Kibernetička sigurnost informacijsko-zabavnih sustava u automobilima

Antunović, Filip

SVEUČILIŠTE JOSIPA JURJA STROSSMAYERA U OSIJEKU

FAKULTET ELEKTROTEHNIKE, RAČUNARSTVA I INFORMACIJSKIH TEHNOLOGIJA

Sveučilišni diplomski studij Automobilsko računarstvo i komunikacije

KIBERNETIČKA SIGURNOST INFORMACIJSKO-ZABAVNIH SUSTAVA U AUTOMOBILIMA

Diplomski rad

Filip Antunović

Osijek, 2019.

Sadržaj

1. UVOD

U današnjem svijetu potrebe i zahtjevi korisnika modernih tehnologija su proširile potrebu za povezanošću i unutar automobila. Kupci novih automobila očekuju i traže od proizvođača sve veću povezanost automobila s drugim uređajima poput GPS-a, raznih senzora na automobilu, od senzora za parking do senzora za nadzor tlaka u gumama, mobilnih uređajima, raznih uređaja koji se mogu povezati s automobilom pomoću USB porta. Ugradnjom sustava koji podržavaju gore navedene potrebe korisnika u automobil otvaraju se nove ranjivosti koje mogu biti korištene za krađu osobnih podataka vlasnika vozila, krađu samoga vozila, preuzimanje kontrole nad vozilom, izmjenu specifikacija vozila te neovlašteno izvršavanje koda na vozilu koje može pružiti dodatne funkcije koje nisu bile predviđene za vozilo. Područje računalne sigurnosti vozila polako postaje jedno od važnijih područja u automobilskoj industriji te će biti fokus ovog diplomskog rada.

Informacijsko-zabavni sustavi u automobilima postaju sve moćniji, kompleksniji i bogatiji funkcijama, te su kao takvi sve sličniji osobnim računalima. Budući da su povezani s komunikacijskim sabirnicama vozila, predstavljaju svojevrsna vrata prema vozilu, te je preko njih moguće upravljati gotovo svime. Zahvaljujući brojnim sustavima povezivanja (USB, Bluetooth, NFC, ethernet, internet), ovakvi sustavi potencijalno otvaraju brojne točke napada na automobil.

U prvom poglavlju razmotrit će se najčešće ranjivosti vozila, s primjerima napada na njih. Alati korišteni za testiranje sigurnosti Yocto linux operativnog sustava su objašnjeni i navedeni u drugom poglavlju. Treće poglavlje opisuje testiranje i rezultate testiranja sustava. U četvrtom poglavlju su predložene sigurnosne mjere koje se mogu poduzeti kako bi se povećala sigurnost informacijsko-zabavnih sustava.

1.1. Zadatak rada

U ovom diplomskom radu je potrebno proučiti mogućnosti napada na automobil, rizike koje to donosi, te metode zaštite automobila od napada. Fokusirati se na:

1. Zaštitu automobila od neovlaštenih modifikacija od strane korisnika
2. Zaštitu automobila od izvršavanje neovlaštenog koda
3. Zaštitu automobila od krađe privatnih podataka

2. Ranjivosti automobila

Moderna vozila današnjice su mnogo više povezana nego što se to isprve čini. Nekad su automobili bili uglavnom mehanička vozila koja su se oslanjala na mehaniku za funkcionalnosti poput upravljanja vozilom i kočenjem. Danas se moderna vozila uglavnom oslanjaju na elektroniku za upravljanje tim sustavima. Takav oblik upravljanja sustavima se naziva engl. "Drive by wire" i ima nekoliko prednosti u odnosu na tradicionalni mehanički pristup. Nekoliko je sigurnosnih značajki omogućeno jer su komponente automobila kontrolirane pomoću elektronike. Na primjer, neki automobili mogu automatski kočiti ako prednji radar otkrije prepreku ispred sebe i zaključi da je sudar neizbježan. Drive by wire se koristi kako bi se vlasnicima automobila pružila luksuzna funkcionalnost poput automatskog parkiranja koja funkcionira na principu da se elektronički preuzima kontrola nad upravljačem te se upravljač okreće u određenom smjeru ovisno o snimci radara ili kamere.

Povećanjem povezanosti automobila broj ranjivosti vozila se automatski povećao. U računalnoj sigurnosti, ranjivost je slabost koja se može iskoristiti od strane aktera prijetnje, kao što je napadač, za obavljanje neovlaštenih radnji unutar računalnog sustava. Za iskorištavanje ranjivosti, napadač mora imati barem jedan primjenjivi alat ili tehniku koja se može povezati na slabost sustava. U ovom okviru ranjivost je također poznata kao površina napada.[1]

Informacijsko-zabavni sustavi danas imaju niz oblika komunikacije koja može biti iskorištena za napad na sustav ili samo vozilo. Neki od najčešćih i najdostupnijih površina za napad su:

- Bluetooth
- Wi-Fi
- USB port
- čitač SD kartica
- CD-ROM/DVD-ROM
- Zaslon osjetljiv na dodir
- Mobilna mreža, GSM
- GPS

Kako bi se dobio bolji pregled ranjivosti vozila, izrađen je model ranjivosti.

2.1. Model ranjivosti

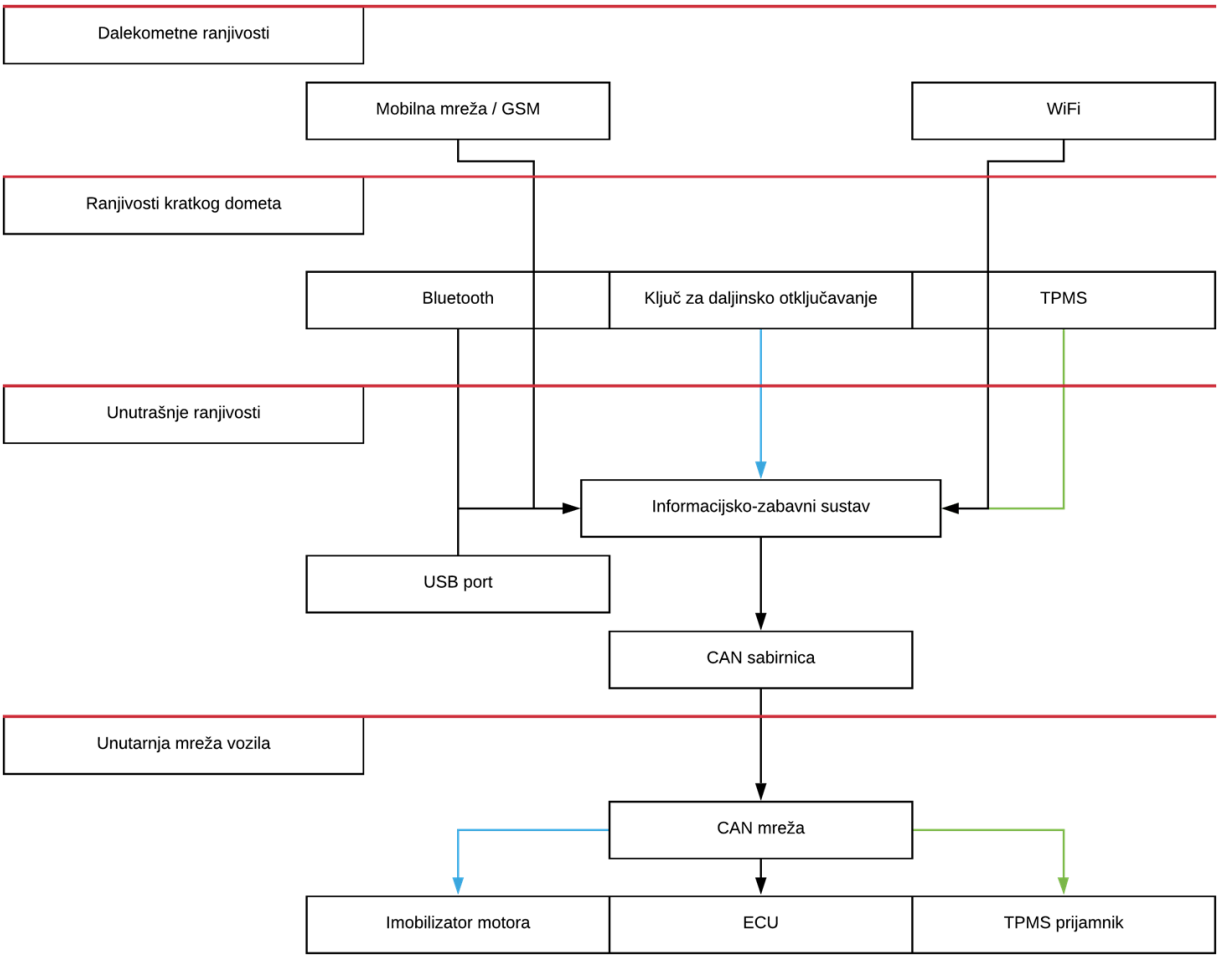
Modeliranjeprijetnji/ranjivosti (engl. *Threat Modeling)* je proces kojim se potencijalne prijetnje, kao što su strukturne ranjivosti, mogu identificirati, nabrojati i odrediti po prioritetima - sve s gledišta hipotetskog napadača. Svrha modeliranja prijetnji je pružiti braniteljima sustavnu analizu vjerojatnog profila napadača, najvjerojatnijih vektora napada i sredstava koja napadač najviše želi[2]. Početnu razinu modela ranjivosti nazvana je "Razina 0" i prikazana je u tablici 2.1.

Tablica 2.1. Prikaz ranjivosti sustava na "Razini 0"

Vanjske ranjivosti	**Unutarnje ranjivosti**
Mobilna mreža/GSM	USB port
WiFi	Bluetooth
Ključ za daljinsko otključavanje	CAN sabirnica
TPMS (engl. *Tire Pressure Monitoring System*)	Ethernet
	Serijski port
	Ekran osjetljiv na dodir
	čitač SD kartica
	CD-ROM / DVD čitač

Model ranjivosti "Razine 0" se dijeli na dva područja ovisno o potrebi za fizičkim kontaktom s vozilom ili nekim njegovim dijelovima. Prvo područje je područje vanjske ranjivosti i ono se odnosi na sve ranjivosti sustava, tj. automobila, za koje nije potreban direktan pristup unutrašnjosti automobila nego se napadi na te ranjivosti mogu poduzeti s određene udaljenosti od automobila, ovisno o ranjivosti koja se pokušava iskoristiti. Na primjer napad na ranjivost TPMS sustava, koji se koristi u većini sustava Bluetooth-om za komunikaciju, zahtijeva određenu blizinu napadača automobilu, dok se napad preko GSM može napraviti s mnogo veće udaljenosti. Drugo područje ranjivosti je područje unutarnjih ranjivosti i ono se odnosi na sve ranjivosti sustava, tj. automobila, za koje je potreban direktan pristup unutrašnjosti automobila.

Nakon što je napravljen prikaz modela ranjivosti na "Razini 0", potrebno je napraviti model ranjivosti "Razine 1" koji je u ovom slučaju koncentriran na prijamnike unutar informacijsko-zabavnog sustava automobila. Na slici 2.1 je prikazana arhitektura prijamnika na "Razini 1".



Slika 2.1. Prikaz arhitekture prijamnika u automobilu

2.2. Informacijsko-zabavni sustav

Informacijsko-zabavni sustav, engl. In-Vehicle Infotainment (IVI), je skup hardvera i softvera u automobilu koji omogućuje audio ili video zabavu. Informacijsko-zabavni sustavi su prvotno nastali kao audio sustavi koji su se sastojali od radija, kaseta i CD-DVD čitača, a sada uključuju navigacijski sustav (GPS), video uređaje, USB i Bluetooth povezivanje, računala unutar vozila (engl. carputers), internet u automobilu i WiFi. Jednom upravljani jednostavnim gumbima i brojčanicima na instrumentnim pločama, IVI sustavi danas mogu uključivati kontrole zvuka na upravljaču i hands free glasovnu kontrolu[3].

Infotainment sustavi najčešće koriste Windows CE ili neku distribuciju Linux-a kao operativni sustav. Tipični infotainment se sastoji od fizičkih ulaza, bežičnih ulaza i mrežno spojenih izlaza.

Neki od tipičnih fizičkih ulaza su [4]:

- USB port
- AUX port
- CD-ROM
- DVD
- Ekran osjetljiv na dodir

Bežične ulaze možemo podijeliti na:

- Bluetooth
- WiFi
- GPS
- GSM
- *Remote Controle*

Izlazi se djele najčešće na:

- mrežu CAN sabirnice
- Ethernet
- *High Speed Media Bus*

Na slici 2.2 prikazan je današnji infotainment sustav zajedno s ilustracijama mogućnosti koje on pruža korisniku, tj. vlasniku vozila.

Slika 2.2. Ilustracija *infotainment* sustava [5]

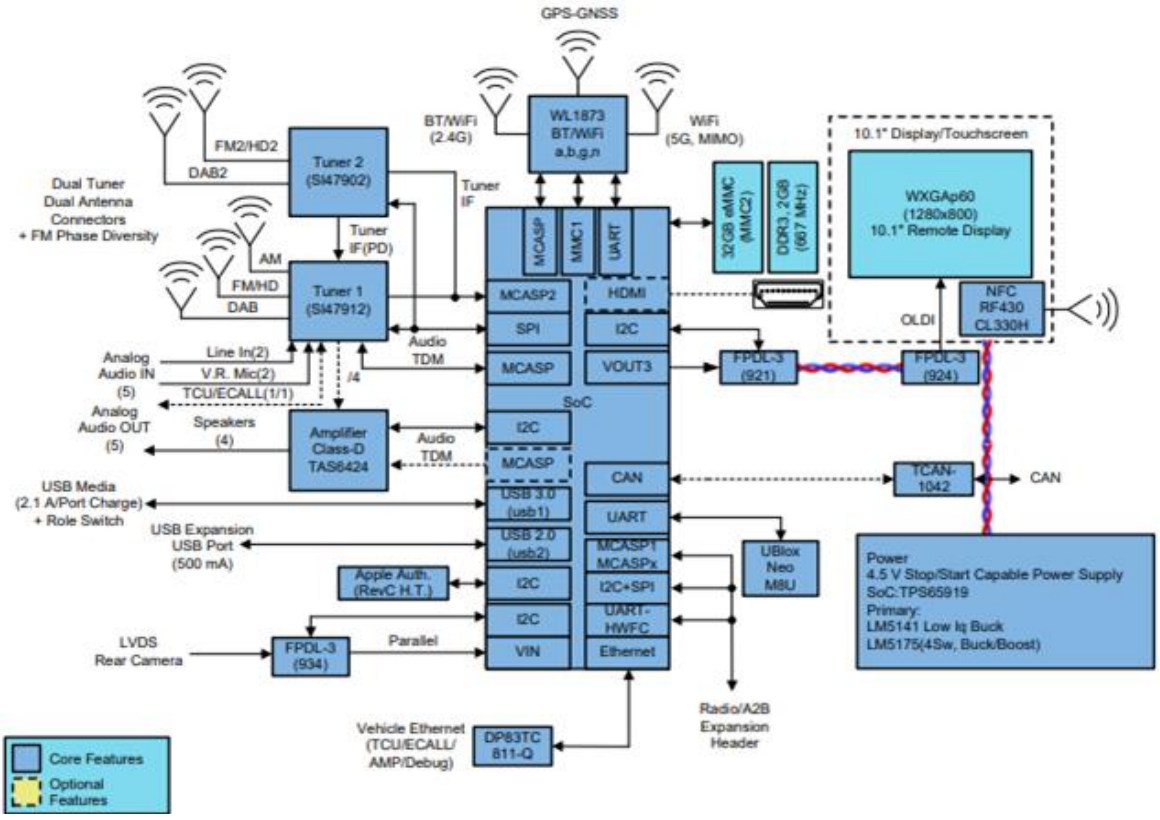
Današnji IVI sustav je multitasking platforma bazirana na višejezgrenom SoC-u koji obavlja funkcije aplikacija sustava kao što su[5]:

- obrada multimedije, uključujući zemaljski i satelitski radio i lokalne medije spojene USB-om ili Bluetooth-om
- ugrađena navigacija uključujući GPS/GNSS
- Hands-free komunikaciju
- I/O kontrola funkcija vozila (klima, preferencije, itd.)
- integracija i prikaz kamere stražnjeg pogleda
- naknadna obrada zvuka
- integracija funkcionalnih perifernih uređaja kao što su tuneri, GPS, zaslon, USB itd.
- upravljanje multimodalnom HMI funkcionalnošću, uključujući govorne, taktilne i zaslonske interakcije

IVI platforma ima i pomoćni MCU koji upravlja niskim razinama sučelja, sabirnica, vozila (CAN, LIN, itd.), taktilnim kontrolama vozila, upravljanjem napajanja, pokretanjem računala itd. Pakiranje IVI-a je ili integrirano s pripadajućim zaslonom ili u jednom modulu raspoređenom pokraj zaslona. Ključne značajke IVI platforme uključuju [5]:

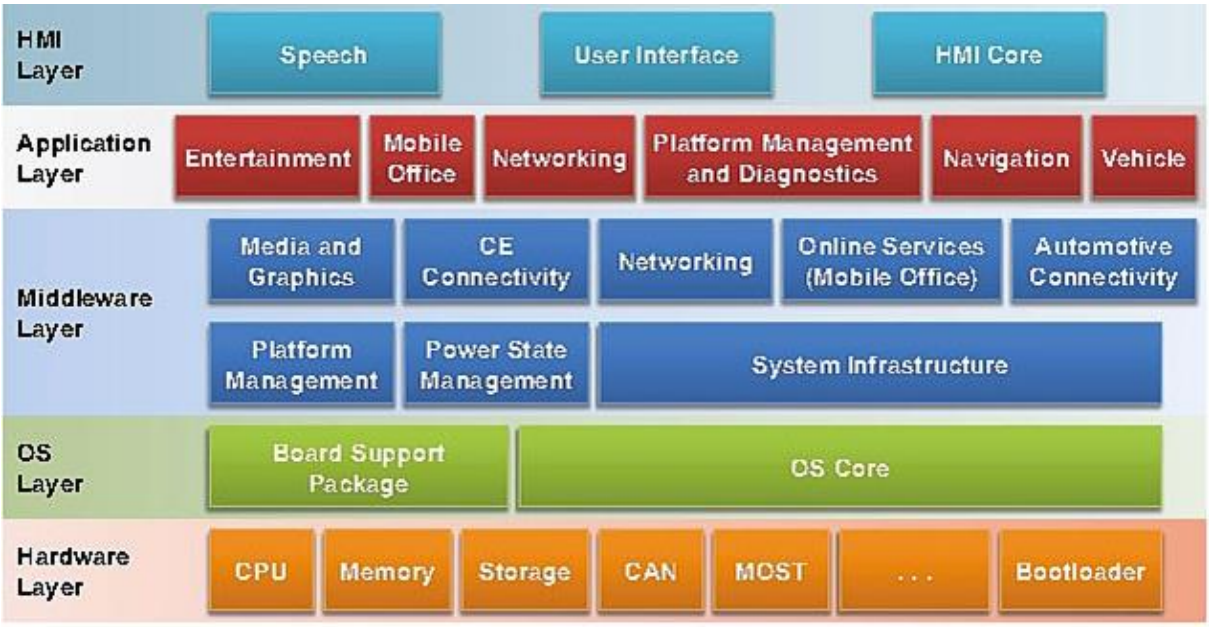
- više jezgreni aplikacijski procesori (2-4 jezgre, najčešće Arm Cortex, GPU, DSP)
- WiFi/Bluetooth periferija, uključujući GPS/GNSS
- analogni i digitalni zemaljski tuneri (AM/FM/DAB/HD antena)
- SDARS prijemnik
- USB 3.0
- Apple autentifikaciju
- Sučelje za stražnju kameru (najčešće LVDS ili FPD)
- zaslon (do 1080P)
- sučelje ekrana osjetljivog na dodir
- audio periferije
- ethernet
- HDMI

Na slici 2.3 prikazana je tipična IVI platforma.



Slika 2.3. Tipična IVI platforma [5]

Softversko okruženje je bazirano na OS-u i sažeto je prikazano na slici 2.4.



Slika 2.4. Softversko okruženje bazirano na OS-u [5]

Na primjer, današnji radio unutar vozila se razvija u kontroler domene kokpita. Taj razvoj se događa zbog potrebe da se na HMI (*engl. Human Machine Interface*) sloju dodaju poboljšanja poput haptike, prepoznavanja gesta i prepoznavanja govora poboljšanog od strane umjetne inteligencije.

2.3. TPMS (engl. Tire Pressure Monitoring System)

TMPS (engl. Tire Pressure Monitoring System) je sustav za nadzor tlaka u gumama koji se nalazi unutar guma vozila. Ovaj uređaj šalje informacije o tlaku zraka u gumama pa čak i druge informacije poput rotacije i temperature. Frekvencija na kojoj TPMS radi varira ovisno o uređaju, ali obično radi na 315 MHz ili 433 MHz UHF i koristi ASK ili FSK modulaciju. Ovi uređaji imaju jedinstveni 32-bitni ID registriran u ECU-u. TPMS su obično u stanju mirovanja dok se vozilo ne kreće većom brzinom od 30 km/h. RF signal također može probuditi TPMS uređaj. RF signal je LF signal frekvencije 125 kHz.

Neki od poznatijih napada na TPMS su [4]:

1. *Praćenje vozila* – moguće je pratiti vozila na temelju njihovog jedinstvenog ID-a. Za praćenje vozila može se postaviti više senzora u cijelom gradu. TPMS emitira svakih 60 do 90 sekundi, ako ih nije pokrenuo RFID odašiljač. Može se koristiti pojačalo niskog šuma, LNA (engl. Low Noise Amplifier), kako bi se poboljšao domet.
2. *Triggered Events* – pomoću jedinstvenog ID-a, dodatni događaji su se mogli pokrenuti kada se vozilo nalazi u blizini. Na primjer, dobar događaj "Otvori garažna vrata", loš događaj "Detonirajte cestovni eksploziv"
3. *Spoofing* – emitiranje vlastitih paketa. Najčešća posljedica je aktiviranje svjetla na nadzornoj ploči

2.4. Ethernet

Ethernet mreže u vozilima su relativno nove, nisu postale niti standard niti ima puno zahtjeva za njima. Minimalni ethernet mrežni kabel sastoji se od četiri žice: *Tx+*, *TX-*, *RX+*, *RX-*. Ethernet priključci za vozila često će imati priključke poput RJFRB priključka.

Kako bi napad na ethernet mrežu uspio mora se napraviti vlastiti prilagođeni konektor za RJ45 kako bi se moglo prisluškivati (engl. sniff) i ubrizgavati (engl. inject) pakete. Osim konektora za RJ45 nije potrebna nikakva posebna oprema, sve se može obaviti pomoću prijenosnog računala i bilo kojeg prisluškivača (engl. sniffer) mreže. Mreže u automobilima imaju CAN-Ethernet gateway, često inkapsuliran u UDP. Ako je vidljivo puno UDP buke, to su najvjerojatnije CAN podaci. Nad tim CAN podacima može se koristiti sve normalne CAN napade i metode za preokretanje (engl. reversing methods) CAN paketa.

Pokretanjem sniffer-a IP adrese i nmap-a ili Zenmap-a provjerava se ima li usluga ili domaćina (engl. hosts). Tako se mogu otkriti uređaji koji imaju druge značajke osim CAN-a koje su potencijalne pristupne točke.

2.5. Ključevi i imobilizatori

Sustavi daljinskog ulaska bez ključa (engl. Remote keyless entry systems) obično rade na 315 MHz za Sjevernu Ameriku i 433.92 MHz za Europu i Aziju. Stariji sustavi su koristili infracrvenom vezom. Sustavi daljinskog ulaska bez ključa obično imaju klizni kod (engl. rolling code).

Ključevi obično imaju transponder u sebi. Ovi transponderi komuniciraju s imobilizatorom pomoću RFID. Imobilizator sprječava paljenje vozila pomoću ožičenja vozila (engl. hot wiring). Transponderi djeluju na 125 kHz.

- Zaustavi se keyfob signal prosljeđivanjem bespotrebnih podataka unutar propusnog opsega prijamnika. Tako se sprečava prijamnik od promjene valjanog, kliznog koda dok istovremeno dopušta napadaču da vidi ispravni slijed ključeva.
- Imobilizatori ponekad zadrže ključ u memoriji i nekoliko minuta nakon što je ključ uklonjen. Ova ranjivost pruža mogućnost ponovnog pokretanja vozila bez ključa.
- Ponavljajući napad. Stariji imobilizatori koristili su statički kod umjesto valjanog, kliznog koda koji se koristi danas.
- Često je moguće preuzeti memoriju transpondera i tako doći do tajnog ključa.
- Dohvati se ID keyfob-a koji se odašilje preko UHF i pokušava se prikupiti keystream reprodukcijom i snimanjem

2.6. Pasivni ulazak bez ključa (engl. Passive Keyless Entry and Start)

Ovi sustavi su vrlo slični tradicionalnom sustavu imobilizatora, osim što ključ može ostati u vlasnikovom džepu bez potrebe da bude u bravi vozila. To se postiže kroz više antena unutar vozila koje pronalaze ključ. Ovi ključevi koriste LF RFID čip i UHF signal za otključavanje i pokretanje vozila. UHF signal će biti ignoriran ako LF RFID nije dovoljno blizu. Sustav funkcionira na principu da RFID prima kripto upit koji mikrokontroler rješava i šalje odgovor preko UHF signala.

Ako se baterija PKES (engl. Passive Keyless Entry and Start) ključa isprazni, obično postoji sakriveni fizički ključ koji će otključati vrata vozila. Imobilizator će i dalje koristiti RFID kako bi potvrdio da je ključ prisutan prije paljenja vozila.

Najčešći napad na ovakvu vrstu ključeva je Relay napad. Relay napad se izvodi tako da napadač postavi uređaj pored vozila i drugi uređaj u blizini žrtve. Uređaj prenosi signale od žrtve do vozila i nazad kako bi se omogućilo napadaču da pokrene vozilo.

2.7. Bluetooth

Većina današnjih vozila ima mogućnost sinkronizacije mobilnih uređaja putem Bluetooth-a. Ta konekcija predstavlja daljinski (engl. remote) signal određene složenosti koji ECU obrađuje. U većini vozila Bluetooth se prima i obrađuje od strane radija, poznate kao i glavne jedinice (engl. head unit) unutar vozila. Ova konekcija omogućuje automobilu pristup kontaktima telefona, upućivanje telefonskih poziva, reprodukciju glazbe, slanje SMS poruka s telefona i ostale funkcionalnosti.

Za razliku od ostalih ranije spomenutih signala, Bluetooth stog (engl. stack) je prilično velik i predstavlja značajnu površinu napada koja je imala ranjivosti u prošlosti.

Općenito postoje dva scenarija napada na Bluetooth *stack*:

1. Napad koji uključuje uređaj koji nije uparen – ovaj napad je najopasniji jer bilo koji napadač može doći do ovog koda na internetu.
2. Napad nakon uparivanja – ova metoda iskorištavanja događa se nakon uparivanja, što je manja prijetnja jer je uključena određena interakcija korisnika. Ranije su dokazane daljinske kompromitacije vozila putem Bluetooth sučelja [6].

2.8. Radio Data System

U današnjim vozilima radio ne prima samo audio signale već i druge podatke. Neki od tih ulaza mogu biti:

- GPS
- AM/FM radio
- Satelitski radio

U većini slučajeva ti se signali jednostavno pretvaraju u audio izlaze i ne predstavljaju značajno raščlanjivanje podataka (engl. parsing of data), što znači da je vjerojatnost sadržavanja ranjivih točaka mala.

Jedna moguća iznimka je slanje podataka dodatnih podataka s FM analognim signalima (ili ekvivalentom u satelitskom radiju). Korisnici obično vide te podatke kao imena radio stanice, nazive pjesama koje se reproduciraju itd. Ovdje se podaci moraju raščlaniti, parsirati, i prikazati, čime se otvara mjesto za sigurnosnu ranjivost.

2.9. Wi-Fi

Neki automobili koji su povezani s internetom putem mobilne mreže mogu tu istu konekciju dijeliti s putnicima u automobilu, ponašajući se kao Wi-Fi žarišna točka (engl. Wi-Fi hotspot). Ovisno o automobilu ta se opcija može kupiti po upotrebi, na primjer na jedan dan ili do mjesec dana. Sigurnost Wi-Fi procjenjivanja je i testirana već godinama, a hakiranje ili napadanje pristupnih točaka je često dokumentirano i dostupno svima, kako laicima tako i profesionalcima. Detaljniji prikaz napada na Wi-Fi je objašnjen u primjeru iz literature [7].

2.10. Telemetrika/Internet/Aplikacije

Mnogi moderni automobili sadrže mobilni radio, generalno nazvan telemetričkim sustavom, koji se koristi za povezivanje vozila na mobilnu mrežu. Ta konekcija vozila na mobilnu mrežu služi kako bi se mogli dohvaćati podatci poput informacija o prometu ili vremenskim prilikama pa sve do over the air ažuriranja vozila.

Ovaj sustav pruža napadaču veoma širok domet u odnosu na vozilo (sve dok je automobil povezan na mobilnu mrežu, napadač ima pristup automobilu). Čak i ako se telemetrična jedinica ne nalazi izravno na CAN sabirnici, onda ima mogućnost daljinskog prijenosa podataka, tj. glasa putem mikrofona na drugu lokaciju. U ranijim istraživanjima dokazana je mogućnost daljinskog iskorištavanja telemetrične jedinice automobila bez interakcije korisnika [6]. Kao primjer je navedeno vozilo marke Jeep gdje telemetriku kontrolira radio vozila koji se nalazi na CAN-IHS sabirnici i na CAN-C sabirnici. Telemetrika, internet, radio i aplikacije se nalaze u zajedničkom sustavu pod nazivom Uconnect. Sve funkcionalnosti koje se asociraju s informacijsko-zabavnim sustavom se često fizički nalaze u jednom uređaju kao što je to i slučaj s vozilom marke Jeep nad kojim je provedeno istraživanje.

