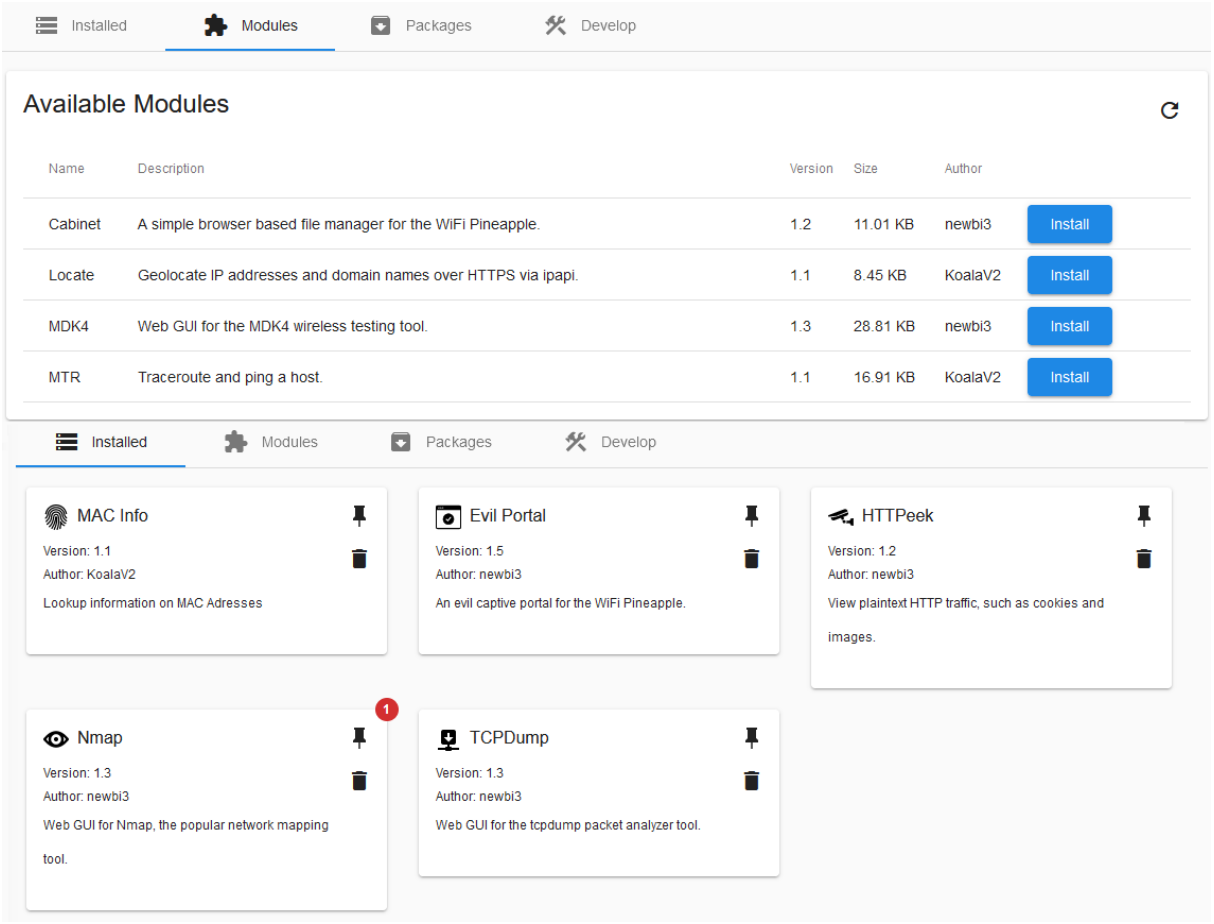
Sivulta löytyy lisäksi SSID-lista, johon kaikki havaitut SSID:t kerätään, mikäli toiminto on valittu käyttöön. Clients-välilehti listaa kaikki kyseisellä hetkellä, sekä aiemmin Wifi Pineapplen muodostamaan tukiasemaan liittyneet päätelaitteet. Laitteita voidaan myös suodattaa. Tukiaseman verkko on avoin, mutta suodatusvälilehdeltä voidaan asettaa rajoituksia verkon käytölle. Suodattimissa on esto- ja pääsytoiminnallisuudet, joita voidaan käyttää hyökkäyksen kohdentamiseen. Mikäli halutaan, että vain kohdelaite voi yhdistää lisätään kohdelaitteen MAC-osoite listalle, tämä onnistuu sen ollessa Salli-tilassa. Salli-tilassa listalla olevien laitteiden sallitaan yhdistää, kun taas Esto-tilassa kaikki muut paitsi listan laitteet voivat yhdistää tukiaseman luomaan verkkoon. Tukiasemat-välilehti sisältää asetukset luotuihin langattomiin verkkoihin. Wifi Pineapplesta löytyy oma tukiasema hallintaa varten, sekä aina avoin tukiasema.

Uudessa ohjelmistoversiossa 1.1.1 mukana tullut Evil WPA Access point, jossa WPA-kättelyiden kaappaaminen on oletustoiminto. Kunkin verkon nimeä voi muuttaa sekä päättää onko SSID näkyvissä vai piilotettu. Hallinta ja Evil WPA Access pointin voi myös halutessaan poistaa käytöstä. Avoimen verkon kohdalla voidaan myös muuttaa maa-asetusta sekä kanavaa. (Hak5, 2022)

4.1.4 Moduulit

Wifi Pineappleen on mahdollista ladata erilaisia lisämoduuleja (Kuva 5). Moduuleiden avulla laitteeseen saadaan lisää toiminnallisuutta jo olemassa olevien toimintojen päälle. Moduulit ovat laitteen käyttäjäyhteisön tekemiä ja kuka tahansa teknisesti kykenevä voi halutessaan tehdä oman lisäosan. Lisäosia on helppo asentaa ja käyttää moduulit välilehdeltä. Välilehdeltä löytyy asennetut ja saatavilla olevat moduulit ja jokaisessa moduulissa on myös lyhyt kuvaus. (Hak5, 2022)

Kuva 5 Saatavilla olevat sekä jo asennetut lisäosat



4.1.5 Deauthentication

Deauthentication on Pineappleen suoraan rakennettu ominaisuus, joka käyttää niin kutsuttua deautentikointihyökkäystä valittuun päätelaitteeseen tai tukiasemaan. Hyökkäyksestä käytetään myös nimitystä langaton erottamishyökkäys (englanniksi wireless disassociation attack).

Kyseinen hyökkäys on vaikea torjua sillä se hyödyntää suoraan 802.11 verkkojen hallintaan tarkoitettua deautentikointi-kehystä, jota asema käyttää, kun se haluaa katkaista päätelaitteen yhteyden. Tässä hyökkäyksessä kolmas osapuoli esiintyy tukiasemana ja lähettää sen nimissä deautentikointi-kehyksen kaikille tai tietylle asiakaslaitteelle, jonka seurauksena verkkoyhteys katkeaa. Tämä onnistuu koska kyseinen kehys liikkuu täysin salaamattomana. Tällaista hyökkäysmenetelmää voidaan erityisesti hyödyntää tilanteessa, jossa halutaan kohteen yhdistävän oman verkkonsa sijaan hyökkääjään verkkoon. (Atlas VPN, 2020; Hak5, 2022; Messer Studios LLC, 2018)

4.1.6 WPA-kättelyn kaappaaminen

WPA-kättelyn kaappaamisella löytyy suoraan oma painike. Kohdeverkon valinnan jälkeen laitteella voi aktivoida toiminnon yksinkertaisesti painamalla Capture handshakes -painiketta. Wifi Pineapple hoitaa hyökkäyksen itsenäisesti ja antaa ilmoituksen, kun kättely on saatu kaapattua. WPA-kättely itsessään on nelivaiheinen prosessi. Prosessilla todennetaan asiakaslaite ja salataan kaikki asiakaslaitteen ja tukiaseman välinen liikenne. (Gridelli, 2019; Hak5, 2022)

