Sigurnost Bluetooth uređaja

Mankas, Igor

Undergraduate thesis / Završni rad

2021

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Zagreb, Faculty of Organization and Informatics / Sveučilište u Zagrebu, Fakultet organizacije i informatike**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:211:258099

Rights / Prava: Attribution 3.0 Unported/Imenovanje 3.0

Download date / Datum preuzimanja: **2024-04-20**

SVEUČILIŠTE U ZAGREBU
FAKULTET ORGANIZACIJE I INFORMATIKE
VARAŽDIN

Repository / Repozitorij:

Faculty of Organization and Informatics - Digital Repository

zir.nsk.hr

DIGITALNI AKADEMSKI ARHIVI I REPOZITORIJI

SVEUČILIŠTE U ZAGREBU

FAKULTET ORGANIZACIJE I INFORMATIKE

V A R A Ž D I N

Igor Mankas

SIGURNOST BLUETOOTH UREĐAJA

ZAVRŠNI RAD

Sisak, 2021.

SVEUČILIŠTE U ZAGREBU

FAKULTET ORGANIZACIJE I INFORMATIKE

V A R A Ž D I N

Igor Mankas

Matični broj: 0016134796 (S-46452)

Studij: Primjena informacijske tehnologije u poslovanju

SIGURNOST BLUETOOTH UREĐAJA

ZAVRŠNI RAD

Mentor:

Doc.dr.sc. Igor Tomičić

Sisak, rujan 2021.

Igor Mankas

Izjava o izvornosti

Izjavljujem da je moj završni rad izvorni rezultat mojeg rada te da se u izradi istoga nisam koristio drugim izvorima osim onima koji su u njemu navedeni. Za izradu rada su korištene etički prikladne i prihvatljive metode i tehnike rada.

Autor potvrdio prihvaćanjem odredbi u sustavu FOI-radovi

_____

Sažetak

Bluetooth, standard za bežični prijenos podataka izumljen je 1994. godine u Ericsson-u, a primarna svrha mu je bila zamijeniti kabelsku odnosno fizičku povezanost između uređaja. Godine 1998. Ericsson se udružio s IBM-om, Intelom, Nokiom i Toshibom kada je osnovana Posebna interesna skupina (eng. Special interest group - SIG), koja je razvila otvoreni industrijski standard za Bluetooth tehnologiju. (Lonzetta, A.M. et al., 2018)

Godine 2001. na tržište je izašao prvi mobilni uređaj s Bluetooth tehnologijom. Radilo se o mobilnom uređaju proizvođača Ericsson, a naziv modela bio je T39 (Peter, 2021). Danas je Bluetooth ugrađen u gotovo sve računalne uređaje kao što su osobna računala, pametni telefoni, pametni satovi itd.

Bluetooth je postao nezaobilazna tehnologija koja se koristi gotovo svaki dan, a navedeno dokazuje i oko 4 milijarde isporučenih uređaja s Bluetooth tehnologijom u 2020. godini dok se u 2025. godini očekuje da će ovaj broj narasti do čak 6,4 milijarde uređaja. (Bluetooth SIG, Inc., 2021)

S obzirom na veliku rasprostranjenost uređaja s Bluetooth tehnologijom, porastao je i interes za zlouporabu ove bežične mreže. Napadači sve češće napadaju Bluetooth tehnologiju s ciljem dolaska do osobnih podataka, dobivanja daljinskog pristupa, reklamiranje, ugrožavanje integriteta ili uskraćivanje usluge.

Ključne riječi: bluetooth, BLE, BR/EDR, protokol, piconet, master, slave, sigurnost, bettercap

Sadržaj

Sadržaj iii
Uvod 1
Teorijski dio 2
1.1. Bluetooth 2
1.2. Vrste Bluetooth tehnologije 4
1.3. Bluetooth verzije 5
1.4. Način rada Bluetooth tehnologije 6
1.5. Postupak povezivanja 7
1.6. Korištenje Bluetooth tehnologije 8
1.7. BLE protokoli 9
1.8. Sigurnost Bluetooth uređaja 10
1.9. Bluetooth napadi 16
1.9.1. BlueJacking 16
1.9.2. BlueSnarfing 17
1.9.3. BlueSniping 17
1.9.4. BlueSmacking 18
1.9.5. BlueBugging 18
1.9.6. KNOB 18
1.10. Alati za Bluetooth napade 19
1.11. Anketa 19
1.12. Zaštita Bluetooth uređaja 22
Praktični dio 1 23
1.13. VirtualBox 23
1.14. Kali Linux 25
1.15. Bettercap 35
1.16. Demonstracija napada 36
Praktični dio 2 49
1.17. Socijalni inženjering 49
1.18. Demonstracija napada 49
Zaključak 54
Popis literature 55
Popis slika 58

Uvod

U ovom radu bit će opisan Bluetooth standard kao jedan od načina bežične razmjene podataka putem radio valova između dva ili više uređaja kao i načini rada posljednjih verzija Bluetooth i BLE protokola. S obzirom da se na tržištu pojavljuje sve više proizvoda i uređaja koji međusobno komuniciraju putem Bluetooth protokola, kao što su slušalice, zvučnici, pametni satovi, pametne žarulje itd., a koji često zahtijevaju konstantno aktivnu Bluetooth vezu, ovaj rad će biti usmjeren na sigurnost Bluetooth uređaja te potencijalne ranjivosti protokola i moguće vektore napada. Detaljnije će biti objašnjen proces uparivanja uređaja kao i proces uspostavljanja sigurne BLE veze koji je zapravo i najranjiviji dio procesa razmjene podataka. U radu će biti opisani i neki od najpoznatijih Bluetooth napada kao što su BlueJacking, BlueSnarfing, BlueSniping, BlueSmacking, BlueBugging i KNOB. Opisat će se i mogući načini obrane od napada kao i opće preporuke za zaštitu od mogućih napada.

U prvom dijelu praktičnog rada bit će demonstriran napad s vektorom ranjivosti Bluetooth uređaja u smislu skeniranja, prikupljanja podataka, identifikacije uređaja i moguće interakcije s napadnutim uređajem putem alata Bettercap instaliranog na operativnom sustavu Kali Linux, Linux distribuciji namijenjenoj digitalnoj forenzici, testiranju probojnosti i etičkom hakiranju. U drugom dijelu praktičnog rada biti će prikazan napad putem Bluetooth veze u kojem će vektor napada biti socijalni inženjering.

Teorijski dio

U teorijskom dijelu završnog rada kratko će biti opisana povijest Bluetooth tehnologije i njezin razvoj. Osim kratkog osvrta na razvoj Bluetooth tehnologije, njezinih verzija i vrsta tehnologije, bit će opisan i način povezivanja, općeniti način rada Bluetooth i BLE uređaja te kategorizacija uređaja koji koriste Bluetooth tehnologiju. S obzirom da BLE protokol polako preuzima klasični Bluetooth protokol, ovaj rad će se detaljnije osvrtati upravo na BLE tehnologiju.

Teorijski dio rada će primarno biti usmjeren na sigurnost Bluetooth uređaja, te će biti opisani neki od najpoznatijih napada na Bluetooth tehnologiju kao i opće preporuke za zaštitu od mogućih napada.

Za potrebe ovog rada napravljena je i kratka anketa. Dobiveni rezultati ankete će biti analizirani i prokomentirani u smislu znanja i upućenosti anketiranih osoba o sigurnosti Bluetooth tehnologije.

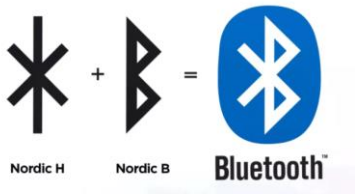
1.1. Bluetooth

Ideja bežičnog prijenosa podataka prvi je puta predstavljena 1989. godine kada su glavni tehnološki direktor Ericson Mobile-a dr. Nils Rydbeck i izumitelj dr. Johan Ullman počeli razvijati ideju o bežičnim slušalicama. Veliku ulogu u provedbi ovog projekta imao je i dr. Jaap Haartsen koji je 1994. godine predstavio prvi protokol za bežični prijenos podataka, a 1999. godine, nakon usavršavanja tehnologije, predstavljene su prve handsfree slušalice. (Bright Side – „How Bluetooth works“, 2019)

Slika 1 Prvi uređaj s Bluetooth tehnologijom - handsfree headset (ERICSSONERS, 2021)

Standard za kratkodometni, bežični prijenos podataka nazvan je Bluetooth, a naziv je dobio po vikinškom kralju Haroldu „plavozubom“ Gormssonsu koji je ujedinio Danska i Norveška plemena. Ovo ujedinjenje postalo je simbol za spajanje uređaja stoga je protokol nazvan po „plavozubom“ vikinškom kralju Haroldu. Također, i sam simbol odnosno logo

Bluetooth-a izvedenica je inicijala „H“ za Harold i „B“ za „Bluetooth“. (Bright Side – „How Bluetooth works“, 2019)



Slika 2 Bluetooh logo (Piper D., 2021)

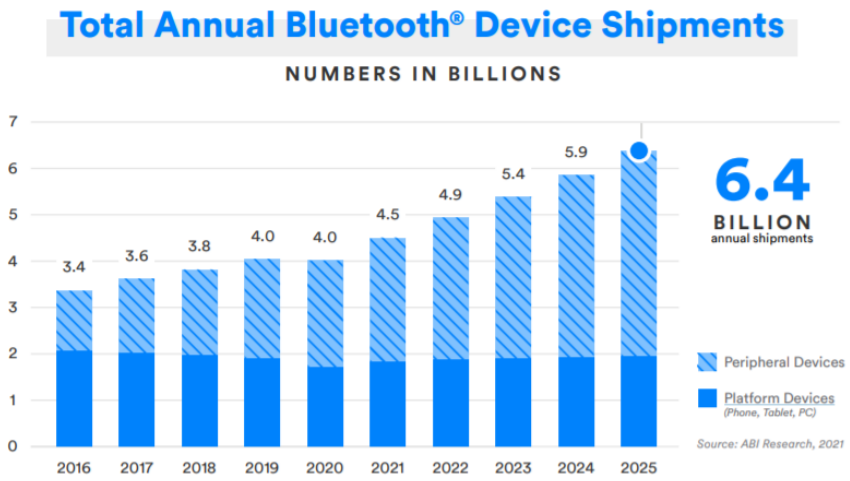
Već 2001. godine na tržište je izašao prvi mobilni uređaj s Bluetooth tehnologijom. Radilo se o mobilnom uređaju proizvođača Ericsson, a naziv modela bio je T39 (Peter, 2021).

Slika 3 Prvi mobilni uređaj s Bluetooh tehnologijom (Peter, 2021)

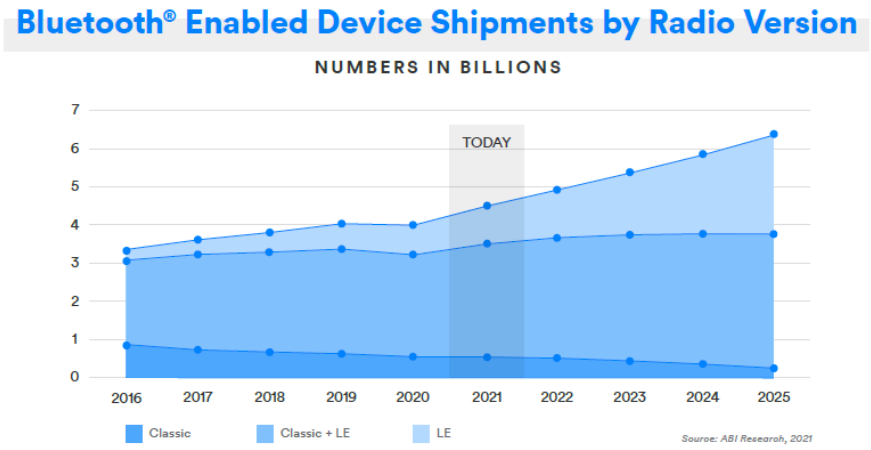
S obzirom da je Bluetooth tehnologija dobro prihvaćena među korisnicima, brojevi uređaja s ugrađenom Bluetooth tehnologijom rasla je iz godine u godinu.

Na Slici 4 prikazani su brojevi isporučenih uređaja s Bluetooth tehnologijom kao i predviđanja za naredne godine. (Bluetooth SIG, Inc., 2021)

Zanimljivo je za primijetiti omjer isporučenih uređaja (računala, tableti, pametni telefoni) s Bluetooth tehnologijom i perifernih uređaja (tipkovnice, miševi, mikrofoni, web kamere). Naime, na Slici 5 može se vidjeti da sve manje uređaja koristi BR/EDR – Bluetooth Classic tehnologiju, a sve više uređaja koristi BLE tehnologiju. Iz ove dvije slike možemo zaključiti da se Bluetooth tehnologija sve više koristi za povezivanje perifernih uređaja BLE tehnologijom. Broj uređaja koji koriste obje verzije ostaje na istoj razini jer se radi o pametnim telefonima koji koriste dual mode (BR/EDR + LE).



Slika 4 Ukupne godišnje isporuke Bluetooth uređaja u milijardama i predviđanja za naredne godine (Bluetooth SIG, Inc., 2021)



Slika 5 Isporučeni Bluetooth uređaji u milijardama s obzirom na verziju (Bluetooth SIG, Inc., 2021)

1.2. Vrste Bluetooth tehnologije

Bluetooth tehnologiju možemo podijeliti u tri glavne grupe, ovisno o uređajima koji tu tehnologiju koriste, a to su:

- BR/EDR – Bluetooth Classic – uglavnom se koristi za prijenos zvuka (bežične slušalice, bežični zvučnici itd.)
- BLE (LE) – Bluetooth Low Energy (Bluetooth Smart) – češće se koristi na nosivim uređajima (oprema za praćenje kondicije – Smartwatch, Smartband) i na baterijski pogonjenim dodacima odnosno perifernim uređajima (bežične tipkovnice, miševi itd.)

- BR/EDR + LE – dual mode Bluetooth – većina pametnih telefona može raditi dvostrukim načinom odnosno podržavaju spajanje i s BR/EDR uređajima i s BLE uređajima

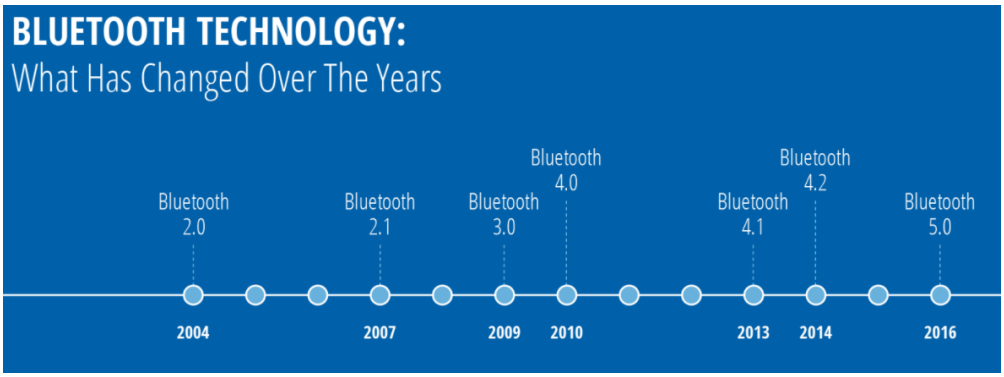
1.3. Bluetooth verzije

Glavne razlike u Bluetooth verzijama odnose se na podržavanje većih brzina prijenosa podataka, domet povezivanja, stabilnost veze, energetsku učinkovitost i bolju sigurnost.

Na Slici 5 prikazan je razvoj Bluetooth verzija kroz godine. Verzije razvijane od 2001. godine do 2009. godine, odnosno od verzije 1.0 do verzije 3.0 odnose se na BR/EDR – Bluetooth Classic tehnologiju, dok sve verzije od 2010. godine (od verzije 4.0 na dalje) koriste BLE (LE) – Bluetooth Low Energy tehnologiju.

Tehnologija uparivanja, enkripcija, pa čak i provjera autentičnosti na ove dvije verzije rade na gotovo isti način, međutim, Bluetooth Low Energy troši znatno manje energije od svojih prethodnih verzija jer radi u posebnom načinu mirovanja i troši energiju samo kada je aktivan.

Potrebno je napomenuti da su novije verzije uvijek kompatibilne sa starijim verzijama, ali je tada veza ograničena na značajke koje podržava starija verzija. Navedeno će dalje u radu biti detaljnije objašnjeno kao jedna od ranjivosti Bluetooth tehnologije u smislu sigurnosti.

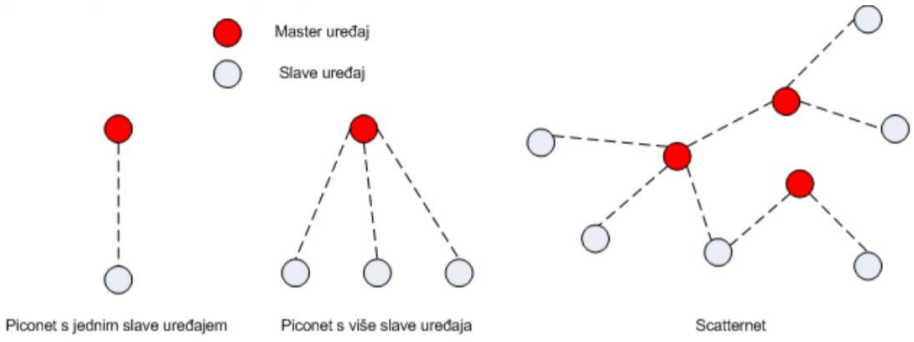


Slika 6 Bluetooth verzije kroz godine (Jaycon Systems, 2017)

1.4. Način rada Bluetooth tehnologije

Bluetooth uređaji rade u spektru radio valova od 2,4 do 2,48 GHz. Ovdje se radi o globalno dostupnom ISM (industrijskom, znanstvenom i medicinskom) opsegu bez licence. S obzirom da je ovaj spektar radio valova otvoren za sve uređaje u industrijskom, znanstvenom i medicinskom opsegu, na istom spektru radio valova rade i neki drugi uređaji kao što su mikrovalne pećnice ili baby monitori. Kako bi Bluetooth spriječio da mu navedeni uređaji stvaraju smetnje, on koristi tzv. frequency hopping tehniku odnosno tehniku frekvencijskog skakanja. Bluetooth BR/EDR u prijenosu podataka „skače“ odnosno mijenja frekvenciju 1.600 puta u sekundi po jednom od 79 dostupnih frekvencijskih koraka širine 1 MHz. Bluetooth LE za razliku od BR/EDR zauzima 37 frekvencijskih koraka širine 2 MHz. (Becker A., 2007)

Kada se dva ili više uređaja upare putem Bluetooth tehnologije, oni stvaraju ad hoc mrežu odnosno bežičnu mrežu za koju nije nužan pristup internetu. Mreža koju stvore Bluetooth-om povezani uređaji zove se piconet. U ovoj mreži uređaji mogu imati dvije uloge. Prva uloga je master ili glavni uređaj i ovu ulogu može imati samo jedan uređaj. Druga uloga je slave i tu ulogu imaju svi ostali uređaji u mreži. Jedan piconet može imati maksimalno 8 uređaja što znači da je jedan master, a ostalih 7 su slave. Master uređaj je uvijek taj koji uspostavlja vezu i određuje frekvenciju na kojoj će se postići uparivanje sa slave uređajem. Moguće je da se više piconeta spoje u jedan. Takvu mrežu tada nazivamo scatternet. Uloge, frekvencije i načini povezivanja u scatternetu i dalje ostaju vrijediti kao i u piconetu. (CARNet CERT i LS&S, 2005)



Slika 7 Načini povezivanja Bluetooth uređaja (CARNet CERT i LS&S, 2005)

Domet Bluetooth veze ovisi o nekoliko čimbenika.

Spektar radiovalova se proteže od 30 Hz do 300 GHz. Što je niža frekvencija to je veći domet. S druge strane, što je niža frekvencija to je manja i brzina prijenosa podataka te je u slučaju radiovalova potrebno odrediti kompromis između dometa i brzine prijenosa podataka. Osjetljivost prijemnika također utječe na domet. On je mjera minimalne jačine

signala koju prijemnik može protumačiti odnosno to je najniža razina snage na kojoj prijemnik može detektirati radio signal, održavati vezu i demodulirati podatke. Snaga odašiljanja je sljedeći čimbenik koji utječe na domet. Kao i kod spektra radio valova i ovdje se radi o kompromisu između dometa, ali u ovom slučaju i potrošnje energije. Povećanje snage odašiljanja povećava potrošnju energije uređaja. Antena pretvara električnu energiju iz odašiljača u elektromagnetsku energiju i obrnuto. Položaj antene, veličina i dizajn utječu na učinkovitost prijenosa i primanja signala. Samim time, vrsta antene je bitan čimbenik u dometu Bluetooth uređaja. Gubitci jačine signala također utječu na domet. Na gubitke utječe okruženje u kojem se signal prenosi. Prepreke, kao što su zidovi, drvo, metalne konstrukcije, staklo pa čak i vlaga i padaline uvelike utječu na domet Bluetooth-a. (Bluetooth SIG, Inc., bez dat.)

1.5. Postupak povezivanja

Postupak stvaranja veze (eng. Pairing) između uređaja putem Bluetooth veze odvija se u više koraka i može imati tri progresivna stanja.

Upit (eng. Inquiry) – Na samom početku postoje dva ili više uređaja koji ne znaju ništa jedan o drugome. U jednom trenutku jedan od uređaja šalje upit za pronalazak drugog uređaja. Svi uređaju koji „slušaju“ zahtjeve odgovaraju svojom adresom, imenom i dodatnim podacima.

Povezivanje (eng. Paging (Connecting)) – Povezivanje ili uparivanje je proces stvaranje veze između dva uređaja i nastaje kada oba uređaja znaju sve podatke jedan o drugome.

Veza (eng. Connection) – Nakon uspješnog povezivanja uređaji ulaze u stanje veze u kojem mogu aktivno sudjelovati (slati i primati podatke) ili mogu biti neaktivni u razmjeni podataka, ali ipak povezani.