3. Korišteni alati i razvojna ploča

Tijekom testiranja korištena je razvojna ploča Toradex Ixora na kojoj se nalazio Yocto Linux operacijski sustav. Za testiranje razvojne ploče, tj. sigurnosti Yocto operacijskog sustava korišteno je više softverskih alata od kojih su najbitniji:

- Zenmap
- Wireshark
- Hydra

Svaki od gore navedenih alata će biti detaljnije opisan i bit će pojašnjena njegova uloga u testiranju operacijskog sustava.

3.1. Toradex Ixora razvojna ploča

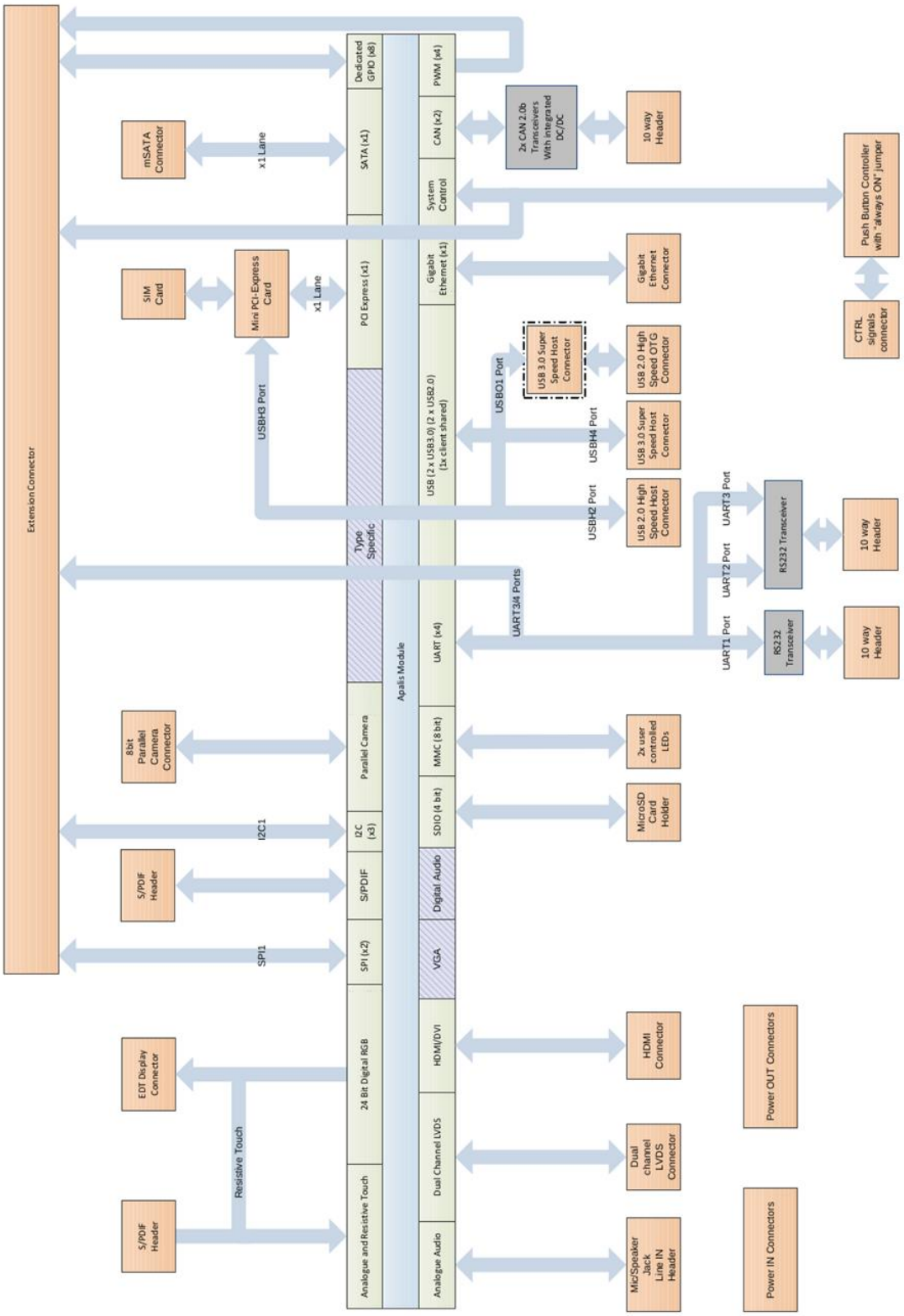
Toradex Ixora razvojna ploča je korištena za testiranje sigurnosti Yocto linux operacijskog sustava. Razvojna ploča Toradex Ixora ima sljedeća komunikacijska sučelja i značajke:

- 1x USB 2.0
- 2x USB 3.0
- USB 2.0 OTG Micro-AB konektor
- RJ45 Ethernet (10/100/1000 Mbit)
- Mini PCIe s konektorom SIM kartice
- Digitalno (TDMS) sučelje na HDMI konektor
- Dvokanalno LVDS sučelje
- 3.5 mm stereo konektor za analogni audio
- konektor za zaslon osjetljiv na dodir
- 2x CAN 2.0B sučelja (do 1Mbit/s)
- 10 bitno paralelno sučelje za kameru
- S/PDIF I/O header
- 3x RS232 serijska sučelja
- 2x I2C
- 1x SPI
- 4x PWM
- 4x analogna ulaza
- 8x GPIO
- GPIO kontrolirane LED
- 1x microSD
- 1x mSATA
- LCD panel konektor

Na slici 3.1 prikazana je Toradex Ixora razvojna ploča.

Slika 3.1. Toradex Ixora razvojna ploča [8]

Arhitektura razvojne ploče je prikazana na slici 3.2 te je iz nje moguće saznati gdje se nalaze konektori na razvojnoj ploči.



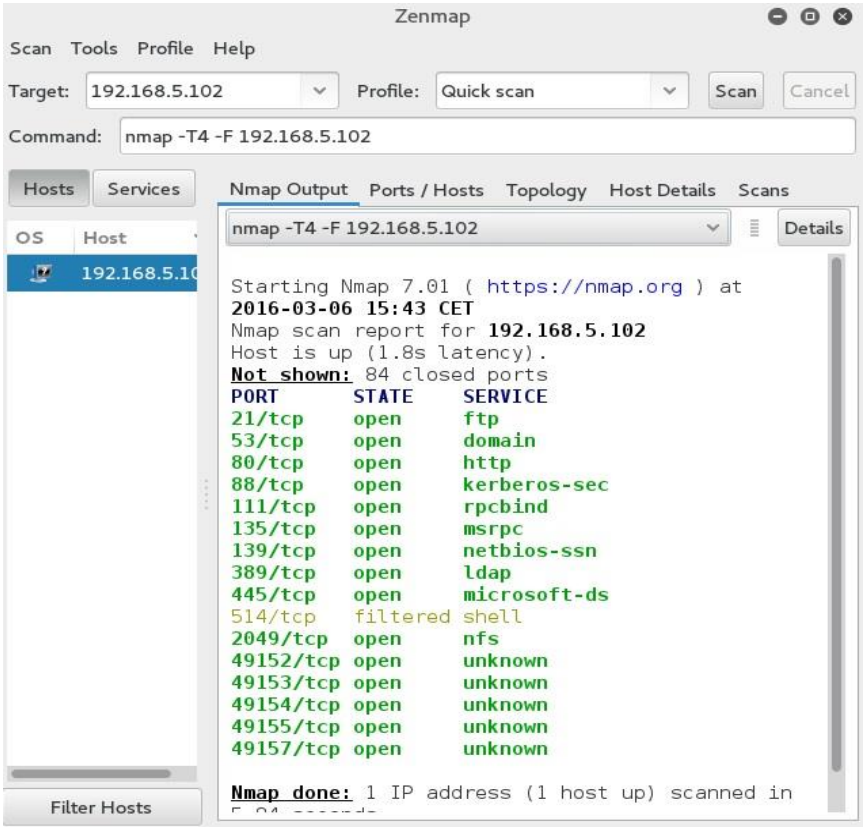
Slika 3.2. Arhitektura Toradex Ixora razvojne ploče [8]

3.2. Zenmap

Zenmap je besplatni i open source GUI za Nmap. Dostupan je za mnoge operacijske sustave (Linux, Windows, Mac OS X, BSD) što Nmap čini lakšim za upotrebu. Namjena Zenmap-a nije zamijeniti Nmap, već ga učiniti korisnijim. Neke od značajki ovog programa su [9]:

- interaktivni i grafički pregled rezultata – Zenmap može prikazati normalni izlaz Nmap-a, ali se može organizirati i njegov prikaz tako da prikazuje sve portove host-a ili sve host-ove koji pokreću određenu uslugu. Sažeto prikazuje detalje o jednom host-u. Zenmap se može koristiti i za crtanje topološke karte otkrivenih mreža.
- usporedba – Zenmap se može koristiti kako bi grafički prikazao razliku između dva skeniranja. Tako Zenmap pomaže korisniku da prati nove host-ove ili usluge koje se pojavljuju na mreži ili nestaju s nje.
- ponovljivost – Zenmap se može upotrebljavati za pokretanje istog skeniranja više puta
- jednostavnost upotrebe – Zenmap je jednostavan za upotrebu i posebno je koristan ljudima koji nemaju puno iskustva s Linux shell-om

Na slici 3.3 prikazano je primjer GUI sučelje Zenmap-a pomoću kojega se vrši skeniranje mreže.



Slika 3.3. Primjer GUI Zenmap skeniranja [9]

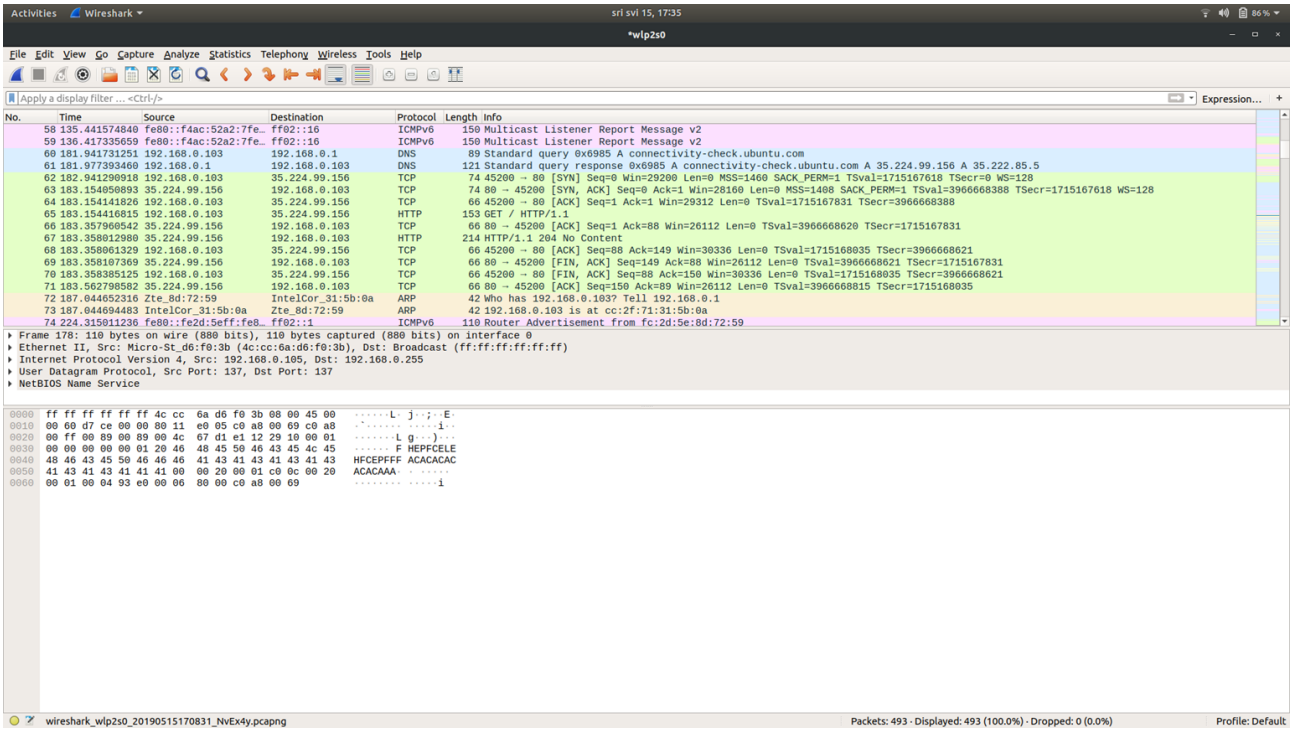
3.3. Wireshark

Wireshark je vodeći svjetski mrežni analizator protokola koji ima široku primjenu. Wireshark omogućuje da se na mikroskopskoj razini vidi što se događa na mreži i kao takav je postao de facto standard u mnogim komercijalnim i neprofitnim poduzećima, vladinim agencijama i obrazovnim institucijama. Razvoj Wiresharka uspijeva zahvaljujući dobrovoljnim doprinosima stručnjaka za umrežavanje širom svijeta i nastavak je projekta kojeg je Gerald Combs pokrenuo 1998. godine [10].

Wireshark ima bogat set značajki koji uključuje sljedeće [10]:

- dubok uvid u stotine protokola, a stalno ih se dodaje više
- snimanje uživo (live capture) i offline analiza
- standardni three-pane packet preglednik
- više platformi: radi na Windows, Linux, macOS, Solaris, FreeBSD, NetBSD i drugi
- uhvaćeni mrežni podaci mogu se pregledavati putem GUI-a
- VoIP analiza
- Čitanje/pisanje različitih formata datoteka za hvatanje: tcpdump (libpcap), Pcap NG, Catapult DCT2000, Cisco Secure IDS iplog, Microsoft Network Monitor, Network General Sniffer® (komprimirani i nekomprimirani), Sniffer® Pro i NetXray®, Network Instruments Observer , NetScreen snoop, Novell LANalyzer, RADCOM WAN / LAN analizator, Shomiti / Finisar Surveyor, Tektronix K12xx, Visual Netual Visual UpTime, WildPackets EtherPeek / TokenPeek / AiroPeek i drugi
- uhvaćene datoteke kompresirane gzip-om mogu se dekompresirati on the fly
- Podaci se mogu čitati uživo s Etherneta, IEEE 802.11, PPP / HDLC, ATM, Bluetooth, USB, Token Ring, Frame Relay, FDDI i drugih (ovisno o platformi)
- Podrška za dešifriranje mnogih protokola, uključujući IPsec, ISAKMP, Kerberos, SNMPv3, SSL / TLS, WEP i WPA / WPA2
- Na listu paketa mogu se primijeniti pravila bojenja za brzu, intuitivnu analizu
- Izlaz se može izvoziti u XML, PostScript, CSV ili obični tekst

Na slici 3.4. prikazano je grafičko sučelje Wireshark-a tijekom analize mreže.



