SVEUČILIŠTE U ZAGREBU
FAKULTET PROMETNIH ZNANOSTI

Luka Brletić

ANALIZA RANJIVOSTI MREŽNIH USMJERNIKA U IoT OKRUŽENJU

DIPLOMSKI RAD

Zagreb, 2018.

Sveučilište u Zagrebu

Sveučilište u Zagrebu
FAKULTET PROMETNIH ZNANOSTI
Vukelićeva 4, 10000 Zagreb
Diplomski studij

P O T V R D A

kojom se potvrđuje da je student

Luka Brletić

izradio diplomski rad pod naslovom (naziv rada na hrv. i engl. jeziku)

ANALIZA RANJIVOSTI MREŽNIH USMJERNIKA U IoT OKRUŽENJU

VULNERABILITY ASSESSMENT OF ROUTERS IN IoT ENVIRONMENT

u skladu sa zadanim zadatkom, tezama i pravilima struke, te može pristupiti tiskanju rada.

Nadzorni nastavnik:

Zagreb, 14.9.2018

Fakultet prometnih znanosti

DIPLOMSKI RAD

ANALIZA RANJIVOSTI MREŽNIH USMJERNIKA U IoT OKRUŽENJU

VULNERABILITY ASSESSMENT OF ROUTERS IN IoT ENVIRONMENT

Mentor: prof. dr. sc. Dragan Peraković.

Student: Luka Brletić

JMBAG: 0135227800

Zagreb, Rujan 2018.

ANALIZA RANJIVOSTI MREŽNIH USMJERNIKA U IOT OKRUŽENJU

SAŽETAK

Sve većom pojavom uređaja interneta stvari u svakodnevnom životu lokalne mreže diljem svijeta se pretvaraju u IoT okruženja čime se povećava potencijalna površina za napad od strane malicioznih aktera. S druge strane unutar takvih IoT okruženja se pojavljuje potreba za sve većim brojem mrežnih usmjernika kako bi se povećao kapacitet mreže. Ranjivosti u tim mrežnim usmjernicima u takvim situacijama direktno utječe na sigurnost cjelokupnog IoT okruženja. Na tri različita mrežna usmjernika je bila provedena detekcija i analiza ranjivosti pomoću programskih alata, ali i pomoću pristupa fizičkom sučelju na tiskanoj pločici na samim uređajima. Na temelju rezultata napravljena je komparativna analiza kako bi se mogla procijeniti potencijalna šteta unutar IoT okruženja i zatim je dan prijedlog načina zaštite usmjernika unutar IoT okruženja.

KLJUČNE RIJEČI: internet stvari, mrežni usmjernici, sigurnost, detekcija ranjivosti

SUMMARY

With the ever-increasing occurrence of internet devices in the everyday life local networks around the world are transformed into IoT environments, thus increasing the potential surface for attack by malicious actors. On the other hand, within such IoT environments there is a need for an increasing number of network routers to increase network capacity. Vulnerabilities in these network routers in such situations directly affect the security of an entire IoT environment. Three different network routers have been tested and analyzed for vulnerabilities using program tools, as well as by accessing a physical interface on a circuit board of a device. Based on the results, a comparative analysis was carried out to assess potential damage within the IoT environment and then a proposal was made on how to protect the routers within such IoT environment.

KEY WORDS: internet of things, network routers, security, vulnerability detection

SADRŽAJ

1. UVOD

Pojavom sve većeg broja uređaja Interneta stvari (*Internet of Things* - IoT) unutar lokalnih mreža sve većeg broja Internet korisnika takve lokalne mreže postaju IoT okruženja. Povećan broj uređaja koji je potrebno povezati na Internet će predstavljati problem samo jednom mrežnom usmjerniku zbog fizičke lokacije unutar rezidencijalne lokalne mreže. Zbog toga će takvi korisnici biti primorani povećati kapacitet mreže po pitanju mrežnih usmjernika kako bi se podržao veći broj IoT uređaja koji su fizički na udaljenijim lokacijama. U takvim okolnostima generirani promet IoT okruženja se preusmjerava kroz mrežni usmjernik i u slučaju gdje maliciozni čimbenik preuzme kontrolu nad takvim mrežnim usmjernikom cijelo IoT okruženje postaje ugroženo.

U ovom radu će biti provedena komparativna analiza nad tri mrežna usmjernika, Asus RT-N12E, D-Link DIR-600 i TP-Link WR741ND. U toj analizi će biti korišteni sigurnosni alati nad samim mrežnim usmjernicima kako bi se objektivno utvrdila njihova tvornička razina zaštite koju pružaju, bez promjena od strane korisnika. Na svakom uređaju će zatim biti iskorištene pronađene ranjivosti kako bi se utvrdio opseg štete koja bi nastala unutar IoT okruženja, odnosno preuzimanjem kontrole nad istim. Početne korisničke postavke se ne mijenjaju jer se pretpostavlja kako većina korisnika neće mijenjati postavke mrežnog usmjernika te će se na taj način dobiti stvarniji prikaz IoT okruženja.

U drugom poglavlju će biti predstavljene osnove sigurnosti i analiza IoT okruženja, biti će opisan pojam IoT-a, zatim opisani temeljni pojmovi sigurnosti informacijsko-komunikacijskog sustava i na kraju poglavlja će biti opisano kako se ti pojmovi prenose u IoT okruženje. U trećem poglavlju će biti napravljena analiza i detekcija ranjivosti nad trima mrežnim usmjernicima Asus RT-N12E, D-Link DIR-600 i TP-Link WR741ND. Nakon toga će u četvrtom poglavlju biti napravljena komparativna analiza dobivenih rezultata kako bi se mogao dobiti uvid u ranjivosti mrežnih usmjernika u kategoriji malih mrežnih usmjernika na temelju čega bi se mogla procijeniti šteta u IoT okruženju.

U petom poglavlju će biti razmatrani dosadašnji prijedlozi za zaštitu mrežnih usmjernika i njihovi nedostaci, zatim će na temelju rezultata komparativne analize iz prethodnog poglavlja biti predstavljen prijedlog načina zaštite mrežnih usmjernika unutar IoT okruženja na način koji najviše ograničava štetu u slučaju sigurnosne ugroze. U šestom, i zadnjem poglavlju, će na temelju dobivenih rezultata komparativne analize i prijedloga rješenja biti izveden zaključak ovoga rada.

2. OSNOVE SIGURNOSTI I ANALIZA IoT OKRUŽENJA

U ovom poglavlju će biti razjašnjeni osnovni pojmovi koji se dotiču glavne teme ovoga rada, kao što je Internet stvari, osnovni pojmovi informacijske sigurnosti te na kraju kako se svaka pojedinačna definicija odnosi na Internet stvari i koje su bitne razlike u takvom okruženju u odnosnu na tradicionalni informacijsko-komunikacijski sustav.

2.1. Internet stvari

Internet stvari (*Internet of Things* - IoT) je jednostavan koncept povezivanja uređaja iz svakodnevne uporabe s Internetom, koji unatoč svojoj jednostavnosti ima široku i složenu primjenu u poslovnom okruženju. IoT čini cijeli sustav svih povezanih uređaja koji mogu biti računalni, mehanički, objekti ili predmeti iz svakodnevne uporabe. Povezivanjem uređaja na Internet originalni proizvođač omogućuje proširenje funkcionalnosti uređaja te može krajnjem korisniku nuditi dodatne usluge koje nisu bile uključene u osnovnu cijenu uređaja ako krajnji korisnik, osoba ili tvrtka koja koristi uređaj/usluge, pristane na dodatni oblik plaćanja. S ovakvim prednostima koje donosi IoT na tržištu se pojavio veliki broj IoT uređaja odnosno veliki broj uređaja je pretvoren u IoT od kojih su najraniji bili IoT termostati, [1].

Jedan od najvećih proizvođača mrežne opreme Cisco Systems, Inc, čija je vrijednost procijenjena na više od 130 milijardi američkih dolara u 2017. godini, nudi svoja IoT rješenja u području energije, manufakture, transporta, gradova, prodaje i edukacije. Cisco proizvodi uređaje te softverska rješenja u području IoT-a te tako nudi cijeli ekosustav. Rješenja se nude za povećanje sigurnosti u prometu do povećanja kompetitivne prednosti u logistici i transportu. Ako se pretpostavi da je cijeli ekosustav siguran i neprobojan, sama komunikacija je komprimirana činjenicom da se može odvijati nesigurnom informacijsko-komunikacijskom mrežom čiji su mrežni usmjernici komprimirani ili imaju instaliran zlćudni softver, [2].

Proizvođači su korištenjem IoT-a dobili mogućnost tranzicije svojeg poslovno modela u softver kao usluga (*Software as a Service* - SaaS). SaaS omogućuje proizvođaču kontrolu softvera na daljinu u obliku softverskih nadogradnji. U slučaju u kojemu krajnji korisnik se ne odluči na novije funkcionalnosti na njegovom uređaju one neće biti omogućene. Ovo omogućuje granulaciju inicijalne baze korisnika na preciznije dijelove koje omogućuju proizvođaču veće profitne marže. Uz to svaki uređaj koji je povezan na Internet može slati i primati informacije te tako proizvođači mogu primati statistike korištenja svojih uređaja i na temelju toga planirati buduće poslovne strategije. IoT uređaji će radi toga unutar sebe imati određeno računalno sklopovlje koje mora podržavati primanje i slanje informacije te djelovanje na temelju dobivenih informacija.

Razvoj IoT tehnologija ujedno zahtijeva i velika ulaganja. Prema *Gartner-u* ulaganja u IoT će dosegnuti preko 3 milijarde američkih dolara u 2021. godini što je prikazano u tablici 1. U njoj se može primijetiti kako se od 3 kategorije na koje je *Gartner* podijelio poslovanje u IoT industriji najveći dio odnosi na profesionalne usluge dok će se najmanje ulagati u sigurnost. Razlog tome se može pretpostaviti što će tvrtke pridodavati veći prioritet djelatnosti koja im donosi dobit. Kako su ulaganja visoka tako i potencijalni gubitci postaju još veći, pogotovo ako se pri napadu na IoT mrežu iskoristi ranjivost u samim IoT uređajima

kao što je to bio napad zlođudnog softvera *Mirai* na web stranicu „Krebs on Security“ 2016. godine koji je iskoristio oko 600 000 zaraženih IoT uređaja i tada oborio rekord i napravio najveći distribuirani napad prekida usluga (*Distributed Denial of Service* - DDoS) napad u povijesti, [3].

Tablica 1.Prognoza ulaganja u IoT prema Gartneru u milijunima američkih dolara

Godina	**2016**	**2017**	**2018**	**2019**	**2020**	**2021**
Krajnja sigurnost	240	302	373	459	541	631
Sigurnost *gateway*-a	102	138	186	251	327	415
Profesionalne usluge	570	734	946	1221	1589	2071
Ukupno	912	1174	1506	1931	2457	3118

Izvor: [4]

Zbog natjecanja na tržištu proizvođači IoT uređaja su potekli iz već postojećih kompanija koje imaju iskustva s elektroničkim uređajima, kao što su Samsung ili Toshiba, ali i iz kompanija koji do sada nisu imali nikakva iskustva s programskom podrškom kao što su proizvođači termostata i kućanskih pomagala kao što je pametna klimatizacija ili pametne utičnice za struju i žarulje [5].