Postupak uparivanja za uređaje s Bluetooth verzijom 4.0 i 4.1, poznato i kao LE Legacy Pairing, koriste prilagođeni protokol razmjene ključeva jedinstven za BLE standard. Uređaji razmjenjuju privremeni ključ (TK) i koriste ga za stvaranje kratkoročnog ključa (STK) koji se koristi za enkripciju veze. Postupak uparivanja za uređaje s Bluetooth verzijom 4.2 i novije mogu stvoriti i LE sigurne veze. Umjesto korištenja TK i STK, LE sigurne veze za enkripciju koriste jedan dugoročni ključ (LTK). LTK se generira pomoću kriptografije javnog ključa koja pruža bolju sigurnost. (Padgette J. et al., 2017)

Nakon uspješno uspostavljene veze uređaji mogu imati nekoliko modaliteta rada.

Aktivni način rada - Uobičajeni povezani način rada gdje uređaji aktivno šalju ili primaju podatke.

„Njuškanje“ - Način uštede energije u kojem je uređaj manje aktivan. Podaci se šalju i primaju samo u zadanom intervalu.

Način čekanja - Način čekanja je privremeni način rada za uštedu energije u kojem uređaj „spava“ određeno vrijeme, a nakon isteka tog intervala vraća se u aktivni način rada. U ovom slučaju master uređaj naređuje slave uređaju odlazak u način čekanja.

„Parkiranje“ - Parkiranje je najdublji način mirovanja. Master uređaj naređuje slave uređaj odlazak na „spavanje“, a slave uređaj tamo ostaje sve dok ga master uređaj ponovno ne „probudi“. (Juha T. Vainio, 2000)

Postupak povezivanja se može podijeliti i na dvije vrste spajanja odnosno veze.

Uparivanje: proces u kojem uređaji razmjenjuju informacije potrebne za uspostavu kriptirane veze. To uključuje provjeru autentičnosti uređaja koji se uparuju, enkripciju veze i distribuciju ključeva u svrhu ponovnog pokretanje sigurne veze.

Stvaranje veze: postupak u kojem se podaci iz procesa uparivanja pohranjuju na uređajima. U ovom slučaju se postupak uparivanja ne mora ponavljati svaki put kada se uređaji povezuju. (Nao L., 2018)

Detaljnije o ključevima, procesu uparivanja i stvaranju veze bit će opisano u poglavlju 1.8. vezanom za sigurnost Bluetooth uređaja.

1.6. Korištenje Bluetooth tehnologije

Uređaji koji koriste Bluetooth tehnologiju se mogu svrstati u četiri kategorije:

- Računala

Bluetooth se u računalima najviše koristi u svrhu povezivanja perifernih uređaja kao što su tipkovnica, miš, zvučnici ili slušalice. Također, Bluetooth se koristi i u svrhu međusobnog prijenosa podataka između dva ili više računala, za povezivanje na pisače ili mobilne uređaje poput tableta ili pametnih telefona. U ovom smislu Bluetooth je idealna tehnologija za urede gdje je moguće povezati više računala sa svim perifernim uređajima u blizini kao i računala međusobno.

- Kućanstvo i automobili

Sve su češće tzv. pametne kuće u kojima Bluetooth ima veliku ulogu. Putem njega se može upravljati termostatima, alarmima, kućanskim aparatima ili svijetlima. Preko Bluetootha

se može upravljati i kućnim zabavnim sadržajem kao što kućna kina i audio sustavi ili sve češće zrcaljenje sadržaja pametnog telefona na televizore. U automobilima Bluetooth može služiti za povezivanje raznih uređaja s automobilom u svrhu upućivanja i primanja poziva, reproduciranja glazbe ili za GPS sustav.

- Zdravlje

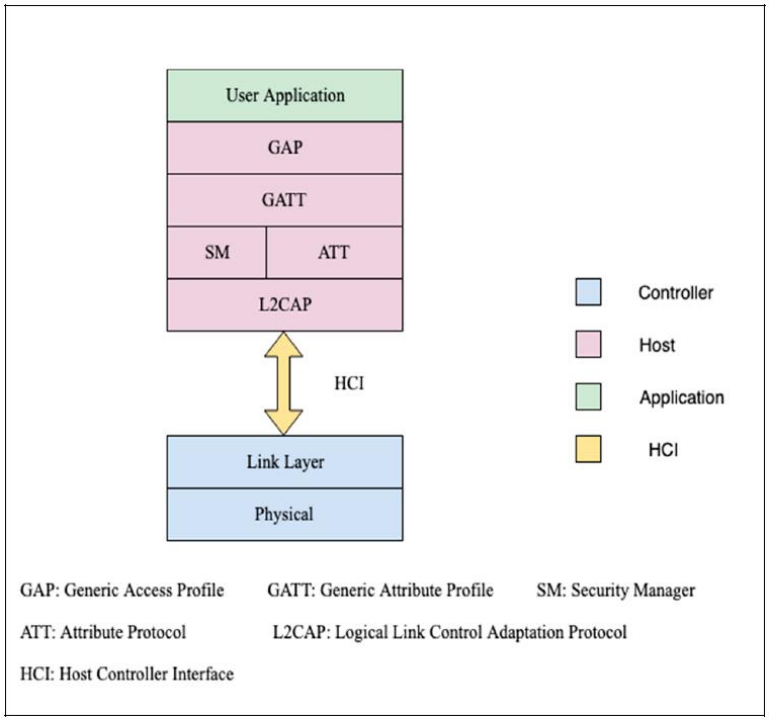
Bluetooth može automatski bilježiti podatke medicinske opreme, poput stetoskopa, pacemakera ili mjerača glukoze u računala. Fitness oprema sve češće koristi Bluetooth za praćenje vježbanja, otkucaja srca ili potrošenih kalorija. Svi podaci se putem Bluetooth-a prenose na pametne telefone. U ovom segmentu se Bluetooth sve češće koristi zbog pogodnosti nedostatka žica koje smetaju kod vježbanja.

- Potrošačka elektronika

Potrošačka elektronika s Bluetooth-om pojednostavljuje dijeljenje podataka između uređaja poput pametnih telefona, kamera, televizora, zvučnika i slušalica.

1.7. BLE protokoli

Na Slici 8 prikazana je BLE arhitektura odnosno BLE protokol.



Slika 8 BLE protokol (Sherali Zeadally et al., 2019)

Fizički sloj se sastoji od primopredajnika odnosno elektroničkog uređaja koji odašilje i prima radio valove pomoću antene. Radi u frekvencijskom pojasu od 2,4 GHz i koristi već

spomenutu tehniku frekvencijskog skakanja. **Sloj veze** nalazi se iznad fizičkog sloja. On je zadužen za skeniranje, stvaranje i održavanje veza. **HCI** omogućuje komunikaciju između kontrolera (eng. Controller) i domaćina (eng. Host). **L2CAP** sloj je zaslužan za segmentaciju, ponovno sastavljanje i prijenos paketa podataka slojevima. **ATT** i **SM** slojevi zaduženi su za provođenje autorizacije, uparivanje i distribuciju ključeva. BLE uređaji komuniciraju putem procedura koje određuje **GATT**. Aplikacije izravno komuniciraju s GATT slojem (npr. za dozvole notifikacija). **GAP** kontrolira veze između Bluetooth uređaja i određuje kako i da li dva uređaja mogu ostvariti međusobnu interakciju. **Aplikacijski sloj** je korisničko sučelje koje uključuje profile aplikacija koji omogućuju korisniku interakciju s Bluetooth aplikacijama. (Sherali Zeadally et al., 2019).

1.8. Sigurnost Bluetooth uređaja

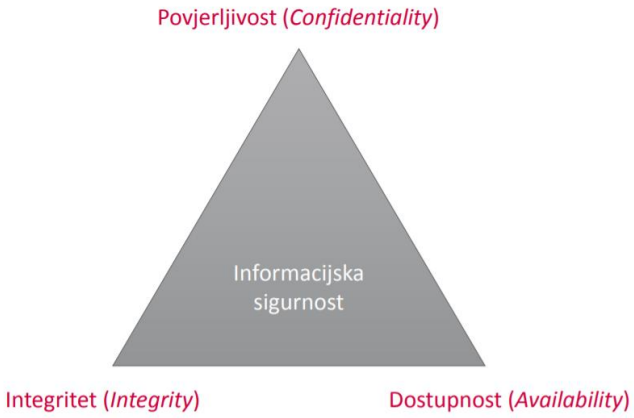
Sigurnost se sve češće navodi kao jedan od gorućih problema i izazova s kojim se susreću tehnološki stručnjaci u razvoju i proizvodnji tehnološke opreme. IoT i sve veća rasprostranjenost povezanih uređaja i sustava, kao i učestalost napada na ove tehnologije podiže ljestvicu potrebne sigurnosti informacijskih sustava.

„Sigurnost informacijskih sustava je disciplina kojoj je osnovni cilj osigurati zaštitu informacija i informacijskih sustava od neovlaštenog pristupa, korištenja, promjene ili uništavanja.“ (Baća, M. et al., 2019/2020)

Temelj zaštite podataka i informacija leži u tri komponente koje su temelj sigurnosti informacijskih sustava:

- Povjerljivost (eng. Confidentiality) – tajnost podataka i dostupnost podataka samo ovlaštenim osobama
- Integritet (eng. Integrity) - sprječavanje modificiranja podataka neovlaštenim osobama
- Dostupnost (eng. Availability) – dostupnost podataka i informacija ovlaštenim osobama (Baća, M. et al., 2019/2020)

Ove tri komponente sigurnosti se povezuju u tzv. sigurnosni trokut (CIA).



Slika 9 CIA trokut (Baća, M. et al., 2019/2020)

S druge strane sigurnosti su napadači koji sa suprotnim, tzv. DAD trokutom napadaju sigurnosne komponente CIA trokuta.

- Razotkrivanje (eng. Disclosure) – razotkrivanje informacija
- Promjena (eng. Alteration) – neautorizirane promjene podataka
- Uskraćivanje (eng. Denial) – onemogućavanje autoriziranom pristupu informacija (Solomon, G. M., Chapple M., 2004)

Zadatak svake nove ili postojeće tehnologije kojom se prenose osjetljivi i privatni podaci je da obuhvati sigurnosne komponente CIA trokuta, a zatim i da nadograđuje tehnologiju kako bi pružena usluga bila što sigurnija.

Posebna interesna skupina (eng. Special interest group - SIG) neprestano nastoji poboljšati sigurnost Bluetooth tehnologije, jačajući postojeće zaštite i uvodeći nove sigurnosne mjere kako bi zadovoljili stalno rastuće zahtjeve za informacijskom sigurnost. (Bluetooth SIG, Inc., 2021)

Bluetooth razvojem dostupnih verzija neprestano poboljšava i samu sigurnost protokola. Gotova svaka verzija imala je promjene, poboljšanja ili zakrpe sigurnosnih propusta. Sigurno je da će se takva praksa nastaviti i dalje zbog stalnih novih načina napadača u pokušajima napada na sigurnosne protokole Bluetooth tehnologije.

Sigurnost protokola od verzije 1.0 do trenutne 5.2 verzije značajno je poboljšano. Bluetooth SIG, Inc., (2021) navodi da je veza 5.2 verzije Bluetooth-a gotovo apsolutno sigurna ako se poštuju sva pravila za uparivanje. Međutim, da bi se uspostavila sigurna veza, uređaji se prvo moraju upariti što je glavna ranjivost BLE tehnologije.

SM (eng. Security Manager) sloj Bluetooth protokola zadužen je za sigurnost BLE tehnologije. SM definira protokole i algoritme za generiranje i razmjenu ključeva između dva uređaja i ima pet zaštitnih obilježja. (Sherali Zeadally et al., 2019).

Uparivanje – proces kreiranja i dijeljenja tajnih ključeva između uređaja.

Stvaranje veze – proces kreiranja i spremanja tajnih ključeva na master i slave uređaje u svrhu naknadnog povezivanja uređaja.

Autentifikacija – proces provjere dijele li dva uređaja iste tajne ključeve.

Enkripcija – proces šifriranja podataka koje dijele dva uređaja. BLE koristi 128-bitni AES kriptografski standard sa simetričnim ključem koji služi i za enkripciju i za dekripciju podataka na povezanim uređajima.

Integritet – proces potpisivanja podataka i potvrđivanja potpisa.

Kao što je već opisano u poglavlju 1.4., master uređaj je taj koji inicira povezivanje, a s iniciranjem povezivanja iniciraju se i sigurnosne procedure. Slave uređaj također može inicirati sigurnosne procedure na način da master uređaju pošalje poruku sa sigurnosnim zahtjevom, ali u tom slučaju opet master uređaj šalje paket kojim službeno započinje sigurnosni proces.

Sigurnosni proces se dijeli na tri faze.

U fazi 1 slave uređaj može poslati zahtjev za uparivanjem (opcionalno). Master uređaj zapravo inicira povezivanje slanjem poruke za zahtjevom za uparivanje, a slave uređaj vraća odgovor na zahtjev za povezivanjem. Zahtjevom za povezivanjem i odgovorom na zahtjev razmjenjuju se značajke koje podržavaju uređaji kao i sigurnosni zahtjevi za svaki uređaj. Sigurnosni zahtjev obuhvaća provjeru autentičnosti, maksimalnu duljinu ključa za enkripciju i različite sigurnosne ključeve koje svaki uređaj zahtijeva koristiti. Značajke koje razmjenjuju uređaji će naknadno biti detaljnije objašnjene.

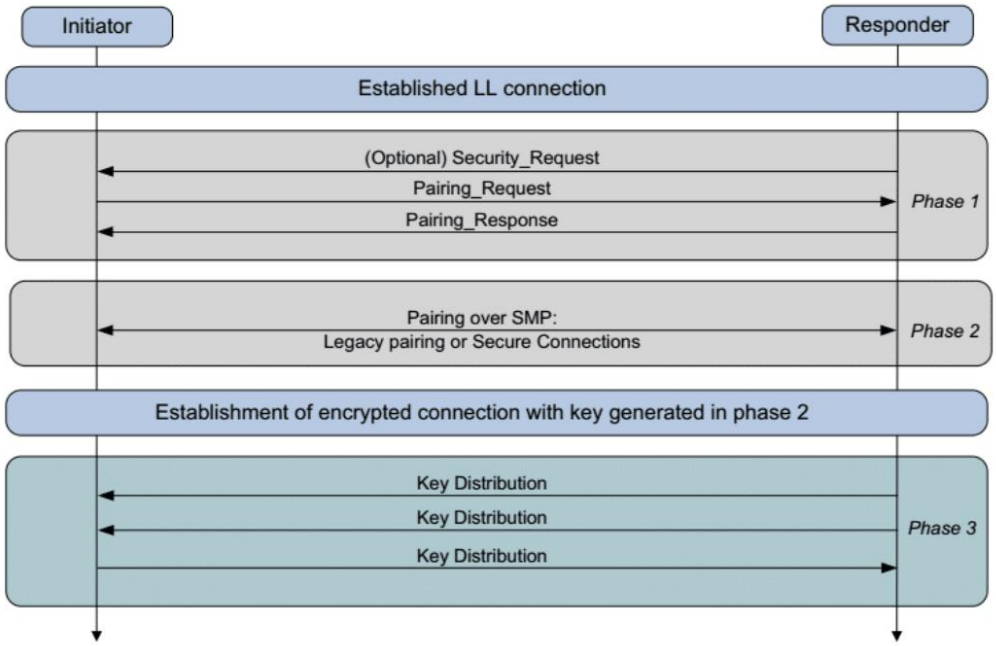
U fazi 2 proces se razlikuje s obzirom na metodu povezivanja, a one mogu biti LE Secure Connections ili LE Legacy Connections.

U LE Secure Connections uređaji koriste ECDH (eng. Elliptic-curve Diffie–Hellman) protokol za generiranje parova privatnih i javnih ključeva. Uređaji zatim razmjenjuju javne ključeve iz kojih generiraju zajednički tajni ključ odnosno LTK ključ (long term key). (Padgette J. et al., 2017)

U LE Legacy Connection koriste se dva ključa, privremeni ključ (TK – temporary key) i kratkoročni ključ (STK – short term key). Privremeni ključ se, uz dodatne podatke koje dijele uređaji, koristi za generiranje kratkoročnog ključa i generira se svaki puta kada se pokreće proces uparivanja. (Padgette J. et al., 2017)

Faza 3 predstavlja proces stvaranja veze. Ovo je opcionalna faza koja se koristi za izbjegavanje potrebe ponovnog uparivanja prethodno uparenih uređaja za stvaranje sigurne

komunikacije. Rezultat stvaranja veze je generiranje seta ključeva koji sprema svaki uređaj i koji se koristi pri svakom sljedećem povezivanju. Na taj način se preskaču faze uparivanja. Ovi ključevi se između uređaja razmjenjuju preko kriptirane veze. Veza se kriptira ključevima generiranim u drugoj fazi.



Slika 10 BLE faze uparivanja (Kai Ren, 2016)

U BLE postoje dva glavna načina zaštite naziva Security Mode 1 i Security Mode 2.

Security Mode 1 odnosi se na enkripciju dok je Security mode 2 zadužen za potpisivanje podataka.

Svaki navedeni način zaštite ima svoje sigurnosne razine. (Woolley M., Bluetooth SIG, 2020)

- Security Mode 1
  - Level 1 – nema sigurnosti (nema autentifikacije i nema enkripcije)
  - Level 2 – neautorizirano uparivanje s enkripcijom
  - Level 3 – autorizirano uparivanje s enkripcijom
  - Level 4 – autorizirano LE Secure Connection uparivanje s enkripcijom
- Security Mode 2
  - Level 1 – neautorizirano uparivanje s potpisom podataka
  - Level 2 – autorizirano uparivanje s potpisom podataka

Ključ za potpisivanje podataka zove se Connection Signature Resolving Key ili kratko CSRK. Ovaj ključ, osim što potpisuje podatke, istovremenu služi i za provjeru potpisa podataka na drugoj strani. (Woolley M., Bluetooth SIG, 2020)

Osim svih spomenutih ključeva u BLE protokolu postoji još i ID ključ odnosno Identity Resolving Key ili kratko IRK. Ovaj ključ je jedinstven za svaki uređaj i kod uparivanja se isti razmjenjuje između master i slave uređaja tako da master zna IRK slave-a, a slave zna IRK master-a. (Woolley M., Bluetooth SIG, 2020)

U fazi 1 spomenuto je da uređaji razmjenjuju opisane sigurnosne značajke (provjera autentičnosti, maksimalna duljina ključa za enkripciju i sigurnosni ključevi), ali i ostale značajke koje podržavaju uređaji. Te značajke zapravo određuju kojeg moda i koje razine sigurnosti će biti veza između uređaja. Naime, svako uparivanje kreće sa Security Mode 1; Level 1 načinom zaštite, a na temelju razmijenjenih značajki povećava se sigurnost veze.

Zahtjev i odgovor za uparivanje sadrže polja pod nazivom I/O Capability, Bonding Flags, SC, MITM, OOB Data Flag, Maximum Encryption Key Size, Initiator Key Distribution i Responder Key Distribution. (Woolley M., Bluetooth SIG, 2020)

Postoji pet mogućih ulazno/izlaznih značajki (eng. I/O Capability) (Woolley M., Bluetooth SIG, 2020)

- DisplayOnly - Uređaj može prikazati brojeve ili tekst, ali ne može prihvatiti unos
- KeyboardOnly - Uređaj može prihvatiti tekstualni ili numerički unos od korisnika
- DisplayYesNo - Uređaj omogućuje korisniku da odgovori sa DA ili NE
- NoInputNoOutput - Uređaj nema ulazne ili izlazne mogućnosti koje korisnik može koristiti
- KeyboardDisplay - Uređaj ima i tipkovnicu i zaslon

Ulazno/izlazne mogućnosti utječu na postupak autentifikacije. Za primjer, ako uređaj ima tipkovnicu, korisnik mora unijeti broj koji vidi na drugom uređaju. S druge strane, ako uređaj ima samo zaslon s tipkama „DA“ ili „NE“, korisnik može samo potvrditi jednakost prikazanih brojeva.

Zastavica za vezu (eng. Bonding Flag) je oznaka koja pokazuje da li uređaj želi stvoriti vezu (eng. Bonding), odnosno za spremanje dobivenih ključeva za kasniju (ponovnu) upotrebu. SC je jednobitna zastavica koja označava podržava li uređaj uparivanje načinom LE Secure Connection. Ako ga uređaj podržava, mora postaviti ovu zastavicu na 1. Ako oba uređaja imaju ovu zastavicu postavljenu na 1 onda obavezno moraju koristiti LE Secure Connection. MITM je također jednobitna zastavica. Postavljanjem ove zastavice uređaj zahtjeva autentifikaciju. Autentifikaciju može zahtijevati jedan ili oba uređaja. OOB (Out Of Band) Data Flag je oznaka kojom uređaji daju do znanja da autentifikaciju žele izvršiti putem protokola koji nije Bluetooth, odnosno putem npr. NFC-a ili preko QR koda. Kod ovog načina

autentifikacije bitno je za napomenuti da za eventualnu ranjivost autentifikacije ovdje nije odgovoran Bluetooth protokol već odabrana tehnologija za provjeru autentičnosti. Maksimalna duljina ključa za enkripciju (eng. Maximum Encryption Key Size) je polje koje omogućuje uređajima koji su upareni da razmijene informaciju o maksimalnoj duljini ključa za enkripciju kojeg posjeduju, a isti može biti u rasponu od 7 do 16 okteta (56 do 128 bit-a). Oba uređaja moraju koristiti istu duljinu ključa, što znači da se manja od dvije vrijednosti koristi za generiranje ključeva. (Woolley M., Bluetooth SIG, 2020)

Distribucija ključa master-a i distribucija ključa slave-a (eng. Initiator Key Distribution i Responder Key Distribution) označava vrste ključeva koje jedna od dvije strane u vezi pruža i vrste ključeva koje zahtjeva od druge strane. Dostupne vrste ključeva su LTK, CSRK i/ili IRK koji su prethodno pojašnjeni.