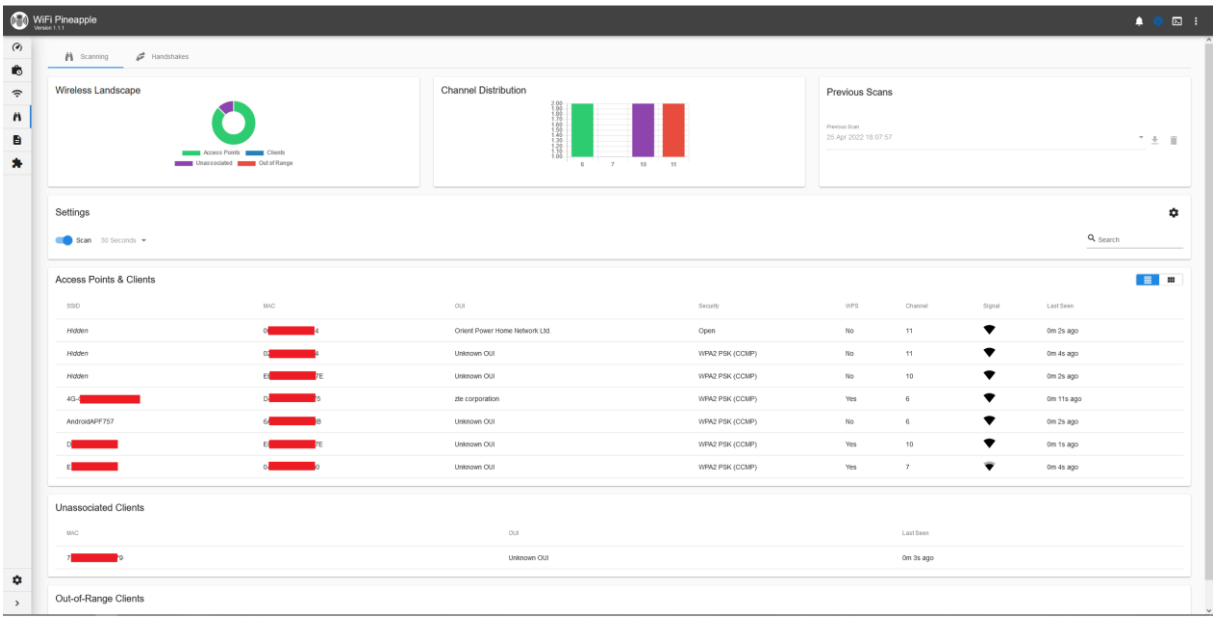
5 Käytännön testaus

Käytännön testien tekemiseen käytetään tässä opinnäytetyössä testiympäristöä, joka koostuu kuluttajalaitteista. Kohdelaitteina on kannettava Windows 10 -tietokone sekä Android-älypuhelin. Valintakriteerinä toimi kyseisen yhdistelmän yleisyys. Moni käyttäjä jakaa verkon kannettavalle tietokoneelleen juuri älypuhelimestaan. Jakamistapaa voidaan pitää yleisenä sekä koti- että työolosuhteissa. Suorittavina laitteina käytetään tehokkaalla grafiikkasuorittimella varustettua Windows 10 -pohjaista pöytäkonetta sekä tässä työssä kuvattua Wifi Pineapple Mark VII -laitetta. Käytössä oleva grafiikkasuoritin on malliltaan Nvidia GForce RTX 3070. Kali-Linux on asennettu Raspberry Pi 4 -versiolle, jossa 8GB muistia.

5.1 WPA2-kättelyn kaappaaminen Wifi Pineapplella

Käynnistetään Wifi Pineapple ja siirrytään Recon-välilehdelle. Koska testiympäristön laitteet ovat toistensa välittömässä läheisyydessä, käytetään testauksessa 30 sekunnin skannauspituutta (Kuva 6).

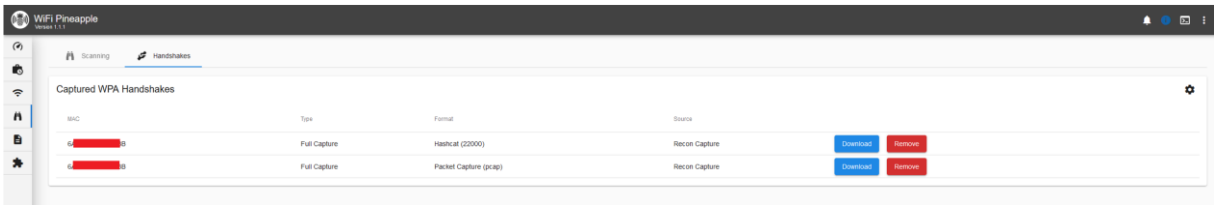
Kuva 6 Recon-näkymä skannauksen jälkeen



Listalta valitaan testaukseen haluttu kohdeverkko. Tässä tapauksessa kohdeverkko on AndroidAPF757, joka on saatavilla testiympäristössä käytetystä Android-älypuhelimesta. Tarkoitus on simuloida käyttäjää, joka jakaa yhteyden kannettavalle tietokoneelleen älypuhelimen kautta.

Verkon valinnan jälkeen käynnistetään Capture handshakes -toiminto. Tässä kohtaa yhdistetään testiympäristön Windows kone kohdeverkkoon, jotta kättely saadaan kaapattua nopeammin. Normaaliolosuhteissa sopivan verkkolaitteen yhdistämistä voi joutua odottamaan. Käyttöliittymä ilmoittaa oikean yläkulman viestikentässä ilmoituskuplalla, kun kättely on kaapattu (Kuva 7).

Kuva 7 Kättely on saatu onnistuneesti kaapattua.



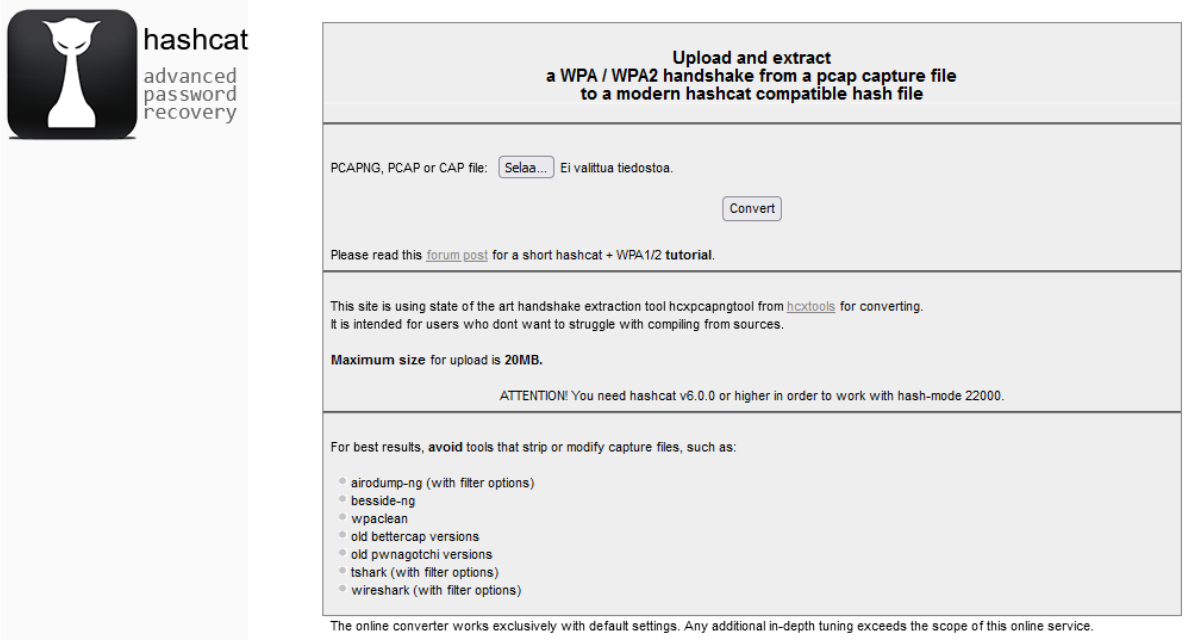
Kaapattu kättely muodostaa automaattisesti kaksi eri tiedostoversiota samasta kättelystä. Molemmat tai vain tarvittavan tiedoston voi ladata Handshakes-välilehden takaa Download-nappia painamalla. Tallennettaessa oletustiedostonimi sisältää aina laitteen MAC-osoitteen, jota kättely koskee, sekä tiedot Half tai Full, joka taas kertoo, onko kaappaus kokonainen vai osittainen. Tiedoston nimen voi halutessaan muuttaa. Tiedostojen päätteet ovat pcap sekä 22000, joista kumpaa tahansa voidaan käyttää murtamisvaiheessa.