Kako se proizvođači međusobno natječu u dostavljanju uređaja na tržište u što kraćem vremenskom periodu tako je sam razvoj softvera ubrzan i naglasak je stavljen na funkcionalnost, a ne sigurnost programskog koda. Ubrzan razvoj softvera većinom podrazumijeva agilni razvoj softvera. Agilni razvoj softvera se temelji na četiri glavna principa prema *Agile Alliance* [6], a to su:

1. Individualizam i interakcije iznad procesa i alata
2. Funkcionalan softver iznad čitljive dokumentacije
3. Suradnja korisnika iznad ugovaranja uvjeta
4. Odgovaranje na promjene iznad slijeđenja plana

Prvi princip stavlja u prednost znanje individualne osobe u timu, iznad korištenja skupocjenih profesionalnih alata. Drugi princip stavlja funkcionalan softver iznad toga da on bude provjeren i dokumentiran dok je treći princip fokusiran na suradnju sa samim naručiteljem softvera, a zadnji se fokusira na ponašanje u varijabilnom tržišnom okruženju. Upravo zbog drugog principa proizlaze ranjivosti u softveru koje se onda manifestiraju u samim IoT uređajima. Sam primjer ranjivosti softvera će biti demonstriran u četvrtom poglavlju ovoga rada.

U slučajevima u kojima su ranjivosti otkrivene dio proizvođača nije u stanju poduzeti konkretne mjere sprečavanja nastajanja štete jer nisu u stanju promijeniti jezgreni softver IoT uređaja, odnosno njegov *firmware* koristeći mrežnu nadogradnju. U tim slučajevima ranjivi IoT uređaji ostaju povezani na Internet od strane korisnika koji nisu ni svjesni rizika. Takvi IoT uređaji postaju dio velikih automatiziranih mreža, takozvanih *botneta*. *Botnet* čini mrežu povezanih uređaja koji su pod kontrolom treće strane, odnosno niti korisnik niti proizvođač ima kontrolu nad njima. Ta treća strana u većini slučajeva ima maliciozne namjere te takve mreže IoT uređaja može koristiti u DDoS napadima..

IoT okruženje se na temelju toga može definirati kao dio mreže u kojoj se osim osobnih računala i pametnih telefona i ostalih mrežnih uređaja nalazi i veliki broj IoT uređaja različitih proizvođača i namjena koji koriste stalni pristup Internetu za obavljanje svoje svrhe. IoT uređaj mora zadovoljiti jednostavnu premisu primanja i slanja informacija te djelovanja na temelju tih informacija. Sama povezanost na Internet omogućuje brojne dodatne funkcionalnosti koje ovise o kontekstu poslovnog okruženja u kojemu se koriste, ali i ujedno stvaraju potencijalnu površinu za napad.

2.2. Sigurnost informacijsko komunikacijskog sustava

Komunikacijska sigurnost se može definirati kao sigurna komunikacija i prijenos podataka između izvorišta i odredišta. Informacijska sigurnost se može definirati kao sprječavanje neautoriziranog pristupa, korištenja, otkrivanja, ometanja ili uništavanja informacije. Sigurnost informacijsko-komunikacijskog (IK) sustava podrazumijeva kombinaciju oba elementa sigurnosti, jednog koji se odnosi na statičku informaciju i drugi koji se odnosni na dinamičku informaciju, odnosno informaciju u transportu što se naziva komunikacija. S obzirom na tip informacije ne rade se podjele već se podrazumijeva informacija u bilo kojem obliku, bilo fizičkom bilo elektroničkom, [7].

Informacijsko-komunikacijski sustav je kompleksan i sastoji se od sklopovlja ili hardvera, softvera, organizacije, mrežnih komponenti, ljudskih resursa te baza podataka. Svaka od ovih komponenti ako je komprimirana predstavlja opasnost za cijeli sustav čak i ako druge komponente nisu ugrožene i normalno izvršavaju svoju zadaću. IK sustav treba održati integritet, dostupnost i povjerljivost i u isto vrijeme održavati fokus na produktivnost. Sa strane obrane sustava moraju se štiti sve tri komponente dok sa strane napadača mora se ugroziti samo jedna kako bi se ugrozio cijeli sustav što čini zadatak obrane IK sustava puno složeniji od napada. IK sigurnost razlikuje prijetnje i ranjivosti, imovinu, kontrolu pristupa te upravljanje rizikom koje podrazumijeva identifikaciju ranjivosti i prijetnji kako bi se mogle uspostaviti protumjere, [7], [8].

Povjerljivost podataka prema ISO 27000 standardu podrazumijeva činjenicu da se informacija ne otkriva i ne čini dostupnom neautoriziranih pojedinaca, entitetima ili procesima. Povjerljivost se može promatrati i kao dio privatnosti koji implementira mehanizme za zaštitu privatnih podataka. Prema ISO 27000 standardu integritetom se smatra jamstvo točnosti podatka tijekom njegovog životnog ciklusa. Što znači kako podaci ne smiju biti modificirani na neautoriziran način ili na način da se ne može detektirati promjena. Dostupnost prema ISO 27000 standardu je svojstvo IK sustava da služi svojoj

svrsi i ispunjava svoj cilj tijekom svog postojanja bez prekida, čak i rijekom održavanja sustava. Visoka dostupnost može zahtijevati visoku razinu ljudskih, materijalnih i novčanih resursa te se s obzirom na namjenu samog sustava dizajnira razina dostupnosti, [9].

Prijetnja predstavlja objekt koji vrši ugrozu na sustav i dolazi u obliku softverskih prijetnji, prijetnji u obliku zlonamjernog osoblja i vanjskih napadača te prirodnih prijetnji. Moguće pripreme na prijetnje su smanjene odnosno izbjegavanje štete gdje je to moguće u slučaju napada na IK sustav, prihvaćanje prijetnji u obliku da se unaprijed izračunaju troškovi kako bi se šteta odmah mogla sanirati te prebacivanje prijetnje gdje se primjena zaštite od ugroze prebacuje na drugi entitet, na primjer *outsourcing* na vanjsku specijaliziranu tvrtku. Prema ISO 27005 standardu za upravljanje rizikom prijetnja je potencijalni uzrok incidenta koji može rezultirati štetom za sustave ili organizacije, [10].

Ranjivošću se smatra onim što se može iskoristiti od strane napadača da ugrozi sustav. Napadači koriste razne tehnike i alate za iskorištavanje takvih ranjivosti. Ranjivosti mogu biti u bilo kojoj komponenti IK sustava. To može biti krivo konfigurirana baza podataka, softver ili hardver s greškama pa i ljudski čimbenici unutar samog sustava. Sama definicija prema ISO 27005 standardu kaže kako je ranjivost imovine ili grupe imovine onaj čimbenik koji može biti iskorišten od jedne ili više prijetnje, [10].

Rizik u IK sustavu je definiran kao potencijal da prijetnja iskoristi ranjivosti sustava i time prouzroči štetu imovini, sve ono što ima vrijednost za ispunjenje cilja sustava. Upravljanje rizikom uključuje metode pomoću kojih se identificiraju i karakteriziraju prijetnje, procijene se ranjivosti imovine, odredi se rizik, pronađu se načini za smanjivanje rizika te se mjere za smanjivanje rizike kategoriziraju po prioritetu, [10].

Šteta je definirana kao posljedice koje nastanu jer je ranjivost iskorištena. Može se procijeniti na temelju vrijednosti imovine koja je se nalazi pod rizikom. Kako bi se smanjila šteta potrebno je provesti kontrolu rizika. Kontrola rizika je niz postupaka čiji je cilj smanjiti ukupnu štetu u slučaju u kojemu je ranjivost iskorištena na dijelu ili cijeloj imovini sustava. Potrebno je identificirati svu imovinu, odnosno sve dijelove sustava koji su bitni za ostvarivanje cilja sustava. Na temelju identificirane imovine se identificiraju prijetnje da bi se na temelju tih prijetnji identificirale ranjivosti koje mogu biti iskorištene. Nakon utvrđivanja rizika na temelju otkrivenih ranjivosti se procjenjuju rizici i metode za njihovo izbjegavanje, [11].

Napadi na sustav će imati manje uspjeha ako je napadačka površina, odnosno sve ranjivosti koje sustav sadržava, manja. Dok se neke ranjivosti mogu ukloniti druge će ostati zbog izvršavanja funkcionalnosti te će se morati raditi protumjere u slučaju da one budu iskorištene. Kako informacijska sigurnost mora štiti informaciju cijeli životni ciklus postoji puno načina kojima se može ugroziti informacijska sigurnost. Pristup zaštiti informacije gdje u slučaju da jedna komponenta IK sustava bude probijena od strane napadača, a druge komponente i dalje pružaju zaštitu se zove obrana u dubinu, [12].

Kako bi se odredila potrebna razina zaštite potrebno je klasificirati informacije prema njihovoj važnosti za funkcioniranje sustava. Na temelju klase kojoj propada određuje se

osoblje koje može rukovati takvim informacijama. Zatim se određuju oznake, kriteriji za određene oznake te se na kraju dodaju sigurnosne kontrole za svaku klasu informacije, [13].

Kontrola pristupa se može podijeliti na tri dijela, identifikaciju, autentikaciju i autorizaciju od koji svaki idući uključuje prethodni, korisniku ne smiju biti dodijeljene autorizacijske ovlasti ako nije identificiran. Identifikacija je pretpostavka o identitetu nečega ili nekoga. Kod web aplikacija identifikacija korisnika se u većini slučajeva vrši na temelju korisničkog imena. Identitet nije potvrđen dok se ne obavi autentikacija. Autentikacija je postupak potvrđivanja iznošenog identiteta nečega ili nekoga. U mrežnoj komunikaciji moguće je koristiti kriptografske ključeve koji će potvrditi identitet, ali samo u slučaju gdje su takvi ključevi distribuirani jednom entitetu jednom i nije ih moguće reproducirati. Korisnici web aplikacija svoj identitet, korisničko ime, potvrđuju lozinkom. Nakon što je pretpostavljen identitet entiteta i potvrđen autentikacijom moguće je provesti autorizaciju. Autorizacija je postupak dodjeljivanja ovlasti korisniku ili entitetu. Korisnicima koji potvrde identitet administratora će biti dodijeljene administratorske ovlasti, [11].

Tako se primjenjujući ove definicije prijava korisnika u web sučelje mrežnog usmjernika može opisati u 3 koraka. Korisnik se identificira unošenjem korisničkog imena u web sučelje mrežnog usmjernika, korisnik potvrđuje svoju identifikaciju unošenjem ispravne lozinke za to korisničko ime i korisniku su dodijeljene ovlasti na mrežnom usmjerniku na temelju razine ovlasti koje su definirane za identificirani korisnički račun. Sva tri mrežna usmjernika nad kojima je provedena analiza u četvrtom poglavlju imaju web sučelje koje funkcionira na opisan način i jedini korisnički račun koji dolazi s tvorničkim postavkama jest administratorski i nije moguće dodati nove korisničke račune.