Kada uređaji prikupe sve potrebne informacije o mogućnostima druge strane, razmjerno mogućnostima se odabire i jedan od modela za uparivanje. (Woolley M., Bluetooth SIG, 2020)

- Just Works (samo radi) - Ne uključuje interakciju s korisnikom i veza jednostavno radi. Ovakva veza je česta kod uređaja koji imaju zaslon, ali ne i tipkovnicu pa nije moguć numerički unos ključa.
- Numeric Comparison (numerička usporedba) - Isti slučajni broj prikazuje se korisniku na oba uređaja. Korisnik mora označiti jesu li dva broja identična ili ne (npr. tipkom za „da“ ili „ne“).
- Passkey Entry (unos zaporke) – Ovaj način uparivanja se može napraviti na dva načina. Korisnik može na oba uređaja upisati istu zaporku ili kao drugi način, korisnik može na uređaj upisati slučajni broj koji se prikazuje na drugom uređaju
- Out-of-Band („izvan veze“) - Prijenos podataka za uparivanje između dva uređaja u jednom ili dvosmjernom načinu pomoću komunikacijskog kanala koji nije Bluetooth (npr. NFC ili QR kod).

Sigurnosne prijetnje na Bluetooth tehnologiju mogu se podijeliti u tri grupe.

1. Prijetnja otkrivanja podataka – napadači mogu prisluškivati ciljani uređaj te ukrasti podatke
2. Prijetnja na integritet – podaci se od pošiljatelja do primatelja mogu neovlašteno izmijeniti
3. Prijetnja uskraćivanja usluge (DoS) – autoriziranom korisniku može biti uskraćena usluga odnosno Bluetooth veza od strane neovlaštenih napadača

Slabosti tehnologije su prvenstveno posljedica nedostataka u protokolu za uspostavu ključa veze odnosno uspostavljanje pouzdane veze pogotovo u slučajevima kada enkripcija nije obavezna kao npr. kod „Just Works“ modela uparivanja.

Iz svega navedenog može se zaključiti da Bluetooth pruža značajnu sigurnost, ali samo u slučaju visoke razine i moda sigurnosnog uparivanja. Kao što je već navedeno, Bluetooth je najnesigurniji u postupku uparivanja, a sigurnost uređaja ovisi o „najslabijoj karici“ unutar piconet-a jer se postupak uparivanja prilagođava uređaju koji ima najslabije ulazno/izlazne mogućnosti i postavke.

Uspoređivanjem sigurnosti Wi-Fi veze i Bluetooth veze, Bluetooth veza je zbog različitih protokola znatno sigurnija iako koriste istu frekvenciju (2,4 GHz) odnosno alati za hakiranje Wi-Fi veze neće raditi na Bluetooth vezi. Zbog već spomenutog neprestanog mijenjanja frekvencija (1600 puta u sekundi) nije moguće pozicionirati se na jednoj frekvenciji i prisluškivati. Također, Wi-Fi „pregovara“ o ključu svaki puta kada uspostavlja vezu što znači da se eventualnom napadaču svaki puta pruža šansa za krađom ključeva, dok se kod Bluetootha ključevi uparuju samo jednom na početku stvaranja veze, zatim se spremaju na uređaje i na njih se referenciraju kada se nađu u dometu. Navedeno znači da eventualni napadač, kako bi saznao ključeve, mora biti prisutan kod prvog povezivanja.

1.9. Bluetooth napadi

Iako Bluetooth SIG, Inc. (2021) navodi da neprestano nastoji poboljšati sigurnost Bluetooth tehnologije, jačajući postojeće zaštite i uvodeći nove sigurnosne mjere kako bi se zadovoljili stalno rastući zahtjevi tog okruženja za povezivanje, neporecivo je da su se tokom razvoja Bluetooth tehnologije od verzije 1.0 pa do zadnje 5.2 verzije pojavljivali napadi zbog eventualnih propusta tehnologije ili njezine ranjivosti.

U nastavku će biti opisani neki od najznačajnijih napada.

1.9.1. BlueJacking

Blueacking ne spada niti u jednu od tri grupe sigurnosnih prijetnji jer ne nanosi štetu uređaju, ne krade niti mijenja podatke i nije zlonamjeran, ali se svakako radi o napadu jer isti nije prihvaćen od strane žrtve. BlueJacking je proces slanja neželjenih poruka na uređaje koji su u dometu, a radi se o krugu od oko 10 metara. Ovi napadi se često koriste u promotivne svrhe gdje žrtve primaju promotivne poruke putem Bluetooth-a. Napadači odaberu lokaciju s mnogo potencijalnih žrtvi, te putem Bluetootha šalju pripremljeni sadržaj svima na listi (svakoj potencijalnoj žrtvi koja u tom trenutku ima aktiviran Bluetooth). Sve žrtve koje prihvate uparivanje s nepoznatim uređajem dobivaju neželjenu poruku. Ovakvi napadi se

mogu izbjeći tako da korisnici ne prihvaćaju nepoznate pozive za uparivanjem, isključuju Bluetooth kada im nije potreban ili da u postavkama svoj uređaj sakriju od ostalih Bluetooth uređaja (nevidljivi način rada). (Colleen R., bez dat.)

1.9.2.BlueSnarfing

BlueSnarfing napad sličan je BlueJacking napadu, ali za razliku od BlueJacking napada BlueSnarf je zlonamjeran u smislu krađe podataka. Naime, u ovom slučaju napadač dobiva pristup osjetljivim podacima, telefonskom imeniku, e-pošte, porukama, fotografijama i slično, a može upućivati i pozive sa žrtvinog uređaja. Napad se, kao i kod BlueJacking-a, događa u kratkom dometu i može se izbjeći ako je Bluetooth isključen ili u nevidljivom načinu rada. Napad se izvodi putem BlueSnarf aplikacija koje su dostupne na internetu. (Colleen R., bez dat.)

Ovakvi napadi iskorištavaju slabu implementaciju protokola za razmjenu objekata (eng. OBEX – object exchange protocol) koji je implementiran u već spomenuti L2CAP protokol zadužen za segmentaciju, ponovno sastavljanje i prijenos paketa podataka slojevima. OBEX je vrlo sličan HTTP protokolu, ali za razliku od HTTP-a koji zahtjeve i odgovore prikazuje u čitljivom tekstu, OBEX koristi binarno oblikovane trojke (tip-duljina-vrijednost). Objekt se sastoji od polja i zaglavlja, i kao što je već navedeno, poruka je slična HTTP poruci. Kod zahtjeva za podacima u polju se navodi naredba GET (0x03) i duljina objekta (npr. 0x00 0x29), dok se u zaglavlju objekta nalazi ID veze i ime objekta koji se traži u binarnom obliku.

Napadač može u nesigurnim implementacijama OBEX protokola izvršiti OBEX GET zahtjev za poznatu ili očekivanu lokaciju i ime datoteke (npr. pictures/slika1.jpg). Rezultat ovog zahtjeva je preuzimanje datoteke slika1.jpg bez znanja žrtve. (Becker A., 2007)

1.9.3.BlueSniping

Radi se o napadu iste svrhe kao i kod BlueSnarfinga, ali s većim dometom. Napadači koriste tzv. BlueSniper topove koji su opremljeni snažnim usmjerenim antenama, Bluetooth modulom i operacijskim sustavom Linux. Domet ovog uređaja može biti i preko 1,5 km. (CARNet CERT i LS&S, 2009)

Slika 11 Uređaj za izvođenje BlueSniping napada (CARNet CERT i LS&S, 2009)

1.9.4.BlueSmacking

BlueSmacking napad je napad uskraćivanja usluge (DoS napad). On koristi L2CAP sloj za prijenos velikih paketa na povezani uređaj. Svaki uređaj ima ograničenu veličinu L2CAP ping-a. Ako uređaj dobije L2CAP ping paket koji je veći od ograničenja, prestat će s radom. BlueSmack napad se odnosi na slanje velikih paketa na povezani uređaj koji zbog premašenog ograničenja gasi Bluetooth i na taj način uskraćuje uslugu žrtvi. (Sherali Zeadally et al., 2019)

1.9.5.BlueBugging

BlueBugging napad izvršava se na način da se na upareni uređaj instalira malware koji služi kao „backdoor“ odnosno kao alat za zaobilaženje autentifikacije uređaja. Napadač nakon toga ima puni neautorizirani pristup podacima žrtvinog uređaja. (Sherali Zeadally et al., 2019)

1.9.6.KNOB

KNOB (eng. Key Negotiation of Bluetooth Attack) je tzv. MITM (eng. Man in the middle) vrsta napada. Ovakva vrsta napada uključuje „čovjeka u sredini“ odnosno napadača koji istovremeno napada i master i slave uređaj odnosno njihov postupak uparivanja. Master uređaj šalje slave uređaju zahtjev za uparivanjem i to predloženim sigurnim 16 byte-nim kriptiranim ključem. Napadač presreće ovaj zahtjev te mijenja duljinu ključa u 1 byte. Slave uređaj dobiva modificiranu poruku i prihvaća enkripciju ključem od 1 byte-a. Napadač presreće poruku slave uređaja i modificiraju ju na način da slave predlaže ključ od 1 byte-a. Master prihvaća enkripciju 1 bytnim ključem (postupak uparivanja prilagođava se najslabijim postavkama uređaja u mreži. U ovom trenutku master uređaj ne zna da slave zapravo podržava 16 bytni ključ). Master šalje poruku u kojoj prihvaća enkripciju 1 byte-nim ključem. Napadač presreće i ovu poruku te ju briše iz razloga što slave uređaj ne očekuje potvrdu

mastera jer je on poslao potvrdu, a ne zahtjev masteru. U ovom trenutku master i slave imaju dogovorenu enkripciju 1 byte-nim ključem iako oboje podržavaju ključ od 16 byte-a. S obzirom na loše kriptirano uparivanje, napadač sada lako može prisluškivati ili presretati podatke koji se razmjenjuju. (Umawing J., 2019)

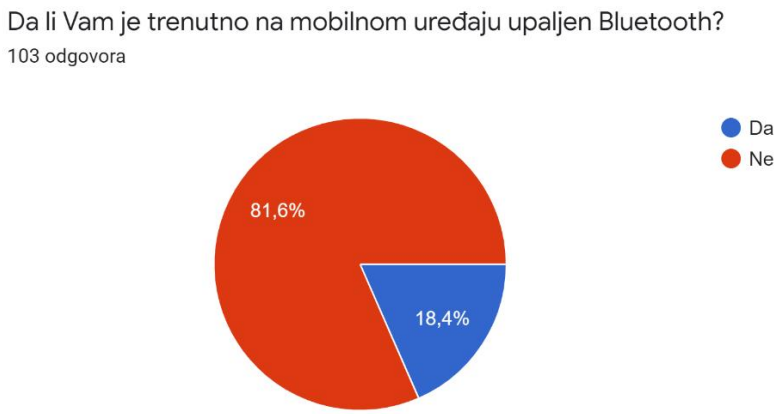
1.10. Alati za Bluetooth napade

U nastavku će biti opisani neki od alata za provođenje navedenih Bluetooth napada. (HackersEnigma, 2016)

- **BlueSanner** – alat za traženje uređaja s omogućenim Bluetooth-om i pretraživanje informacija o uređaju.
- **BlueBugger** – iskorištava sigurnosne propuste i ranjivosti Bluetooth uređaja za pristup slikama, imeniku, porukama i drugim osobnim podacima.
- **Bluediving** – alat za testiranje Bluetooth penetracija. Izvršava više vrsta napada kao što su već navedeni Bluebug, BlueSnarf i BlueSmack.
- **BTCrack** – rekonstruira PIN-ove i ključeve tijekom uparivanja. Dobiveni PIN može se koristiti za autentifikaciju s uređajem u načinu uparivanja, a ključevi se mogu iskoristiti za potpuni pristup uređaju i dešifriranje prijenosa podataka između uređaja.
- **Ettercap** – alat za MITM napade koji pretražuje Bluetooth veze, filtrira i prikazuje podatke o Bluetooth uređajima.
- **Bettercap** – bolji (eng. Better) nasljednik Ettercap alata koji se koristi u svrhu istraživanja sigurnosti i MITM napada u smislu skeniranje Bluetooth LE uređaja, otkrivanje uređaja, prikaz informacija o uređajima i interakciju čije će mogućnosti biti prikazane u praktičnom dijelu rada.

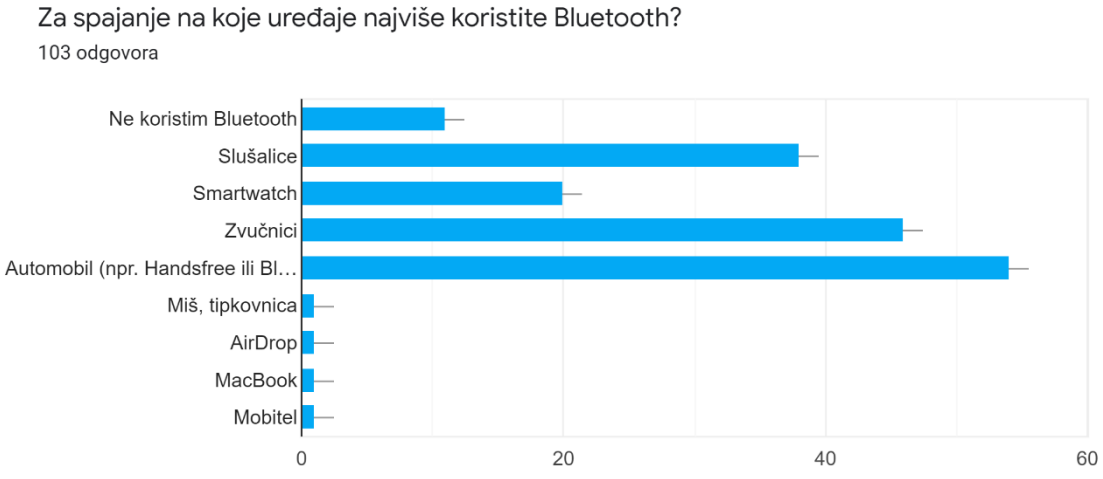
1.11. Anketa

Za potrebe pisanja ovog rada napravljeno je kratko anketiranje studenata Fakulteta organizacije i informatike Varaždin, te centara Zabok, Križevci i Sisak o korištenju Bluetooth-a. U anketi su sudjelovala 103 studenta prve, druge i treće godine stručnog studija Primjena informacijske tehnologije u poslovanju u periodu od 2. lipnja 2021. godine do 5. kolovoza 2021. godine.

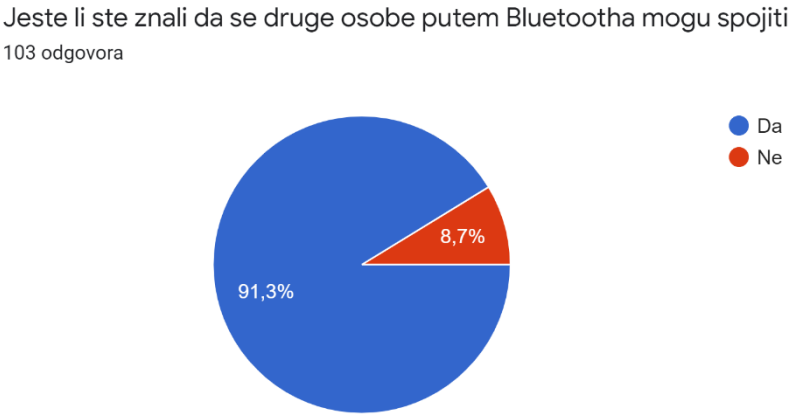


Slika 12 Pitanje 1 - Anketa (Google Forms)

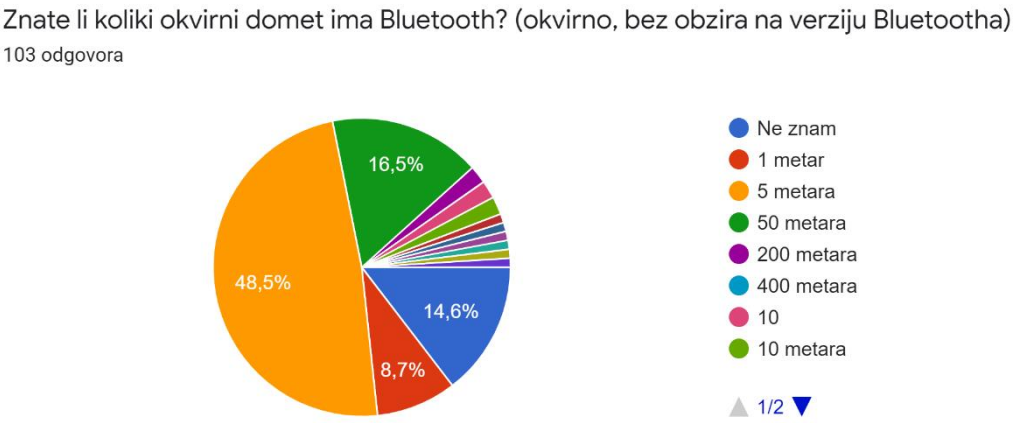
Slika 13 Pitanje 2 - Anketa (Google Forms)



Slika 14 Pitanje 3 - Anketa (Google Forms)



Slika 15 Pitanje 4 - Anketa (Google Forms)



Slika 16 Pitanje 5 - Anketa (Google Forms)

Analizom ankete možemo zaključiti da ispitanici najčešće nemaju konstantno upaljen Bluetooth iako postoji dio ispitanika koji Bluetooth uvijek ima upaljen bez obzira da li isti koristi ili ne. Ispitanici najčešće Bluetooth koriste za multimediju odnosno slušanje glazbe ili za handsfree razgovore gdje podaci iz uređaja tehnički nisu ugroženi jer se radi o prijenosu zvuka. Gotovo 20% ispitanika Bluetooth koristi za povezivanje s pametnim satovima koji često imaju starije verzije Bluetooth protokola, a ipak se u ovom slučaju radi o slave uređaju koji može primati osjetljive podatke od strane master uređaja (npr. prikaz poruka, e-pošte itd.). Više od 8% ispitanika nije upoznato s činjenicom da njihov uređaj može biti ugrožen putem Bluetooth veze, a gotovo pola ispitanika smatra da je domet Bluetootha samo 5 metara.

1.12. Zaštita Bluetooth uređaja

Analizom teorijskog dijela ovog rada mogu se donijeti zaključci i preporuke za zaštitu Bluetooth uređaja odnosno za povećanje sigurnosti kod korištenja. Prije svega, ranjivost najčešće dolazi od strane korisnika stoga je bitno da korisnici Bluetooth tehnologije budu svjesni prijetnji koje ona može nositi. Kada postoji svijest o mogućim prijetnjama logički se može zaključiti da je najbolja zaštita isključivanje Bluetootha kada isti nije potreban ili na uređaju uključiti nevidljivi način rada. Ako se ipak Bluetooth koristi aktivno i često, trebalo bi provjeravati i ažurirati dostupne zakrpe i firmware-e uređaja kao i instalirati i ažurirati antivirusni programi. Također, ni u kojem slučaju se ne smiju prihvaćati nepoznati pozivi za uparivanje. Jednako bitno je i da se aktivno prate novosti vezane za eventualne novootkrivene prijetnje kao i nove verzije Bluetooth-a kako bi pri kupnji uređaja imali dovoljno znanja o verziji koju uređaj koristi, koje su njezine sigurnosne mogućnosti i da li iste osobno pružaju dovoljnu zaštitu i sigurnost. U slučaju krađe uređaja potrebno je na ostalim uređajima koji su bili upareni na ukradeni uređaj prekinuti sve veze i ukloniti s liste sigurnih uređaja. Svakako izbjegavati uređaje čiji je maksimum „Just Works“ model za uparivanje jer su isti najranjiviji u smislu sigurnosti uređaja.

Praktični dio 1

U praktičnom dijelu rad bit će demonstriran napada na Bluetooth Low Energy uređaje putem alata Bettercap instaliranog na virtualni operativni sustav Kali Linux preko aplikacije VirtualBox. U praktičnom dijelu će biti prikazano skeniranje dostupnih BLE uređaja, identifikacija uređaja u dometu, prikupljanje podataka o odabranim uređajima i eventualni napadi na navedene uređaje.

1.13. VirtualBox

Praktični dio rada bit će prikazan u virtualnom operativnom sustavu Kali Linux. Virtualni operativni sustav bit će instaliran preko aplikacije VirtualBox.

VirtualBox je aplikacijski proizvod za virtualizaciju operativnih sustava za poslovnu i osobnu potrebu. VirtualBox je aplikacija visokih performansi i bogata postavkama te je i jedino profesionalno rješenje koje je slobodno dostupno kao softver otvorenog koda. VirtualBox radi na Windows, Linux, Macintosh i Solaris domaćinima i podržava veliki broj gostujućih operativnih sustava uključujući Windows (NT 4.0, 2000, XP, Server 2003, Vista, Windows 7, Windows 8, Windows 10), DOS/Windows 3.x, Linux (2.4, 2.6, 3.x i 4.x), Solaris i OpenSolaris, OS/2 i OpenBSD. (Oracle VM VirtualBox)

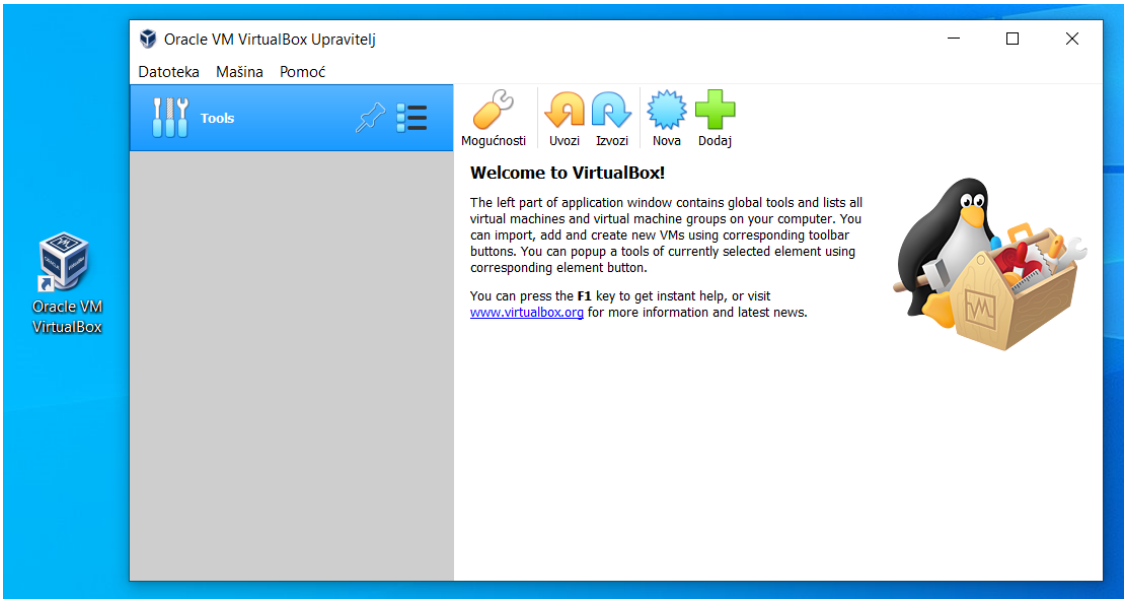
U VirtualBox-u moguće je pokrenuti više operativnih sustava istovremeno, a nakon instaliranja, virtualni stroj i njegovi virtualni tvrdi diskovi mogu se smatrati spremnikom koji se može proizvoljno zamrznuti, probuditi, kopirati, sigurnosno kopirati i transportirati između računala. Pomoću druge značajke Oracle VM VirtualBox-a koja se naziva snimke, može se spremiti određeno stanje virtualnog stroja i po potrebi vratiti u to spremljeno stanje. Na taj se način može eksperimentirati s računalnim okruženjem. Ako nešto pođe po zlu, poput problema nakon instaliranja softvera ili zaraze računala virusom, može se jednostavno vratiti na prethodnu snimku i izbjeći potreba za čestim sigurnosnim kopijama. (Oracle VM VirtualBox)

Slika 17 VirtualBox logo (Oracle VM VirtualBox)

Za virtualizaciju OS-a Kali Linux koristit će se VirtualBox verzija 6.1 preuzeta s https://www.virtualbox.org/.