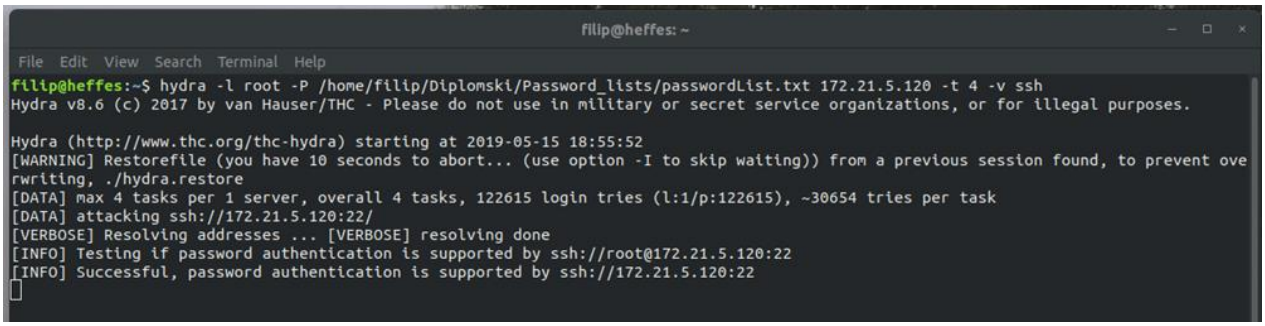
Slika 3.4. Grafičko sučelje Wireshark-a

3.4. Hydra

Hydra je paralelni kreker za prijavu koji podržava brojne protokole za napad. Vrlo je brz i fleksibilan, a novi moduli se lako dodaju. Ovaj alat omogućuje istraživačima i sigurnosnim savjetnicima da pokažu koliko je lako daljinski dobiti neovlašteni pristup nekom sustavu.

Hydra podržava protokole: Cisco AAA, Cisco auth, Cisco enable, CVS, FTP, HTTP (S) -FORM-GET, HTTP (S) -FORM-POST, HTTP (S) -GET, HTTP (S) -HEAD, HTTP- Proxy, ICQ, IMAP, IRC, LDAP, MS-SQL, MySQL, NNTP, Oracle Listener, Oracle SID, PC-Anywhere, PC-NFS, POP3, PostgreSQL, RDP, Rexec, Rlogin, Rsh, SIP, SMB (NT) , SMTP, SMTP Enum, SNMP v1 + v2 + v3, SOCKS5, SSH (v1 i v2), SSHKEY, Subverzija, Teamspeak (TS2), Telnet, VMware-Auth, VNC i XMPP.

Na slici 3.5 prikazano je korištenje Hydra-e putem Linux terminala.



Slika 3.5. Prikaz izvršavanja naredbe Hydra-e u Linux terminalu

4. Testiranje sigurnosti

Testiranje sigurnosti informacijsko-zabavnog sustava koji se nalazi na razvojnoj ploči je podijeljeno u tri dijela:

1. Skeniranje mreže pomoću Zenmap-a kako bi se otkrilo postoje li otvoreni portovi informacijsko-zabavnog sustava koji bi omogućili pristup i eskalaciju privilegija.
2. Analiza mrežnih protokola pomoću Wireshark-a kako bi se utvrdilo postoje li nesigurni prijenosi podataka.
3. Pokušaj *brute force*-anja informacijsko-zabavnog sustava kako bi se dobilo korisničko ime i zaporka pomoću kojeg bi se preuzela kontrola nad sustavom.

Testiranje je ograničeno na samo ta tri koraka zato što uz razvojnu ploču nisu bili dostavljeni i razni moduli koji bi mogli proširiti granice testiranja poput:

- Bluetooth modula
- Modula za mobilnu mrežu
- GPS modula

Kada je dobiven pristup informacijsko-zabavnom sustavu testiranje se smatra uspješnim i nema potrebe za pokušavanjem odašiljanja paketa preko CAN sabirnice zato što pristup ECU nije bio omogućen tijekom testiranja.

4.1. Skeniranje mreže pomoću Zenmap-a

Prvi korak u testiranju sigurnosti informacijsko-zabavnog sustava je skeniranje mreže informacijsko-zabavnog sustava zbog otkrivanja postoje li otvoreni portovi na koje bi se moglo usredotočiti i pomoću njih dobiti pristup informacijsko-zabavnom sustavu.

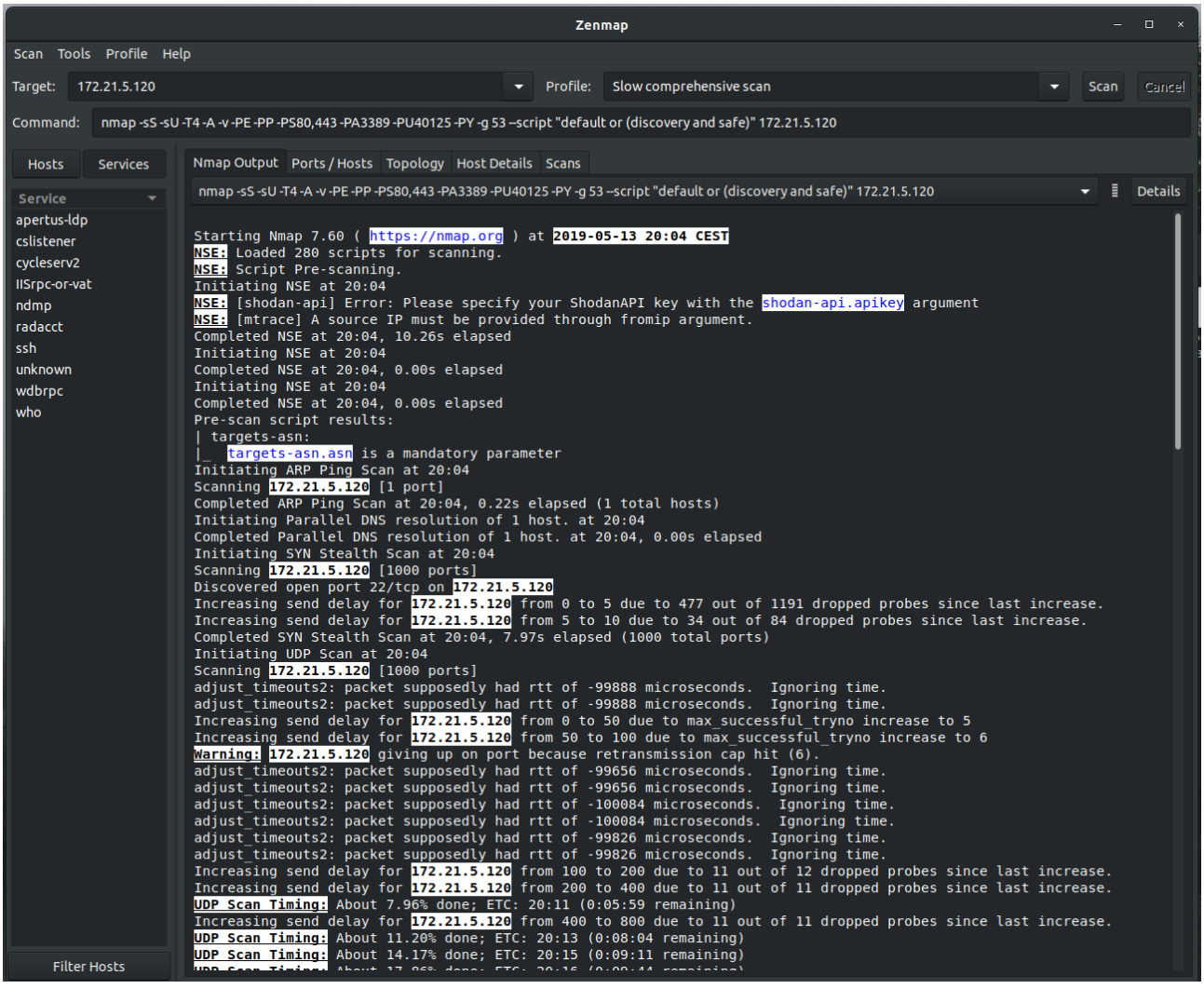
Potrebno je pokrenuti Zenmap i unijeti sve potrebne podatke kako bi skeniranje mreže moglo započeti. Potrebni podaci koji se trebaju unijeti su:

- IP adresa mete
- tip/profil skeniranja mreže koji želimo
- komandu koja će biti izvršena u terminalu (komanda može biti proizvoljna ili odabrana iz ponude Zenmap-a)

Za potrebe testiranja podaci koji su uneseni u Zenmap su:

- IP adresa: 172.21.5.120
- Profil skeniranja: slow comprehensive scan
- komanda: "nmap -sS -sU -T4 -A -v -PE -PP -PS80,443 -PA3389 -PU40125 -PY -g 53 --script "default or (discovery and safe)" 172.21.5.120"

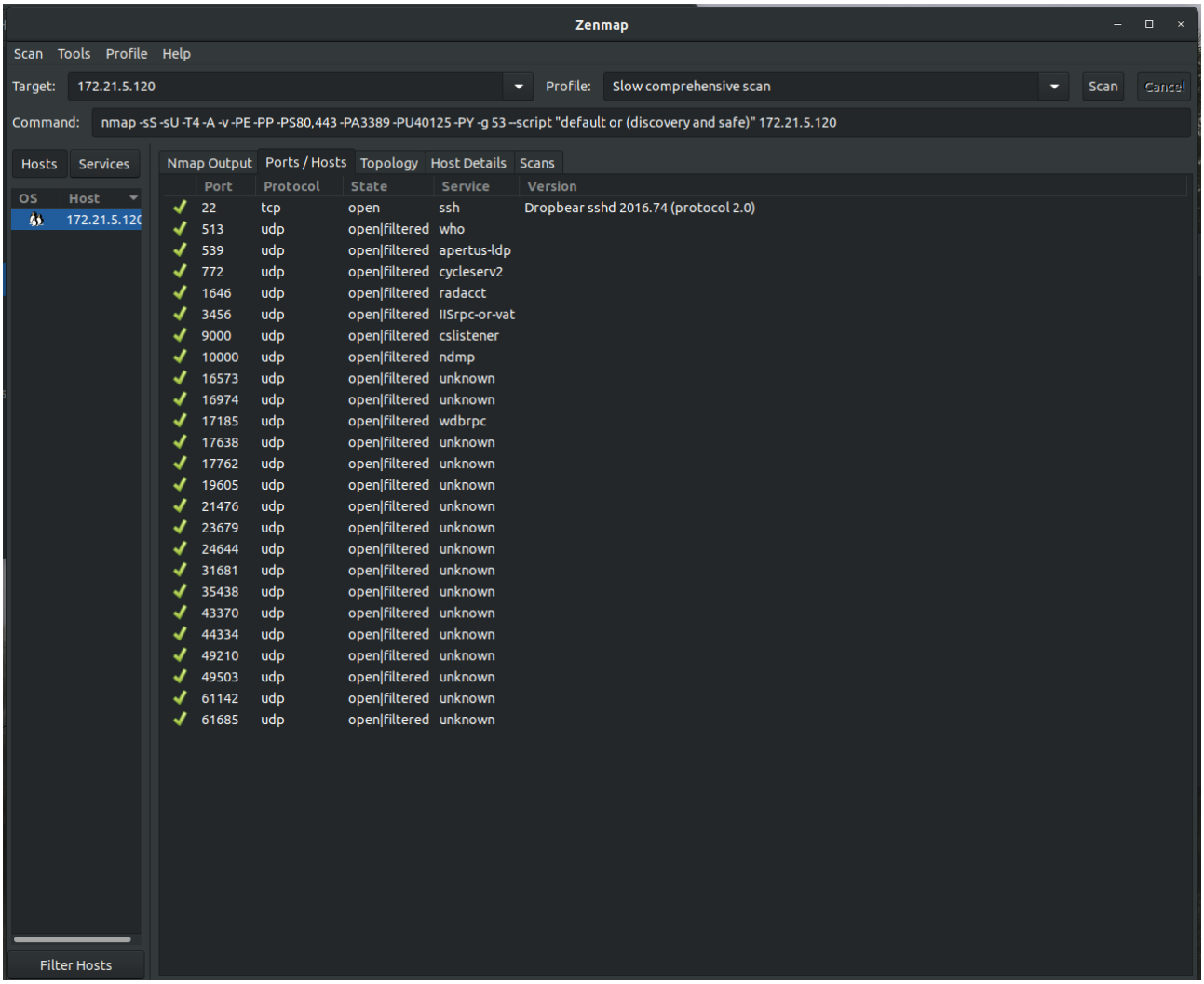
Nakon unosa potrebnih parametra, Zenmap je pokrenut i počinje skeniranje mreže. Na slici 4.1 prikazano je skeniranje pomoću Zenmapa s gore navedenim parametrima. Rezultati skeniranja se nalaze u prilogu.



Slika 4.1. Prikaz početka skeniranja informacijsko-zabavnog sustava pomoću Zenmap-a

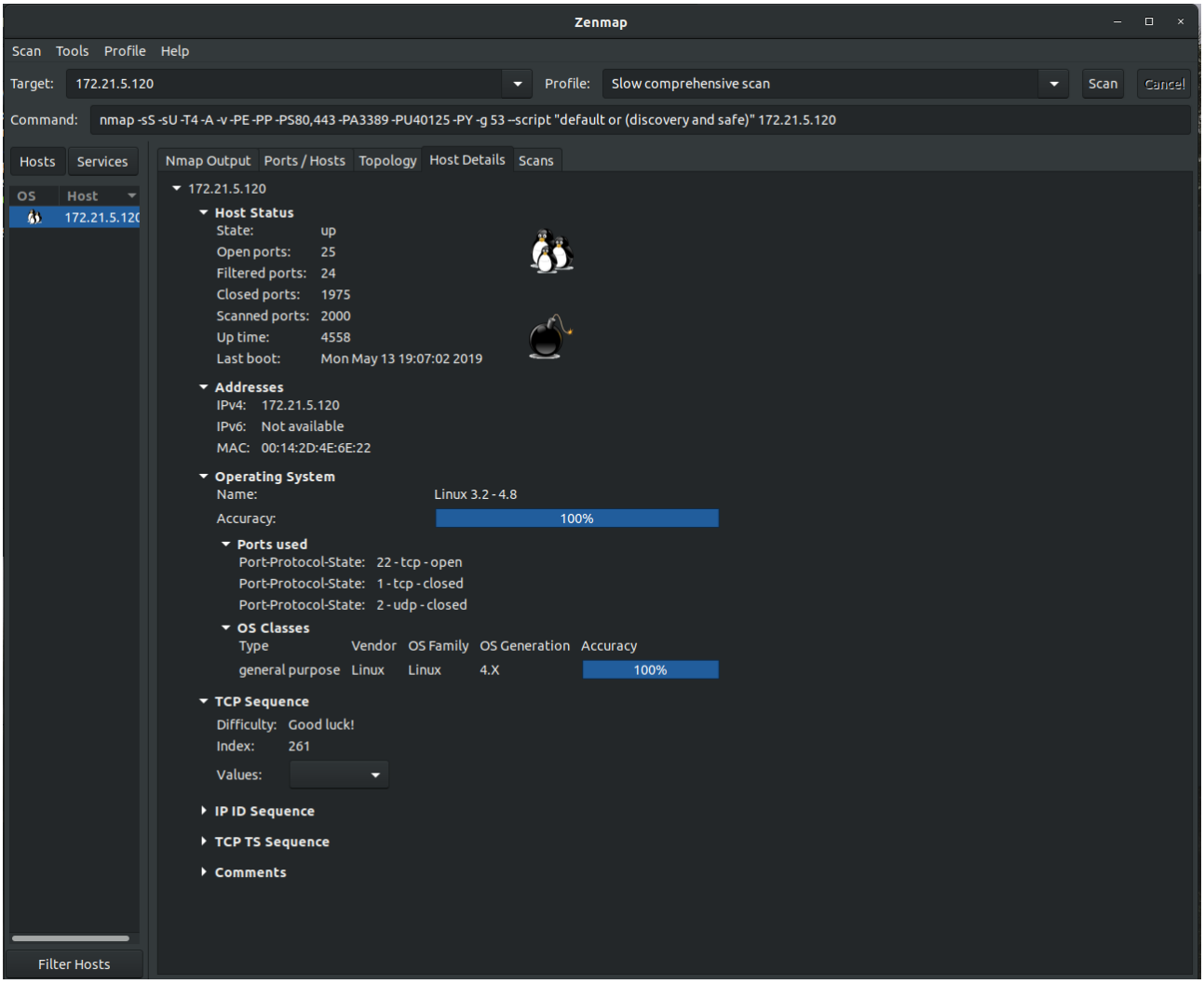
Nakon završetka skeniranja mreže, dobiven je popis svih portova uz njihove statuse, jesu li su otvoreni ili ne, jesu li su filtrirani ili ne, te koji protokol koriste. Osim informacija o portovima Zenmap također pruža neke od osnovnih informacija o operacijskom sustavu ciljanog sustava. Također Zenmap može kreirati topologiju mreže ciljanog sustava.