2.3. Sigurnost u IoT okruženju

Ako se IoT okruženje promatra iz perspektive IK sustava onda su svi elementi koji su podložni napadu, odnosno sadržavaju ranjivosti, koji odgovaraju elementima IK sustava su potencijalna površina za napad. Jedna od najvećih prepreka masovnom usvajanju IoT uređaja je upravo sigurnost, u anketi „Buisness Insider Intelligence Survey“ koju je provela američka publikacija *Buisness Insider* 39% ispitanika se izjasnilo da je sigurnost i privatnost IoT okruženja njihova najveća zabrinutost, [14].

Kako bi se bolje odgovorilo na prijetnje koje su se pojavile u IoT okruženju, 2015. godine je osnovana zaklada za sigurnost interneta stvari (*Internet of Things Security Foundation – IoTSF*) čija je glavna zadaća promicanje znanja i najboljih praksi za IoT uređaje i okruženje. Osnivačka skupina se sastoji od pružatelja telekomunikacijskih usluga kao što su BT, Vodafone, Imagination Technologies i Pen Test Partners. IoTSF izdaje dokument za najbolje prakse i na temelju provođenja tih praksi kompanije dobivaju službenu oznaku, [15].

IoTSF kategorizira pridržavanje najboljih praksi u 5 klasa i u 3 glavna cilja informacijske sigurnosti, integritet, dostupnost i povjerljivost. Svaku klasu obilježavaju

različite razine integriteta, dostupnosti i povjerljivosti. Navedena kategorizacija se može vidjeti u tablici 2.

Tablica 2. IoTSF tablica klasa pridržavanja najboljih praksi sigurnosti u IoT okruženju

Klasa najboljih praksi	**Sigurnosni cilj**		
	Integritet	**Dostupnost**	**Povjerljivost**
Klasa 0	Osnovni	Osnovna	Osnovna
Klasa 1	Srednji	Srednja	Osnovna
Klasa 2	Srednji	Visoka	Srednja
Klasa 3	Srednji	Visoka	Visoka
Klasa 4	Visoki	Visoka	Visoka

Izvor: [16]

Osnovni integritet je opisan kao skup uređaja čija ugroza mogu prouzročiti malu ili srednju štetu pojedinim osobama ili poduzećima. Srednji integritet označava uređaje čija ugroza uzrokuje ograničene posljedice na poduzeće dok visoki stupanj integriteta označava uređaje čija ugroza znači katastrofalne posljedice za pojedinu osobu ili poduzeće. Osnovna dostupnost označava uređaje čiji se nedostatak u mreži može jedva primijetiti u okviru posljedica. Srednja razina dostupnosti označava uređaje čiji nedostatak uzrokuje ograničenu štetu dok visoka razina dostupnosti označava uređaje čiji nedostatak izvršavanja njihove zadaće ima značajan utjecaj na pojedinca ili poduzeće, [16].

Također kod povjerljivosti osnovna razina označava usluge ili uređaje koji obrađuju javne informacije, srednja razina povjerljivosti označava uređaje i usluge koji obrađuju osjetljive informacije, uključujući informacije koje se neposredno mogu povezati s osobama i čije kršenje povjerljivosti može imati ograničeni utjecaj na pojedinca ili poduzeće i dok na kraju visoka razina povjerljivosti se odnosi na uređaje i usluge koji obrađuju jako osjetljive informacije, [16].

Što se tiče površine napada IoT uređaji imaju otvorenu još jednu stranu napada koja nije prisutna kod klasičnih poslužitelja i opreme poduzeća, a to jest fizički pristup IoT uređaju od strane napadača. Ova površina napada je prisutna zbog toga što je većina IoT uređaja komercijalno dostupna i time napadači mogu analizirati sve ranjivosti opreme bez prijetnje od otkrivanja napada. Kao primjer mogu poslužiti IoT termostati koji mogu biti instalirani kod pojedinca ili u zgradi poduzeća, ali ih i napadač može nabaviti u komercijalnoj prodaji i pronaći njihove ranjivosti. Time cijeli koncept „pametne kuće“ takozvani *Smart Home* postaje

nova površina za napad koja se mora štititi i imati određenu razinu povjerljivosti, integriteta i dostupnosti, [17].

S gledišta IK mrežne komponente sustava, napad na IoT uređaj se može izvršiti na sam IoT uređaj, na njegovu komunikaciju i na odredište njegove komunikacije. U slučaju napada uređaju može biti komprimiran *firmware*, uređaj može imati grešku u hardveru, ili platforma na kojoj je sagrađen ima temeljne propuste u sebi. Napad na komunikaciju se može izvršiti u bilo kojoj točci komunikacije, koja može biti prisluškivana čime se narušava povjerljivost, može biti izmijenjena čime se narušava integritet ili može biti prekinuta ili preusmjerena na drugu lokaciju čime je narušena dostupnost.

Kako se komunikacija na Internetu odvija pomoću mrežnih usmjernika komprimiranjem mrežnog usmjernika se može narušiti komunikacija IoT uređaja bilo presretanjem bilo preusmjeravanjem ili jednostavnim prekidom. Ovaj dio se najviše odnosi na IoT uređaje koji koriste način komunikacije objavljivanje-pretplata. Taj način komunikacije rješava problem objavljivanja informacije svim zainteresiranim stranama, ali krivo implementiran predstavlja ranjivost što je otkriveno od strane računalnog znanstvenika Junade Ali iz tvrtke *Cloudflare* koji je primijetio kako većina proizvođača radi krivu implementaciju ove vrste komunikacije između IoT uređaja. Kod takve vrste komunikacije IoT uređaj A koji očekuje pri ispunjenju zadanih uvjeta poruku od drugog IoT uređaja B će poslati zahtjev za „pretplatu“. U njemu će biti opisani uvjeti pod kojima će IoT uređaj B slati poruku i što će u njoj biti sadržano. Time se IoT uređaj A „pretplatio“ na poruke IoT uređaja B. Problem kod ovakve vrste komunikacije između IoT uređaja jest što proizvođači ne implementiraju provjeru identiteta pošiljatelja poruke i zbog toga je moguće napraviti DDoS napad slanjem ovakvih poruka između IoT uređaja, [18].

Uz komunikaciju, ono što je primijećeno u istom istraživanju jest kako proizvođači IoT uređaja ne enkriptiraju *bootloader*. *Bootloader* je programski kod na samom IoT uređaju koji se nalazi u stalnoj memoriji i kod paljenja uređaja on se prvi pokreće i njegova zadaća je pokretanje glavnih softverskih komponenti IoT uređaja. Kako sam *bootloader* nije enkriptiran tako je moguće pri rastavljanju IoT uređaja fizičkim spajanjem na uređaj preuzeti *bootloader* na računalo. Napadač zatim može analizirati *bootloader* i pronaći ranjivosti te ga izmijeniti i instalirati izmijenjeni na uređaj. Takav IoT uređaj je komprimiran i s njega se maliciozni kod može širiti na ostale IoT uređaje u mreži slanjem komunikacijskih poruka s malicioznim kodom, [18], [19].

3. DETEKCIJA RANJIVOSTI U MREŽNIM USMJERNICIMA

Osim drugih IoT uređaja koji sudjeluju u komunikaciji i mogu biti maliciozni jer u sebi sadržavaju zloćudan softver, mrežni uređaji kao što su preklopnici i usmjernici također mogu biti maliciozni ako su pod nadzorom napadača ili krivo konfigurirani. Krivo konfiguriran mrežni usmjernik može slati razne poruke u IoT mreži na krivo odredište i nenamjerno na tom odredištu izazvati prekid dostupnosti. Poruke mogu biti presretane i njihov sadržaj zatim otkrivan trećoj strani ili se mogu krivo konfigurirati sigurnosni certifikati.

Kako bi se otkrile takve ranjivosti moguće je koristiti softverski i hardverski pristup. Softverski pristup podrazumijeva korištenje programskih alata koji su napravljeni za analizu i pronalaženje ranjivosti kao što je *Routersploit*, jedan od standardnih alata koji dolazi s operativnim sustavom Kali Linux, čija je svrha penetracijsko testiranje IK sustava ili alate za presretanje komunikacije kao što je *Burp Proxy*. Hardverski pristup podrazumijeva fizički pristup komunikacijskim sučeljima kao što je univerzalni asinkroni primopredajno sklopovlje (*Universal Asynchronous Receiver-Transmitter* - UART) koji se nalazi na tiskanoj pločici od mrežnog usmjernika, ili bilo kojem drugom sklopovlju kojemu je moguće fizički pristupiti, a nalaze se na tiskanoj pločici, [20], [21].

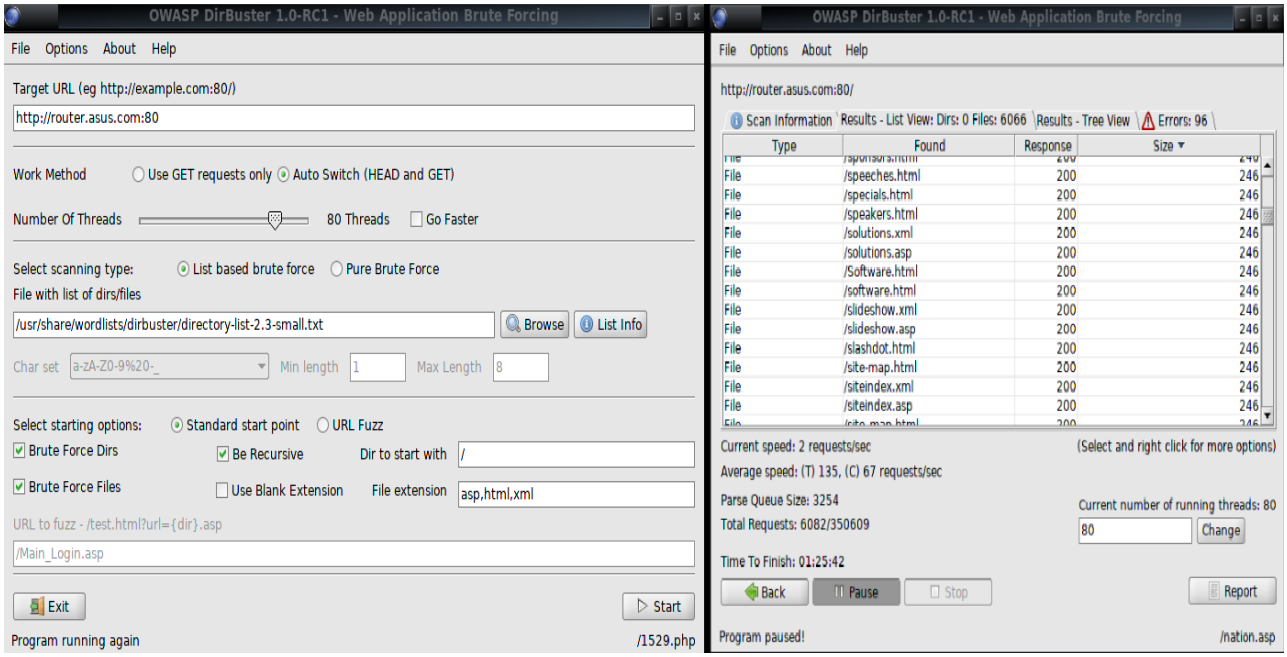
3.1. Detekcija ranjivosti korištenjem softverskih alata

Softverski alati za analizu i detekciju ranjivosti koriste hipertekst transportni protokol (*Hyper Text Transport Protocol* – HTTP) za skeniranje adrese na kojoj se nalazi mrežni usmjernik ili koriste baze poznatih ranjivosti i automatski ih testiraju dok i time pronalaze sve ranjivosti koje se mogu iskoristiti. U ovom poglavlju će biti objašnjen postupak korištenja alata *DirBuster*, *Nmap*, *Routersploit* i *Burp Proxy*.