Slika 18 Preuzimanje i instalacija VirtualBox aplikacije (Oracle VM VirtualBox; autorski rad)

Nakon preuzimanja `VirtualBox-6.1.26-145957-Win.exe` datoteke slijedi jednostavna instalacija aplikacije, a nakon uspješne instalacije otvara se početni ekran preko kojeg se instaliraju operativni sustavi po izboru.



Slika 19 Početni ekran VirtualBox-a (autorski rad)

Slijedeći korak je preuzimanje Kali Linux platforme koja će biti dodana kao novi stroj u VirtualBox-u.

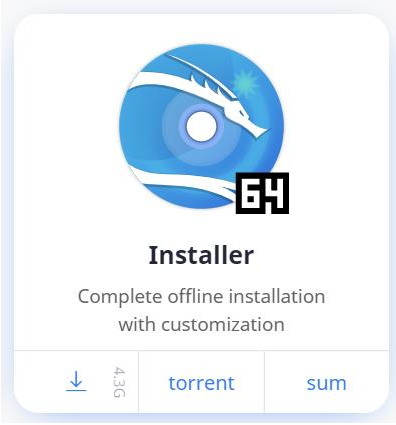
1.14. Kali Linux

Kali Linux je distribucija Linuxa s otvorenim kodom, zasnovana na Debianu i usmjerena na različite zadatke sigurnosti informacija, poput testiranja prodora, sigurnosnih istraživanja, računalne forenzike i obrnutog inženjeringa. (OffSec Services Limited 2021.)

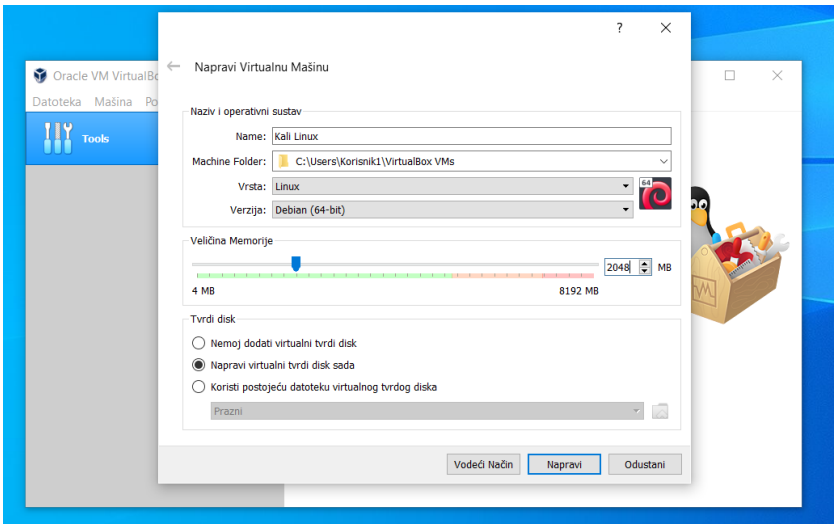
Kali Linux ima preko 600 unaprijed instaliranih aplikacija i alata za sakupljanje informacija, analize ranjivosti, bežične napade, eksploataciju, digitalnu forenziku, napade na zaporke, hakiranje hardvera i sl. (OffSec Services Limited 2021.)

Slika 20 Kali Linux logo (OffSec Services Limited 2021.)

Kali Linux za VirtualBox preuzima se sa web stranice https://www.kali.org/get-kali/ . Na navedenoj lokaciji nalazi se `.iso` format Kali Linux-a koji se preuzima na računalo.



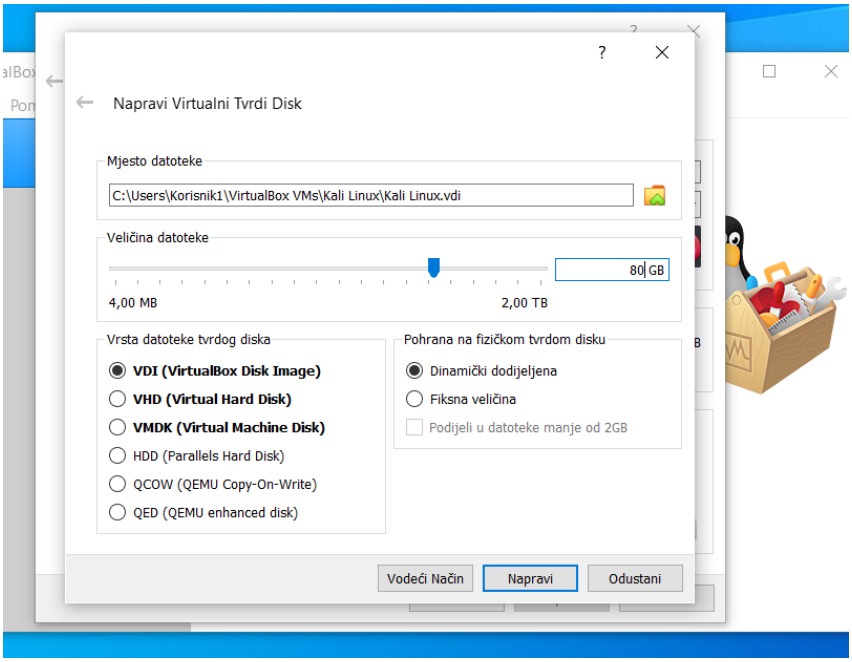
Nakon preuzimanja `kali-linux-2021.2-installer-amd64.iso` datoteke potrebno je vratiti se na početni ekran VirtualBox-a i započeti instalaciju.



Nakon pritiska na gumb

otvara se ekran za dodavanje novog Virtualnog stroja. Upisuje se ime, postavlja se verzija i prilagođava se veličina memorije.

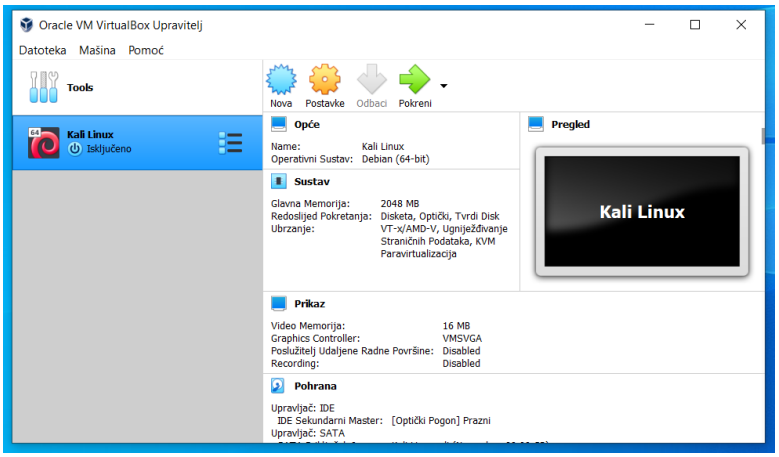
Slika 21 Postavljanje Kali Linux-a 1 (autorski rad)



Nakon postavljanja stroja postavljaju se opcije za Virtualni tvrdi disk.

Slika 22 Postavljanje Kali Linux-a 2 (autorski rad)

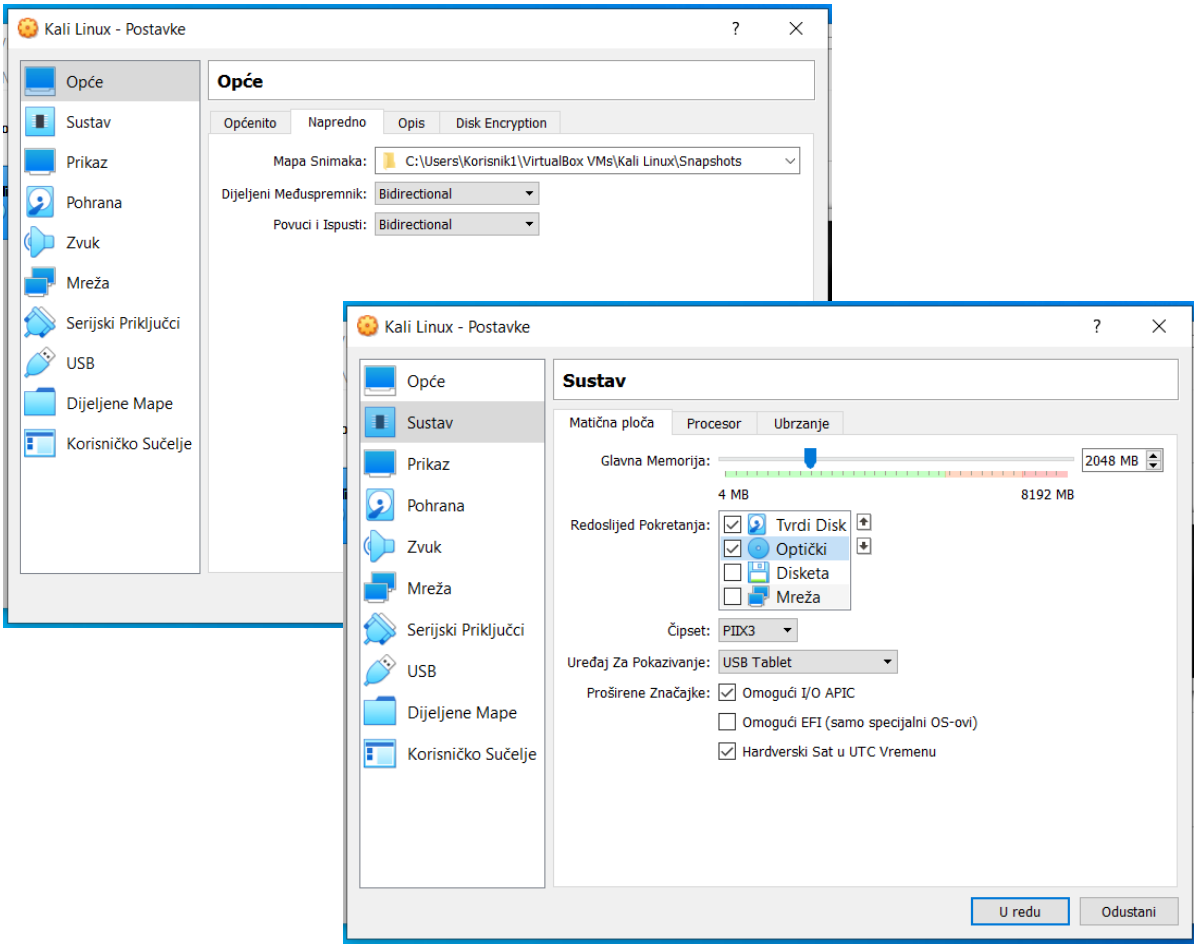
Nakon postavljanja osnovnih opcija napravljen je virtualni stroj Kali Linux-a. Sada je potrebno postaviti dodatne opcije kako bi se optimizirao rad virtualnog stroja.



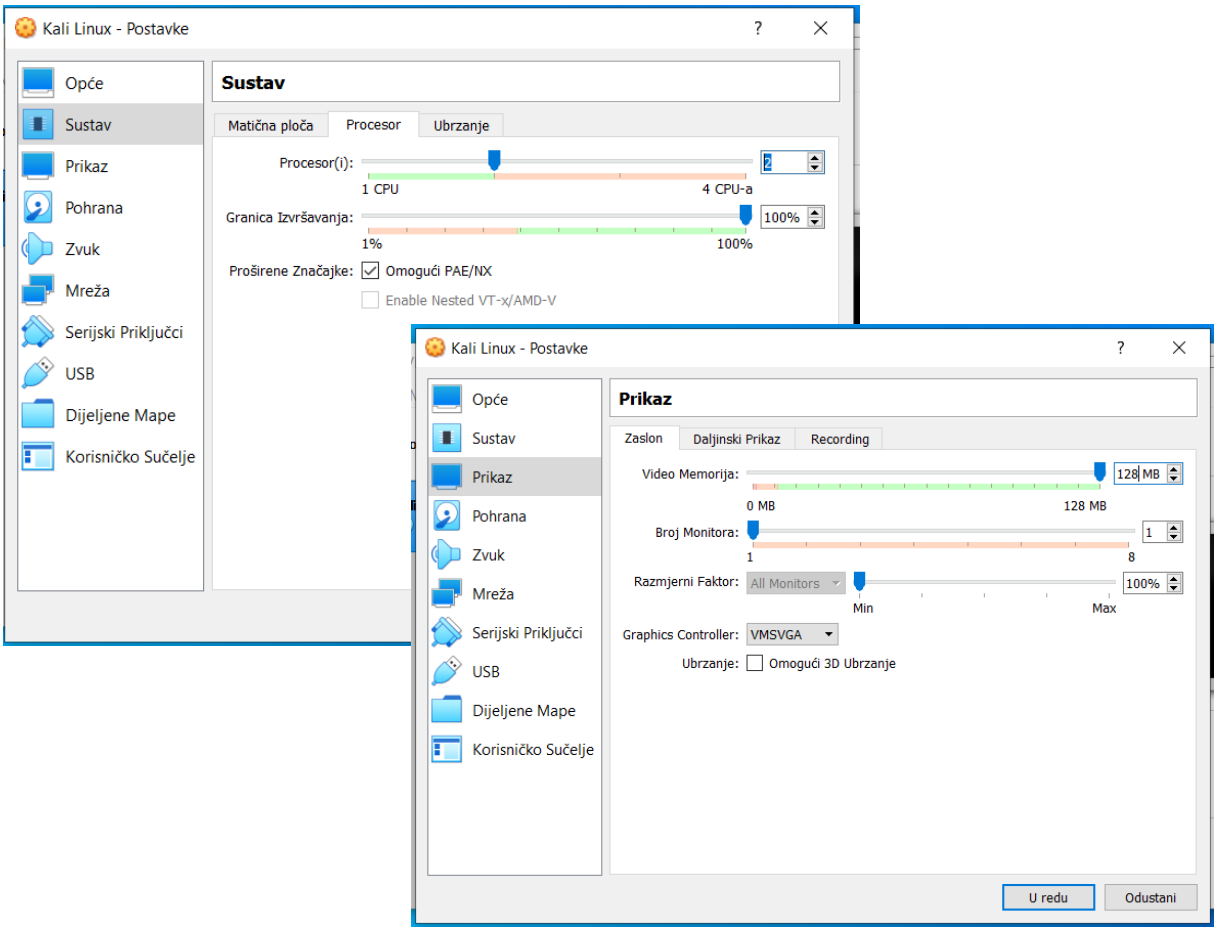
Slika 23 Postavljanje Kali Linux-a 3 (autorski rad)

Pritiskom na gumb

postavljaju se optimalne postavke na temelju preporuka s Kali Linux web stranice https://www.kali.org/docs/virtualization/install-virtualbox-guest-vm/



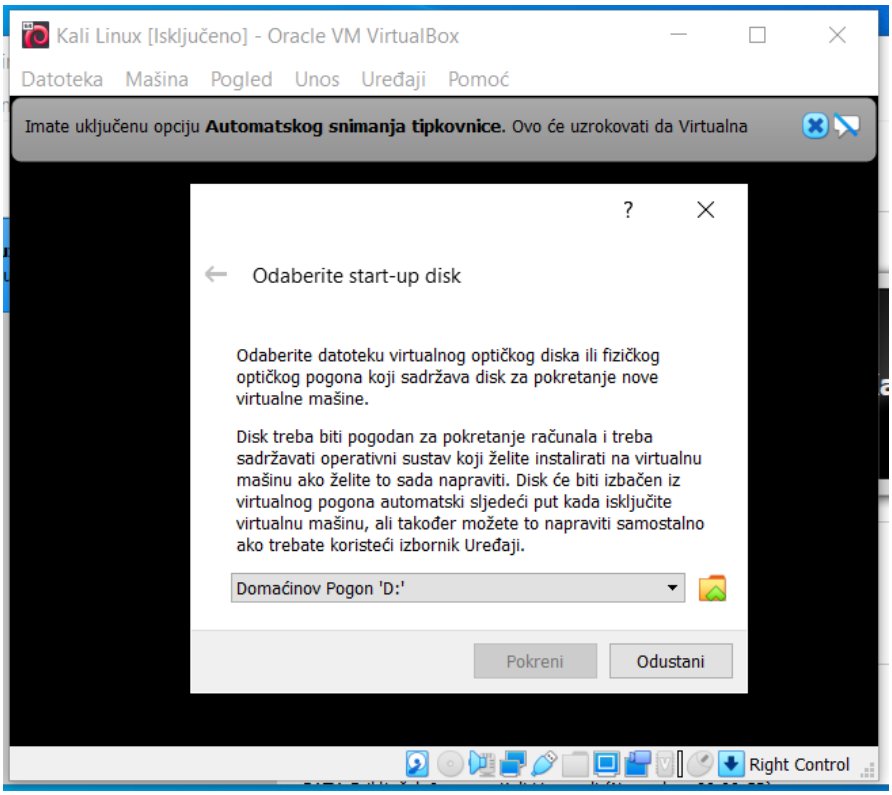
Slika 24 Postavljanje Kali Linux-a 4 (autorski rad)



Slika 25 Postavljanje Kali Linux-a 5 (autorski rad)

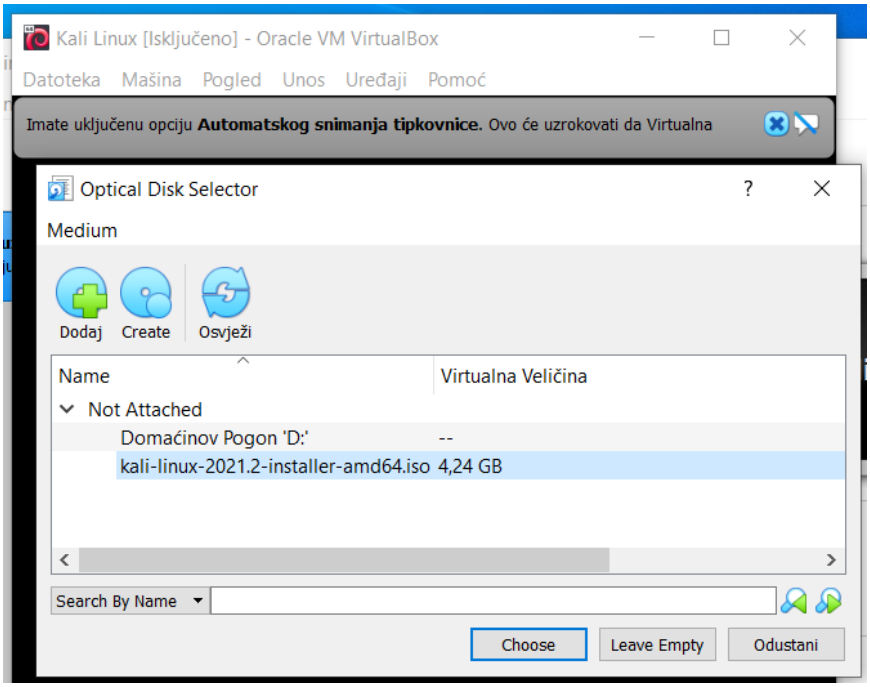
Nakon postavljanja svih preporučenih postavka pokreće se Virtualni stroj putem gumba

.