5.2 WPA2 Brute-force -murtaminen

Kun kättely on saatu kaapattua, voidaan aloittaa sen murtaminen. Tätä tarkoitusta varten käytetään Windowsille saatavilla olevaan ohjelmaa hashcat, joka hyödyntää laskennassa koneen grafiikkasuoritinta. Ohjelma on ladattavissa hashcatin verkkosivuilta. Hashcat ei tue pcap -tiedostoja, joka tarkoittaa, että ne on muutettava tuettuun muotoon. Muuttaminen onnistuu suoraan hashcatin sivuilta löytyvällä selainpohjaisella työkalulla cap2hashcat (Kuva 8).

Koska testiympäristössä kättelyn kaappaaminen on tehty Wifi Pineapplella, ovat tiedostot (22000) suoraan yhteensopivia hascatille, eikä muuntamiselle ole tarvetta.

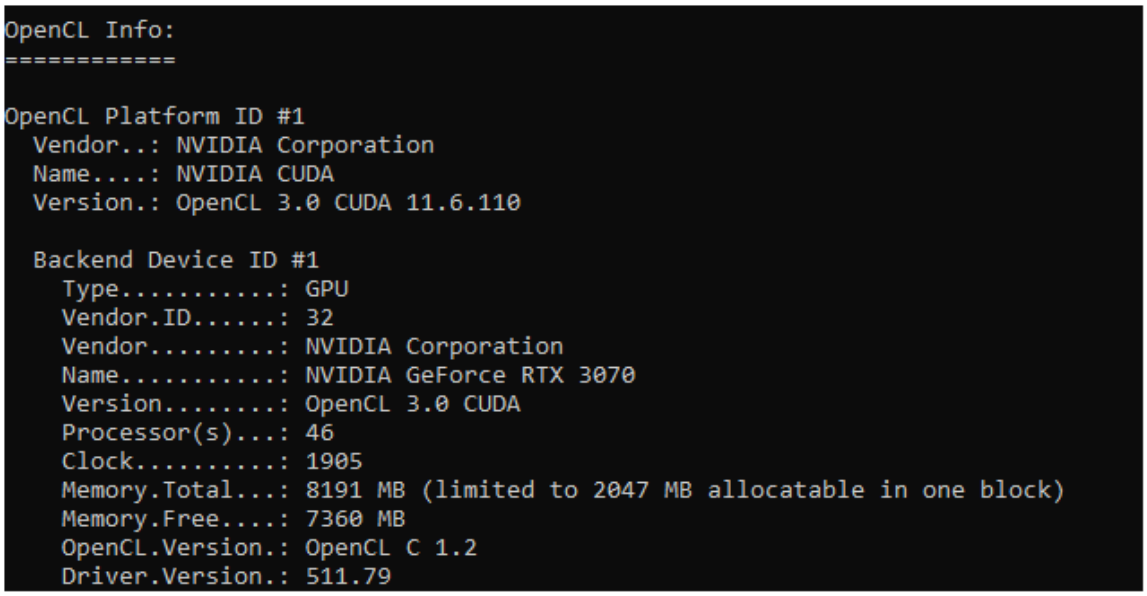
Kuva 8 cap2hashcat työkalu. (hashcat.net)



Hashcat on komentorivityökalu ja tätä varten avataan Windows 10 -komentorivi (command prompt) ja siirrytään kansioon johon hashcat on tallennettu. Tätä ennen kohdetiedosto (22000 tiedosto tai muunnettu pcap) siirretään samaan kansioon ohjelman kanssa. Jotta murtaminen voidaan aloittaa, luodaan tätä tarkoitusta varten käynnistyskomento, jossa määritellään mitä halutaan tehdä.

Komennolla hashcat.exe -I voidaan tarkistaa, löytyykö koneesta tarvittavat resurssit, eli onko koneessa salasanan murtamiseen soveltuva näytönohjain. Komennon tulos kertoo käytössä olevan näytönohjaimen tiedot, tehon sekä ominaisuudet (Kuva 9).

Kuva 9 hashcat.exe -I-komennon antama tulos



Itse murtamisen käynnistyskomento koostuu seuraavista osista:

1. Moodi: määritellään kohtaan -m, tässä tapauksessa 22000
2. Käytettävä hyökkäystapa määritellään kohtaan -a, tässä tapauksessa 3 eli Brute-force
3. Tiedoston nimi kokonaisuudessaan demo_full.22000
4. Lopuksi määritellään maksimi merkkimäärä sekä mitä merkkiryhmää tai merkkiryhmiä käytetään esimerkiksi, ?d tarkoittaa 1 arvattavaa merkkiä ja kokeiltavana pelkät numerot.
5. Loppuun voi halutessaan laittaa –show, joka näyttää lopputuloksen, mikäli murtaminen onnistuu.

Valmiiksi luodun merkkiryhmät ovat seuraavat:

?l = abcdefghijklmnopqrstuvwxyz

?u = ABCDEFGHIJKLMNOPQRSTUVWXYZ

?d = 0123456789

?h = 0123456789abcdef

?H = 0123456789ABCDEF

?s = «space»!"#$%&'()*+,-./:;<=>?@[\]^_`{|}~

?a = ?l?u?d?s

?b = 0x00 - 0xff

Kuvassa 10 nähdään komento, jolla käynnistetään murtoyritys sekä murron lopputulos. Rivin lopussa on verkon nimi sekä salasana kaksoispisteellä erotettuna (Kuva 10).

Kuva 10 Murtokomennon jälkeen saatu tulos

```
C:\Users\[redacted]\Downloads\hashcat>hashcat.exe -m 22000 -a 3 demo_full.22000 ?d?d?d?d?d?d?d?d --show
99b0db46615c8df1d0438f2d5378f5fe:6a42bb87be3b:d8f2ca1e9740:AndroidAPF757:62855277
```