3.1.1. *DirBuster*

DirBuster je programski alat napisan u Java programskom jeziku koji radi na principu generiranja svih mogućih kombinacija lokatora sadržaja (*Uniform Resuorce Locator* – URL). URL je putanja do određene datoteke ili mape koji se nalazi na poslužitelju. Kako mrežni usmjernici podržavaju web sučelje preko kojeg se vrši administracija uređaja moguće je pomoću *DirBustera* otkriti sakrivene mape kojima je moguće pristupiti bez autorizacije, a u kojima se može nalaziti osjetljivi sadržaj, [22].

Alat se koristi grafičkim sučeljem i podržava samo operativne sustave temeljene na Linux kernelu. Na lijevoj strani slike 1 je primjer korištenja navedenim alatom. Potrebno je upisati URL koji vodi do poslužitelja na kojemu se žele pronaći sve mape. U slučaju ovog rada to je adresa 192.168.1.1 što je standardna adresa za komercijalne mrežne usmjernike. Na slici 1 je moguće vidjeti dobivene rezultate. *DirBuster* nema mogućnost iskorištavanja ranjivosti, njegova uloga je samo detekcija dok se drugim alatima ranjivosti mogu iskoristiti.



Slika 1. Lijevo: početno sučelje *DirBuster* programskog alata. Desno: prikaz rezultata skeniranja web poslužitelja

U rezultatima je prikazan URL put do sadržaja, tip koji može biti datoteka ili mapa, vrsta odgovora, veličina datoteke ili mape te status. Odgovori su u standardnom HTTP troznamenkastom obliku, gdje prva znamenka označuje vrstu odgovora dok ostali brojevi označuju kontekst odgovora. HTTP odgovori koji započinju sa znamenkom dva označuju uspješno povezivanje na URL poslužitelja, i vraćaju se od strane poslužitelja samo u uspješnom slučaju. U slučaju krivog URL-a ili neke druge pogreške na strani klijenta koji generira URL zahtjeve prema poslužitelju poslat će se odgovor koji započinje sa znamenkom četiri, [23].

3.1.2. *Nmap*

Nmap je programski alat otvorenog koda koji služi za otkrivanje uređaja na mreži kao i potencijalnih ranjivosti. Koristi se IP paketima na način na kojem je moguće otkriti spojene uređaje na mreži i skenirati njihove portove. U stanju je pružiti informacije i koja se aplikacija koristi iza porta te u nekim slučajevima čak i njenu verziju. U stanju je detektirati ako mreža koristi vatrozid ili oblik filtracije paketa, [24].

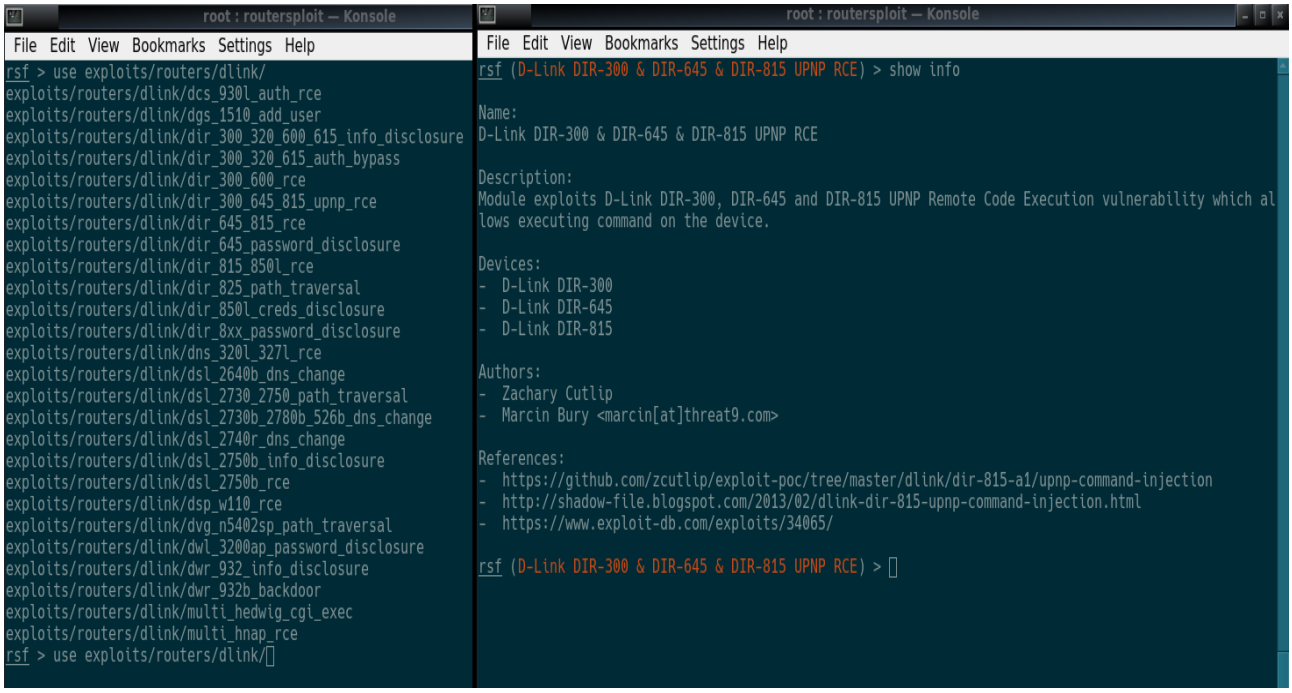
Iako je dizajniran za brzo skeniranje velikih mreža može se i koristiti i za analizu mrežnog sučelja samo jednog uređaja na mreži. Za razliku od ostalih alata dostupan je za sve glavne operativne sustave te osim tekstualnog sučelja ima i grafičko sučelje naziva *Zenmap*. Glavni parametri bez kojih alat ne može početi skeniranje su IP adresa jednog ili više uređaja koji se žele skenirati. U ovom radu *Nmap* će se koristiti za otkrivanje otvorenih portova mrežnog usmjernika na strani lokalne mreže.

3.1.2. *Routersploit*

Routersploit je programski alat koji je isključivo napravljen za analizu, otkrivanje i iskorištavanje ranjivosti na mrežnim usmjernicima. Ima i mogućnost probijanja lozinki kojima su zaštićena administrativna sučelja. Alat je otvorenog koda i osnovna zadaća mu je pomoći pri penetracijskom testiranju. Za razliku od prošlog alata *DirBuster*, puno je opširnijih

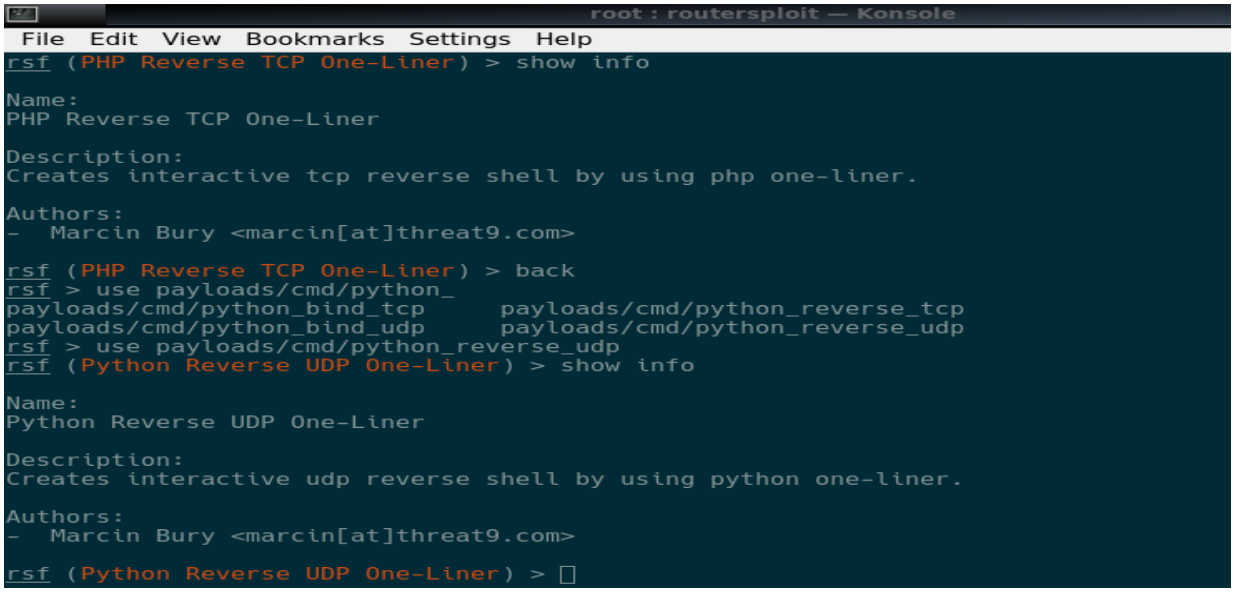
mogućnosti, ali ima samo tekstualno sučelje te također radi samo na operativnim sustavim koji se temelje na Linux kernelu, [20].

Na lijevoj strani slike 2 je moguće vidjeti naveden popis ranjivosti koje su pronađene za mrežne usmjernika od proizvođača D-Link. Pri odabiru određene ranjivosti moguće je dobiti uvid u njene specifičnosti što se vidi na desnoj strani slike 2.



Slika 2. Lijevo: popis ranjivosti koji su pronađene za mrežne usmjernika od proizvođača D-Link. Desno: informacije o modulu za iskorištavanje ranjivosti

Alat djeluje preko modula, koji mogu biti skeneri, koji skeniraju zadanu adresu u potrazi za ranjivostima i parametri koji će se pokušavati iskoristiti. Alat je također u mogućnosti prikazati koji su otvoreni portovi na adresi mete nakon skeniranja. Na temelju toga korisnik može donijeti daljnju odluku kojom metodom iskorištavanja ranjivosti će se koristiti. Dok neke ranjivosti kao ulazni parametar koriste samo adresu mrežnog usmjernika drugi podržavaju ubacivanje zloćudnog tereta, takozvanog *payload*-a u samu poruku koja će se poslati, od kojih su dva takva prikazana na slici 3, jedan koji koristi protokol za kontrolu transmisije (*Transmission Control Protocol* – TCP), dok drugi koji koristi protokol s korisničkim datagramima (*User Datagram Protocol* – UDP).