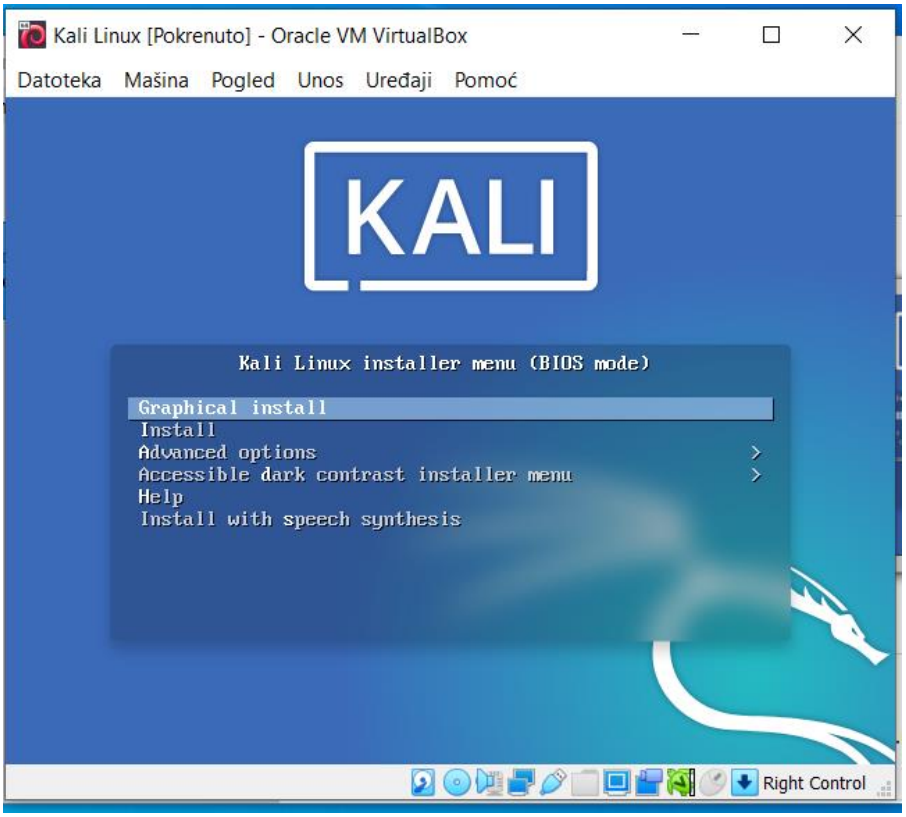
Slika 26 Postavljanje Kali Linux-a 6 (autorski rad)

U ovom koraku dodaje se prethodno preuzeta `kali-linux-2021.2-installer-amd64.iso` datoteka.



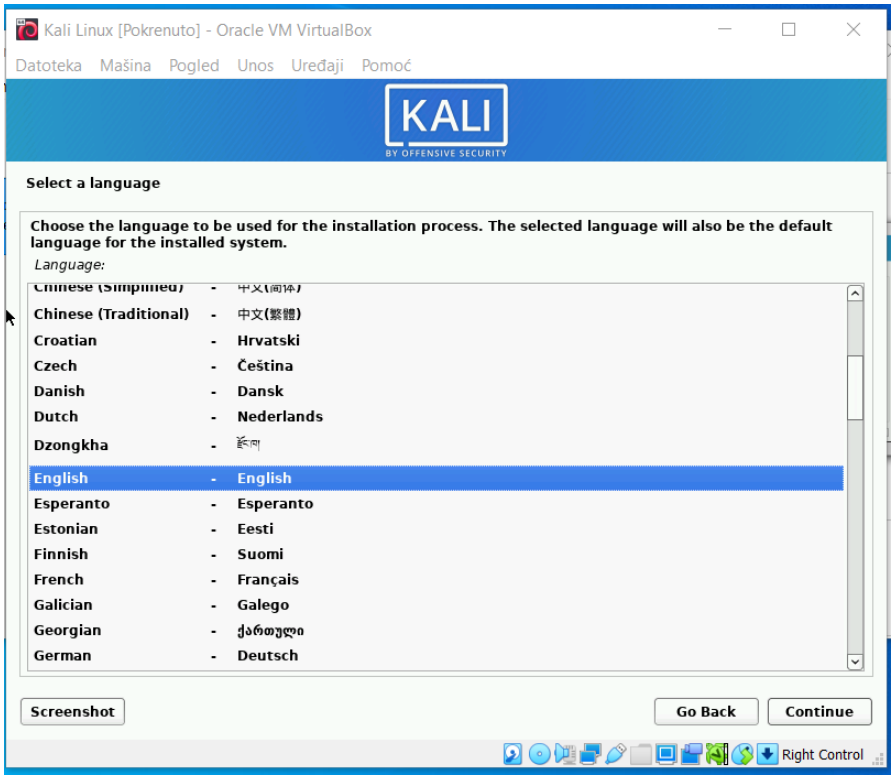
Odabire se datoteka i pokreće postupak instalacije operativnog sustava Kali Linux.

Slika 27 Postavljanje Kali Linux-a 6 (autorski rad)



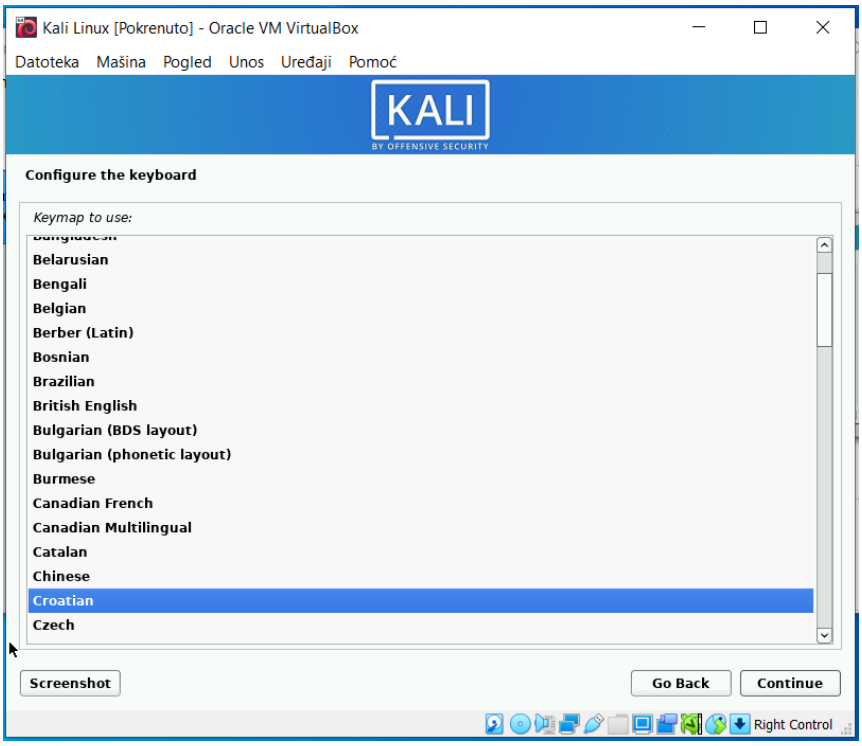
Slika 28 Postavljanje Kali Linux-a 7 (autorski rad)

Sučelje za instalaciju slično je kao i kod ostalih operativnih sustava odnosno kao i kod instalacije „stvarnih“ operativnih sustava.



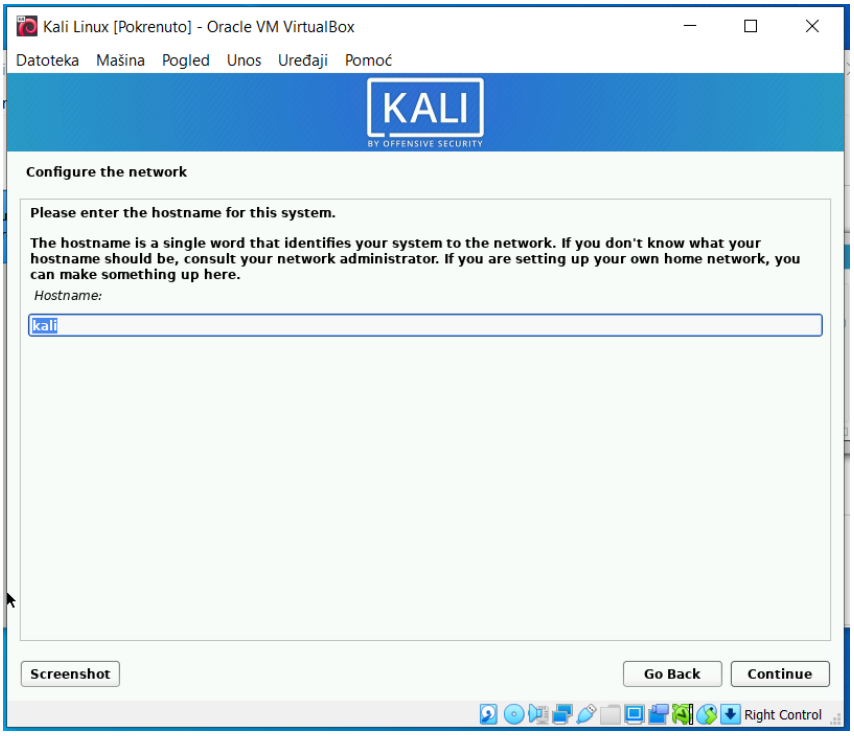
Slika 29 Postavljanje Kali Linux-a 8 (autorski rad)

Odabir jezika operativnog sustava.



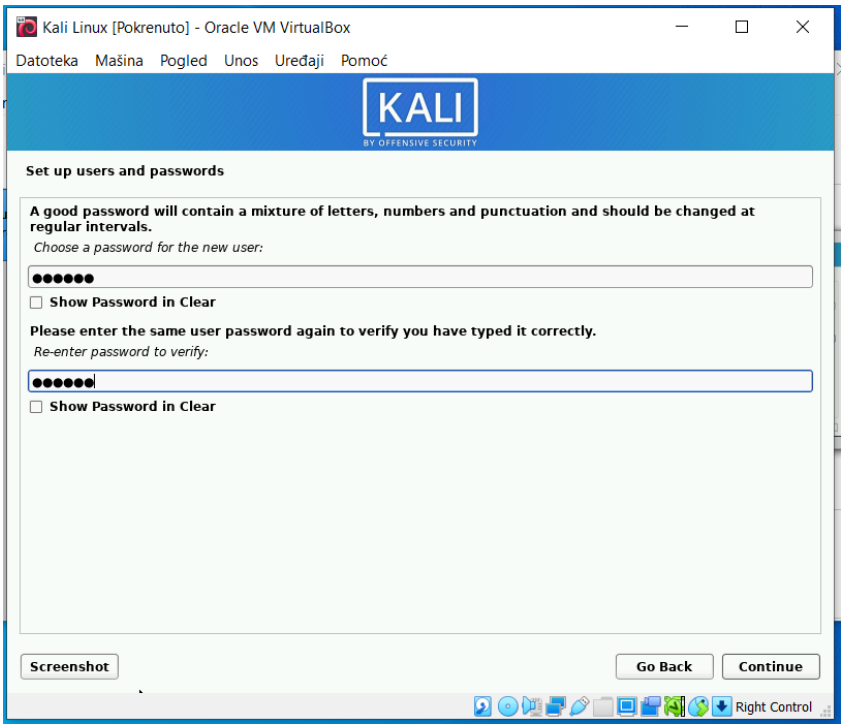
Konfiguracija jezika tipkovnice.

Slika 30 Postavljanje Kali Linux-a 9 (autorski rad)



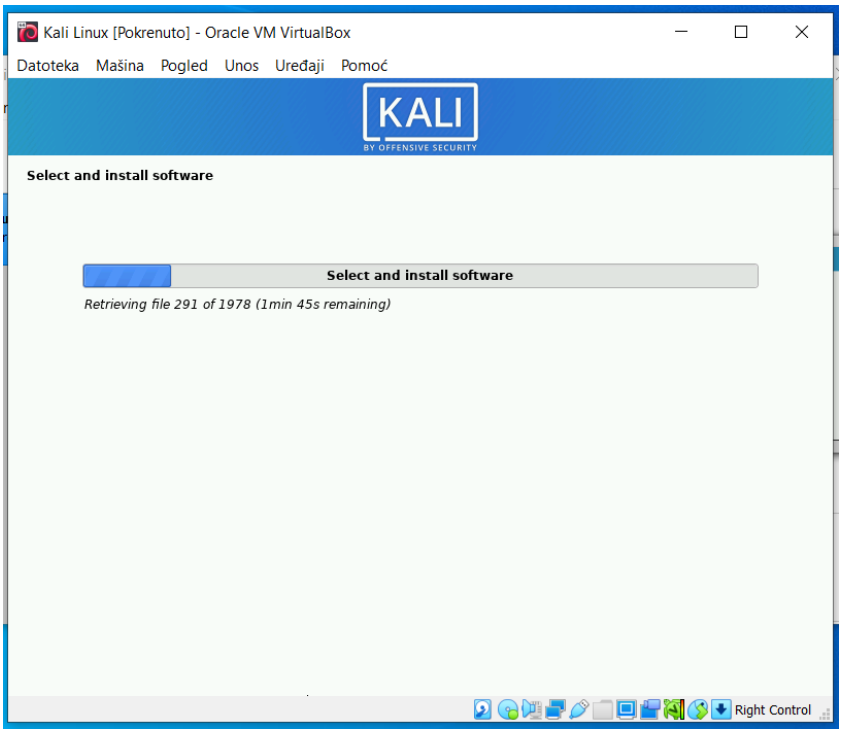
Odabir korisničkog imena.

Slika 31 Postavljanje Kali Linux-a 10 (autorski rad)



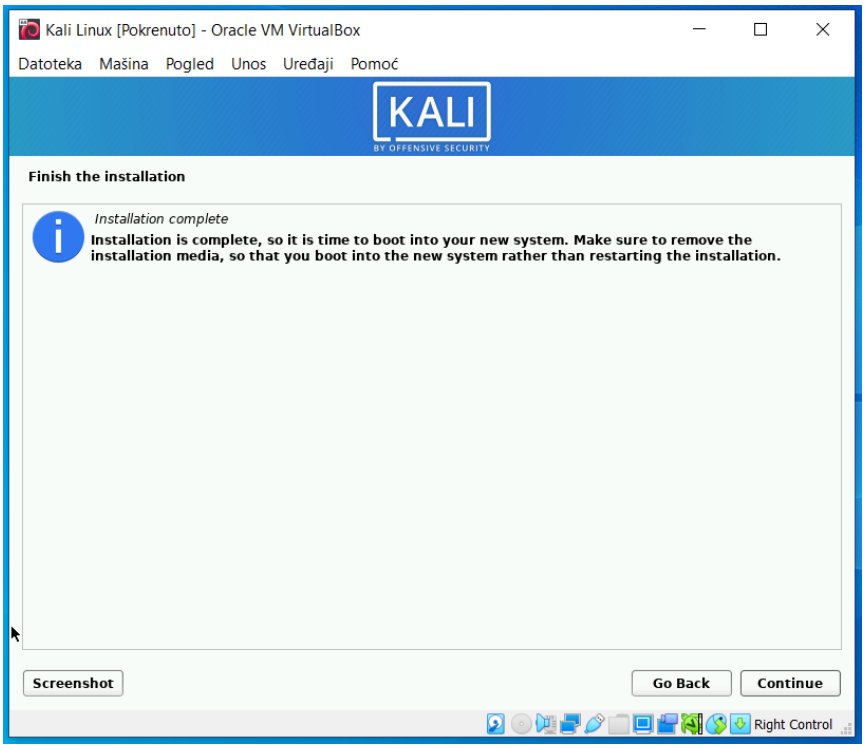
Postavljanje zaporke.

Slika 32 Postavljanje Kali Linux-a 11 (autorski rad)



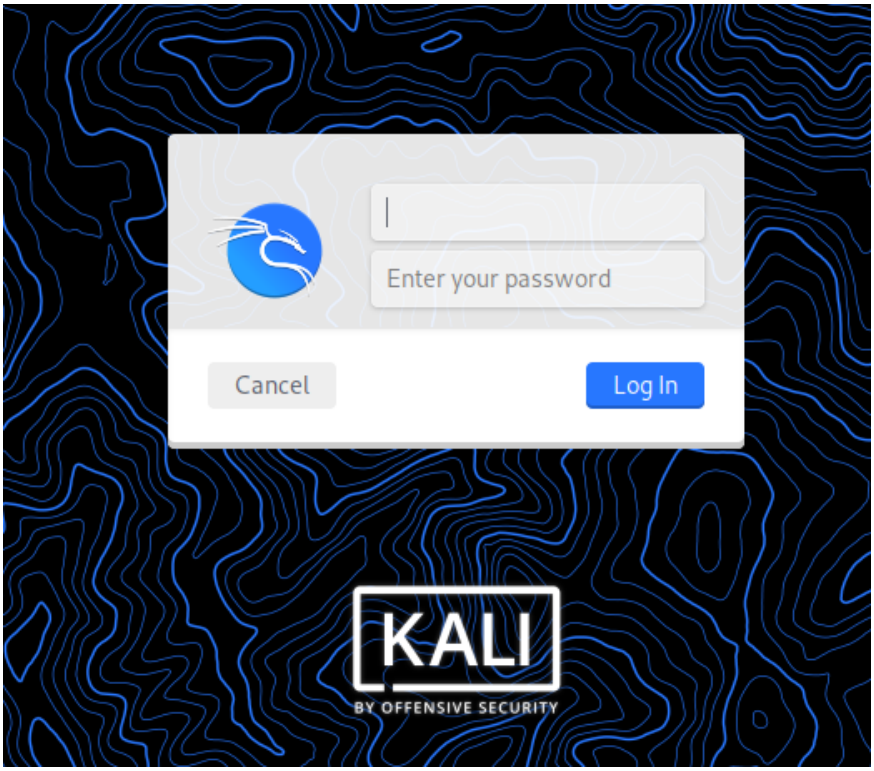
Instalacija operativnog sustava.

Slika 33 Postavljanje Kali Linux-a 12 (autorski rad)



Završetak instalacije Kali Linux operativnog sustava.

Slika 34 Postavljanje Kali Linux-a 13 (autorski rad)



Login u operativni sustav Kali Linux prema postavljenim parametrima (korisničko ime i zaporka).

Slika 35 Postavljanje Kali Linux-a 14 (autorski rad)

Virtualni operativni sustav Kali Linux je uspješno instaliran. Na Slici 36 prikazuje se slika ekrana radne površine Kali Linux operativnog sustava.

Slika 36 Radna površina Kali Linux-a (autorski rad)

Kao što je već navedeno, Kali Linux dolazi s unaprijed instaliranim aplikacijama i alatima za sakupljanje informacija, analize ranjivosti, bežične napade, eksploataciju, digitalnu forenziku, napade na zaporke, hakiranje hardvera i sl., a neki od njih se mogu vidjeti na Slici 37.

Slika 37 Aplikacije i alati unutar Kali Linux-a (autorski rad)

1.15. Bettercap

Za demonstraciju napada na Bluetooth uređaje koristit će se alat Bettercap.

Bettercap je moćan, lako proširiv i prenosiv alat koji se koristi u svrhu istraživanja sigurnosti i MITM napada na WiFi mreže, Bluetooth LE uređaje i IPv4/IPv6 mreže. (Bettercap, bez dat.)

Slika 38 Bettercap logo (bettercap.org)

Informacije su prvi potreban element za početak svakog napada. Bettercap je alat koji pruža takve informacije i isti prikazuje informacije kao što je npr. proizvođač uređaja. Ovom, na prvi pogled, jednostavnom informacijom može se saznati tvornički PIN za uparivanje. Jedna od informacija koju prikazuje Bettercap je i softver koji uređaj koristi. Ako se radi o starijem softveru mogu se istražiti informacije o ranjivostima tog softvera koje se zatim mogu iskoristiti.

Ključna informacija koju Bettercap prikazuje je MAC adresa uređaja koja se zatim iskorištava za daljnje povezivanje s uređajima, prikazivanje povratnih informacija o uređajima i zapisivanje podataka na uređaje. Bluetooth MAC adresa je 48-bitna vrijednost koja jedinstveno identificira Bluetooth uređaj. U Bluetooth specifikaciji naziva se BD_ADDR.

U praktičnom dijelu rada, a nastavno na temu rada, Bettercap će se koristiti za skeniranje Bluetooth LE uređaja, otkrivanje uređaja, prikaz informacija o uređajima i eventualna interakcija s uređajima.

Operacijski sustavi općenito imaju dva sučelja za rad, GUI (grafičko korisničko sučelje) i CLI (sučelje naredbenog retka). Iako postoji unaprijed instaliran Bettercap s grafičkim sučeljem, u radu će se koristiti Bettercap u Linux sučelju naredbenog retka koji se zove „Terminal“.

U nastavku će biti opisane dostupne naredbe Bettercap modula za BLE uređaje (Bettercap, bez dat.):

```
ble.recon on
```

Naredba za pokretanje otkrivanja Bluetooth Low Energy uređaja.

```
ble.recon off
```

Naredba za zaustavljanje otkrivanja Bluetooth Low Energy uređaja.

```
ble.clear
```

Naredba za brisanje otkrivenih BLE uređaja.

```
ble.show
```

Naredba za prikaz popisa otkrivenih BLE uređaja. Neki od stupaca koje ova tablica uključuje su indikator jačine primljenog signala (kratica: RSSI; eng. Received Signal Strength Indication) odnosno jačina signala koju prima antena, Prodavatelj/Proizvođač (eng. Vendor) gdje se može vidjeti naziv proizvođača otkrivenog uređaja, Zastavice (eng. Flags) koje su bile opisane u poglavlju 1.8 i kao najbitniji element MAC adresa uređaja.

```
ble.enum MAC
```

Naredba za prikaz liste servisa i karakteristika odabranog uređaja. Ova naredba otkriva najviše podataka o odabranom uređaju odnosno već u ovom koraku napadač ima podatke koje prelaze iz javnog u privatno odnosno iz sigurnog u nesigurno. Neki od podataka koje ova tablica prikazuje su karakteristike grupirane prema servisima, njihova svojstva, podaci i sl.

```
ble.write MAC UUID HEX_DATA
```

Naredba za pisanje heksadekadskog zapisa na uređaj s upisanom MAC adresom na karakteristiku koja ima upisanu UUID vrijednost.

Korištenjem nabrojanih i nekih dodatnih naredbi bit će demonstriran napad na BLE uređaj.