Na slici 4.2 prikazani su svi otvoreni portovi koji su pronađeni pomoću skeniranja informacijsko-zabavnog sustava. Iz prikaza je vidljivo kako je najbolji kandidat za daljnje testiranje port 22 koji je otvoren i na njemu se nalazi SSH, verzije Dropbear sshd 2016.74.



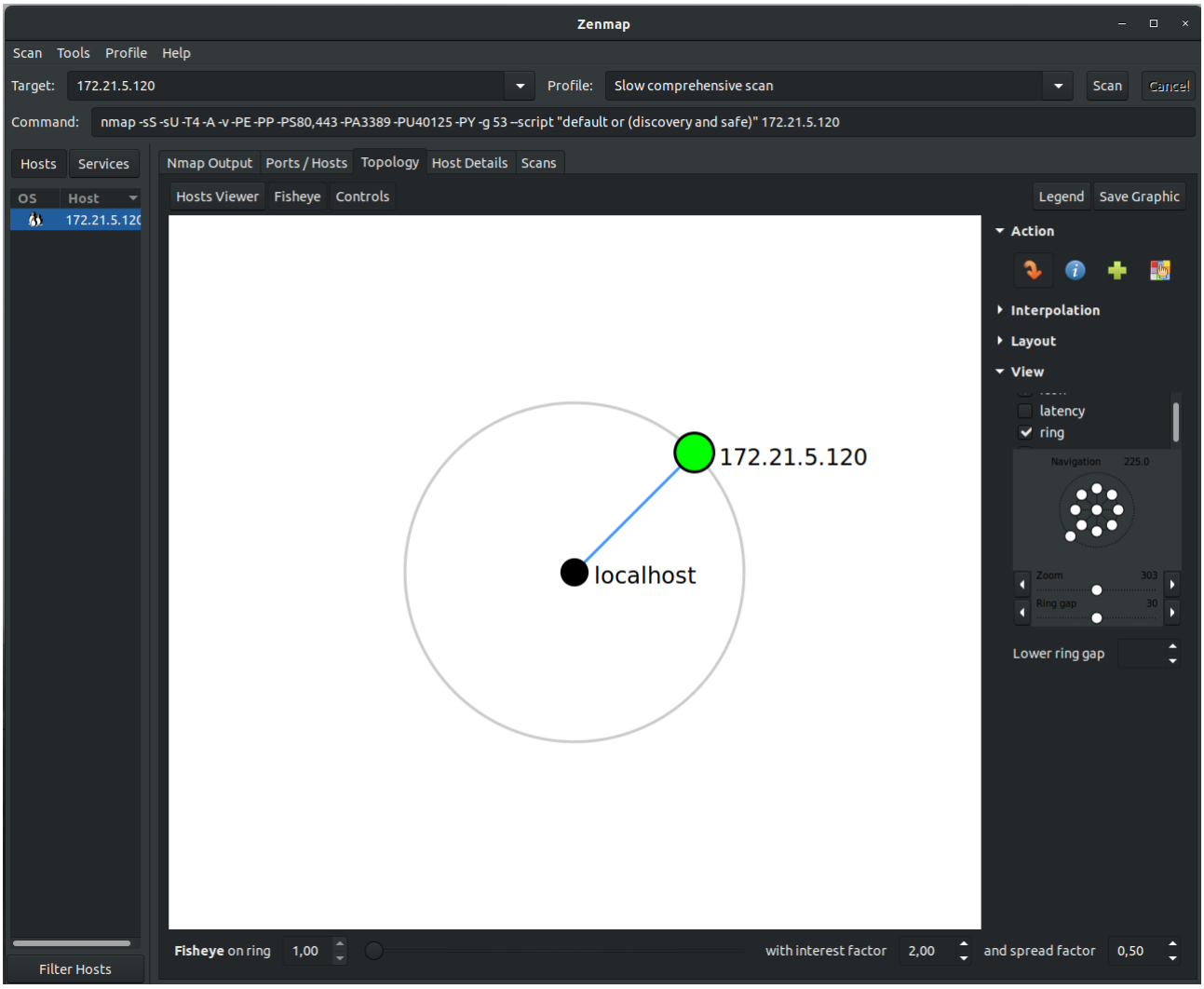
Slika 4.2. Popis otvorenih portova i njihovih protokola

Na slici 4.3 prikazan je sažetak svih informacija koje je Zenmap prikupio o informacijsko-zabavnom sustavu tijekom izvršavanja skeniranja. Iz sažetka je vidljivo kako su skenirane dvije tisuće portova informacijsko-zabavnog sustava od kojih je samo 25 portova otvoreno, a od tih 25 portova samo jedan port nije filtriran, a taj port je port 22 na kojemu se nalazi SSH. Vidljivo je da je IP adresa informacijsko-zabavnog sustava 172.21.5.120, a njegov MAC 00:14:2D:4E:6E:22. Nadalje, Zenmap je detektirao da je operacijski sustav korišten na informacijsko-zabavnom sustavu Linux operacijski sustav 4.X generacije.



Slika 4.3. Detaljan prikaz mete pronađene Zenmapom

Na slici 4.4. je prikazana topologija mreže u kojoj se nalaze "localhost" i informacijsko-zabavni sustav. Informacijsko-zabavni sustav je bio povezan na localhost pomoću mrežnog kabla, gdje je localhost osobno računalo. Kada bi bilo više uređaja povezanih na informacijsko-zabavni sustav topologija mreže bi bila opširnija i imala bi veću primjenu od trenutne.



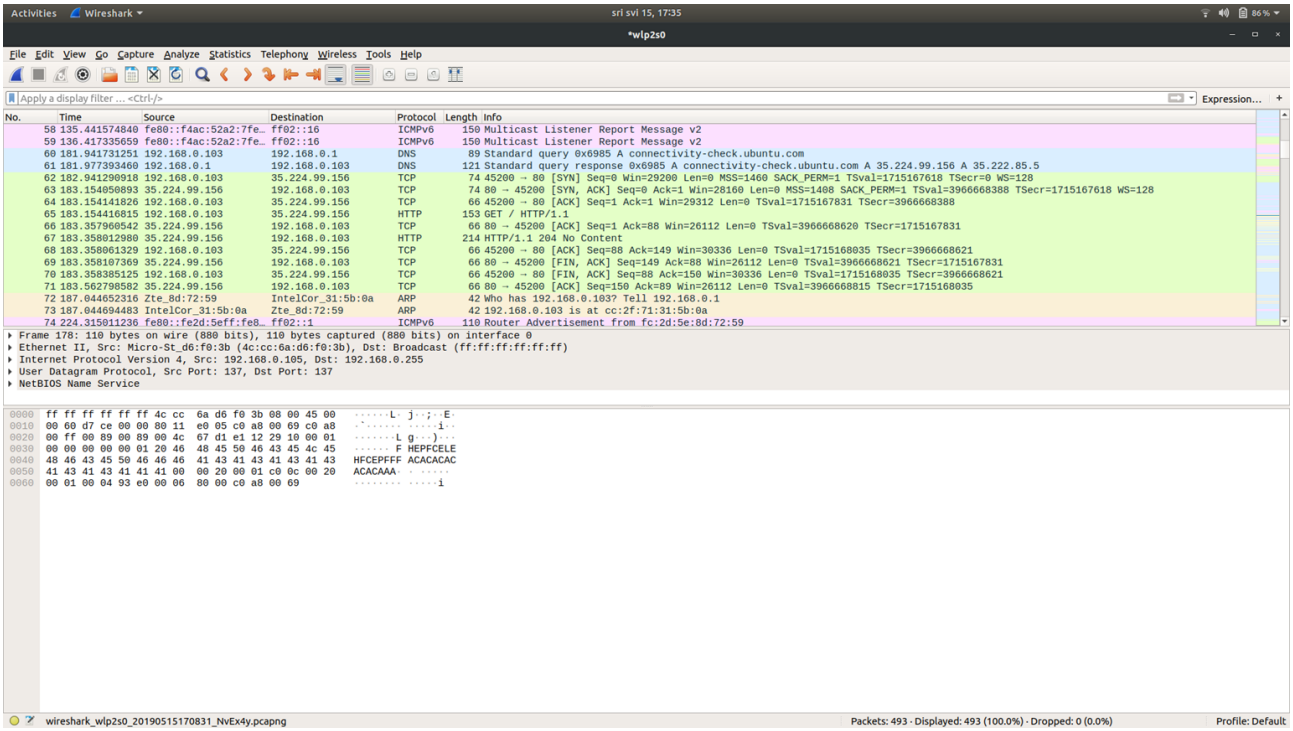
Slika 4.4. Prikaz topologije mreže pomoću Zenmap-a

Nakon uspješnog korištenja Zenmap-a za skeniranje informacijsko-zabavnog sustava kao konačni rezultat dobivena su ranije opisana saznanja. Sigurnost portova informacijsko-zabavnog sustava je skoro pa savršeno izvedena, ali je ostao otvoreni port 22 pomoću kojeg će se probati dobiti pristup informacijsko-zabavnom sustavu.

4.2. Wireshark analiza

Nakon provedenog skeniranja informacijsko-zabavnog sustava pomoću Zenmap-a napravljeno je skeniranje pomoću Wireshark-a kako bi se utvrdilo odašilje li informacijsko-zabavni sustav pakete koji nisu adekvatno zaštićeni i koji bi mogli dovesti do toga da se dobije pristup informacijsko-zabavnom sustavu.

Na slici 4.5. su prikazani rezultati skeniranja informacijsko-zabavnog sustava pomoću Wireshark-a. Detaljnijim proučavanjem paketa koji su uhvaćeni pomoću Wireshark-a nije pronađen niti jedan paket koji nije bio adekvatno zaštićen te je otkrivao ikakve informacije o informacijsko-zabavnom sustavu.



Slika 4.5. Prikaz Wireshark rezultata

Analiza pomoću Wireshark-a nije ponudila niti jednu drugu opciju za pokušaj dobivanja pristupa informacijsko-zabavnom sustavu, stoga se usredotočilo na otvoreni port 22 koji je pronađen tijekom analize provedene pomoću Zenmap-a.

Ispis jednog dijela Wireshark analize nalazi se u prilogu i može biti promatran kako bi se uvidjelo koji paketi se odašilju, pomoću kojeg protokola i što ti paketi sadrže.

4.3. Hydra

Nakon analize pomoću Zenmap-a i Wireshark-a kao jedina moguća meta je određen otvoreni port 22 na kojemu se nalazi SSH. SSH je mrežni računalni protokol koji korisnicima omogućuje uspostavu sigurnog komunikacijskog kanala između dva računala putem računalne mreže [12].

Princip rada Hydre je *brute force*-anje korisničkog imena i zaporke koja se koristi prilikom komunikacije putem SSH. Kako bi Hydra mogla pokušati dobiti pristup informacijsko-zabavnom sustavu potrebne su liste riječi (*engl*. word list) koje sadrže često korištena korisnička imena i zaporke. Napad pomoću lista riječi je najefikasniji način napada jer je veća vjerojatnost da je netko ponovno iskoristio isto korisničko ime i zaporku prilikom kreiranja korisničkog računa.

Hydra se pokreće pomoću terminala i potrebno je odrediti parametre naredbe poput:

- korisničkog imena, ako je poznato
- zaporke, ako je poznata
- IP adrese mete koja se napada
- tip protokola koji se koristi
- apsolutne adrese .txt datoteke koja će biti korištena za *brute force*, ako nije poznato korisničko ime
- apsolutne adrese .txt datoteke koja će biti korištena za *brute force*, ako nije poznata zaporka korisničkog računa

Proces *brute force*-anja je vremenski intenzivan proces osim ako korisničko ime i zaporka nisu jedno od najčešćih korisničkih imena i zaporki poput root, admin, administrator, toor ili ako korisnički račun nema zaporke.

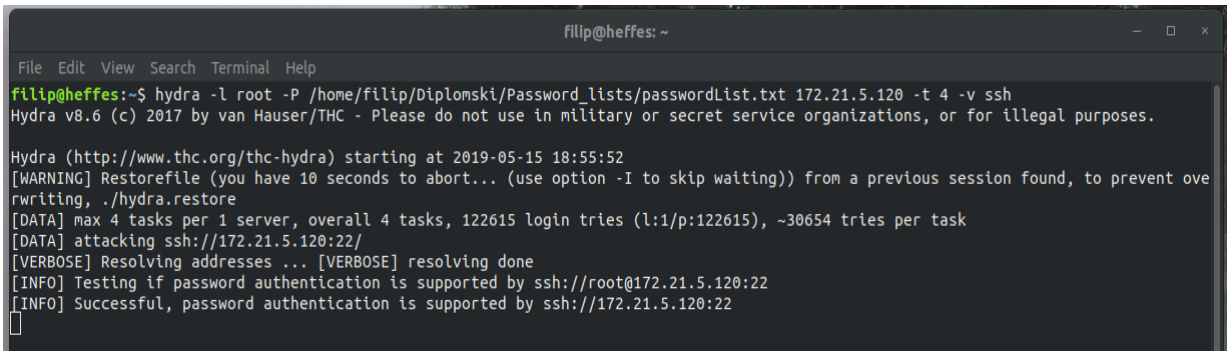
U prvom slučaju *brute force*-anja pristup informacijsko-zabavnom sustavu ostvaren je unutar nekoliko minuta. Kao i kod mnogih drugih ugradbenih računalnih sustava, česta pogreška developera je ta što ne promijene korisničko ime i zaporku na neku kompliciranu inačicu nego ostave jednostavno korisničko ime i zaporku. Ovaj problem je izrazito dokumentiran u raznim ugradbenim sustavima od sigurnosnih kamera, senzora za nadzor pametnih uređaja unutar kućanstva ili samih pametnih uređaja, sve do kontrolera unutar industrijskih postrojenja i automobila.