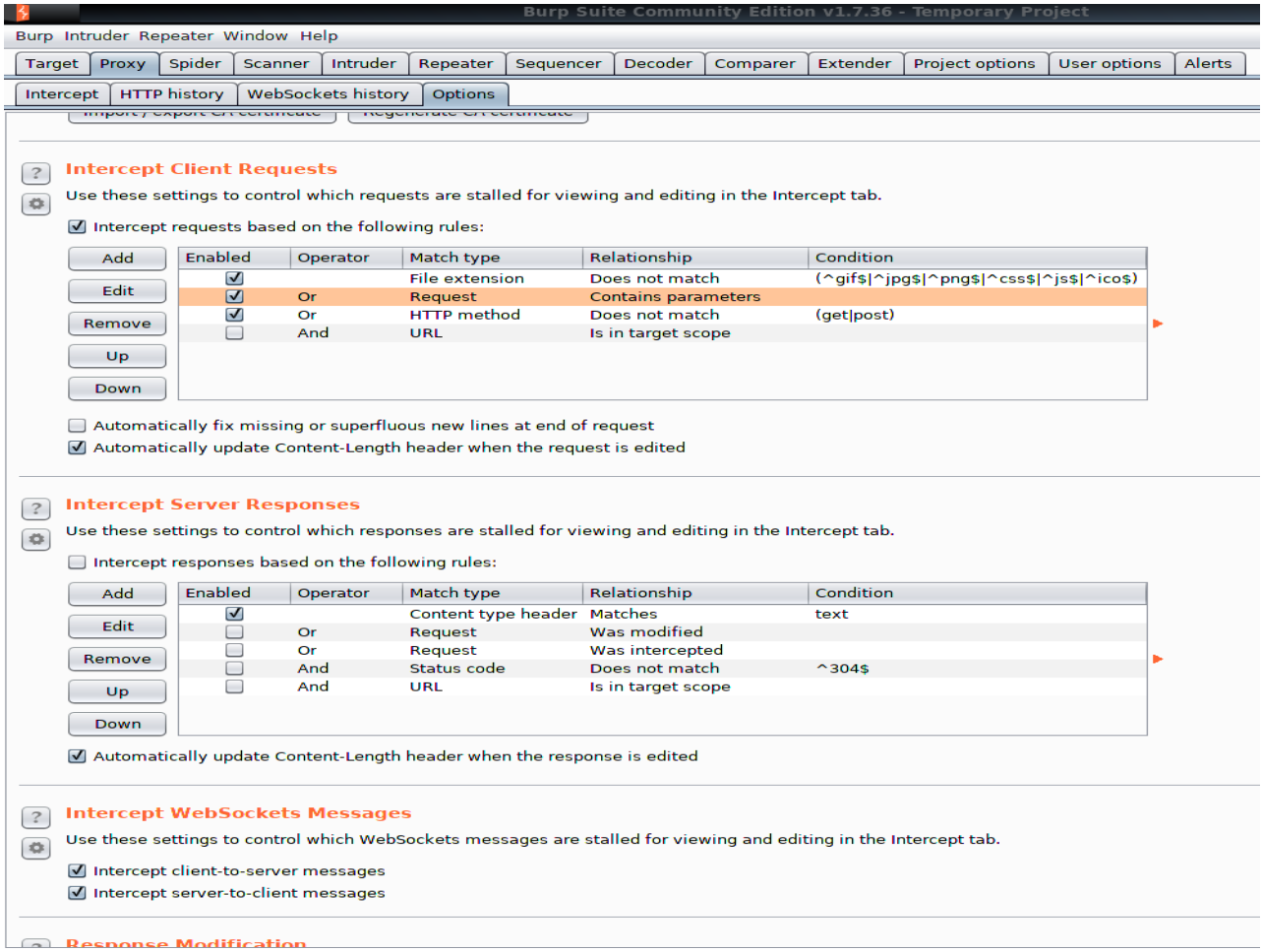
Slika 3. Informacije o zlođudnim teretima za udaljeno izvršavanje koda preko UDP i TCP protokola u programskom alatu *Routersploit*

Kako se povećavaju poznate baze ranjivosti tako se ažuriraju i moduli unutar samog alata čime mu se povećavaju mogućnosti. Uz to kako je alat otvorenog koda podržava ubacivanjem modula od strane korisnika čime mu se dodatno mogu proširiti mogućnosti.

3.1.3. *Burp Proxy*

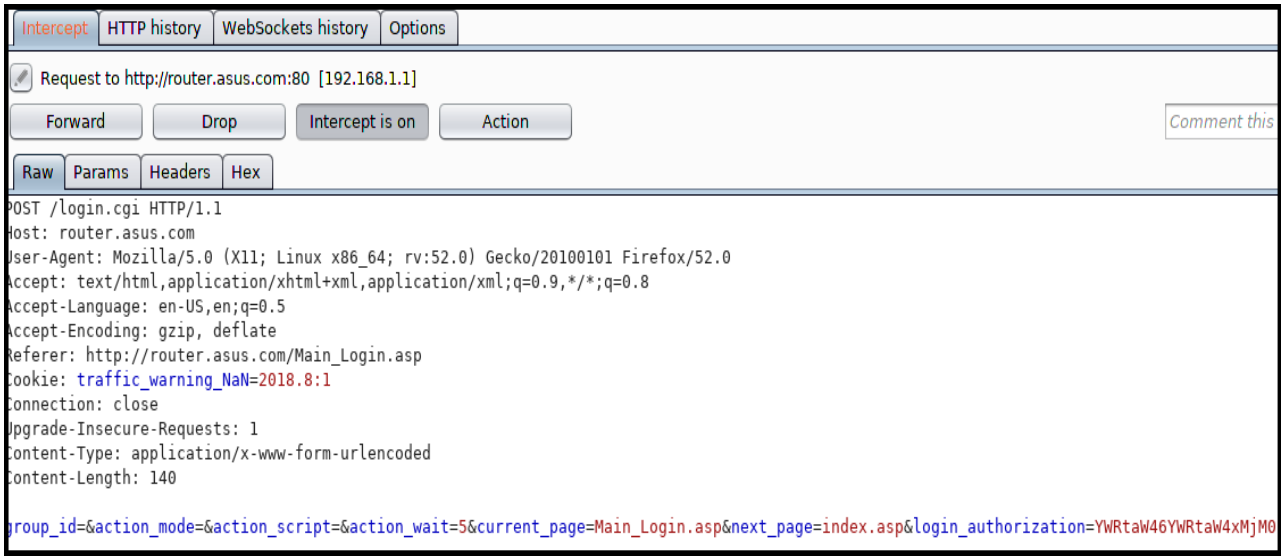
Burp Proxy je svestrani programski alat za analizu, presretanje komunikacije te iskorištavanje ranjivosti koji je dio većeg programske platforme *Burp Suite*. Primarna namjena mu je integracija s web aplikacijama u svrhu njihovog sigurnosnog testiranja. Također sadrži i modul za automatsko skeniranje i traženje ranjivosti web aplikacije na zadanoj Internet adresi. Mogućnost alata koja je najviše korisna u traženju ranjivosti mrežnih usmjernika jest mogućnost konfiguriranja *Burp Proxy* alata za presretanje komunikacije između web preglednika i odredišta, [25].

Na slici 4 su vidljive opcije koje moraju biti omogućene za uključivanje prisluškivanja komunikacije između web preglednika i poslužitelja web lokacije. *Burp Proxy* će nakon toga bilježiti svaku HTTP poruku, ali neće izmjenjivati komunikaciju. Kako bi se to omogućilo potrebno je propustiti HTTP poruku nakon što je poslana od strane klijenta odnosno web preglednika. Nakon što se poruka presretne moguće ju je modificirati i zatim poslati prema odredištu. Ovo predstavlja ranjivost u slučaju u kojemu se autorizacija i autentikacija korisnika na web odredištu radi na strani klijenta u web pregledniku.



Slika 4. Opcije za uključivanje prisluškivanja komunikacije web sučeljem u *Burp Proxy* programskom alatu

Na slici 5 je vidljiv primjer HTTP poruke koja služi za autentikaciju korisnika na web sučelju Asus RT-N12E mrežnog usmjernika. Poruka se pošalje nakon što korisnik otvori web sučelje za administraciju uređaja te upiše korisničko ime i lozinku i nakon toga pritisne tipku za novi redak.



Slika 5. HTTP poruka za autentikaciju korisnika na web sučelju mrežnog usmjernika Asus RT-N12E uhvaćena programskim alatom *Burp Proxy*

Programski alat *Burp Proxy* i platforma *Burp Suite* na kojoj se on temelji imaju primarnu zadaću napada na web aplikacije. Kako su administratorska sučelja na mrežnim usmjernicima napravljena u obliku web aplikacije tako i ona postaju potencijalna meta ovog programskog alata. Ako mrežni usmjernici provjere autentikacije i autorizacije rade na strani klijenta, čime se oslobađa snaga procesora za druge zadaće, moguće je presresti takav promet i promijeniti odgovor čime je moguće autorizirati korisnike koji nemaju pristup mrežnom usmjerniku.