1.16. Demonstracija napada

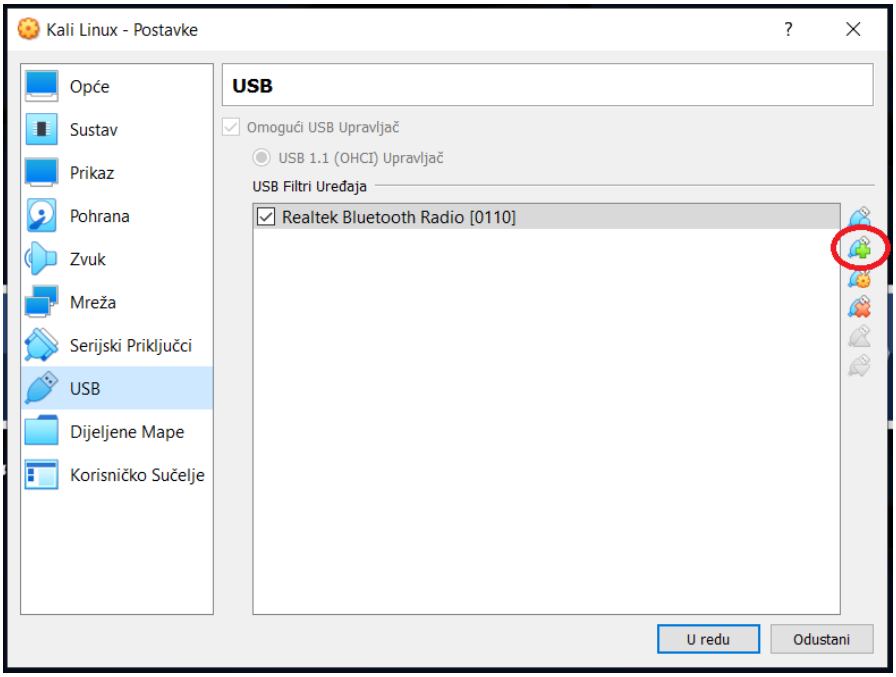
Prije početka same demonstracije napada na BLE uređaje potrebno je napraviti nekoliko pripremnih radnji.

S obzirom da se putem Bettercap alata pretražuju BLE uređaji potrebno je dati dozvolu VirtualBox-u za korištenje Bluetooth antene računala na kojem se radi. U padajućem

izborniku „Uređaji“, u dijelu „USB“ provjerava se popis dostupnih uređaja računala domaćina. Na Slici 39 vidljivo je da VirtualBox vidi „Realtek Bluetooth Radio [0110]“. Kako bi priključak bio aktiviran potrebno je odabrati opciju „Postavke USB-a…“. (Slika 39)

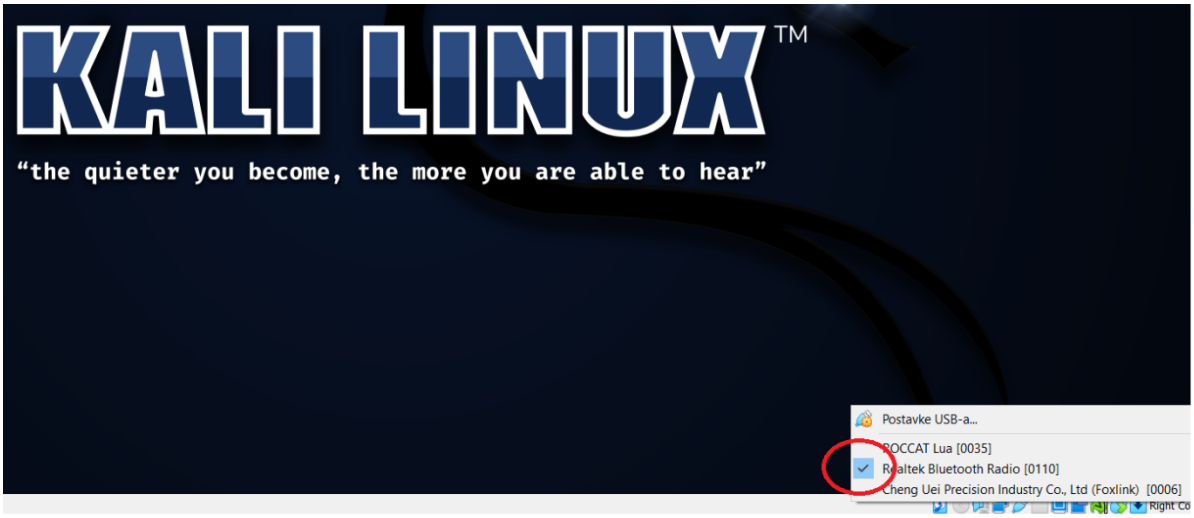
Slika 39 Postavke USB-a (autorski rad)

U postavkama USB-a potrebno je na popis dodati Bluetooth uređaj odabirom opcije označene na Slici 40.



Slika 40 Dodavanje Bluetooth uređaja (autorski rad)

Nakon dodavanja Bluetooth uređaja potrebno je isti aktivirati na način da se na alatnoj traci u podnožju VirtualBox-a označi Bluetooth uređaj. (Slika 41)



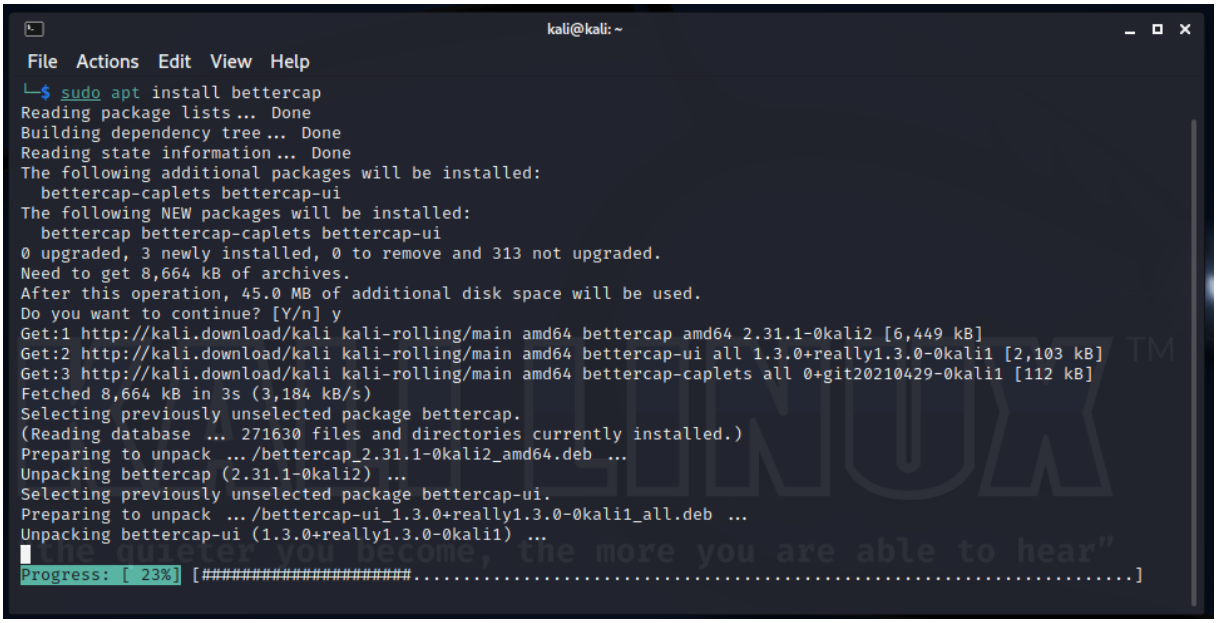
Slika 41 Aktiviranje Bluetooth uređaja (autorski rad)

Nakon dodavanja i aktiviranja Bluetooth uređaja pokreće se sučelje naredbenog retka odnosno Linux Terminal Emulator.

Prije samo pokretanja Bettercap modula provjerava se aktivna verzija alata naredbom `apt-cache show bettercap | grep 'Version: '` (Slika 42).

Slika 42 Provjera verzije alata Bettercap (autorski rad)

Nakon provjere verzije, naredbom `sudo apt install bettercap` instalira/ažurira se posljednja verzija Bettercap alata. (Slika 42).

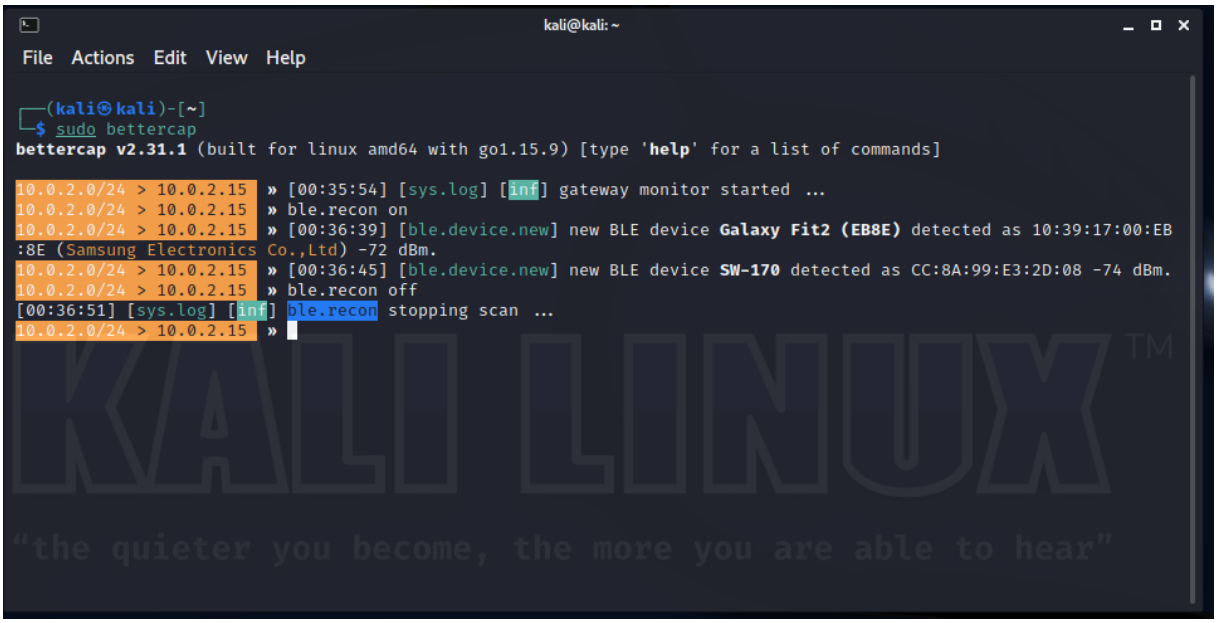


Slika 43 Ažuriranje/instaliranje Bettercap-a (autorski rad)

Nakon provedenih provjera pokreće se Bettercap naredbom `sudo bettercap`. Slijedi unos zaporke koju zahtjeva sudo (SuperUser DO), te se pokreće Bettercap modul. (Slika 44).

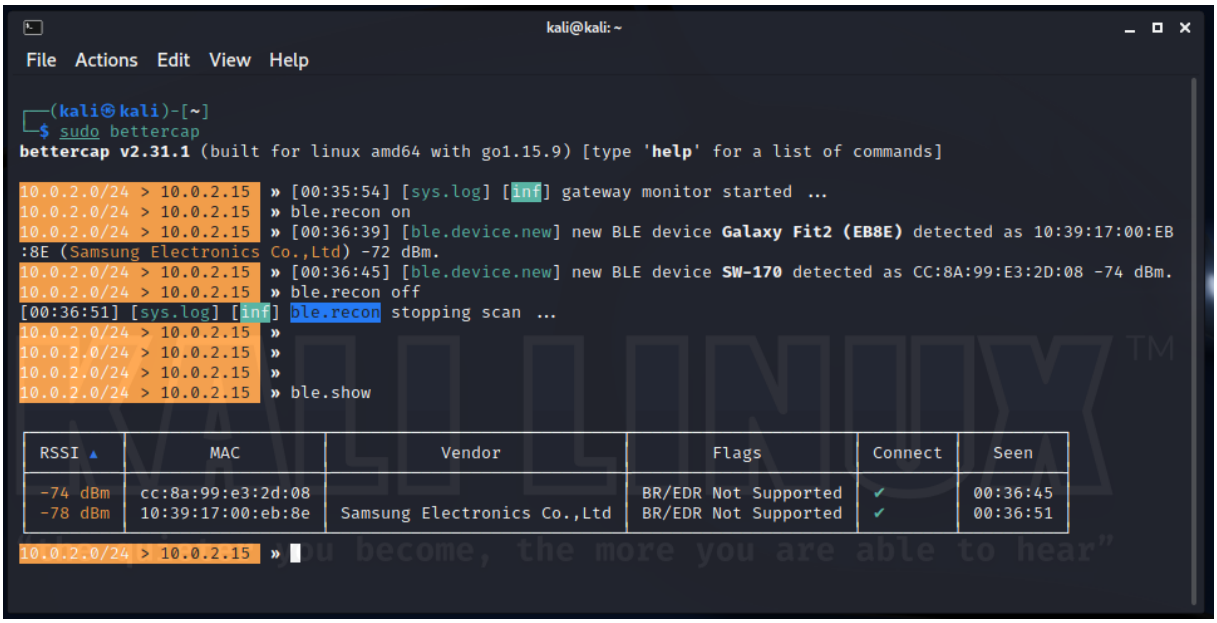
Slika 44 Pokretanje Bettercap modula (autorski rad)

Naredbom `ble.recon on` pokreće se otkrivanje dostupnih BLE uređaja, te se na Slici 45 može uočiti da je Bettercap otkrio dva BLE uređaja, Galaxy Fit2 i SW-170 te se trenutno mogu vidjeti i njihove MAC adrese i jačina signala.



Slika 45 Pronađeni uređaji u Bettercap modulu (autorski rad)

Naredbom `ble.recon off` zaustavlja se otkrivanje BLE uređaja, te se naredbom `ble.show` prikazuje tablica otkrivenih uređaja s dodatnim podacima. (Slika 46).

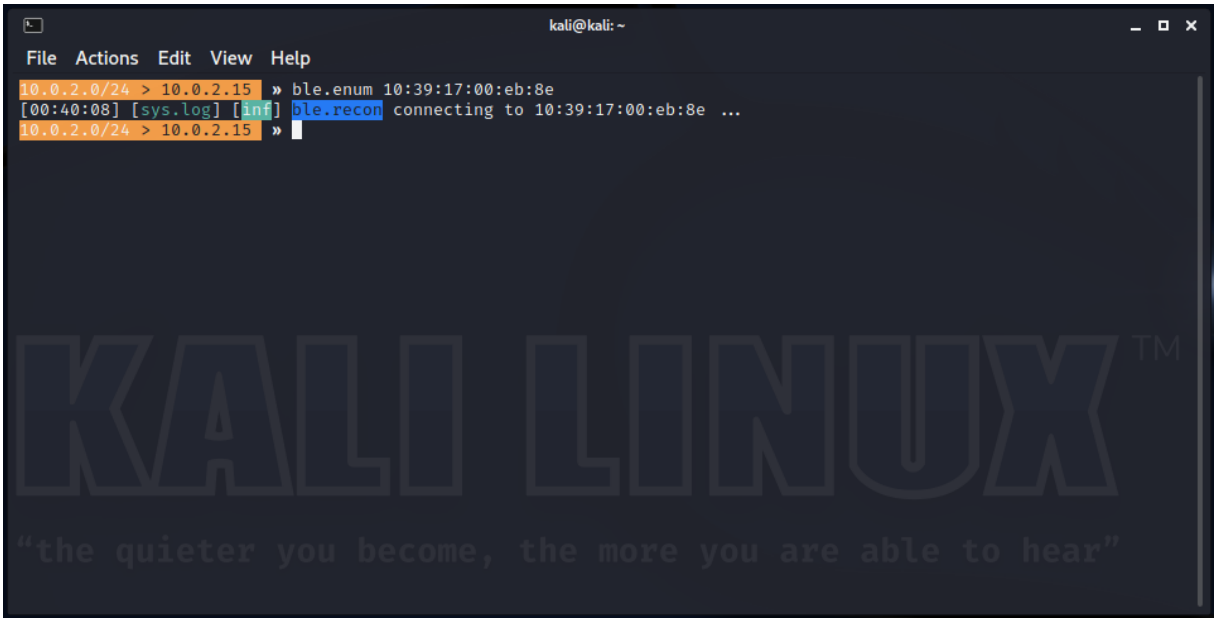


Slika 46 Tablica otkrivenih uređaja (autorski rad)

Kao što je već navedeno, u tablici su vidljivi podaci o RSSI (jačina signala), MAC adresa uređaja, prodavatelj/proizvođač uređaja u kojoj se može vidjeti da je jedan proizvođač poznat (Samsung Electronics Co., Ltd), dok za drugi uređaj nije naveden proizvođač.

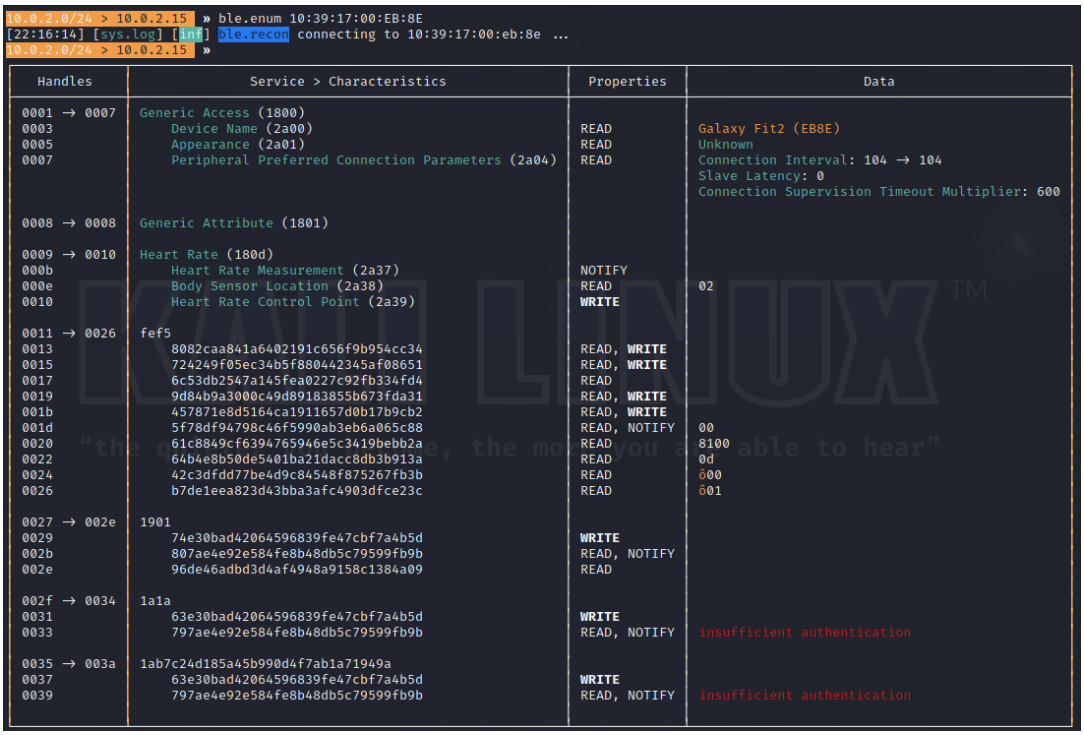
U tablici su vidljiva i dva dodatna stupca, Connect za status veze i Seen za posljednju primljenu vremensku oznaku odašiljača.

Naredbom `ble.enum [odabrana MAC adresa]` otkrivaju se detaljniji podaci o odabranom uređaju. (Slika 47 i Slika 48).



Slika 47 Pokretanje otkrivanja detalja o odabranom uređaju (autorski rad)

Naredbom `ble.enum 10:39:17:00:eb:8e` otkrivaju se podaci uređaja od prije poznatog proizvođača (Samsung Electronics Co., Ltd), ali se ovom naredbom prikazuju i dodatni podaci o servisima i karakteristikama. (Slika 48).



Slika 48 Servisi i karakteristike - Galaxy Fit2 (autorski rad)

U poglavlju 1.7 opisani su BLE protokoli te je spomenut i GATT protokol kao procedura putem koje komuniciraju dva BLE uređaja. GATT određuje kako dva BLE uređaja međusobno komuniciraju koristeći koncepte kao što su servisi i karakteristike. Ovaj protokol sprema sve servise i karakteristike u tablicu pomoću 16-bitnih ili 128-bitnih identifikatora. (Fotios C. et al., 2021)

Servisi i karakteristike su dva glavna koncepta koji čine GATT.

- Servisi se mogu opisati kao kontejneri za karakteristike. Servis može imati više karakteristika, a svaki je Servis jedinstven i označava se univerzalnim jedinstvenim identifikatorom (UUID) koji može biti duljine 16 bita za službene servise ili 128 bita za prilagođene servise.
- Karakteristike su temeljni koncept GATT transakcija i slične su servisima, odnosno svaka karakteristika također ima svoj UUID po kojem se razlikuje od ostalih karakteristika. (Fotios C. et al., 2021)

Službene UUID duljine 16 bita (npr. Device Name (2a00)) propisuje Bluetooth SIG, Inc., odnosno svaki uređaj na tržištu mora servise i karakteristike označiti identifikatorima

prema uputama koje propisuje Bluetooth SIG, Inc. Prilagođene UUID duljine 128 bita (npr. 8082caa841a6402191c656f9b954cc34) definira proizvođač. Značenje službenog UUID-a je poznato, dok je značenje prilagođenih UUID-a nepoznato, te je za otkrivanje značenja potrebno dodatno istražiti službenu dokumentaciju uređaja, ako ista postoji. (Ethical hacking and penetration testing, 2021)

U stupcu Properties prikazana su svojstva karakteristike i ona mogu biti READ, WRITE, INDICATE, NOTIFY ili kombinacija više navedenih svojstava.