5.3 WPA2 murtaminen sanakirjahyökkäyksellä

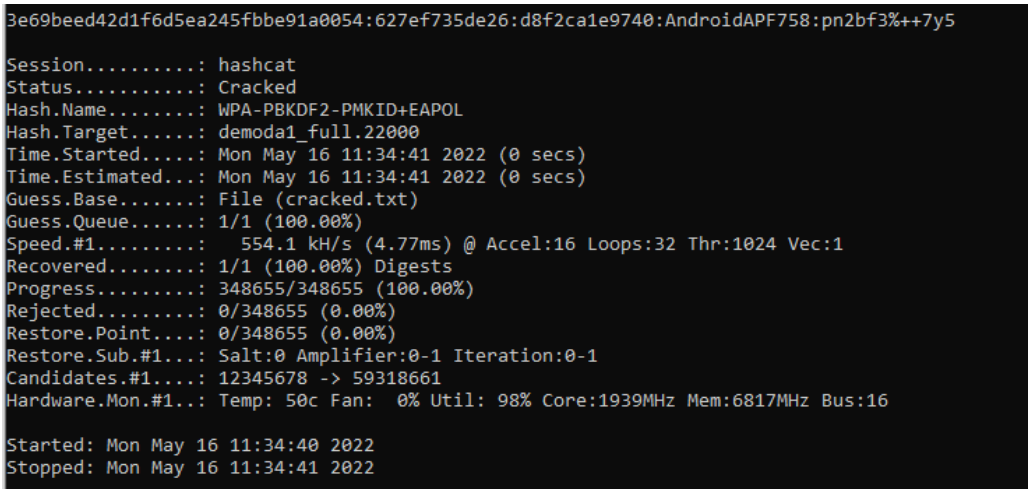
Sanakirjahyökkäyksen alkuvaiheet ovat samat kuin brute-force-hyökkäyksessä. Siirretään murrettava kättelytiedosto hashcat -kansion alle ja käynnistetään komentorivi. Hyökkäyksen toteutusta varten tarvitaan sanalista (englanniksi wordlist), joka sisältää murtamiseen kokeiltavia sanoja. Tätä testiä varten sanalista (cracket.txt) ladattiin suoraan hashcatin sivulta löytyvän linkin kautta. Cracked.txt tiedostossa oli salasanoja noin listattu 350 000 kappaletta. Toinen erittäin käytetty sanalista on nimeltään rockyou, joka rajattiin testauksen ulkopuolelle.

5.3.1 Testaus 1

Testaustarkoitusta varten WPA-kättelyn kaappausosiossa kuvattua langatonta verkkoa muutettiin selkeämmäksi vaihtamalla verkon nimi ja salasana. Testissä verkon nimeksi valikoitui AndroidAPF757 ja uudeksi salasanaksi käytettävältä listalta pn2bf3%++7y5, joka saattaa vaikuttaa melko vahvalta salasanalta. Tässä piileekin yksi sanakirjahyökkäyksen etu, jos salasana on jo vuotanut jossain yhteydessä ja päätynyt tällaiselle listalle. Tässä yhteydessä on hyvä korostaa, että samojen salasanojen käyttäminen eri palveluissa ole tietoturvallista ja että salasana on hyvä muuttaa ainakin silloin, kun palveluntarjoaja siihen kehottaa.

Testauksessa voidaan tehdä havainto, että vaikka salasana olisikin melko kompleksinen, ei sen murtamiseen mene kuin sekunti. Yhtä lailla, jos salaukseen on käytetty huonoa salasanaa kuten password1 tai ylipäätään mitä tahansa salasanaa, joka on vuotanut selkokielisenä tietomurron yhteydessä esimerkiksi cracket.txt tyyppiselle sanalistalle on salasana helppo murtaa. Sanakirjahyökkäystä käytettäessä ei salasanan kompleksisuudella tai pituudella ole merkitystä (Kuva 11).

Kuva 11 Murtokomennon jälkeen saatu tulos

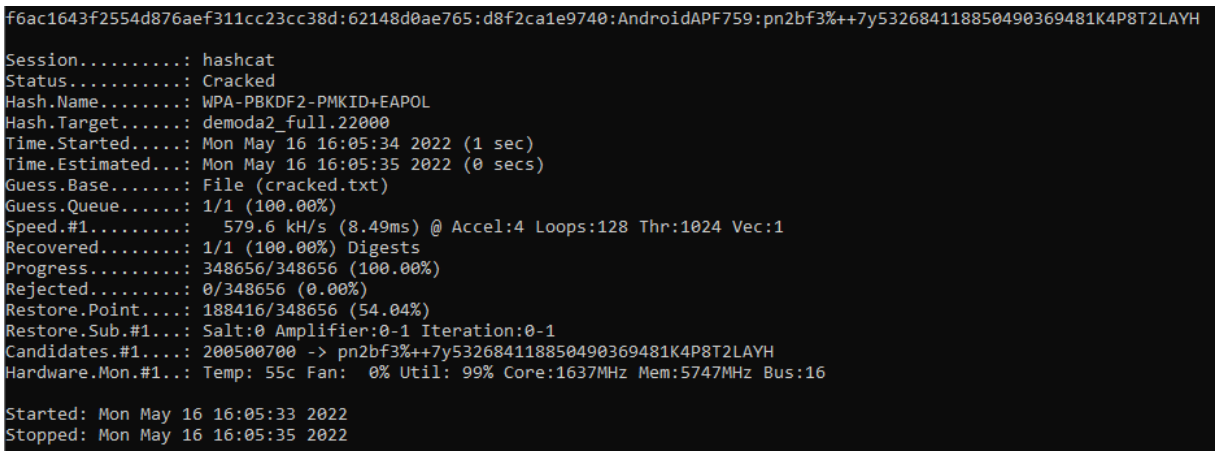


5.3.2 Testaus 2

Toisena testausesimerkkinä laadittiin toinen verkko ja siihen salasanaksi yhdistelmä kolmesta listalla olleesta salasanasta. Testaussalasanasta pn2bf3%++7y532684118850490369481K4P8T2LAYH saatiin näin yhteensä 43 merkin pituinen, kaikkia eri merkkityyppejä sisältävä pätevä salasana. Tällaisen salasanan murtaminen brute-forcella veisi esimerkiksi How secure is my password -sivuston (https://www.security.org/how-secure-is-my-password/) mukaan 13 novemdecillionaa vuotta (10^{60}). Tässä yhteydessä on hyvä todeta huomio siitä, että pätevien salasanojen laatimisen haasteeksi muodostuu yleisesti se mihin kyseistä salasanaa käytät ja kuinka monessa paikassa.

Testaussalasana lisättiin salasanalistalle. Komento käynnistämiselle on sama, muutettiin vain kohdetiedoston nimi. Tällä kertaa testikaappauksen onnistumiseen aikaa kului kaksi sekuntia (Kuva 12). Luonnollisesti oikean salasanan löytäminen kestää mitä enemmän on testattavaa, jos listalla olisi 350000 sanan sijaan esimerkiksi 10 miljoonaa sanaa.

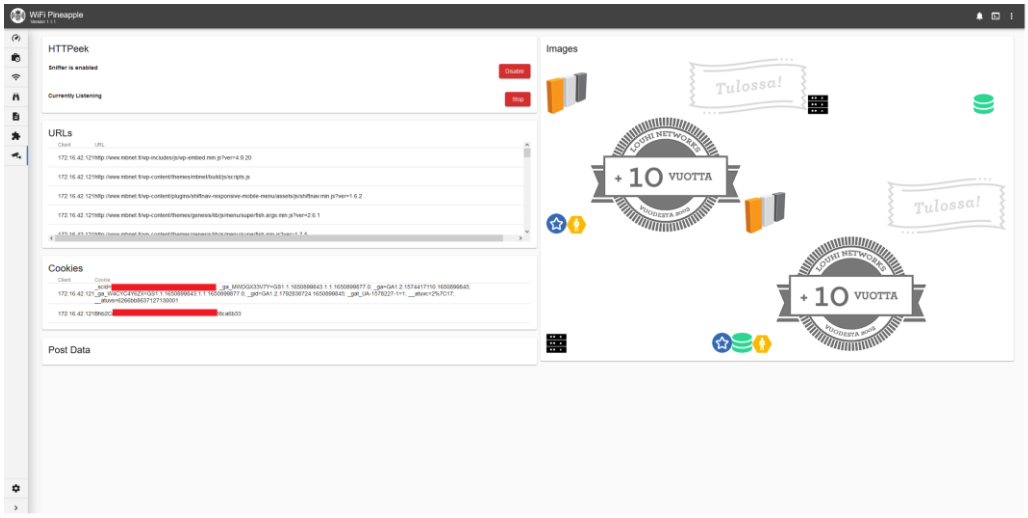
Kuva 12 Tulos pitkän salasanan murtamisesta