3.2. Detekcija ranjivosti pomoću fizičkog sučelja usmjernika

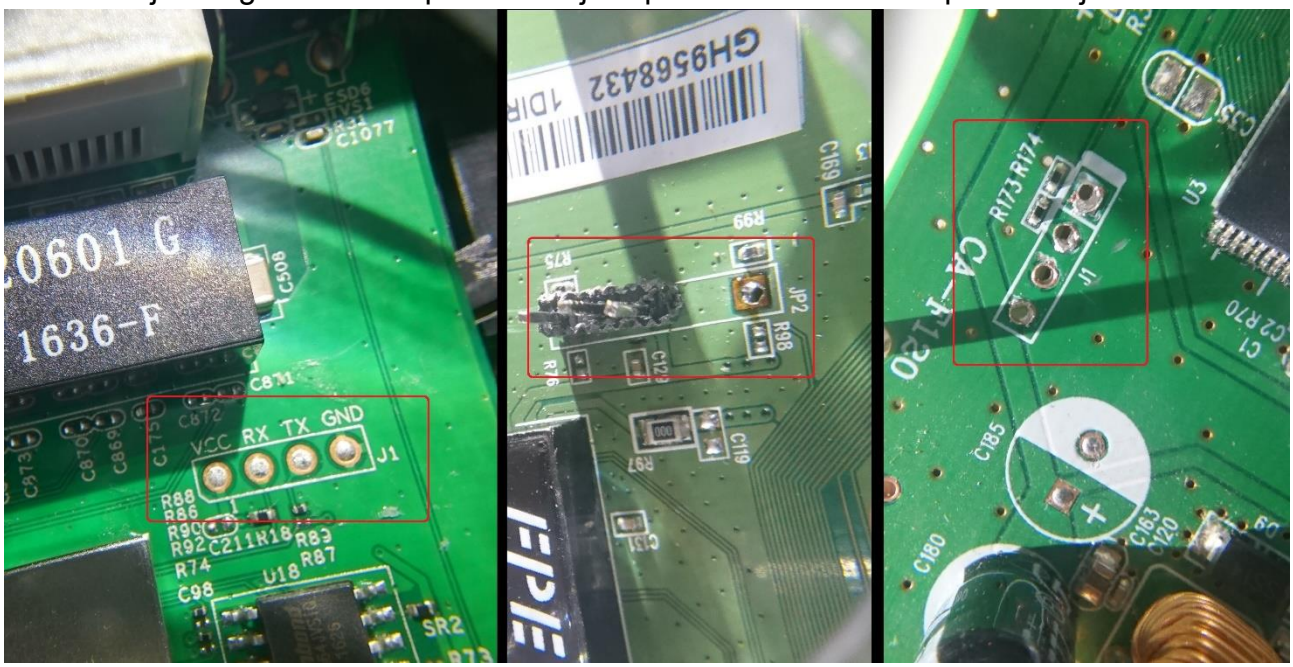
Od proizvodnje mrežnog usmjernika na tiskanoj pločici uređaja mogu ostati različiti pinovi koji su se koristili za testiranje ili uklanjanja grešaka u samom procesu proizvodnje. Jedan od standardnih pinova koji se mogu nalazi jest standard zajedničke grupe za testiranje (*Joint Test Action Group* – JTAG). JTAG je industrijski standard definiran u IEEE 1149.1 standardu. JTAG definira logiku testiranja integriranih krugova pomoću vanjskog serijskog sučelja koje se može ugraditi u integrirani krug, [26].

JTAG služi za testiranje veza između integriranih krugova nakon što su ugrađeni u tiskanu pločicu, testiranje samog integriranog kruga te je moguće promatrati i izmijeniti način ponašanja integriranog kruga. Upravo zbog tog zadnjeg svojstva je moguće pomoću JTAG-a pristupiti procesoru na mrežnom usmjerniku te je moguće preuzeti *firmware* s uređaja i modificirati ga i na kraju pomoću JTAG-a instalirati modifikaciju na uređaj.

Mrežni usmjernici danas imaju UART pinove koji se mogu isto koristiti umjesto JTAG-a i zbog jednostavnijeg protokola se lakše implementira. UART koristi 4 pina za komunikaciju, jedan za slanje oznake Tx, jedan za primanje oznake Rx, jedan za ulazni napon oznake Vcc te uzemljenje oznake Gnd. UART je asinkrona vrsta komunikacije što znači kako je moguće slati i primati u isto vrijeme. Veličina kojom se mjeri komunikacija se naziva baud, i predstavlja 1 simbol. Standardne brzine su definirane od 1200, 2400, 4800, 9600, 38400 bauda po sekundi i njihovim faktorima. UART definira jedan simbol komunikacije kao jedan bit što znači kako je ekvivalentna brzina u bitima jednaka brzini bauda, [21].

UART sučelja na tiskanim pločicama mrežnih usmjernika proizvođača Asus, Tp-Link i D-link su prikazani na slici 6. Proizvođači nakon procesa testiranja uređaja uklone pinove, ali i dalje ostave aktivan port. Za spajanje računala na UART sučelje potrebno je koristiti pretvornik. Jedan od takvih je USB-UART pretvornik signala. Pretvornik signala prevodi

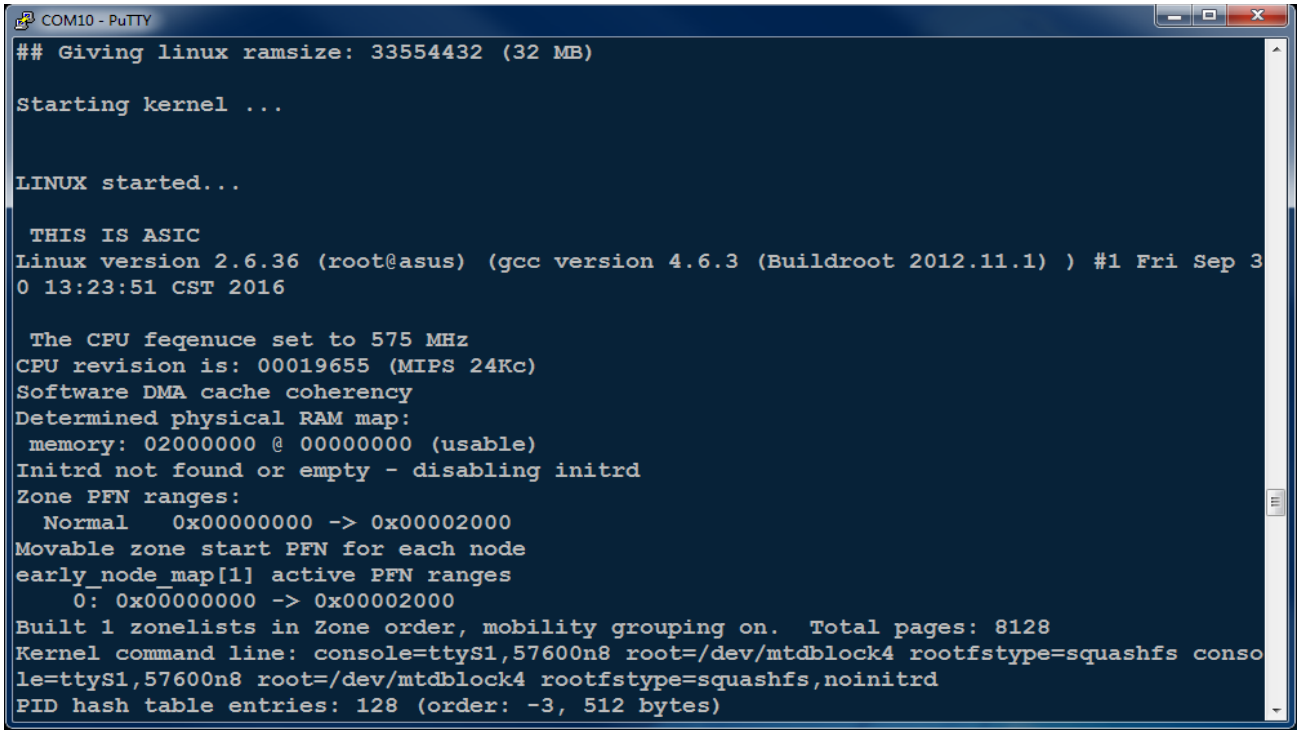
UART serijske signale u USB protokol koji se pomoću USB kabela potom šalje na računalo.



Slika 6. UART portovi označeni crvenim pravokutnicima na mrežnim usmjernicima s lijeva na desno Asus RT-N12E, D-Link DIR-600 i TP-Link WR741ND

Na strani računala je potrebno imati instaliran softver koji podržava dvosmjernu serijsku komunikaciju koristeći USB sučelje na računalu. Na slici 7 su prikazani rezultati komunikacije kada se poveže programski alata *Putty* s UART sučeljem mrežnog usmjernika Asus RT-N12E. U slučaju u kojemu je moguće doći do administrativne konzole moguće je izvršiti prikupljanje podataka o unutarnjoj strukturi samog operativnog sustava. Unutar te strukture je moguće pronaći ranjivosti ili skrivene datoteke i mape koje nisu bile otkrivene softverskim alatima.

Osim toga moguće je započeti postupak izvlačenja *firmware*-a te pronalaženja procesa koji se koriste na mrežnom usmjerniku. Na temelju prikupljenih informacija moguće je napisati set instrukcija, *shellcode*, koje se mogu ubaciti preko jednog od vanjskih sučelja usmjernika, a koje će izvršiti maliciozni program na mrežnom usmjerniku. *Shellocde* koristi direktnu kontrolu nad registrima i funkcije ostalih programa kako bi izvršio maliciozni kod. Zbog toga je u većini slučajeva napisan u *assemlber-u* i zatim preveden u heksadecimalne kodove, [27].



Slika 7. Rezultati ostvarene serijske komunikacije s UART sučeljem Asus RT-N12E mrežnog usmjernikom pomoću programskog alata *Putty*

Nakon što je dobiven izravan pristup u operativni sustav usmjernika prikupljanjem podataka je moguće dobiti informacije o operativnom sustavu i na temelju tih informacija dalje pristupiti povećavanju privilegija na uređaju kako bi se došlo do administratorskih prava. Kako je ovaj postupak kompleksan jer uključuje rastavljanje samog uređaja i spajanje na njegovo fizičko sučelje time je ograničen samo na uređaje koji su lako dostupni napadaču i komercijalno dostupni. Oštećivanje uređaja prilikom ovakvog postupka ga može učinit neuporabljivim čime se prekida bilo kakva daljnja analiza.

4. KOMPARATIVNA ANALIZA REZULTATA I PRIMJERI ISKORIŠTAVANJA RANJIVOSTI

Kako IoT uređaji postaju sve više prisutni u rezidencijalnim mrežama svojom općom primjenom tako će većina IoT uređaja biti spojena na mrežne usmjernike koji su komercijalno dostupni rezidencijalnim korisnicima. Prema istraživanju *Gartner-a* iz 2017. godine broj IoT uređaja će 2020. godine doseći 20.4 milijarde, od kojih će 67% uređaja biti geografski smješteno na području Kine, Sjeverne Amerike i Zapadne Europe. Najveći broj uređaja će pripadati kategoriji uređaja za obične rezidencijalne potrošače, čak preko 12 milijardi uređaja. Takvi IoT uređaji uključuju pametne mjerače, senzore kao i lokacijske senzore i senzore za praćenje zdravlja u stvarnom vremenu. Detaljan broj uređaja po kategorijama je vidljiv u tablici 3, [28].

Tablica 3. Broj IoT uređaja po kategorijama potrošača, brojevi u milijunima

Kategorija/Godina	2016	2017	2018	2020
Rezidencijalni korisnici	3 963.0	5 244.3	7 036.3	12 863.0
Poslovni korisnici: Hibridna Industrija	1 102.1	1 501.0	2 132.6	4 381.4
Poslovni korisnici: Vertikalna integracija	1 316.6	1 635.4	2 027.7	3 171.0
Ukupno	6 381.8	8 380.6	11 196.6	20 415.4

Izvor:[28]

Ako se uzme u obzir kako će većina takvih uređaja biti spojena na mrežne usmjernike, sigurnost IoT uređaja ovisi o sigurnosti mrežnih usmjernika i njihovim potencijalnim ranjivostima. U ovom poglavlju će biti napravljena analiza otkrivanja te iskorištavanja ranjivosti na tri različita komercijalno dostupna mrežna usmjernika koji su po cijeni i sposobnostima namijenjeni upravo rezidencijalnim korisnicima. Ta tri uređaja su Asus RT-N12E mrežni usmjernik, D-Link DIR-600 mrežni usmjernik i TP-Link WR741ND. Na sva tri uređaja je instaliran *firmware* koji sadrži ranjivosti kako bi se simuliralo okruženje gdje su IoT uređaji spojeni na Internet preko ranjivog mrežnog usmjernika.