Kako bi se testirala metoda *brute force*-anja promijenjena je zaporka kako bi se smanjila vjerojatnost pogađanja točne zaporke i povećalo potrebno vrijeme za pogađanje iste, ako je uspješno. Tijekom testiranja korišteno je više lista riječi kako bi se povećala vjerojatnost pogađanja točne zaporke. Dio jedne od lista riječi se nalazi u prilogu kako bi se mogla predočiti lista riječi.

Naredba koja je korištena za pokretanje testiranja pomoću Hydra-e je:

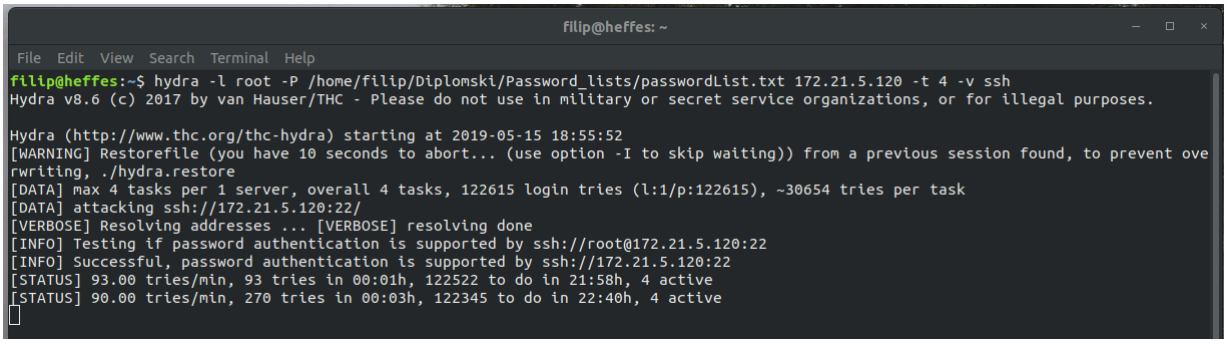
hydra -l root -P /home/filip/Diplomski/Password_lists/passwordList.txt 172.21.5.120 -t 4 -v ssh

Unos gore navedene naredbe u terminal osobnog računala omogućiti će vršenje *brute force*-a. Nakon što je pokrenuta naredba, Hydra će provjeriti da li je autentifikacije korisničkog imena i zaporke podržana na zadanoj IP adresi. To je prikazano na slici 4.6.



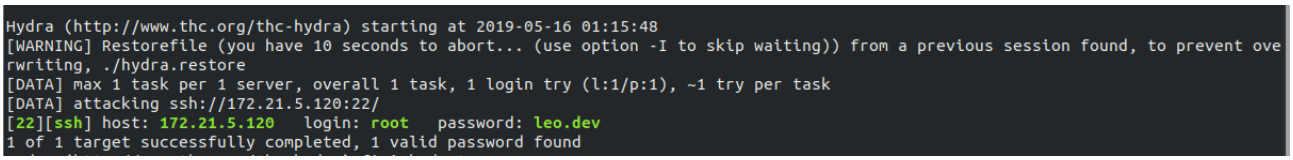
Slika 4.6. Početak *brute force*-anja

Nakon što je postupak započeo Hydra će periodično ispisivati svoj napredak u kojemu ispisuje koliko je vremena prošlo te je li pronađeno odgovarajuće korisničko ime i/ili zaporka s kojima bismo mogli ostvariti pristup informacijsko-zabavnom sustavu. Na slici 4.7. je prikazan periodični ispis podataka Hydre.



Slika 4.7. Periodični ispis o napretku Hydre

Za pronalazak točnog korisničkog imena i zaporke informacijsko-zabavnog sustava bilo je potrebno približno tri dana. Vrijeme pronalaska je moguće skratiti spajanjem više lista riječi u jedno uz brisanje svih duplikata, ili uz korištenje jače računalo. Također, korištenjem više računala omogućilo bi paralelno provjeravanje više kombinacija. Na slici 4.8 prikazan je završetak potrage za korisničkim imenom i zaporkom informacijsko-zabavnog sustava iz koje je vidljivo da niti korisničko ime niti zaporka nisu bili visoke razine sigurnosti.



Slika 4.8. Pronalazak odgovarajućeg korisničkog imena i zaporke

Nakon pronalaska korisničkog imena i zaporke, pristup informacijsko-zabavnom sustavu je omogućen. Ulaskom u informacijsko-zabavni sustav utvrđeno je da je razina privilegije root te da nema potrebe za eskalacijom privilegija.

Ulaskom u informacijsko-zabavni sustav utvrđene su sljedeće mogućnosti:

- neovlašteno modificiranje informacijsko-zabavnog sustava
- izvršavanje neovlaštenog koda
- krađa privatnih podataka korisnika informacijsko-zabavnog sustava

5. Poboljšanje sigurnosnih mjera informacijsko-zabavnog sustava

Uvidom u pronađene ranjivosti informacijsko-zabavnog sustava automobila moguće je uvesti odgovarajuće sigurnosne mjere koje bi otežale napadačima pristup informacijsko-zabavnom sustavu. Predložene mjere se odnose samo na osnovne ranjivosti koje su pronađene testiranjem informacijsko-zabavnog sustava i ne odnose se na potencijalne ranjivosti koje mogu nastati dodavanjem raznih modula na razvojnu ploču informacijsko-zabavnog sustava.

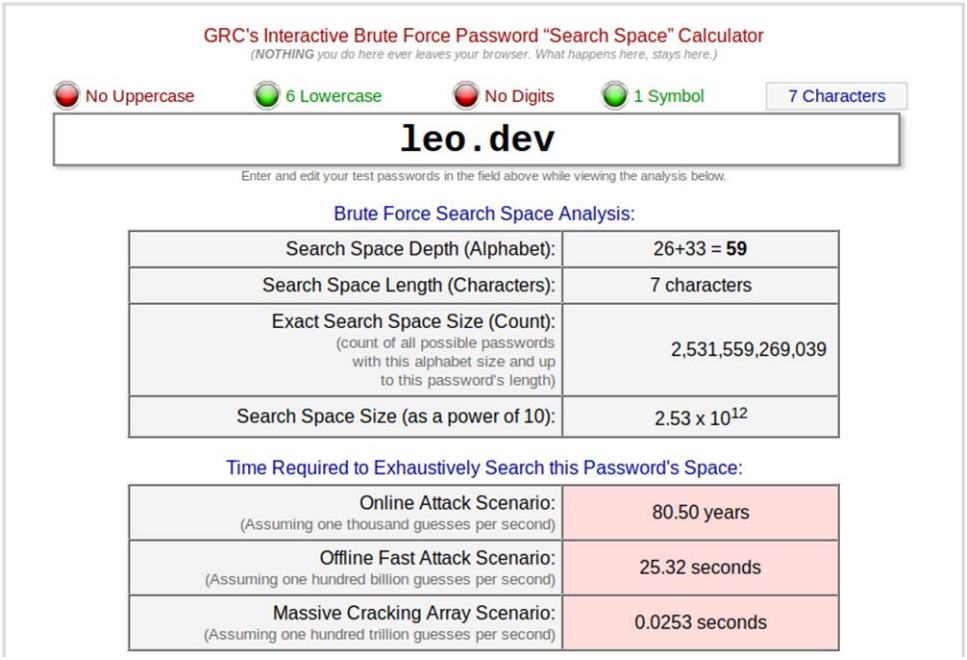
Primjeri tih mjera su:

- povećanje kompliciranosti korisničkog imena i zaporke
- zatvaranje ili filtriranje otvorenih portova
- uvođenje certificiranja umjesto korištenja korisničkog imena i zaporke

5.1. Povećanje kompliciranosti korisničkog imena i zaporke

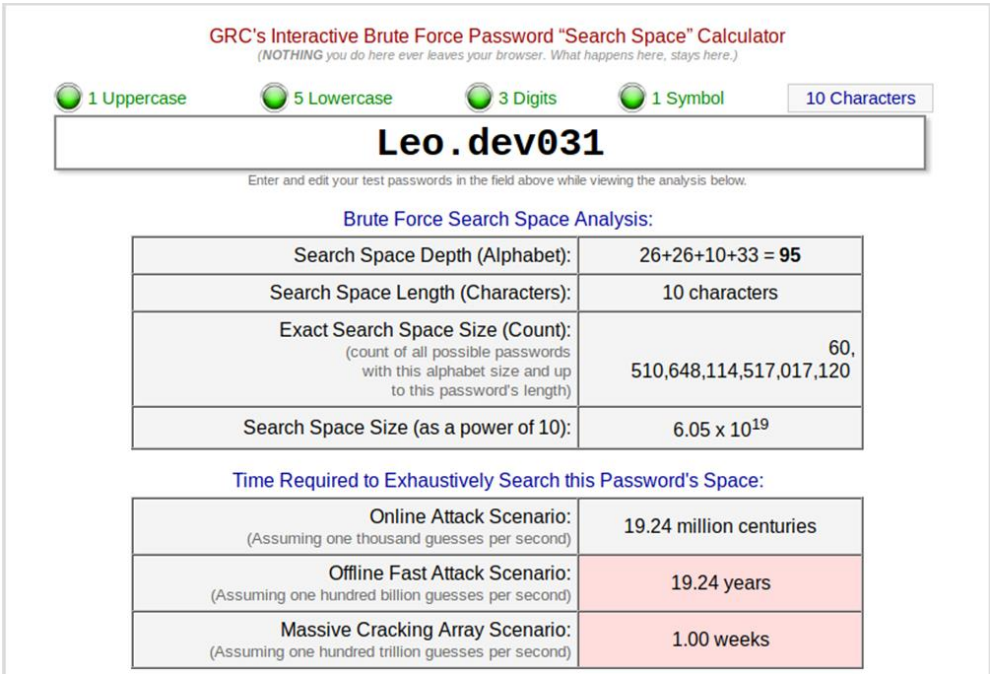
Najjednostavnija mjera povećanja sigurnosti informacijsko-zabavnog sustava je povećanje kompliciranosti korisničkog imena i zaporke. Ako se u korisničko ime i zaporku dodaju velika i mala slova, simboli ili znakovi te brojevi, kompliciranost istih raste te se vjerojatnost pogađanja tog korisničkog imena i zaporke smanjuje. Uz kompliciranost korisničkog imena i zaporke dolazi do povećanja potrebnog vremena za pogađanje točnog korisničkog imena i zaporke što uzrokuje povećanje potrebe za računalnim resursima. Povećanje potrebe računalnih resursa u određenom trenutku dovodi računicu u stanje u kojem više nije isplativo pokušavati pogoditi točno korisničko ime i zaporku ili će proći previše vremena da bi te informacije imale ikakvu korist.

Na slici 5.1 prikazano je estimirano vrijeme potrebno za pogađanje zaporke "leo.dev" koja je bila proizvoljno postavljena na informacijsko-zabavni sustava kako bi otežala pogađanje u odnosu na početnu zaporku.



Slika 5.1. Predviđeno vrijeme potrebno za pogađanje zaporke

Kada bi se povećala kompliciranost zaporke, odnosno kada bi ona postala "Leo.dev031", potrebno vrijeme se povećava i metoda *brute force*-anja postaje beskorisna. Na slici 5.2 prikazano je estimirano vrijeme potrebno za točno pogađanje nove, kompliciranije zaporke.



Slika 5.2. Predviđeno vrijeme potrebno za pogađanje unaprijeđene zaporke

5.2. Zatvaranje ili filtriranje otvorenih portova

Tijekom testiranja kibernetičke sigurnosti informacijsko-zabavnog sustava pronađen je otvoreni port 22 na kojemu se nalazio SSH. Otvoreni port 22 predstavlja sigurnosni rizik te ga je potrebno zatvoriti ili filtrirati kako bi se sigurnosni rizik za informacijsko-zabavni sustav smanjio. Postoji više načina za zatvaranje ili filtriranje porta, na primjer [14]:

- korištenjem TCP wrapper-a
- filtriranjem porta u vatrozidu (engl. firewall)
- automatskim blokiranjem brute force napada
- limitiranjem maksimalnog broja autentifikacijskih pokušaja
- omogućiti login notifikacije pomoću e-mail-a

Kako je tijekom testiranja korišten *brute force* napad, postoji više načina za zaustavljanje takvih napada. Ručni način je raščlanjivanjem zapisnika sustava i provjeravanjem tko se pokušava povezati s poslužiteljem te ih zatim blokirati pomoću vatrozida. Međutim, postoji nekoliko alata koji mogu te ručne zadatke obaviti na učinkovit i automatiziran način. Neki od tih alata su SSHGuard, Fail2ban, DenyHosts [14].

5.3. Certificiranje

Korištenje kriptografskog javnog ključa za provjeru autentičnosti zahtijeva kopiranje javnog ključa sa svakog klijenta na svaki poslužitelj na koji se klijent namjerava prijaviti. Ovaj se sustav ne skalira dobro i može predstavljati administrativni teret. Upotreba javnog ključa od strane certifikacijskog tijela (engl. certificate authority, CA) za provjeru autentičnosti certifikata klijenta uklanja potrebu za kopiranjem ključeva između više sustava. Dok X.509 sustav certifikata o javnom ključu nudi rješenje za ovo pitanje, postoji postupak podnošenja i provjere valjanosti, s pripadajućim naknadama, da bi se potpisao certifikat. Kao alternativa, OpenSSH podržava stvaranje jednostavnih certifikata i pridružene CA infrastrukture.

OpenSSH certifikati sadrže javni ključ, podatke o identitetu i ograničenja valjanosti. Potpisani su sa standardnim SSH javnim ključem pomoću uslužnog programa ssh-keygen. Format certifikata opisan je na lokaciji " /usr/share/doc/openssh-version/PROTOCOL.certkeys".

Uslužni program ssh-keygen podržava dvije vrste certifikata: korisnički (engl. user) i domaćin (engl. host). Korisnički certifikati provjere autentičnost korisnika na poslužiteljima, dok certifikati domaćina potvrđuju poslužitelje. Da bi se certifikati koristili za autentifikaciju korisnika ili host-a, SSHD mora biti konfiguriran za povjerenje javnom ključu CA [15].

6. Zaključak

U ovom diplomskom radu obrađena je tema računalne sigurnosti informacijsko-zabavnih sustava unutar automobila. Za cilj diplomskog rada zadano je proučiti ranjivosti informacijsko-zabavnog sustava i proučiti moguća rješenja koja bi spriječila te ranjivosti informacijsko-zabavnog sustava. Za praktični dio diplomskog rada provedeno je testiranje računalne sigurnosti informacijsko-zabavnog sustava unutar automobila. Testiranje informacijsko-zabavnog sustava izvršeno je pomoću Ubuntu 18.04 operacijskog sustava i softverskih alata Zenmap, Wireshark i Hydra.