5.4 Salaamattoman liikenteen monitorointi

Vaikka salaamaton verkkoliikenne (http) alkaa olla poistuva tapa ja lähes kaikki selaimet pakottavat salatun verkkoliikenteen https-protokollan kautta, ei se kuitenkaan ole täysin poistunut käytöstä. Tässä testissä luodaan Wifi Pineapplella tarkoitusta varten esimerkiksi kahvilan avointa verkkoa demonstroiva asiakasverkko. Annettiin verkon nimeksi Demo ja muutettiin Wifi Pineapplen suodatin deny-toiminnolle. Tämä suodatin vaihtaa toimivuuden niin, että listatut Mac-osoitteet eivät pääse yhdistämään luotuun verkkoon ja listaamattomat taas pääsevät. Tämä on menetelmässä helpoin tapa sallia verkkoliikenne juuri pystytetylle tukiasemalle. Deny-toimintovalinnan jälkeen yhdistettiin testiympäristön kone kyseiseen verkkoon. Monitoroinnissa hyödynnetään yhtä saatavilla olevaa HTTPeek-moduulia, joka näyttää käyttöliittymässä mitä salaamatonta liikennettä kukin yhdistänyt laite tuottaa (Kuva 13).

Kuva 13 HTTPeek-näkymä skannauksen jälkeen



Testausta varten selattiin tarkoituksella salaamattomia sivuja kuten http://mbnet.fi. Tällaisten sivujen vierailut näkyivät heti listalla, kuten myös vieraillulla sivulla olevat kuvat. HTTPeek listaa myös suojaamattomien sivujen evästeet. Vaikka sivusto saattaisikin olla suojatun yhteyden takana, voi siitä olla kuitenkin olemassa myös suojaamaton versio, mikä saattaa vuotaa suojatulle sivustolle mentäessä. Sivustoilla voi lisäksi olla elementtejä suojaamattomista lähteistä, jotka paljastavat sivun, jossa käyttäjä vierailee vaikkei itse sivustolle meneminen näkyisi.

Yhtenä havaintona testauksessa tehtiin, että myös Microsoft käyttää päivitysten tai muiden vastaavien kyselyihin tai jakeluun http-osoitteiden takana olevia tiedostoja. Ilman selaimen avaamista listalle alkoi kertyä näitä osoitteita, joihin jokin käytettävän Windows koneen taustapalvelu yhdisti.

5.5 WPA2-kättelyn kaappaaminen ja murtaminen Kali-Linuxilla

Testeissä käytetty Kali-Linux oli asennettu Raspberry Pi tietokoneelle käyttäen sille tarkoitettua tiedostoa, joka on ladattavissa Kalin verkkosivuilta. Kali-Linuxista löytyy valmiiksi asennettuna useampikin ohjelmisto, jolla kaappaaminen voidaan suorittaa tai joilla sitä voidaan ainakin yrittää. Tässä testauksessa käytetään Aircrack-Ng työkalua. Koska työkaluja ei tarvitse asentaa voidaan aloittaa prosessi suoraan tarkistamalla langattoman verkkokortin nimi ja tila (Komento 1).

Komento 1 Verkkokortin nimi ja tila komento

```
iwconfig
```

Kun nimi on tiedossa, voidaan asettaa verkkokortti monitorointitilaan. Verkkosovittimen on oltava malliltaan sellainen, että se tukee monitorointitilaa. Listat tuettuihin verkkosovittimiin löytyy Kali-Linuxin sivuilta. Sopivista korteista löytyy myös paljon vertailua. Tässä tapauksessa Raspberry Pi:n integroitu sovitin toimii suoraan ja sen nimi on wlan0. Ennen aloitusta voi olla hyvä sulkea prosesseja, jotka saattavat vaikuttaa monitoroinnin onnistumiseen (Komento 2). Aircrack-Ng huomauttaa asiasta, mikäli tätä ei ole tehty ennen verkkokortin tilan muutosta (Komento 3).

Komento 2 Häiritsevien prosessien sulkeminen ennen aloitusta

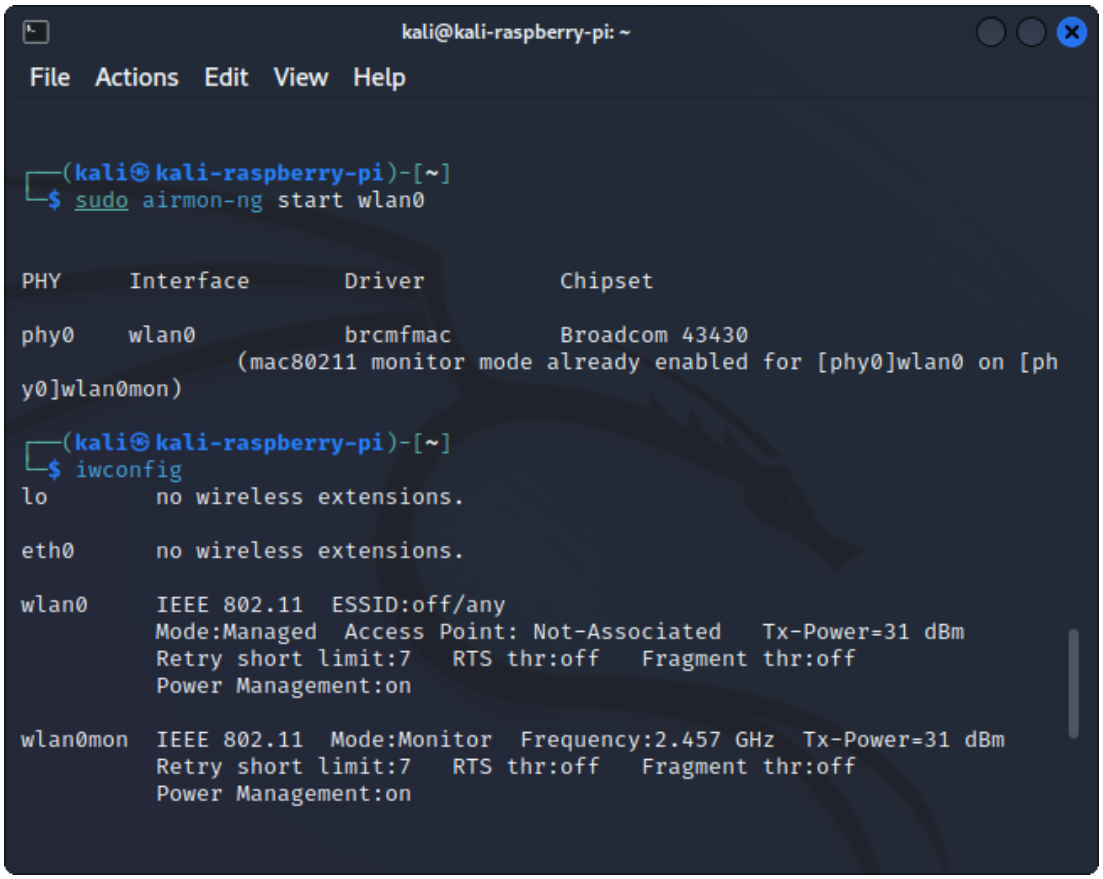
```
sudo airmon-ng check kill
```

Komento 3 Monitorointi tilan käynnistäminen

```
sudo airmon-ng start wlan0
```

Kun monitorointi tila on kytketty päälle, voidaan vielä varmistaa, että tila on vaihtunut (Kuva 14).