READ - aplikacije mogu čitati vrijednost ove karakteristike BLE uređaja

WRITE - aplikacije mogu promijeniti vrijednost ove karakteristike BLE uređaja

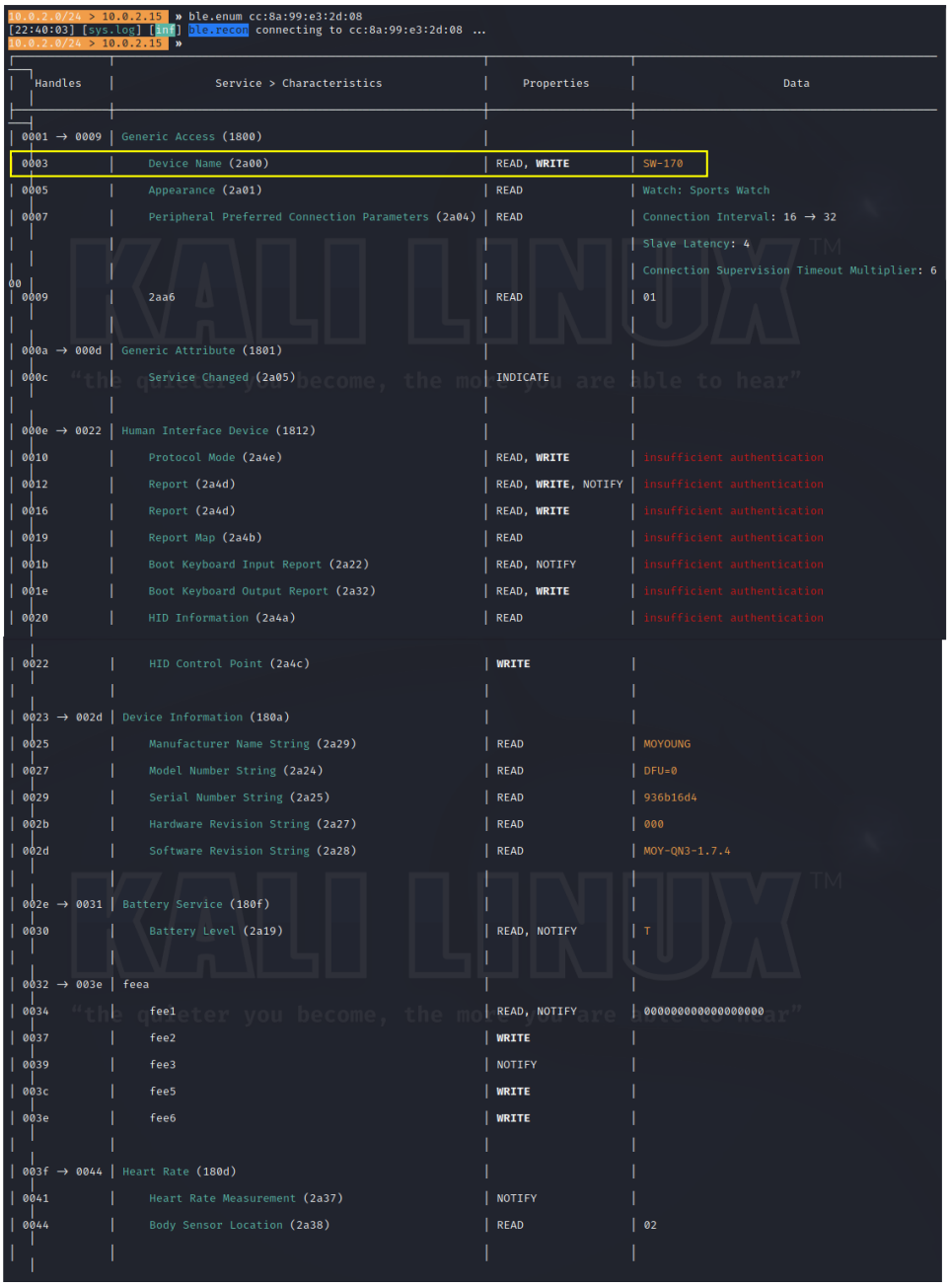
INDICATE i NOTIFY: aplikacije dobivaju obavijesti ako se promijeni ova karakteristika. Razlika u ova dva svojstva je postojanje slanja potvrde o promjeni od aplikacije do poslužitelja.

Stupac Data sadrži trenutnu vrijednost karakteristike ili dodatne informacije o karakteristici.

Za izvršenje napada kojem je cilj neovlaštena modifikacija podataka, odnosno prisilno mijenjanje informacija, potrebno je usmjeriti se na karakteristike koje imaju svojstvo WRITE jer se vrijednosti ovih karakteristika mogu mijenjati.

Za demonstraciju promjene vrijednosti odabrane karakteristike odabrat će se uređaj nepoznatog proizvođača, MAC adrese `cc:8a:99:e3:2d:08` .

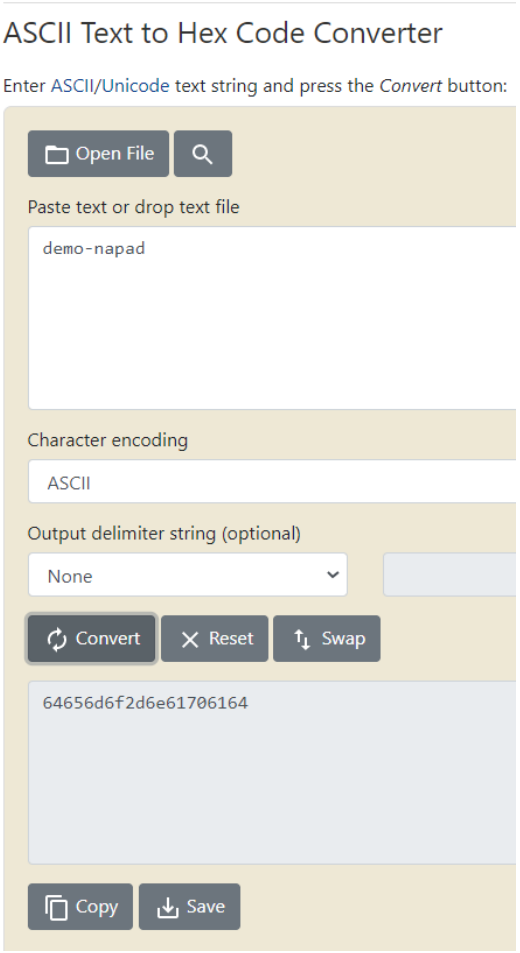
Naredba `ble.enum cc:8a:99:e3:2d:08` pokazuje servise, karakteristike, svojstva i podatke odabranog uređaja, te se na Slici 49 može vidjeti da se radi o sportskom satu imena SW-170, proizvođača Moyoung.



Slika 49 Servisi i karakteristike - SW-170 (autorski rad)

Može se primijetiti da je na otkrivenom uređaju prvi 16-bitni UUID s WRITE svojstvom karakteristike njegov naziv (eng. Device Name) „SW-170“.

U teoriji su ispunjene sve pretpostavke za mogući napad naredbom `ble.write MAC UUID HEX_DATA` jer je poznata MAC adresa uređaja (`cc:8a:99:e3:2d:08`), UUID s WRITE svojstvom (Device Name (`2a00`)), a za `HEX_DATA` iskoristit će se online ASCII Text to Hex Code Converter s web adrese https://www.rapidtables.com/convert/number/ascii-to-hex.html.

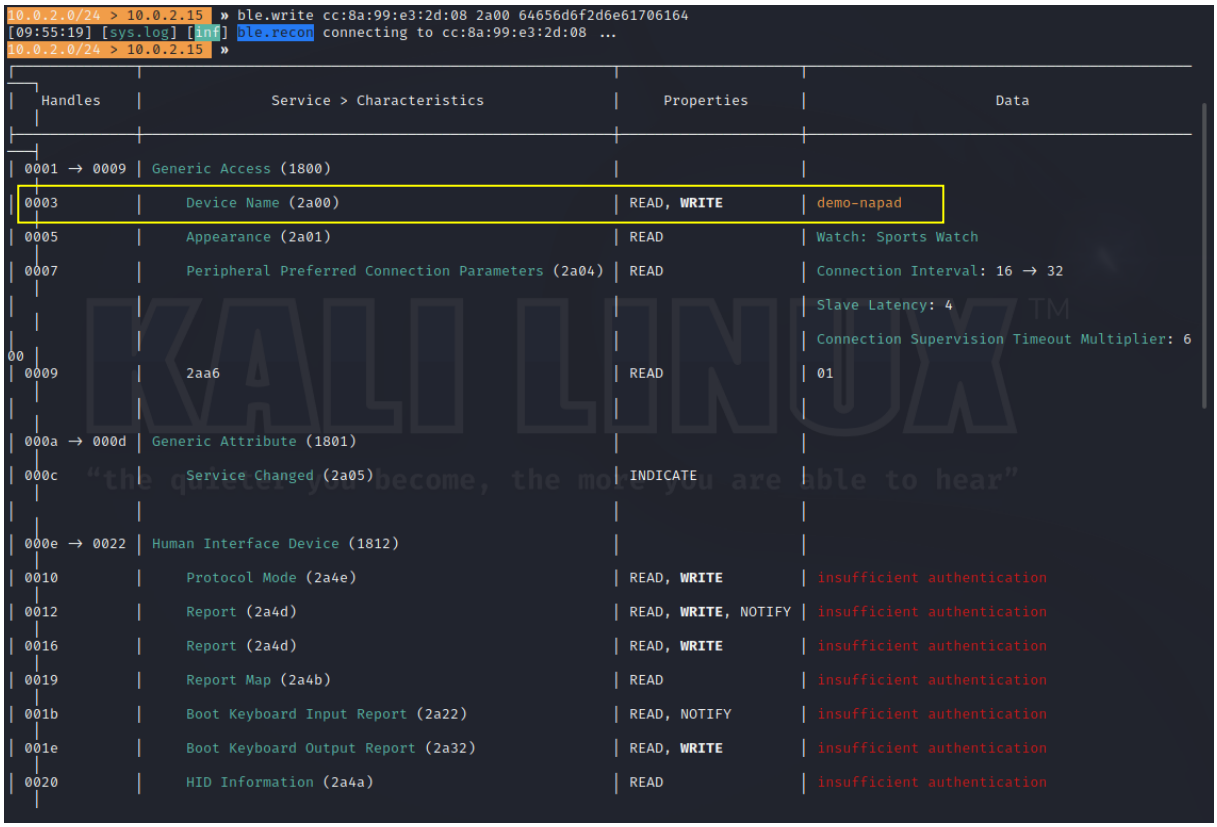


Slika 50 Text to Hex Code Converter (autorski rad)

Za pokušaj izmjene imena uređaja preko `ble.write` naredbe u converter je upisan ASCII tekst „demo-napad“, a preko online convertera dobiva se heksadekadski zapis upisanog teksta koji glasi „64656d6f2d6e61706164“.

Puna naredba `ble.write cc:8a:99:e3:2d:08 2a00 64656d6f2d6e61706164` upisuje se u Bettercap modul.

Na Slici 51 može se vidjeti rezultat navedene naredbe. Bettercap modul po izvršenju `ble.write` naredbe automatski pokreće `ble.enum` naredbu, te su promjene automatski vidljive.



Slika 51 Izmijenjeni naziv uređaja (autorski rad)

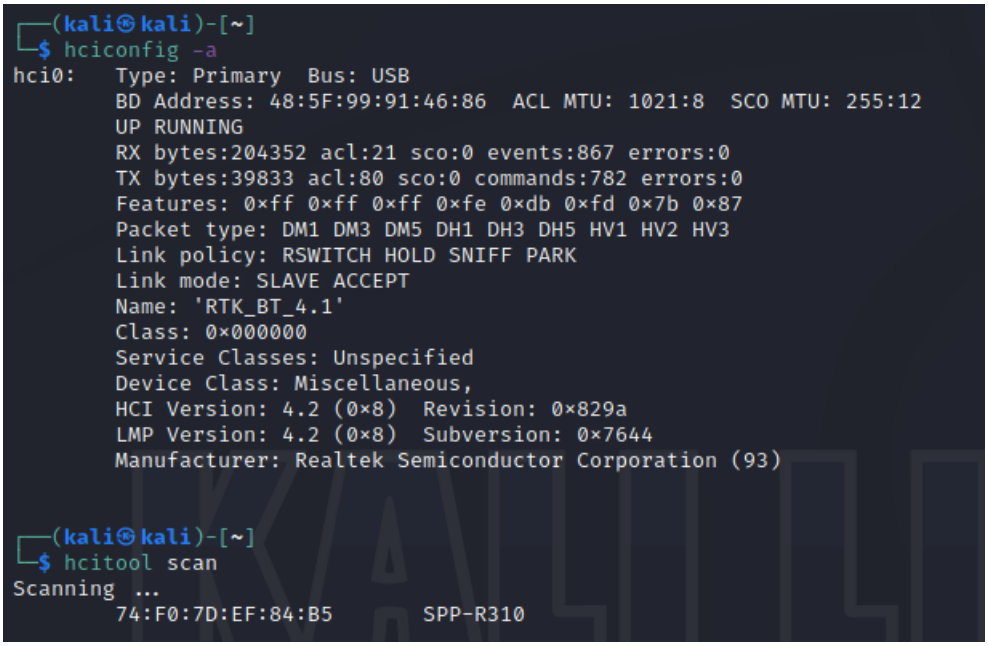
Na Slici 51 vidljiva je promjena podatka karakteristike Device Name. Tvornički naziv „SW-170“ promijenjen je u željeno novo ime „demo-napad“ te je interakcija s uređajem i napad na uređaj uspješno izveden.

Iako je demonstracija MITM napada izvedena na karakteristiku koja ne utječe na funkcionalnost uređaja, na popisu karakteristika može se vidjeti da postoji nekoliko karakteristika koje dopuštaju pisanje (eng. WRITE), a po nazivima karakteristike se može zaključiti da su iste vezane za funkcionalnost uređaja. Sama tablica pokazuje poruku „insufficient authentification“ za takve karakteristike jer dopušta napadaču pristup osjetljivom sadržaju ili funkcionalnosti bez ispravne provjere autentičnosti.

Za pretpostaviti je da je proizvođač ovog uređaja svjesno ili nesvjesno ostavio ovaj BLE uređaj ranjivim na ovakav tip vektora napada. S druge strane, na Slici 48 vidljiv je popis servisa i karakteristika ozbiljnijeg proizvođača elektronike gdje se može vidjeti da karakteristike s porukom „insufficient authentification“ ne dopuštaju pisanje, te bi za napad na takav uređaj trebalo više vještine, znanja i potrebnih alata što je pokazatelj da je uređaj sigurniji.

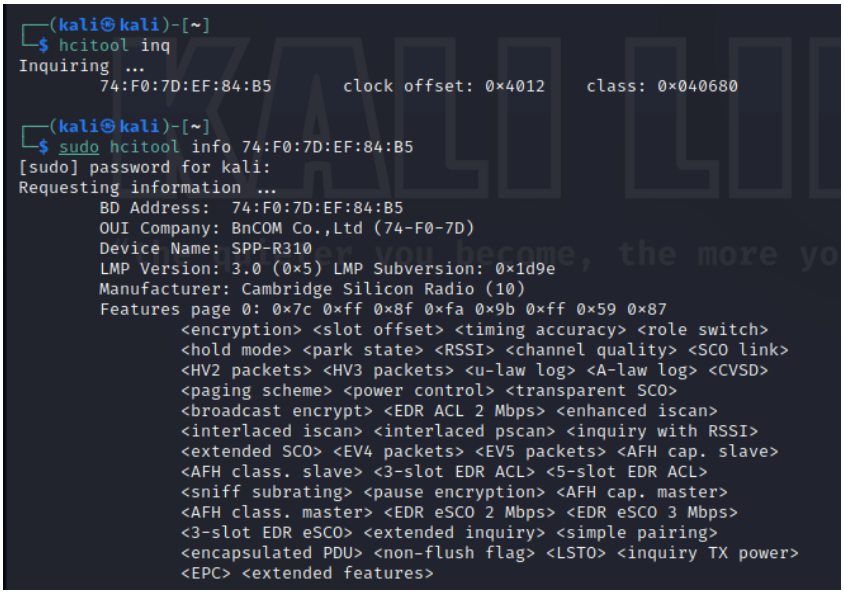
Koliko malo informacija je potrebno za iskorištavanje sigurnosnih mehanizama uređaja prikazano je i u sljedećem primjeru. U sučelju naredbenog retka Linux OS-a

naredbom `hciconfig -a` provjerava se rad Bluetooth uređaja, te se naredbom `hcitool scan` pokreće skeniranje dostupnih uređaja.



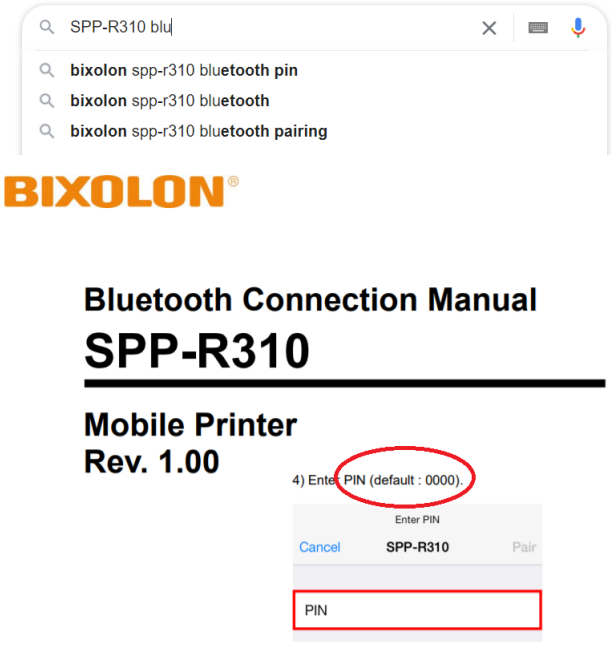
Slika 52 Skeniranje dostupnih Bluetooth uređaja - hcitool (autorski rad)

Već kod početnog rezultata pronađen je uređaj naziva SPP-R310 te njegova MAC adresa. Bitno je za napomenuti da `hcitool scan` otkriva tvorničko ime uređaja koje od strane vlasnika može biti izmijenjeno. Dakle, pri pretraživanju dostupnih Bluetooth uređaja putem npr. pametnog telefona prikazuje se informacija o imenu koje postavlja vlasnik dok `hcitool` otkriva njegovo stvarno, tvorničko ime. Detalji o uređaju dobivaju se naredbom `hcitool info [MAC adresa] 74:F0:7D:EF:84:B5.`



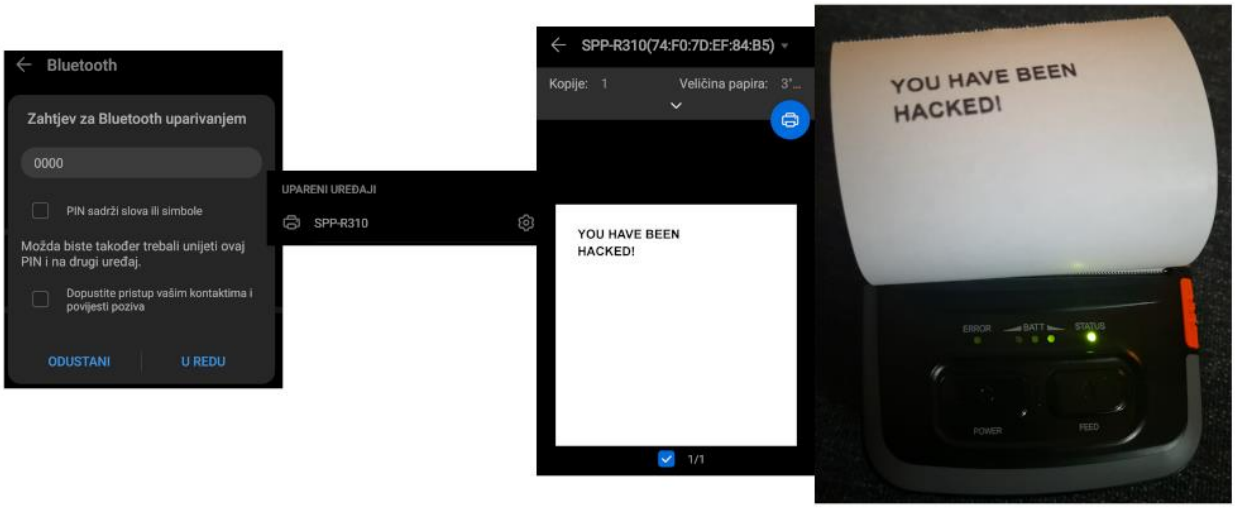
Slika 53 Detalji uređaja SPP-R310 (autorski rad)

Ako se u tražilicu upiše dobiveni naziv ovog uređaja, prilično jednostavno se može doći do njegovih uputa u kojima, osim što se saznaje da se radi o Bluetooth POS uređaju, piše i zadani PIN za Bluetooth uparivanje. Da je ime ovog uređaja bilo izmijenjeno od strane vlasnika, uobičajenim pretraživanjem Bluetooth uređaja ne bi mogli saznati o kojem i kakvom uređaju se radi.



Slika 54 PIN uređaja SPP-R310 (autorski rad)

Dobivenim informacijama se zatim bez ograničenja može upariti s uređajem i koristiti ga bez znanja vlasnika.



Slika 55 Neovlašteni ispis poruke na SPP-R310 (autorski rad)

Praktični dio 2

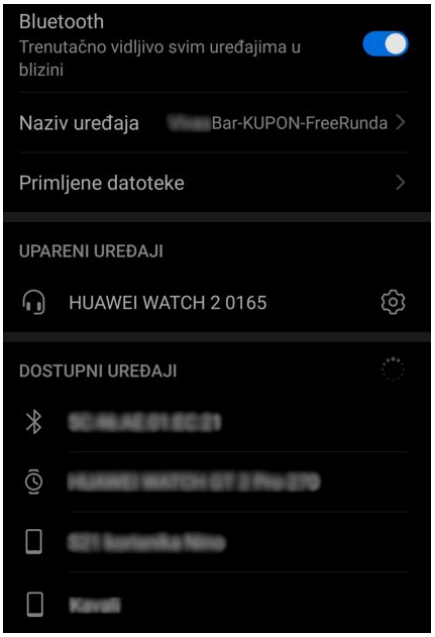
1.17. Socijalni inženjering

U drugom dijelu praktičnog rada demonstrirat će se napad na Bluetooth uređaje gdje će vektor napada biti socijalni inženjering. Socijalno inženjerstvo podrazumijeva različite načine manipulacije u svrhu dobivanja pristupa korisnim informacijama. (Baća, M. et al., 2019/2020).

Napomena: Svi osobni podaci nepoznatih osoba čiji su podaci namjerno ili nenamjerno prikupljeni (u smisli naziva Bluetooth uređaja) će biti sakriveni zbog zaštite osobnih podataka.