U prvom poglavlju razmotrene su najčešće ranjivosti vozila, zajedno s primjerima napada na njih. Alati korišteni za testiranje sigurnosti Yocto linux operativnog sustava su objašnjeni i navedeni u drugom poglavlju. Treće poglavlje opisuje testiranje i rezultate testiranja sustava. U četvrtom poglavlju su predložene sigurnosne mjere koje se mogu poduzeti kako bi se povećala sigurnost informacijsko-zabavnih sustava.

Softverski alat Zenmap korišten je za skeniranje mreže informacijsko-zabavnog sustava. Nakon skeniranja mreže informacijsko-zabavnog sustava pomoću Zenmap-a otkriven je jedan otvoreni port, port 22 koji je koristio SSH protokol za komunikaciju. Nakon provedenog skeniranja informacijsko-zabavnog sustava pomoću Zenmap-a napravljeno je skeniranje pomoću Wireshark-a kako bi se utvrdilo da li informacijsko-zabavni sustav odašilje pakete koji nisu adekvatno zaštićeni i koji bi mogli dovesti do toga da se dobije pristup informacijsko-zabavnom sustavu. Nakon analize pomoću Zenmap-a i Wireshark-a kao jedina moguća meta je određen otvoreni port 22 na kojemu se nalazi SSH.

Testiranje ranjivosti informacijsko-zabavnog sustava je moguće proširiti dodavanje novih modula sustavu poput *Bluetooth* modula, modula za mobilnu mrežu, itd. S obzirom na pronađene ranjivosti informacijsko-zabavnog sustava predložene su sigurnosne mjere koje mogu smanjiti te ranjivosti ili ih ukloniti u potpunosti. Neke od tih mjera su povećanje kompliciranosti korisničkog imena i zaporke, zatvaranje ili filtriranje otvorenih portova, uvođenje certificiranja umjesto korištenja korisničkog imena i zaporke. Dodavanjem novih modula na informacijsko-zabavni sustav moralo bi se ponovo izvršiti testiranje kako bi se pronašlo nove ranjivosti i moglo predložiti moguća rješenja za te ranjivosti.

Literatura

[1] Adequate, Vulnerability (computing), https://en.wikipedia.org/wiki/Vulnerability_(computing) [07.06.2019.]

[2] Velle, Threat Model, https://en.wikipedia.org/wiki/Threat_model [08.06.2019.]

[3] Reshamtalawila, In-car entertainment, https://en.wikipedia.org/wiki/In- car_entertainment [08.06.2019.]

[4] C. Smith, "Car Hacker's Handbook", Creative Commons, 2014.

[5] Michael Burk, "The Evolution of In-Vehicle Infotainment Sytems, part two", https://www.micron.com/about/blog/2019/march/evolution-of-in-vehicle-infotainment-systems-part-two [08.06.2019.]

[6] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, T. Kohno, "Comprehensive Experimental Analyses of Automotive Attack Surfaces"

[7] Marco Vaz, From 0-day to exploit - Buffer overflow in Belkin N750 (CVE-2014-1635), https://labs.integrity.pt/articles/from-0-day-to-exploit-buffer-overflow-in-belkin-n750-cve-2014-1635/ [15.08.2019.]

[8] razvojna ploča Toradex Ixora https://datasheet.ciiva.com/22754/apalis-arm-ixora-datasheet-22754751.pdf [20.08.2019.]

[9] Zenmap, https://geek-university.com/nmap/what-is-zenmap/ [25.08.2019.]

[10] Wireshark, https://www.wireshark.org/ [25.08.2019.]

[11] Hydra, https://directory.fsf.org/wiki/Hydra [25.08.2019.]

[12] Argo Navis, Secure Shell, https://hr.wikipedia.org/wiki/Secure_Shell [16.09.2019.]

[13] GRC's Interactive Brute Force Password "Search Space" Calculator, https://www.grc.com/haystack.htm [17.09.2019.]

[14] Securitytrails team, "Mitigating SSH based attacks - Top 15 Best SSH Security Practices", 29.08.2018., https://securitytrails.com/blog/mitigating-ssh-based-attacks-top-15-best-security-practices [19.09.2019.]

[15] Red Hat, "14.3. Using OpenSSH Certificate Authentication", https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/6/html/deployment_guide/sec-using_openssh_certificate_authentication [19.09.2019.]

Sažetak

Cilj ovog diplomskog rada je testiranje sigurnosti informacijsko-zabavnog sustava koji se nalazi unutar automobila. Za izradu diplomskog rada i testiranje korišten je Ubuntu 18.04 operacijski sustav, softverski alati Zenmap, Wireshark i Hydra. Testiranjem zadanog informacijsko-zabavnog sustava uspiješno je ostvaren pristup istom i omogućene su sve zloupotrebe sustava. Predložene su neke moguće mjere koje bi onemogućile ostvarivanje pristupa informacijsko-zabavnom sustavu u odnosu na provedeno testiranje.

Ključne riječi: sigurnost informacijskih sustava, informacijsko-zabavni sustav, Zenmap, Hydra, Wireshark

Abstract

The aim of this thesis "Cybersecurity of In-Vehicle Infotainment Systems" is to test the security of an infotainment system inside a car. Ubuntu 18.04 operating system, Zenmap, Wireshark, and Hydra software tools were used to create the thesis and test it. By testing the default infotainment system, the system was successfully accessed and all system abuses were enabled. Some possible measures have been proposed that would prevent access to the infotainment system in relation to the testing carried out.

Key words: security of information systems, infotainment system, Zenmap, Hydra, Wireshark

Životopis

Filip Antunović rođen je u Osijeku 30.01.1995. U Tenju završava Osnovnu školu "Tenja" i upisuje Prvu gimnaziju Osijek 2010. godine. Naziv prvostupnika računarstva na Fakultetu elektrotehnike, računarstva i informacijskih tehnologija u Osijeku stječe 2017. godine te nastavlja svoje obrazovanje upisujući diplomski studij Automobilskog računarstva i komunikacija na istoimenom fakultetu.

_____

Filip Antunović

Prilozi

Prilog 1. Skeniranje pomoću Zenmap-a

```
Starting Nmap 7.60 ( https://nmap.org ) at 2019-05-13 20:04 CEST
NSE: Loaded 280 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 20:04
NSE: [shodan-api] Error: Please specify your ShodanAPI key with the shodan-
api.apikey argument
NSE: [mtrace] A source IP must be provided through fromip argument.
Completed NSE at 20:04, 10.26s elapsed
Initiating NSE at 20:04
Completed NSE at 20:04, 0.00s elapsed
Initiating NSE at 20:04
Completed NSE at 20:04, 0.00s elapsed
Pre-scan script results:
| targets-asn:
|_  targets-asn.asn is a mandatory parameter
Initiating ARP Ping Scan at 20:04
Scanning 172.21.5.120 [1 port]
Completed ARP Ping Scan at 20:04, 0.22s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 20:04
Completed Parallel DNS resolution of 1 host. at 20:04, 0.00s elapsed
Initiating SYN Stealth Scan at 20:04
Scanning 172.21.5.120 [1000 ports]
Discovered open port 22/tcp on 172.21.5.120
Increasing send delay for 172.21.5.120 from 0 to 5 due to 477 out of 1191 dropped
probes since last increase.
Increasing send delay for 172.21.5.120 from 5 to 10 due to 34 out of 84 dropped
probes since last increase.
Completed SYN Stealth Scan at 20:04, 7.97s elapsed (1000 total ports)
Initiating UDP Scan at 20:04
Scanning 172.21.5.120 [1000 ports]
adjust_timeouts2: packet supposedly had rtt of -99888 microseconds. Ignoring time.
adjust_timeouts2: packet supposedly had rtt of -99888 microseconds. Ignoring time.
Increasing send delay for 172.21.5.120 from 0 to 50 due to max_successful_tryno
increase to 5
Increasing send delay for 172.21.5.120 from 50 to 100 due to max_successful_tryno
increase to 6
Warning: 172.21.5.120 giving up on port because retransmission cap hit (6).
adjust_timeouts2: packet supposedly had rtt of -99656 microseconds. Ignoring time.
adjust_timeouts2: packet supposedly had rtt of -99656 microseconds. Ignoring time.
adjust_timeouts2: packet supposedly had rtt of -100084 microseconds.Ignoring time.
adjust_timeouts2: packet supposedly had rtt of -100084 microseconds.Ignoring time.
adjust_timeouts2: packet supposedly had rtt of -99826 microseconds.Ignoring time.
adjust_timeouts2: packet supposedly had rtt of -99826 microseconds. Ignoring time.
Increasing send delay for 172.21.5.120 from 100 to 200 due to 11 out of 12 dropped
probes since last increase.
Increasing send delay for 172.21.5.120 from 200 to 400 due to 11 out of 11 dropped
probes since last increase.
UDP Scan Timing: About 7.96% done; ETC: 20:11 (0:05:59 remaining)
Increasing send delay for 172.21.5.120 from 400 to 800 due to 11 out of 11 dropped
probes since last increase.
UDP Scan Timing: About 11.20% done; ETC: 20:13 (0:08:04 remaining)
UDP Scan Timing: About 14.17% done; ETC: 20:15 (0:09:11 remaining)
UDP Scan Timing: About 17.86% done; ETC: 20:16 (0:09:44 remaining)
UDP Scan Timing: About 35.14% done; ETC: 20:18 (0:09:04 remaining)
```

```
UDP Scan Timing: About 42.11% done; ETC: 20:19 (0:08:20 remaining)
UDP Scan Timing: About 48.04% done; ETC: 20:19 (0:07:35 remaining)
UDP Scan Timing: About 53.89% done; ETC: 20:19 (0:06:49 remaining)
UDP Scan Timing: About 59.71% done; ETC: 20:19 (0:06:01 remaining)
UDP Scan Timing: About 65.24% done; ETC: 20:19 (0:05:14 remaining)
UDP Scan Timing: About 70.77% done; ETC: 20:20 (0:04:26 remaining)
UDP Scan Timing: About 75.99% done; ETC: 20:20 (0:03:39 remaining)
UDP Scan Timing: About 81.50% done; ETC: 20:20 (0:02:50 remaining)
UDP Scan Timing: About 86.73% done; ETC: 20:20 (0:02:02 remaining)
UDP Scan Timing: About 91.96% done; ETC: 20:20 (0:01:14 remaining)
Completed UDP Scan at 20:21, 971.32s elapsed (1000 total ports)
Initiating Service scan at 20:21
Scanning 25 services on 172.21.5.120
Service scan Timing: About 8.00% done; ETC: 20:33 (0:11:30 remaining)
Completed Service scan at 20:22, 82.57s elapsed (25 services on 1 host)
Initiating OS detection (try #1) against 172.21.5.120
NSE: Script scanning 172.21.5.120.
Initiating NSE at 20:22
Completed NSE at 20:22, 31.30s elapsed
Initiating NSE at 20:22
Completed NSE at 20:23, 1.23s elapsed
Initiating NSE at 20:23
Completed NSE at 20:23, 0.02s elapsed
Nmap scan report for 172.21.5.120
Host is up (0.00090s latency).
Not shown: 1975 closed ports
PORT      STATE         SERVICE       VERSION
22/tcp    open          ssh           Dropbear sshd 2016.74 (protocol 2.0)
| banner: SSH-2.0-dropbear_2016.74\x0D\x0A\x00\x00\x02d\x0A\x14\x06\xD4\x
|_AB\x90\x1AQ\xA8\x82'^\xD2W\xDD\x1A2\xAD\x00\x00\x00\xA6curve25519-sh...
513/udp   open|filtered who
539/udp   open|filtered apertus-ldp
772/udp   open|filtered cycleserv2
1646/udp  open|filtered radacct
3456/udp  open|filtered IISrpc-or-vat
9000/udp  open|filtered cslistener
10000/udp open|filtered ndmp
16573/udp open|filtered unknown
16974/udp open|filtered unknown
17185/udp open|filtered wdbrpc
17638/udp open|filtered unknown
17762/udp open|filtered unknown
19605/udp open|filtered unknown
21476/udp open|filtered unknown
23679/udp open|filtered unknown
24644/udp open|filtered unknown
31681/udp open|filtered unknown
35438/udp open|filtered unknown
43370/udp open|filtered unknown
44334/udp open|filtered unknown
49210/udp open|filtered unknown
49503/udp open|filtered unknown
61142/udp open|filtered unknown
61685/udp open|filtered unknown
MAC Address: 00:14:2D:4E:6E:22 (Toradex AG)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.8
```

```
Uptime guess: 0.053 days (since Mon May 13 19:07:02 2019)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=261 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
Host script results:
|_fcrdns: FAIL (No PTR record)
| firewalk:
| HOP  HOST         PROTOCOL  BLOCKED PORTS
|_0    172.21.5.69  udp       513,539,772,1646,3456,9000,10000,16573,16974,17185
|_ipidseq: All zeros
|_path-mtu: PMTU == 1500
| qscan:
| PORT  FAMILY  MEAN (us)  STDDEV  LOSS (%)
| 1     0       881.50     208.56  0.0%
|_22    0       877.60     187.69  0.0%
| traceroute-geolocation:
|   HOP  RTT   ADDRESS       GEOLOCATION
|_  1    0.90  172.21.5.120  - ,-
TRACEROUTE
HOP RTT     ADDRESS
1   0.90 ms 172.21.5.120
NSE: Script Post-scanning.
Initiating NSE at 20:23
Completed NSE at 20:23, 0.00s elapsed
Initiating NSE at 20:23
Completed NSE at 20:23, 0.00s elapsed
Initiating NSE at 20:23
Completed NSE at 20:23, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1107.54 seconds
           Raw packets sent: 3268 (127.511KB) | Rcvd: 2451 (116.596KB)
```