Kuva 14 Kuvakaappaus komentojen tuloksista



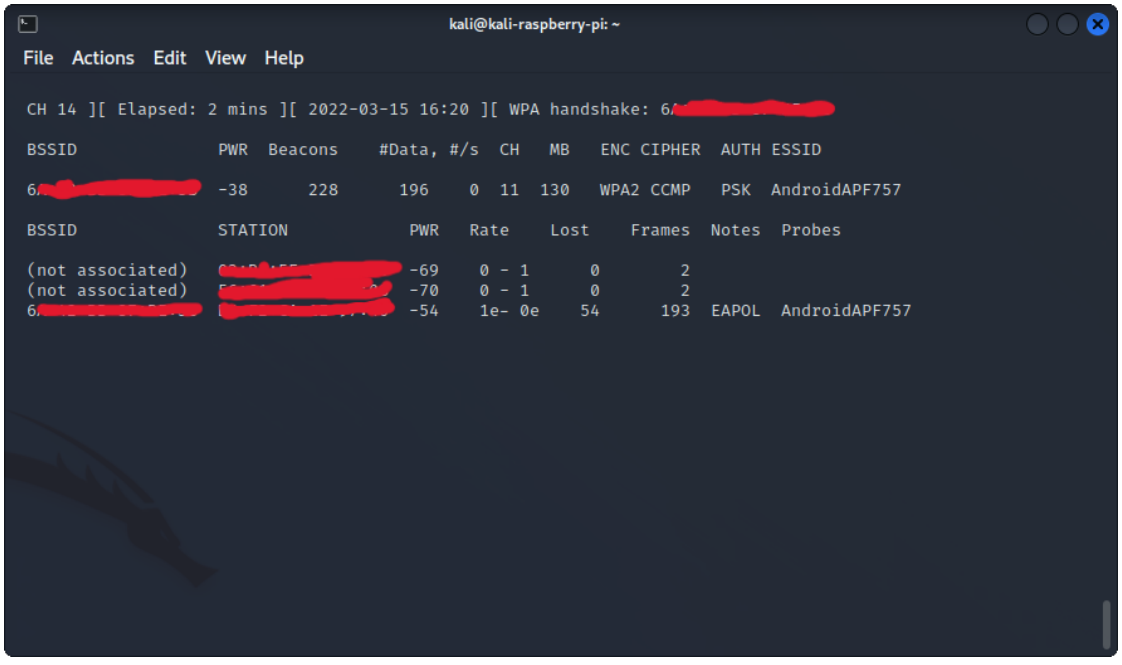
Seuraava vaihe on aloittaa liikenteen monitorointi WPA-kättelyn kaappaamiseksi. Kohdeverkon nimen ollessa tiedossa voidaan monitorointi kohdistaa suoraan vain haluttuun kohdeverkkoon, AndroidAPF757 (Komento 4).

Komento 4 Käynnistä liikenteen monitorointi

```
sudo airodump-ng --essid AndroidAPF757 -w psk wlan0mon
```

Kättelyn onnistunut kaappaaminen saattaa viedä aikaa, mikäli ei haluta käyttää deautentikointia jotta asiakaslaitteet yhdistäisivät uudelleen. Testissä ajan säästämiseksi asiakaslaitteen WLAN-yhteyttä yhdistettiin ja katkaistiin laitteen päästä. Kättelyn kaappaamiseen kului lopulta aikaa kaksi minuuttia (Kuva 15).

Kuva 15 Kuvakaappaus monitorointi ja onnistunut kättelyn kaappaus



Kättelyn kaappauksen jälkeen seuraava vaihe on murtaa kättely, joka onnistuu myös Aircrack-Ng-ohjelmaa käyttämällä. Avataan uusi Aircrack-Ng-istunto ja laaditaan komento kättelyn murtamista varten. Tätäkin komentoa on mahdollista muokata tarkoitukseen sopivaksi. Käytetään sanakirjahyökkäystä ja samaa aiemmassakin testauksessa käytettyä cracked.txt tiedostoa, johon on lisätty oikea salasana demotarkoituksessa. Komennossa määritellään mitä ollaan tekemässä, käytettävä sanalista ja sen sijainti sekä kohde (Komento 5).

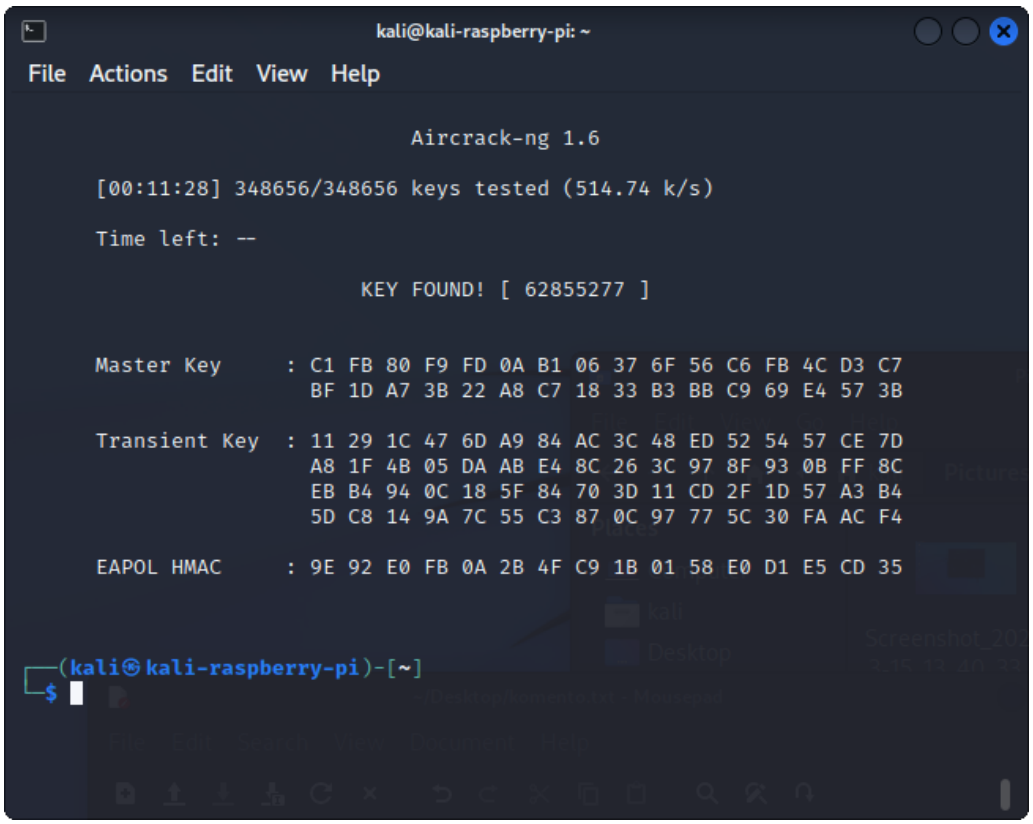
Komento 5 Käynnistä kättelyn murtaminen

```
sudo aircrack-ng -w /home/kali/Desktop/cracked.txt -e AndroidAPF757 psk*.cap
```

Monitorointi luo psk-01.cap mallisia tiedostoja, joissa numerointi on juokseva. Komennon psk*.cap osiolla haetaan kaikkia .cap-tiedostoja, joiden nimessä esiintyy psk. -w määrittelee käytettävän sanalistan. -e kertoo kohteen, tässä tapauksessa -e sillä käytetään essid:tä -b olisi vaihtoehtoisesti bssid. Komennon syöttämisen jälkeen tarkennetaan vielä avautuvalta listalta oikea kohde. Listalla näkyy myös, että verkosta on saatavilla kättely.