4.1. Primjeri iskorištavanja pronađenih ranjivosti

Za traženje, analizu i iskorištavanje ranjivosti na mrežnim usmjernicima koristiti će se programski alati *Nmap*, *Routersploit*, *Burp Proxy* i *DirBuster* na operativnom sustavu Kali Linux. Računalo s kojeg se vrši analiza će biti spojeno na lokalnu mrežu koja će se sastojati od mrežnog usmjernika i još dva IoT Raspberry Pi uređaja koji će biti spojeni na istu mrežu. Metodologija testiranja će biti prilagođena metodologiji naziva okvir za procjene sigurnosti informacijskih sustava (*Information Systems Security Assessment Framework* – ISSAF) verzija 0.2.1, [29].

ISSAF definira postupak procjene ranjivosti za mrežne usmjernike. Glavni problemi kod sigurnosti mrežnih usmjernika se prema ISSAF-u javljaju u krivoj konfiguraciji, specifični proizvodi koji su masovno prisutni na tržištu mogu imati ranjivosti koje nisu otkrivene tijekom

proizvodnog procesa te komprimiran mrežni uređaj može komprimirati cijeli mrežni promet. Zbog toga nije potrebno izravno ugroziti pojedinačni uređaj na mreži i komprimirani mrežni uređaj može preusmjeravati promet bez mogućnosti detekcije od uređaja u mreži koji generiraju navedeni promet.

Pravci za iskorištavanje ranjivosti koje će se koristiti u ovom radu su nesigurno konfiguriran HTTP pristup mrežnom sučelju, nesigurnost otvorenih portova i mapiranje datoteka i mapa bez administratorskih ovlasti. Sa strane sklopovlja će biti istraženo koji od navedenih uređaja ima uključen UART port te ako imaju uključen je li uključena Linux konzola. Na temelju toga će biti napravljena komparativna analiza u idućem potpoglavlju.

4.1.1. Asus RT-N12E

U prvom koraku je pokrenuto *Nmap* skeniranje mrežnog usmjernika, čiji rezultati su vidljivi na slici 8. Skeniranje je pokrenuto s opcijom -A koja koristi sve metode skeniranja portova TCP i UDP protokola.

192.168.0.1

Address

- 192.168.0.1 (ipv4)
- C4:12:F5:70:24:C6 - D-Link International (mac)

Ports

The 996 ports scanned but not shown below are in state: **closed**

- 996 ports replied with: **resets**

Port		State (toggle closed [0] | filtered [1])	Service	Reason	Product	Version
53	tcp	open	domain	syn-ack	dnsmasq	2.45
	dns-nsid	bind.version: dnsmasq-2.45				
80	tcp	open	http	syn-ack	D-Link DIR-600 WAP http config	2.14
	http-favicon	Unknown favicon MD5: 107579220745D3B21461C23024D6C4A3				
	http-methods	Supported Methods: GET HEAD POST				
	http-server-header	Linux, HTTP/1.1, DIR-600 Ver 2.14				
	http-title	D-LINK SYSTEMS, INC. | WIRELESS ROUTER | HOME				
49152	tcp	open	upnp	syn-ack	D-Link DIR-600 WAP UPnP	2.14

Remote Operating System Detection

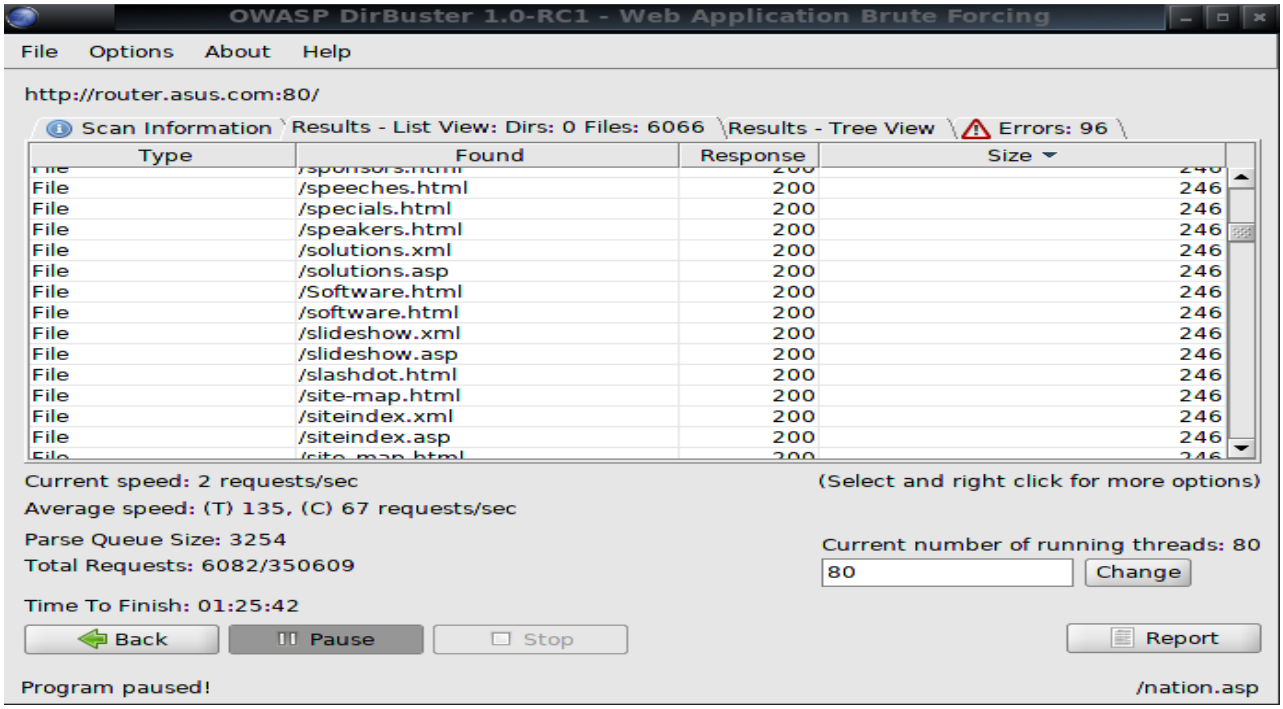
- Used port: **53/tcp (open)**
- Used port: **3/tcp (closed)**
- Used port: **36993/udp (closed)**
- OS match: **D-Link DIR-600 or DIR-645 WAP (Linux 2.6.33) (100%)**

Slika 8. Rezultati skeniranja mrežnog usmjernika Asus RT-N12E s programskim alatom *Nmap*

Iz dobivenih rezultata vidljivo je kako mrežni usmjernik ima otvorene portove 53 i 80, dok su aktivni, ali zatvoreni portovi 1 i 39467. Operativni sustav koji je detektiran se temelji na Linux verziji 2.6.23-2.6.38 što je utvrđeno sa 100% točnosti. Na portu 53, koji se koristi za prevođenje mrežnih adresa iz alfanumeričkih oznaka u brojčane, je pokrenuta aplikacija *dnsmasq* verzija 2.76. Na portu 80 navedene su podržane http metode koje je moguće koristiti, odnosno na koje mrežni usmjernik vraća odgovore. Na temelju ovih informacija napadač je u stanju odrediti kojim će pravcem dalje ići, odnosno već početna analiza daje naznake kako je HTTP nesigurno konfiguriran na mrežnom usmjerniku dok je verzija operativnog sustava dosta zastarjela i najvjerojatnije postoji poznate ranjivosti za tu verziju.

Nakon toga pokrenut je alat *DirBuster* koji je pokrenuo traženje skrivenih mapa i datoteka na web adresi *http://router.asus.com:80* što odgovara web sučelju mrežnog

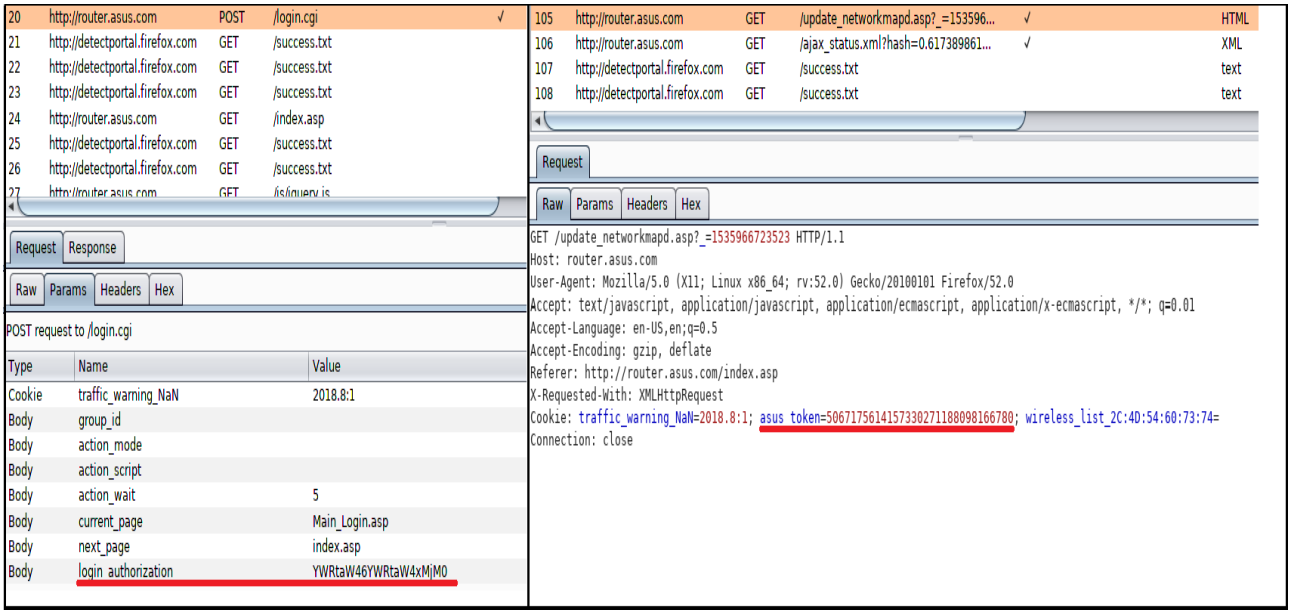
usmjernika. Analiza ja trajala nekoliko minuta jer je zbog velikog broja zahtjeva usmjernik prestao odgovarati na zahtjeve, zapravo se slanjem puno HTTP zahtjeva nenamjerno izvršio DoS napad na mrežni usmjernik iako generirani promet nije bio ni blizu reklamiranoj brzini usmjeravanja od 150 Mbita/s. Iz toga se može izvući neizravni zaključak kako je ovakvo ograničenje prouzrokovano *firmwareom* usmjernika koji nije u stanju toliko HTTP zahtjeva obrađivati. Na slici 9 se vide rezultati skeniranja koje je trajalo nekoliko minuta, svi zahtjevi su odgovoreni s odgovorom 200 koji označuje kako datoteka odnosno mapa postoji iako to nije slučaj kada se napravila nasumična ručna provjera za neke zahtjeve.