Prilog 2. Wireshark ispis

```
Frame 192: 305 bytes on wire (2440 bits), 305 bytes captured (2440 bits) on
interface 0
Ethernet II, Src: Micro-St_d6:f0:3b (4c:cc:6a:d6:f0:3b), Dst: Broadcast
(ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 192.168.0.105, Dst: 192.168.0.255
User Datagram Protocol, Src Port: 54915, Dst Port: 54915
Data (263 bytes)

0000  00 44 45 53 4b 54 4f 50 2d 41 56 52 38 30 30 37   .DESKTOP-AVR8007
0010  00 b2 ff 0b dd 00 00 00 00 00 00 00 00 00 00 00   ................
0020  33 27 00 00 00 00 00 00 10 57 fe 84 1f 02 00 00   3'.......W......
0030  10 1d e7 85 1f 02 00 00 00 f6 38 84 1f 02 00 00   ..........8.....
0040  00 00 00 00 00 00 00 00 7c 6a ba 5f 00 00 00 00   ........|j._....
0050  f0 a4 68 60 00 00 00 00 09 b7 ff 0b dd 00 00 00   ..h`............
0060  00 00 00 00 00 00 00 00 90 19 e7 85 1f 02 00 00   ................
0070  54 b3 ff 0b dd 00 00 00 70 b3 ff 0b dd 00 00 00   T.......p.......
0080  58 53 32 7b 66 64 62 66 63 34 61 65 2d 38 63 65   XS2{fdbfc4ae-8ce
0090  63 2d 34 65 66 31 2d 38 36 34 36 2d 32 36 31 37   c-4ef1-8646-2617
00a0  39 37 62 38 36 63 31 34 7d 00 00 00 00 00 00 00   97b86c14}.......
00b0  01 00 00 00 00 00 00 00 50 b3 ff 0b dd 00 00 00   ........P.......
```

```
00c0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00d0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00e0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00f0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0100  00 00 00 71 69 b7 32                              ...qi.2

No.     Time           Source                Destination           Protocol Length
Info
    193 967.449103731  192.168.0.105         192.168.0.255         NBNS     92
Name query NB DESKTOP-AVR8007<1c>

Frame 193: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) on interface
0
Ethernet  II,  Src:  Micro-St_d6:f0:3b  (4c:cc:6a:d6:f0:3b),  Dst:  Broadcast
(ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 192.168.0.105, Dst: 192.168.0.255
User Datagram Protocol, Src Port: 137, Dst Port: 137
NetBIOS Name Service

No.     Time           Source                Destination           Protocol Length
Info
    194 967.756008612  Micro-St_d6:f0:3b     Broadcast             ARP      60
Who has 192.168.0.118? Tell 192.168.0.105

Frame 194: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface
0
Ethernet  II,  Src:  Micro-St_d6:f0:3b  (4c:cc:6a:d6:f0:3b),  Dst:  Broadcast
(ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)

No.     Time           Source                Destination           Protocol Length
Info
    195 967.962760730  192.168.0.105         192.168.0.255         UDP      305
54915 → 54915 Len=263

Frame 195: 305 bytes on wire (2440 bits), 305 bytes captured (2440 bits) on
interface 0
Ethernet  II,  Src:  Micro-St_d6:f0:3b  (4c:cc:6a:d6:f0:3b),  Dst:  Broadcast
(ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 192.168.0.105, Dst: 192.168.0.255
User Datagram Protocol, Src Port: 54915, Dst Port: 54915
Data (263 bytes)

0000  00 44 45 53 4b 54 4f 50 2d 41 56 52 38 30 30 37   .DESKTOP-AVR8007
0010  00 b2 ff 0b dd 00 00 00 00 00 00 00 00 00 00 00   ................
0020  33 27 00 00 00 00 00 00 10 57 fe 84 1f 02 00 00   3'.......W......
0030  10 1d e7 85 1f 02 00 00 00 f6 38 84 1f 02 00 00   ..........8.....
0040  00 00 00 00 00 00 00 00 7c 6a ba 5f 00 00 00 00   ........|j._....
0050  f0 a4 68 60 00 00 00 00 09 b7 ff 0b dd 00 00 00   ..h`............
0060  00 00 00 00 00 00 00 00 90 19 e7 85 1f 02 00 00   ................
0070  54 b3 ff 0b dd 00 00 00 70 b3 ff 0b dd 00 00 00   T.......p.......
0080  58 54 32 7b 66 64 62 66 63 34 61 65 2d 38 63 65   XT2{fdbfc4ae-8ce
0090  63 2d 34 65 66 31 2d 38 36 34 36 2d 32 36 31 37   c-4ef1-8646-2617
00a0  39 37 62 38 36 63 31 34 7d 00 00 00 00 00 00 00   97b86c14}.......
00b0  01 00 00 00 00 00 00 00 50 b3 ff 0b dd 00 00 00   ........P.......
00c0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00d0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00e0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00f0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
```

```
0100  00 00 00 e5 d8 82 9e                                .......

No.     Time           Source                Destination           Protocol Length
Info
    196 968.064146705  192.168.0.105          192.168.0.255          NBNS     92
Name query NB WPAD<00>

Frame 196: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) on interface
0
Ethernet   II,   Src:   Micro-St_d6:f0:3b   (4c:cc:6a:d6:f0:3b),   Dst:   Broadcast
(ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 192.168.0.105, Dst: 192.168.0.255
User Datagram Protocol, Src Port: 137, Dst Port: 137
NetBIOS Name Service

No.     Time           Source                Destination           Protocol Length
Info
    197 968.064190143  192.168.0.105          224.0.0.251            MDNS     70
Standard query 0x0000 A wpad.local, "QM" question

Frame 197: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface
0
Ethernet  II,  Src:  Micro-St_d6:f0:3b  (4c:cc:6a:d6:f0:3b),  Dst:  IPv4mcast_fb
(01:00:5e:00:00:fb)
Internet Protocol Version 4, Src: 192.168.0.105, Dst: 224.0.0.251
User Datagram Protocol, Src Port: 5353, Dst Port: 5353
Multicast Domain Name System (query)

No.     Time           Source                Destination           Protocol Length
Info
    198 968.065921443  fe80::ac53:29d8:c946:4b39 ff02::fb             MDNS     90
Standard query 0x0000 A wpad.local, "QM" question

Frame 198: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface
0
Ethernet  II,  Src:  Micro-St_d6:f0:3b  (4c:cc:6a:d6:f0:3b),  Dst:  IPv6mcast_fb
(33:33:00:00:00:fb)
Internet Protocol Version 6, Src: fe80::ac53:29d8:c946:4b39, Dst: ff02::fb
User Datagram Protocol, Src Port: 5353, Dst Port: 5353
Multicast Domain Name System (query)

No.     Time           Source                Destination           Protocol Length
Info
    199 968.780167050  192.168.0.105          192.168.0.255          NBNS     92
Name query NB WPAD<00>

Frame 199: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) on interface
0
Ethernet   II,   Src:   Micro-St_d6:f0:3b   (4c:cc:6a:d6:f0:3b),   Dst:   Broadcast
(ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 192.168.0.105, Dst: 192.168.0.255
User Datagram Protocol, Src Port: 137, Dst Port: 137
NetBIOS Name Service

No.     Time           Source                Destination           Protocol Length
Info
    200 968.986920102  192.168.0.105          192.168.0.255          UDP      305
54915 → 54915 Len=263
```

```
Frame 200: 305 bytes on wire (2440 bits), 305 bytes captured (2440 bits) on
interface 0
Ethernet II, Src: Micro-St_d6:f0:3b (4c:cc:6a:d6:f0:3b), Dst: Broadcast
(ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 192.168.0.105, Dst: 192.168.0.255
User Datagram Protocol, Src Port: 54915, Dst Port: 54915
Data (263 bytes)

0000  00 44 45 53 4b 54 4f 50 2d 41 56 52 38 30 30 37   .DESKTOP-AVR8007
0010  00 b2 ff 0b dd 00 00 00 00 00 00 00 00 00 00 00   ................
0020  33 27 00 00 00 00 00 00 10 57 fe 84 1f 02 00 00   3'.......W......
0030  10 1d e7 85 1f 02 00 00 00 f6 38 84 1f 02 00 00   ..........8.....
0040  00 00 00 00 00 00 00 00 7c 6a ba 5f 00 00 00 00   ........|j._....
0050  f0 a4 68 60 00 00 00 00 09 b7 ff 0b dd 00 00 00   ..h`............
0060  00 00 00 00 00 00 00 00 90 19 e7 85 1f 02 00 00   ................
0070  54 b3 ff 0b dd 00 00 00 70 b3 ff 0b dd 00 00 00   T.......p.......
0080  58 55 32 7b 66 64 62 66 63 34 61 65 2d 38 63 65   XU2{fdbfc4ae-8ce
0090  63 2d 34 65 66 31 2d 38 36 34 36 2d 32 36 31 37   c-4ef1-8646-2617
00a0  39 37 62 38 36 63 31 34 7d 00 00 00 00 00 00 00   97b86c14}.......
00b0  01 00 00 00 00 00 00 00 50 b3 ff 0b dd 00 00 00   ........P.......
00c0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00d0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00e0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00f0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0100  00 00 00 b9 88 3e a7                              .....>.

No.     Time           Source                Destination           Protocol Length
Info
    201 968.989516220  192.168.0.105          224.0.0.251            MDNS     70
Standard query 0x0000 A wpad.local, "QM" question

Frame 201: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface
0
Ethernet II, Src: Micro-St_d6:f0:3b (4c:cc:6a:d6:f0:3b), Dst: IPv4mcast_fb
(01:00:5e:00:00:fb)
Internet Protocol Version 4, Src: 192.168.0.105, Dst: 224.0.0.251
User Datagram Protocol, Src Port: 5353, Dst Port: 5353
Multicast Domain Name System (query)

No.     Time           Source                Destination           Protocol Length
Info
    202 968.989579192  fe80::ac53:29d8:c946:4b39 ff02::fb             MDNS     90
Standard query 0x0000 A wpad.local, "QM" question

Frame 202: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface
0
Ethernet II, Src: Micro-St_d6:f0:3b (4c:cc:6a:d6:f0:3b), Dst: IPv6mcast_fb
(33:33:00:00:00:fb)
Internet Protocol Version 6, Src: fe80::ac53:29d8:c946:4b39, Dst: ff02::fb
User Datagram Protocol, Src Port: 5353, Dst Port: 5353
Multicast Domain Name System (query)

No.     Time           Source                Destination           Protocol Length
Info
    203 969.496965723  Micro-St_d6:f0:3b     Broadcast              ARP      60
Who has 192.168.0.118? Tell 192.168.0.105

Frame 203: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface
0
```

```
Ethernet II, Src: Micro-St_d6:f0:3b (4c:cc:6a:d6:f0:3b), Dst: Broadcast
(ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)

No.     Time           Source                Destination           Protocol Length
Info
    204 969.498351120  192.168.0.105          192.168.0.255          NBNS      92
Name query NB WPAD<00>

Frame 204: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) on interface
0
Ethernet II, Src: Micro-St_d6:f0:3b (4c:cc:6a:d6:f0:3b), Dst: Broadcast
(ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 192.168.0.105, Dst: 192.168.0.255
User Datagram Protocol, Src Port: 137, Dst Port: 137
NetBIOS Name Service

No.     Time           Source                Destination           Protocol Length
Info
    205 970.011775292  192.168.0.105          192.168.0.255          UDP       305
54915 → 54915 Len=263

Frame 205: 305 bytes on wire (2440 bits), 305 bytes captured (2440 bits) on
interface 0
Ethernet II, Src: Micro-St_d6:f0:3b (4c:cc:6a:d6:f0:3b), Dst: Broadcast
(ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 192.168.0.105, Dst: 192.168.0.255
User Datagram Protocol, Src Port: 54915, Dst Port: 54915
Data (263 bytes)

0000  00 44 45 53 4b 54 4f 50 2d 41 56 52 38 30 30 37   .DESKTOP-AVR8007
0010  00 b2 ff 0b dd 00 00 00 00 00 00 00 00 00 00 00   ................
0020  33 27 00 00 00 00 00 00 10 57 fe 84 1f 02 00 00   3'.......W......
0030  10 1d e7 85 1f 02 00 00 00 f6 38 84 1f 02 00 00   ..........8.....
0040  00 00 00 00 00 00 00 00 7c 6a ba 5f 00 00 00 00   ........|j._....
0050  f0 a4 68 60 00 00 00 00 09 b7 ff 0b dd 00 00 00   ..h`............
0060  00 00 00 00 00 00 00 00 90 19 e7 85 1f 02 00 00   ................
0070  54 b3 ff 0b dd 00 00 00 70 b3 ff 0b dd 00 00 00   T.......p.......
0080  58 56 32 7b 66 64 62 66 63 34 61 65 2d 38 63 65   XV2{fdbfc4ae-8ce
0090  63 2d 34 65 66 31 2d 38 36 34 36 2d 32 36 31 37   c-4ef1-8646-2617
00a0  39 37 62 38 36 63 31 34 7d 00 00 00 00 00 00 00   97b86c14}.......
00b0  01 00 00 00 00 00 00 00 50 b3 ff 0b dd 00 00 00   ........P.......
00c0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00d0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00e0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00f0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0100  00 00 00 5d 78 fa ed                              ...]x..

No.     Time           Source                Destination           Protocol Length
Info
    206 972.059068353  192.168.0.105          192.168.0.255          UDP       305
54915 → 54915 Len=263

Frame 206: 305 bytes on wire (2440 bits), 305 bytes captured (2440 bits) on
interface 0
Ethernet II, Src: Micro-St_d6:f0:3b (4c:cc:6a:d6:f0:3b), Dst: Broadcast
(ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 192.168.0.105, Dst: 192.168.0.255
User Datagram Protocol, Src Port: 54915, Dst Port: 54915
```

```
Data (263 bytes)

0000  00 44 45 53 4b 54 4f 50 2d 41 56 52 38 30 30 37   .DESKTOP-AVR8007
0010  00 b2 ff 0b dd 00 00 00 00 00 00 00 00 00 00 00   ................
0020  33 27 00 00 00 00 00 00 10 57 fe 84 1f 02 00 00   3'.......W......
0030  10 1d e7 85 1f 02 00 00 00 f6 38 84 1f 02 00 00   ..........8.....
0040  00 00 00 00 00 00 00 00 7c 6a ba 5f 00 00 00 00   ........|j._....
0050  f0 a4 68 60 00 00 00 00 09 b7 ff 0b dd 00 00 00   ..h`............
0060  00 00 00 00 00 00 00 00 90 19 e7 85 1f 02 00 00   ................
0070  54 b3 ff 0b dd 00 00 00 70 b3 ff 0b dd 00 00 00   T.......p.......
0080  58 58 32 7b 66 64 62 66 63 34 61 65 2d 38 63 65   XX2{fdbfc4ae-8ce
0090  63 2d 34 65 66 31 2d 38 36 34 36 2d 32 36 31 37   c-4ef1-8646-2617
00a0  39 37 62 38 36 63 31 34 7d 00 00 00 00 00 00 00   97b86c14}.......
00b0  01 00 00 00 00 00 00 00 50 b3 ff 0b dd 00 00 00   ........P.......
00c0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00d0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00e0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00f0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0100  00 00 00 34 1d e0 6e                              ...4..n

No.     Time           Source                Destination           Protocol Length
Info
    207 972.979975344  192.168.0.105         192.168.0.255         UDP      305
54915 → 54915 Len=263
```

Prilog 3. Lista riječi

password	111111	george	redskins	gators
123456	shadow	fucker	peanut	fuckoff
tuscl	fuckyou	taylor	heather	florida
stripper	dallas	football	asshole	dancer
qwerty	andrew	blahblah	whatever	cookie
12345	trustno1	biteme	strippers	chicken
12345678	corvette	1escobar2	prince	charlie
1234	sunshine	1111	orange	canada
baseball	harley	tigger	m0ntlure	blowme
monkey	hello	ranger	jeremy	austin
princess	gaydar	chicago	hunter	1234567
stripclub	dragon	bandit	golfer	tarheels
strip	butthead	123456789	yellow	silver
mustang	love	welcome	titties	samantha
abc123	jordan	testing	tiger	private
jennifer	danielle	phoenix	thomas	peekaboo
pussy	buster	jessica	superman	midnight
letmein	batman	gemini	robert	merlin
lapdance	6969	gateway	redsox	lucky1
jmh1978	yankees	badboy	pepper	jasmine
696969	password1	aaaaaa	master	jackass
michelle	michael	654321	maggie	hawaii
brooklyn	lasvegas	tennis	lucky	falcon
braves	hockey	summer	kitten	doctor
brandy	ginger	secret	killer	diamond
boston	8675309	wolfpack	vegas	rogina