Kun kohde on valittu alkaa itse murtaminen. Käytössä olleella sanalistalla oli noin 350 000 salasanaa sekä viimeisenä oikea, käytössä oleva salasana. Raspberry Pi:n suorituskyvyllä koko listan läpikäyminen vei aikaa yksitoista minuuttia. Tuloksena saatiin sama salasana 62855277, joka havainnollistuu Kuvasta 16 selviää myös testattujen sanojen kokonaismäärä ja aika jota testaamiseen käytettiin (Kuva 16). Raspberry Pi ei missään tapauksessa ole tarkoitukseen erityisen tehokas, mutta se suoriutui tehtävästä melko nopeasti.

Kuva 16 Kuvakaappaus onnistuneesta kättelyn murtamisesta.



6 Yhteenveto, johtopäätökset ja pohdinta

Hyvän tietoturvan rooli korostuu etenkin langattomissa verkoissa. Yhä useampi kodin toiminto nojaa verkkoyhteyksiin. Langattomien verkkojen avulla nykyisin esimerkiksi kodissa avataan ovia, käynnistetään laitteita sekä valvotaan tiloja kameroin. Kaikki edellä mainitut esimerkit ovat sellaisia toimintoja, joihin ei halua ulkopuolisten pääsevän käsiksi, vaan ne halutaan turvata.

Opinnäytetyön tavoitteena oli käytännön ja teorian kautta antaa hyvä peruskäsitys siitä, mitä on langattoman verkon tietoturva. Työssä tavoitteena oli lisäksi kuvata langattomien verkkojen penetraatiotestaus menetelmänä sekä millaisia testaustyökaluja on olemassa ja miten niitä käytetään. Käytännön osuudessa onnistuttiin hyödyntämään Wifi Pineapplea testiympäristöön kohdistetussa hyökkäyksessä. Myös verrokkihyökkäys Kali-Linux käyttöjärjestelmää käyttäen toteutui onnistuneesti. Wifi Pineapple on hyvä ja tehokas työkalu, mutta käyttötarkoitus on rajattu. Wifi Pineapple toimii nimenomaan täsmätyökaluna langattomien lähiverkkojen testaamiseen. Kali-Linux oli myös yllättävän helppokäyttöinen. Hyökkäysten toteutus ei kuitenkaan ollut yhtä jouhevaa kuin Wifi Pineapplella.

Verrattaessa Kali-Linuxia ja Wifi Pineapplea toistensa kesken on selvää, että Kali-Linux on huomattavasti kattavampi työkalu penetraatiotestaamiseen. Kali-Linuxilla pystyy siis tekemään kaiken sen mitä Wifi Pineapplella, ja huomattavasti enemmänkin. Jos kuitenkin tarkastellaan näitä kahta ainoastaan langattomien verkkojen näkökulmasta, Wifi Pineapplen etu on käytettävyys ja käytettävyyden helppous. Ei ole tarvetta miettiä yhteensopivaa langatonta USB-verkkoadapteria, sillä laitteessa on niitä kolme kappaletta. Myös liikuteltavuus on etu, koska Wifi Pineapplelle voi antaa suoraan virran tavallisesta puhelimelle tarkoitetusta varavirta-akusta. Molemmat voi sijoittaa vaikkapa reppuun. Selainpohjaisen käyttöliittymän sekä WiFi-käytön avulla voi repussa olevasta Wifi Pineapplesta käynnistää hyökkäyksiä ja skannauksia ilman, että fyysisesti ihmisten nähtävillä on mitään erikoisia laitteita. Kokonaisuus mahtuu periaatteessa jopa taskuun. Kaikki vieläpä onnistuu tuolloin vain älypuhelinta vilkaisemalla, joka nykyaikana ei edes pidempikestoisena katseluna herätä epäilyksiä ihmisissä. Huomaamattomuus on myös etu.

Kali-Linux on myös ajettavissa erilaisissa laitteissa, mutta sen käytettävyys eikä huomaamattomuus ole aivan samaa luokkaa. Kovin usein käytössä on kannettava tietokone ja siinä johdolla kiinni Alfan valmistama USB-verkkosovitin pitkällä antennillaan. Tietysti on mahdollista ajaa Kali-Linuxia

myös huomaamattomammin, kuten vaikkapa Raspberry Pi:lla. Kali-Linux on hyvinkin tunnistettava, mikäli joku asiaan vihkiytynyt voi nähdä tietokoneen näytön. Ulkopuolelle kytketyt isot kojeet ja antennit eivät myöskään ole peruskäytössä tätä päivää, jolloin sellaisen käyttö julkisella paikalla voi jo herättää maalikoissakin ihmetystä. Verkkokaappauksissa ylimääräinen huomio on tietysti huono asia, mikäli tarkoituksena on olla herättämättä huomiota. Wifi Pineapplessa sen toiminnot ovat graafisessa käyttöliittymässä, jonka seurauksena vaikkapa WPA-kättelyn kaappaaminen tietystä verkosta on parin valinnan takana.

Vaikka Kali-Linuxissa onkin hieno graafinen käyttöliittymä, ovat työkalut käytännössä kaikki kuitenkin komentorivityökaluja, joka tarkoittaa sitä, että asioiden aikaansaaminen vaatii komentojen osaamista tai muistilistan käyttöä. Toimivien komentojen aikaansaaminen aiheutti testausta tehdessä jonkin verran haasteita. Lopputulos oli kuitenkin onnistunut.

Kali-Linux sisältää suoraan mittavan määrän työkaluja ilman, että niitä tarvitsee erikseen etsiä ja asentaa. Valmiina löytyvät myös ne työkalut, joita tässä opinnäytetyössä on käytetty aiemmin, mutta siitä itsestään puuttuu verkkotoiminnallisuus, kun taas Wifi Pineapplesta puuttuu monia toimintoja Kali-Linuxiin verrattuna, mutta langaton verkkotoiminnallisuus löytyy. Molemmille on siis paikkansa.

Omat tavoitteeni oli opinnäytetyön aikana oppia käyttämään Wifi Pineapplea ja Kali-Linuxia sekä perehtyä siihen mitä penetraatiotestaaminen on käytännössä. Mielestäni onnistuin vastaamaan tutkimuskysymyksiin hyvin. Wifi Pineapplesta muodostui hyvä kuva mikä se on ja mitä sillä pystytään tekemään. Kuvan muodostumista tuki mahdollisuus itse käyttää laitetta. Aihe on mielenkiintoinen ja tarkoitus on kerätä tietoa ja osaamista tietoturvasta myös tulevaisuudessa. Toivottavasti työ innoittaa myös muita tietoturvasta kiinnostuneita tutkimaan aihetta.

Lähteet

Armitage, S. (2011, lokakuuta). *Known wireless attacks | Jisc community*. https://community.jisc.ac.uk/library/advisory-services/known-wireless-attacks

Atlas VPN, C. R. (2020, marraskuuta 5). *What is a deauthentication attack? - Atlas VPN*. https://atlasvpn.com/blog/what-is-a-deauthentication-attack

BackTrack. (ei pvm.). *BackTrack Linux—Penetration Testing Distribution*. Noudettu 16. elokuuta 2022, osoitteesta https://www.backtrack-linux.org/

Bayley, D., & Halliday, F. (2022, heinäkuuta). *Mesh Wi-Fi vs Traditional Routers: Which is better? - PC World Australia*. https://www.pcworld.idg.com.au/article/659354/mesh-wi-fi-vs-traditional-routers-which-better/

”Bronze Hacker” Spinning Security. (2021, kesäkuuta 22). *WiFi Pentesting Complete Guide for Beginners 2022*. https://spinningsecurity.com/wifi-pentesting-guide-for-beginners/

Burns, W. J. (2018). *Common Password List (rockyou.txt)*. https://www.kaggle.com/datasets/wjburns/common-password-list-rockyoutxt

CenturyLink. (2022). *2.4 GHz vs. 5 GHz WiFi*. https://www.centurylink.com/home/help/internet/wireless/which-frequency-should-you-use.html