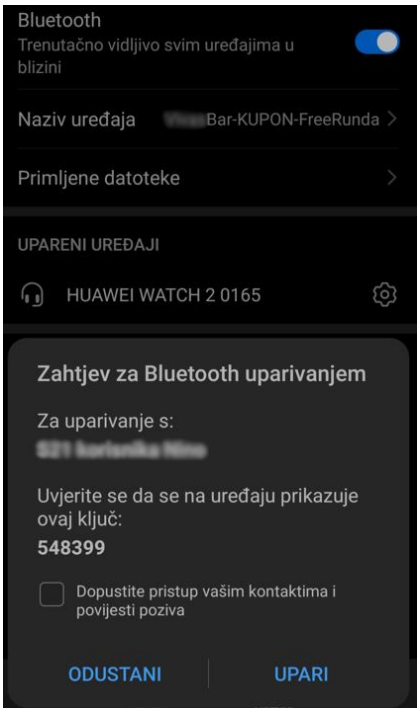
1.18. Demonstracija napada

Za potrebu provedbe drugog dijela praktičnog rada, na pametnom telefonu stvoren je Bluetooth profil s nazivom koji sugerira na podjelu kupona za besplatna pića u poznatom Caffe Bar-u. Za lokaciju demonstracije napada odabrano je omiljeno okupljalište mladih u Sisku. Na lokaciji je uključen Bluetooth i pokrenuto je pretraživanje dostupnih uređaja. (Slika 52).



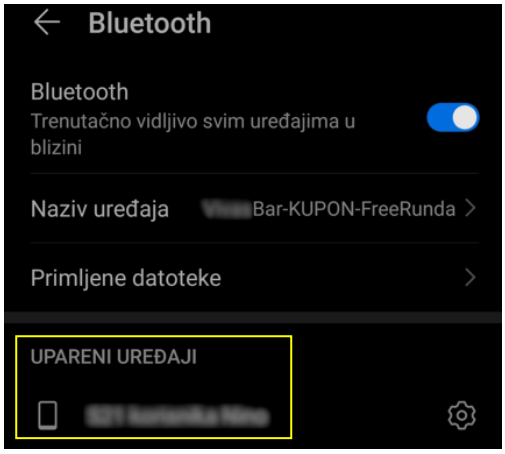
Slika 56 Popis Bluetooth uređaja (autorski rad)

Nakon pregleda dostupnih uređaja odabran je jedan s popisa i poslan je zahtjev za uparivanjem. (Slika 53).



Slika 57 Slanje zahtjeva za uparivanjem (autorski rad)

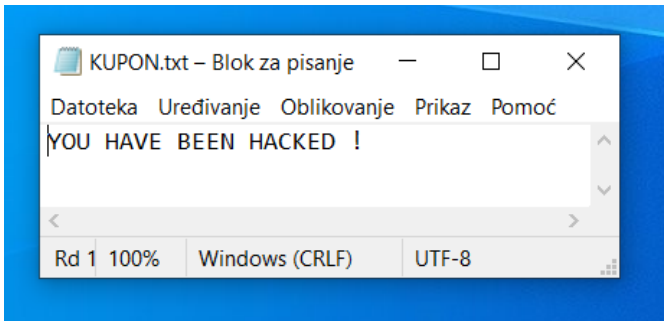
Nakon vrlo kratkog vremena žrtva s druge strane, bez obzira na provjeru jednakosti ključa i adekvatne provjere u sigurnost zahtjeva, prihvaća uparivanje. (Slika 54)



Slika 58 Prihvaćanje zahtjeva za uparivanjem (autorski rad)

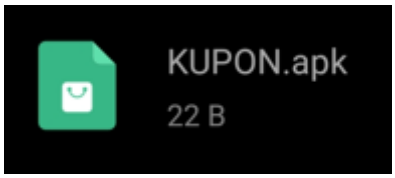
Navedeno prikazuje samo jedan primjer prihvaćanja nepoznatog zahtjeva koji je poslan u svrhu praktičnog pokazatelja socijalnog inženjeringa kao jedne vrste vektora napada. Ovakav zahtjev je poslan na osam različitih uređaja, a zahtjev za uparivanjem su prihvatila čak tri uređaja.

Za dodatni primjer u napad je uključeno i slanje datoteke drugoj odabranoj žrtvi. Na računalu je stvorena datoteka naziva `KUPON.txt`.



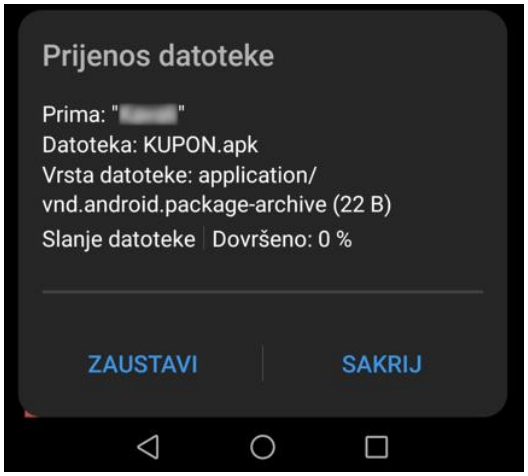
Slika 59 Txt datoteka (autorski rad)

Kako bi se dodatno potvrdila ranjivost vektorom socijalnog inženjeringa, datoteci se mijenja ekstenzija iz `.txt` u `.apk`. APK datoteke su instalacijske datoteke za Android operativni sustav. Dakle, primatelj datoteke će, ako istu prihvati, vidjeti da se radi o `.apk` datoteci odnosno instalacijskoj datoteci.



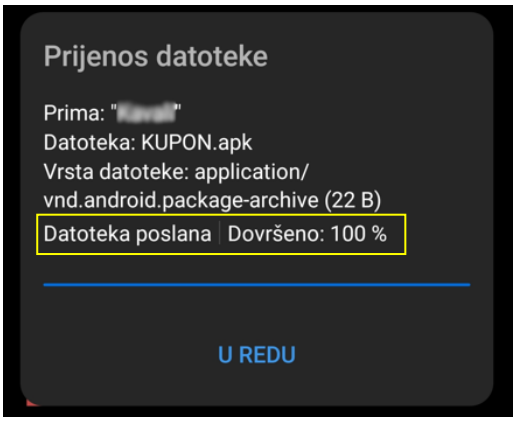
Slika 60 Apk datoteka (autorski rad)

Odabire se datoteka `KUPON.apk` te se dijeli putem Bluetooth veze odabranoj unaprijed uparenoj žrtvi. (Slika 56).



Slika 61 Slanje datoteke KUPON.apk (autorski rad)

Kao što se može vidjeti na Slici 58, žrtva prihvaća datoteku i ista se sprema na njezin pametni telefon.



Slika 62 Datoteka KUPON.apk prihvaćena (autorski rad)

Žrtva primitkom i otvaranjem datoteke primljene preko Bluetooth veze u ovom slučaju neće napraviti štetu jer ista nije stvarna instalacijska datoteka. Ako je žrtvina namjera bila iskoristiti kupon za besplatno piće pošiljatelja kojem je ime poznati Caffe Bar, za pretpostaviti je da će ovu datoteku pokušati i otvoriti kako bi vidjela sadržaj.

Drugi dio praktičnog rada proveden je sukcesivno u periodu od 25. kolovoza 2021. do 10. rujna 2021. godine. Na mjestima s povećanom koncentracijom ljudi u Sisku (šetnica, tržnica, Caffe Bar-ovi) uzastopno su slani zahtjevi za uparivanje otkrivenim uređajima putem pametnog telefona. Od ukupno 23 poslana zahtjeva, 4 uređaja je prihvatilo nepoznati zahtjev.

Ovakav tip manipulacije žrtvama ovisi i o preferencijama, dobi, lokaciji i aktivnostima žrtve. Prvi dio praktičnog rada koji je proveden na skupinama mladih ljudi pokazuje da je tri od osam zahtjeva za uparivanjem prihvaćeno od strane potencijalne žrtve što je gotovo 40%. U drugom dijelu se radi o 4 prihvaćena zahtjeva od ukupno 23 poslana što je nešto više od 15%. Aktivnosti, lokacije i dob potencijalnih žrtvi u prvom i drugom dijelu se razlikuju na način da su u prvom dijelu ovog testa sudjelovali mladi ljudi koji češće koriste svoje mobilne uređaje i iste gotovo konstantno provjeravaju, a zbog lokacije je i samo iskorištavanje slabosti žrtve bilo uspješnije. U drugom dijelu testa se radi o osobama srednje životne dobi koji ne posežu za mobilnom uređajima toliko često kao mladi te se nalaze na lokacijama primjerenijim za opuštanje ili kupovinu gdje kupon za besplatno piće u Caffe Bar-u nije bio primamljiv. Također, zahtjev za uparivanjem u drugom slučaju nije bio toliko primijećen od strane žrtvi zbog rijetkog korištenja mobilnog uređaja odnosno smanjenog provjeravanja obavijesti koje bi mogle rezultirati prihvaćanjem zahtjeva za uparivanje.

Dakle, u socijalnom inženjeringu napadač iskorištava ljudske pogreške i slabosti. Ovi primjeri pokazuje da za napad putem Bluetooth veze nije potrebno složeno znanje korištenja naprednih alata za otkrivanja MAC adrese, poznavanje OBEX protokola i sl. već je dovoljno

žrtvu uvjeriti u legitimnost poruke, e-maila, telefonskog poziva ili u ovom slučaju prihvaćanje nepoznate datoteke ili zahtjeva za uparivanjem putem Bluetooth veze.

Zaključak

Bluetooth tehnologija, kao tehnologija koja bez upotrebe internetske veze stvara mrežu između uređaja, je svakako jedna od tehnologija koja će se i dalje razvijati zbog brojnih prednosti koje ima kao što je brzina prijenosa podataka, jednostavna upotreba i široki spektar različitih mogućnosti upotrebe. Zbog svega navedenog, a u smislu sigurnosti informacija, može se reći da su upravo njezine brojne prednosti njezin najveći nedostatak. Naime, kao što je u radu navedeno, sa današnjih 4,5 milijarde Bluetooth uređaja, ovaj broj će za nekoliko godina predviđeno narasti na čak 6,5 milijardi, a uz poznatu dobru i opću prihvaćenost kod korisnika postat će meta sve brojnijih pokušaja pronalaska ranjivosti, sve učestalijih napada odnosno rast će sigurnosni rizici.

Bluetooth SIG koji razvija otvoreni industrijski standard za Bluetooth tehnologiju svakom novom verzijom implementira sigurnije protokole za prijenos podataka, međutim proizvođači Bluetooth uređaja najčešće odabiru starije verzije protokola zbog cijene proizvodnje i proizvoda, a ujedno na taj način kupcima olakšavaju korištenje uređaja u smislu jednostavnosti uparivanja. Jednako važna činjenica je i da sve više uređaja koji koriste Bluetooth za prijenos podataka nemaju ekrane i tipkovnice zbog čega je ograničeno korištenje naprednih sigurnosnih protokola kod uparivanja i stvaranja veze između uređaja.

Na primjerima upotrebe može se zaključiti da se Bluetooth tehnologija koristi za povezivanje uređaja, stvaranje malih mreža i slanje uobičajenih odnosno napadačima relativno nevažnih podataka, te se može zaključiti da je sigurnost posljednjih verzija adekvatna za takve vrste upotrebe. Zbog svoje rasprostranjenosti i dobre prihvaćenosti kod korisnika, moguće je da se ovakva tehnologija implementira i za veće mreže, za slanje osjetljivih podataka ili čak i za transakciju novca. Za ovakve ozbiljnije načine upotrebe sigurnosni protokoli ove tehnologije su još nedovoljni.

Iz praktičnog dijela rada može se zaključiti da jednaku ulogu u sigurnosti Bluetooth uređaja imaju proizvođači i korisnici. Proizvođači koji uređaje stavljaju na tržište trebali bi u iste implementirati najnovije Bluetooth verzije sa sigurnijim protokolima. S druge strane, praktični dio napada korištenjem socijalnog inženjeringa pokazao je da korisnici još nisu svjesni opasnosti koju nosi korištenje Bluetooth tehnologije. U današnje vrijeme kada je korištenje elektroničkih uređaja, bežični prijenos podataka i sama digitalna transformacija društva u središtu pozornosti i uzlaznoj putanji, potrebna je ista razina informacijske pismenosti kao preduvjet za sigurno korištenje informacijskih tehnologija.

Popis literature

Baća M., Gerić S., Grd P., Tomičić I., Garafolić N. (2019/2020). *Sigurnost informacijskih sustava* [Moodle]. Sveučilište u Zagrebu, Fakultet organizacije i informatike, Varaždin

Becker Andreas, (2007). *Bluetooth Security & Hacks*

Bettercap, (bez dat.). *INTRODUCTION. Preuzeto 12.08.2021. sa https://www.bettercap.org/intro/*

Bettercap, (bez dat.). *BLUETOOTH LE. Preuzeto 15.08.2021. sa https://www.bettercap.org/modules/ble/*

Bluetooth SIG, Inc. (2021). *2021 Market Update*

Bluetooth SIG, Inc. (2021). *Enabling a Secure, Connected World*. Preuzeto 03.08.2021. sa https://www.bluetooth.com/learn-about-bluetooth/key-attributes/bluetooth-security/

Bluetooth SIG, Inc. (bez dat.). *Understanding Bluetooth Range.* Preuzeto 08.08.2021. sa https://www.bluetooth.com/learn-about-bluetooth/key-attributes/range/

Bright Side (04.07.2019). *How Bluetooth Works* [Video file]. Preuzeto 26.07.2021. s https://www.youtube.com/watch?v=jzxZUJmOu3o

CARNet CERT i LS&S (2005). *Bluetooth Sigurnost*

CARNet CERT i LS&S (2009), *Ranjivosti Bluetooth tehnologije*

ERICSSONERS, (2021). *Prvi uređaj s Bluetooth tehnologijom - handsfree headset*. Preuzeto 19.07.2021. sa https://ericssoners.wordpress.com/2014/09/02/bluetooth-headset-hbh-10-limited-edition-kit/

Ethical hacking and penetration testing, (2021). *What is Bluetooth Low Energy (BLE) and how to hack it.* Preuzeto sa https://miloserdov.org/?p=3405

Fotios Chantzis, Ioannis Stais, Paulino Calderon, Evangelos Deirmentzoglou, Beau Woods (2021). *Practical IoT Hacking: The Definitive Guide to Attacking the Internet of Things*

HackersEnigma; an ethical hacking blog, (2016). *Bluetooth Hacking Tools Part – I.* Preuzeto 11.09.2021. sa http://hackersenigma.com/bluetooth-hacking-tools-part-i/

Infor, (2009). *Prvi mobilni uređaj s Bluetooth tehnologijom*. Preuzeto 19.07.2021. sa http://abouthandphone-infor.blogspot.com/2009/07/ericsson-t39-champion.html

Jaycon Systems (2017). *Bluetooth Technology: What Has Changed Over The Years*. Preuzeto 27.07.2021. sa https://medium.com/jaycon-systems/bluetooth-technology-what-has-changed-over-the-years-385da7ec7154

Juha T. Vainio (2000). *Bluetooth Security*

Kai Ren, (2016). *Bluetooth Pairing Part 1 – Pairing Feature Exchange*. Preuzeto 04.08.2021. sa https://www.bluetooth.com/blog/bluetooth-pairing-part-1-pairing-feature-exchange/

Lonzetta A.M., Cope P., Campbell J., Mohd B.J., Hayajneh T. (2018). *Security Vulnerabilities in Bluetooth Technology as Used in IoT*

Nao Laura, (2018). *BLE Pairing and Bonding*. Preuzeto 31.07.2021. sa https://www.kynetics.com/docs/2018/BLE_Pairing_and_bonding/

OffSec Services Limited 2021. *The Most Advanced Penetration Testing Distribution.* Preuzeto sa https://www.kali.org/

OffSec Services Limited 2021. *Kali Linux Tools Listing*. Preuzeto 12.08.2021. sa https://tools.kali.org/tools-listing

Oracle VM VirtualBox*. Welcome to VirtualBox.org!* Preuzeto 10.08.2021. sa https://www.virtualbox.org/

Padgette J., Bahr J., Batra M., Holtman M., Smithbey R., Chen L., Scarfone K., (2017). *Guide to Bluetooth Security*

Peter, (2021). *Flashback: a brief history of Bluetooth*. Preuzeto 17.7.2021. s https://www.gsmarena.com/flashback_a_brief_history_of_bluetooth-news-49119.php

Piper Daniel, (2021). *Bluetooth logo*. Preuzeto 19.07.2021. sa https://www.creativeblog.com/news/bluetooth-logo-secret

Rhodes Colleen, (bez dat.). *Bluetooth Security*

Sherali Zeadally, Farhan Siddiqui, Zubair Baig (2019). *25 Years of Bluetooth Technology*

Solomon, G. Michael, Chapple Mike (2004). *Information security Iluminated*

Umawing Jovi, (2019). *Bluetooth vulnerability can be exploited in Key Negotiation of Bluetooth (KNOB) attacks. Preuzeto 08.08.2021. sa https://blog.malwarebytes.com/awareness/2019/08/bluetooth-vulnerability-can-be-exploited-in-key-negotiation-of-bluetooth-knob-attacks/*

Woolley M., Bluetooth SIG (2020). *Developer Study Guide: Bluetooth® Low Energy Security*

Popis slika

Slika 1 Prvi uređaj s Bluetooth tehnologijom - handsfree headset (ERICSSONERS, 2021)... 2
Slika 2 Bluetooh logo (Piper D., 2021)... 3
Slika 3 Prvi mobilni uređaj s Bluetooh tehnologijom (Peter, 2021)... 3
Slika 4 Ukupne godišnje isporuke Bluetooth uređaja u milijardama i predviđanja za naredne godine (Bluetooth SIG, Inc., 2021)... 4
Slika 5 Isporučeni Bluetooth uređaji u milijardama s obzirom na verziju (Bluetooth SIG, Inc., 2021)... 4
Slika 6 Bluetooth verzije kroz godine (Jaycon Systems, 2017)... 5
Slika 7 Načini povezivanja Bluetooth uređaja (CARNet CERT i LS&S, 2005)... 6
Slika 8 BLE protokol (Sherali Zeadally et al., 2019)... 9
Slika 9 CIA trokut (Baća, M. et al., 2019/2020)...11
Slika 10 BLE faze uparivanja (Kai Ren, 2016)...13
Slika 11 Uređaj za izvođenje BlueSniping napada (CARNet CERT i LS&S, 2009)...18
Slika 12 Pitanje 1 - Anketa (Google Forms)...20
Slika 13 Pitanje 2 - Anketa (Google Forms)...20
Slika 14 Pitanje 3 - Anketa (Google Forms)...20
Slika 15 Pitanje 4 - Anketa (Google Forms)...21
Slika 16 Pitanje 5 - Anketa (Google Forms)...21
Slika 17 VirtualBox logo (Oracle VM VirtualBox)...23
Slika 18 Preuzimanje i instalacija VirtualBox aplikacije (Oracle VM VirtualBox; autorski rad)24
Slika 19 Početni ekran VirtualBox-a (autorski rad)...24
Slika 20 Kali Linux logo (OffSec Services Limited 2021.)...25
Slika 21 Postavljanje Kali Linux-a 1 (autorski rad)...26
Slika 22 Postavljanje Kali Linux-a 2 (autorski rad)...26
Slika 23 Postavljanje Kali Linux-a 3 (autorski rad)...27
Slika 24 Postavljanje Kali Linux-a 4 (autorski rad)...27
Slika 25 Postavljanje Kali Linux-a 5 (autorski rad)...28
Slika 26 Postavljanje Kali Linux-a 6 (autorski rad)...29
Slika 27 Postavljanje Kali Linux-a 6 (autorski rad)...29
Slika 28 Postavljanje Kali Linux-a 7 (autorski rad)...30
Slika 29 Postavljanje Kali Linux-a 8 (autorski rad)...30
Slika 30 Postavljanje Kali Linux-a 9 (autorski rad)...31
Slika 31 Postavljanje Kali Linux-a 10 (autorski rad)...31
Slika 32 Postavljanje Kali Linux-a 11 (autorski rad)...32
Slika 33 Postavljanje Kali Linux-a 12 (autorski rad)...32
Slika 34 Postavljanje Kali Linux-a 13 (autorski rad)...33
Slika 35 Postavljanje Kali Linux-a 14 (autorski rad)...33
Slika 36 Radna površina Kali Linux-a (autorski rad)...34
Slika 37 Aplikacije i alati unutar Kali Linux-a (autorski rad)...34
Slika 38 Bettercap logo (bettercap.org)...35
Slika 39 Postavke USB-a (autorski rad)...37
Slika 40 Dodavanje Bluetooth uređaja (autorski rad)...37
Slika 41 Aktiviranje Bluetooth uređaja (autorski rad)...38
Slika 42 Provjera verzije alata Bettercap (autorski rad)...38
Slika 43 Ažuriranje/instaliranje Bettercap-a (autorski rad)...39
Slika 44 Pokretanje Bettercap modula (autorski rad)...39
Slika 45 Pronađeni uređaji u Bettercap modulu (autorski rad)...40
Slika 46 Tablica otkrivenih uređaja (autorski rad)...41
Slika 47 Pokretanje otkrivanja detalja o odabranom uređaju (autorski rad)...41
Slika 48 Servisi i karakteristike - Galaxy Fit2 (autorski rad)...42
Slika 49 Servisi i karakteristike - SW-170 (autorski rad)...44

Slika 50 Text to Hex Code Converter (autorski rad)....45
Slika 51 Izmijenjeni naziv uređaja (autorski rad)....46
Slika 52 Skeniranje dostupnih Bluetooth uređaja - hcitool (autorski rad)....47
Slika 53 Detalji uređaja SPP-R310 (autorski rad)....47
Slika 54 PIN uređaja SPP-R310 (autorski rad)....48
Slika 55 Neovlašteni ispis poruke na SPP-R310 (autorski rad)....48
Slika 56 Popis Bluetooth uređaja (autorski rad)....49
Slika 57 Slanje zahtjeva za uparivanjem (autorski rad)....50
Slika 58 Prihvaćanje zahtjeva za uparivanjem (autorski rad)....50
Slika 59 Txt datoteka (autorski rad)....51
Slika 60 Apk datoteka (autorski rad)....51
Slika 61 Slanje datoteke KUPON.apk (autorski rad)....51
Slika 62 Datoteka KUPON.apk prihvaćena (autorski rad)....52