Core Security. (2022). *What is Penetration Testing? | Core Security*. https://www.coresecurity.com/penetration-testing

Cubrilovic, N. (2009, joulukuuta 15). RockYou Hack: From Bad To Worse. *TechCrunch*. https://social.techcrunch.com/2009/12/14/rockyou-hack-security-myspace-facebook-passwords/

Darchis, N. (2010, lokakuuta 25). *802.11 frames: A starter guide to learn wireless sniffer traces*. https://community.cisco.com/t5/wireless-mobility-documents/802-11-frames-a-starter-guide-to-learn-wireless-sniffer-traces/ta-p/3110019

EUI. (2022, marraskuuta 4). *Technical Overview of Wireless Networking, Security and Compliance*. European University Institute. https://www.eui.eu/ServicesAndAdmin/ComputingService/Network/WiFiOverview

FINLEX Rikoslaki, E. P. O. (2022, kesäkuuta 27). *FINLEX ® - Ajantasainen lainsäädäntö: Rikoslaki 39/1889*. Oikeusministeriö, Edita Publishing Oy. https://www.finlex.fi/fi/laki/ajantasa/1889/18890039001#L38P9

FINLEX Tietosuojalaki, E. P. O. (2022, heinäkuuta 27). *FINLEX ® - Ajantasainen lainsäädäntö: Tietosuojalaki 1050/2018*. Oikeusministeriö, Edita Publishing Oy. https://www.finlex.fi/fi/laki/ajantasa/2018/20181050#L4P26

Forcepoint. (2018, marraskuuta 9). *What is a Brute Force Attack? Forcepoint*. https://www.forcepoint.com/cyber-edu/brute-force-attack

Fruhlinger, J., & Prorup, J. M. (2021, joulukuuta 13). *11 penetration testing tools the pros use*. CSO Online. https://www.csoonline.com/article/2943524/11-penetration-testing-tools-the-pros-use.html

Ghimiray, D. (2022). *Wi-Fi Security: WEP vs WPA or WPA2*. Wi-Fi Security: WEP vs WPA or WPA2. https://www.avast.com/c-wep-vs-wpa-or-wpa2

Gridelli, S. (2019, kesäkuuta 26). How a WiFi connection works. *NetBeez*. https://netbeez.net/blog/how-wifi-connection-works/

Grigas, L. (2022, tammikuuta 4). *What is a dictionary attack?* https://nordpass.com/blog/what-is-a-dictionary-attack/

Grimmick, R. (2022, heinäkuuta 8). *What is Wireless Sniffing? (With pictures)*. EasyTechJunkie. http://www.easytechjunkie.com/what-is-wireless-sniffing.htm

Hak5. (2022, huhtikuuta 19). *WiFi Pineapple Documentation*. https://docs.hak5.org/wifi-pineapple/

Hoffman, C. (2013, heinäkuuta 6). *Brute-Force Attacks Explained: How All Encryption is Vulnerable*. How-To Geek. https://www.howtogeek.com/166832/brute-force-attacks-explained-how-all-encryption-is-vulnerable/

Hoffman, C. (2017). *Wi-Fi Security: Should You Use WPA2-AES, WPA2-TKIP, or Both?* How-To Geek. https://www.howtogeek.com/204697/wi-fi-security-should-you-use-wpa2-aes-wpa2-tkip-or-both/

HYPR. (ei pvm.). *What is a Dictionary Attack? | Security Encyclopedia*. HYPR. Noudettu 7. toukokuuta 2022, osoitteesta https://www.hypr.com/dictionary-attack/

Jevtic, G. (2019, toukokuuta 9). *17 Powerful Penetration Testing Tools The Pros Use*. PhoenixNAP Blog. https://phoenixnap.com/blog/best-penetration-testing-tools

Kyberturvallisuuskeskus. (2014). *Langattomasti, mutta turvallisesti*. Kyberturvallisuuskeskus. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Langattomasti_mutta_turvallisesti._Langattomien_lahiverkkojen_tietoturvallisuudesta.pdf

Linux Shell Tips. (2022, heinäkuuta 29). *The History of Kali Linux [Penetration Testing] Distribution*. https://www.linuxshelltips.com/kali-linux-history/

Lutkevich, B. (2022, toukokuuta 10). *What is a Wi-Fi Pineapple?* TechTarget SearchSecurity. https://www.techtarget.com/searchsecurity/definition/Wi-Fi-Pineapple

Messer Studios LLC. (2018, huhtikuuta 30). *Wireless Deauthentication—CompTIA Network+ N10-007—4.4*. Professor Messer IT Certification Training Courses. https://www.professormesser.com/network-plus/n10-007/wireless-deauthentication/

NACDL. (2022). *NACDL - Computer Fraud and Abuse Act (CFAA)*. NACDL - National Association of Criminal Defense Lawyers. https://www.nacdl.org/Landing/ComputerFraudandAbuseAct

OffSec Services Limited. (2022, toukokuuta 16). *Kali Docs | Kali Linux Documentation*. Kali Linux. https://www.kali.org/docs/

Panda Security. (2020, huhtikuuta 8). WPA vs WPA2: Which WiFi Security Should You Use? *Panda Security Mediacenter*. https://www.pandasecurity.com/en/mediacenter/security/wpa-vs-wpa2/

Poston, H. (2021, toukokuuta 6). *13 popular wireless hacking tools [updated 2021]*. Infosec Resources. https://resources.infosecinstitute.com/topic/13-popular-wireless-hacking-tools/

Ronder, A. (2020, tammikuuta 16). The 4-way handshake WPA/WPA2 encryption protocol. *Medium*. https://medium.com/@alonr110/the-4-way-handshake-wpa-wpa2-encryption-protocol-65779a315a64

Roomi, M. (2020, maaliskuuta 6). *6 Advantages and Disadvantages of Wifi | Drawbacks and Benefits of Wireless Networks*. https://www.hitechwhizz.com/2020/03/6-advantages-and-disadvantages-drawbacks-benefits-of-wifi.html

Sharp. (2020, heinäkuuta 13). 802.11 Frame Types and Formats. *How I WI-FI*. https://howiwifi.com/2020/07/13/802-11-frame-types-and-formats/

Spadafora, A. (2022, elokuuta 9). *What Is a Mesh Wi-Fi Router, and Do You Need One?* Tom's Guide. https://www.tomsguide.com/us/what-is-mesh-wifi-router,news-24580.html

Sullivan, B. (ei pvm.). *Preventing a Brute Force or Dictionary Attack: How to Keep the Brutes Away from Your Loot*. 5.

Toktabek, T. (2021, lokakuuta 1). *Importance of WIFI Security – How YOU Can Prevent Online Attacks | Mercku Connectivity*. https://www.mercku.com/2021/10/01/importance-of-wifi-security-how-you-can-prevent-online-attacks/

Verizon. (2022). *What is Wi-Fi? | Definition, Meaning & Explanation | Verizon Fios*. https://www.verizon.com/info/definitions/wifi/

Wifi-professionals. (2019, tammikuuta 24). 4-Way Handshake. *WiFi*. https://www.wifi-professionals.com/2019/01/4-way-handshake

Wikipedia. (2022). IEEE 802.11. Teoksessa *Wikipedia*. https://en.wikipedia.org/w/index.php?title=IEEE_802.11&oldid=1100819465

Williams, L. (2020, lokakuuta 12). *Kali Linux Tutorial for Beginners: What is, How to Install & Use*. https://www.guru99.com/kali-linux-tutorial.html

WirelesSHack. (2022, toukokuuta 3). *Best Kali Linux Compatible USB Adapters – WirelesSHack*. https://www.wirelesshack.org/best-kali-linux-compatible-usb-adapter-dongles.html

Zuckerman, K. (2021, lokakuuta 4). Is penetration testing legal? *CYBRI*. https://cybri.com/is-penetration-testing-legal/