Slika 9. Rezultati skeniranja mrežnog usmjernika Asus RT-N12E alatom *DirBuster*

Iz toga se može zaključiti kako je mrežni usmjernik uvijek slao 200 kao odgovor bio zahtjev valjan ili ne što pomaže u sigurnosti jer sakriva otkrivene datoteke i mape među onima koje ne postoje, ali ne daje potpunu sigurnost jer se navedenim mapama i datotekama i dalje može pristupiti.

Za analizu ranjivosti na napad prisluškivanjem, takozvani napad osobe u sredini komunikacije (*Man In The Middle attack* – MITM) se koristio programski alat *Burp Proxy.* U web pregledniku su podešene postavke da sav HTTP promet ide preko porta 8080 na kojemu je uključeno presretanje od strane *Burp Proxy* alata. Svi HTTP zahtjevi i odgovori između web preglednika i web sučelja mrežnog usmjernika su time pročitani od strane *Burp Proxy*-a. Na lijevoj strani slike 10 je vidljivo kako je u zahtjevu vidljiva autorizacijska oznaka od strane klijenta dok je na desnoj strani slike u odgovoru vidljiva autorizacijska oznaka od strane Asus usmjernika koja služi za jedinstveno označavanje sesije prijavljenog korisnika, u ovom slučaju administratora.

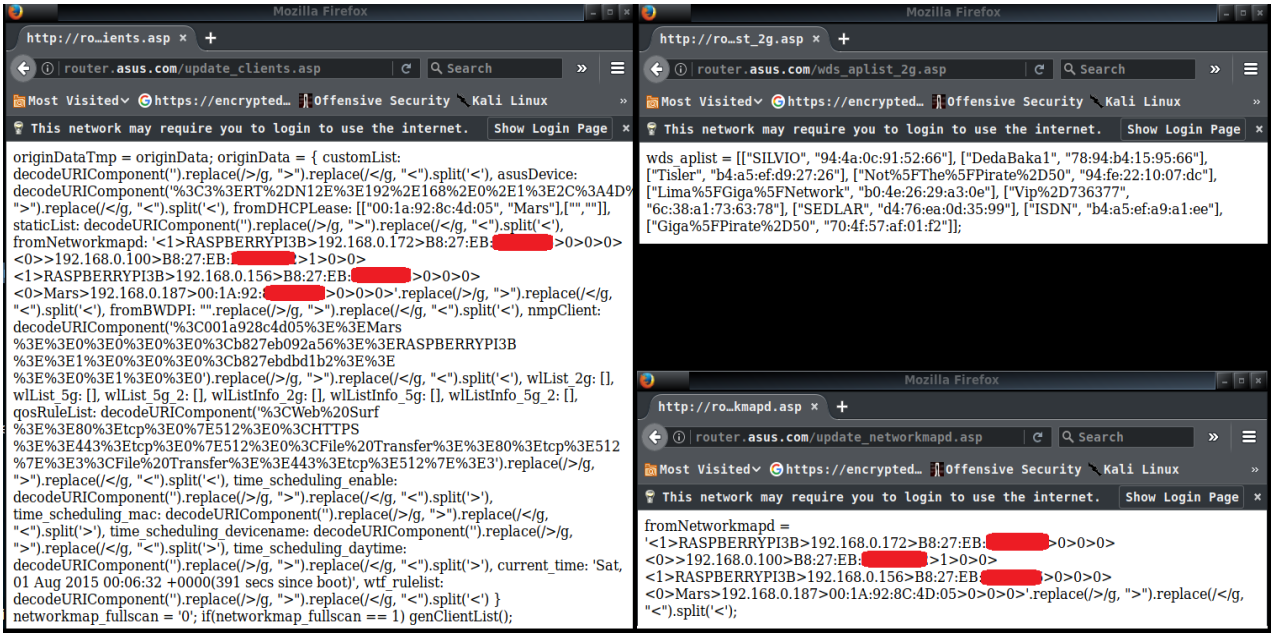


Slika 10. Zahtjev i zaprimljen odgovor od web sučelja Asus usmjernika i autorizacijski parametri vidljivi u njima

Kako se oznake prosljeđuju u obliku kolačića napadač koji presretne ovakvu komunikaciju je u mogućnosti prijaviti se u web sučelje s administrativnim ovlastima bez poznavanja lozinke. Oznaka je kodirana u bazi-64 i dekodiranjem se dobiva njena vrijednost. U ovom slučaju kodirana poruka glasi *YWEtaW46YWRtaW4xMjM0* i dekodirana glasi *admin:admin1234* gdje je lijeva strana od dvotočke korisničko ime, a desna lozinka.

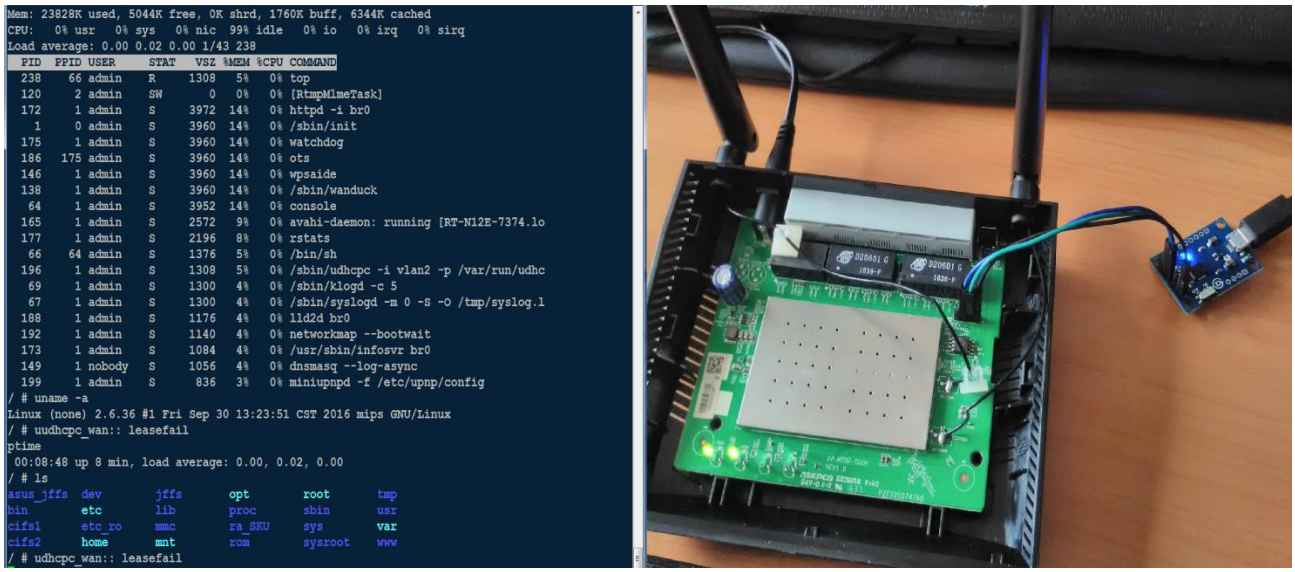
Routersploit sadrži alate za skeniranje ranjivosti, i iako ovaj model Asus mrežnog usmjernika s ovim *firmwareom* ima poznate ranjivosti prema stranicama proizvođača, CVE-2017-5891, CVE-2017-5892, CVE-2017-6549, CVE-2017-6548 i CVE-2017-6547, automatski skener alata za pretragu ranjivosti skeniranjem nije pronašao nikakve poznate ranjivosti koji bi se mogle iskoristiti, [30].

Slijedi primjer iskorištavanja ranjivosti CVE-2017-5892 čijim iskorištavanjem napadač koji je izvan lokalne mreže može saznati informacije o lokalnoj mreži, kao što su unutarnje IP i MAC adrese uređaja, vanjska IP adresa i nazivi i MAC adrese okolnih Wi-Fi mreža. Ove informacije se dalje mogu iskoristiti u napadu na IoT okruženje ako kroz sučelje na tiskanoj pločici mrežnog usmjernika dobiju informacije o unutarnjoj strukturi *firmware*-a uređaja. Na slici 11 su vidljive dobivene informacije. Prema njima se vidi da se mreža sastoji od 3 uređaja, od tih 3 uređaja dva su IoT uređaja, Raspberry Pi mikroračunala, a treći je računalo korisnika koji je otvorio nesigurnu stranicu koja je izvršila CVE-2017-5892, [31].



Slika 11. Informacije o unutarnjoj konfiguraciji mreže koje mrežni usmjernik izlaže trećim stranama izvan lokalne mreže

Pristup UART sučelju je izveden pomoću osobnog računala, USB kabla i USB-UART adaptera koji UART signal sa sučelja usmjernika pretvara u USB signal za osobno računalo. Na računalu je pokrenut program *Putty* koji podržava serijsku komunikaciju. Na slici 12 je vidljiv način spajanja kao i Linux konzola koja podržava osnovne Linux naredbe te je vidljivo vrijeme koliko je usmjernik upaljen, verzija Linux kernela, te programi koji su upaljeni i pod kakvim privilegijima korisnika.



Slika 12. Lijevo: Linux konzola s ispisanim osnovnim informacijama o sustavu. Desno: način spajanja na usmjernik kako bi se pristupilo Linux konzola

Vidljivo je kako je web sučelje pokrenuto s administratorskim ovlastima, samo je sustav za prijevod domena (*Domain Name System* – DNS) pokrenut bez privilegija. S ovakvim ovlastima napadač je u stanju izmijeniti datoteke koje definiraju pristup web sučelju, a nalaze se u mapi /www/. Tim postupkom je *firmware* ovog usmjernika moguće komprimirati još više s fizičkim pristupom.

4.1.2. D-Link DIR-600

Kako bi se dobio prvotni uvid u mrežno sučelje D-Link mrežnog usmjernika pokrenuto je skeniranje programskim alatom *Nmap*. Na slici 13 se vide rezultati skeniranja, kao i na prijašnjem mrežnom usmjerniku port 53 je otvoren jer on služi za prevođenje DNS adresa. Uz to otvoren je port 80 na kojemu je pokrenuto web sučelje, ali otvoren je i port 49152 na kojemu je pokrenuta aplikacija *Universal Plug & Play* (UPnP). Aplikacija UPnP služi za automatsko otvaranje portova prema vanjskoj mreži ako aplikacije na unutarnjoj strani mreže preko UPnP protokola zatraže otvaranje porta. *Nmap* je sa 100% točnošću utvrdio kako je verzija Linux kernela 2.6.33. što ju čini starijom verzijom od Asus mrežnog usmjernika. Također je moguće direktno iz rezultata očitati verziju *firmware*-a koja ima numeričku oznaku 2.14.

192.168.0.1

Address

- 192.168.0.1 (ipv4)
- C4:12:F5:70:24:C6 - D-Link International (mac)

Ports

The 996 ports scanned but not shown below are in state: **closed**

- 996 ports replied with: **resets**

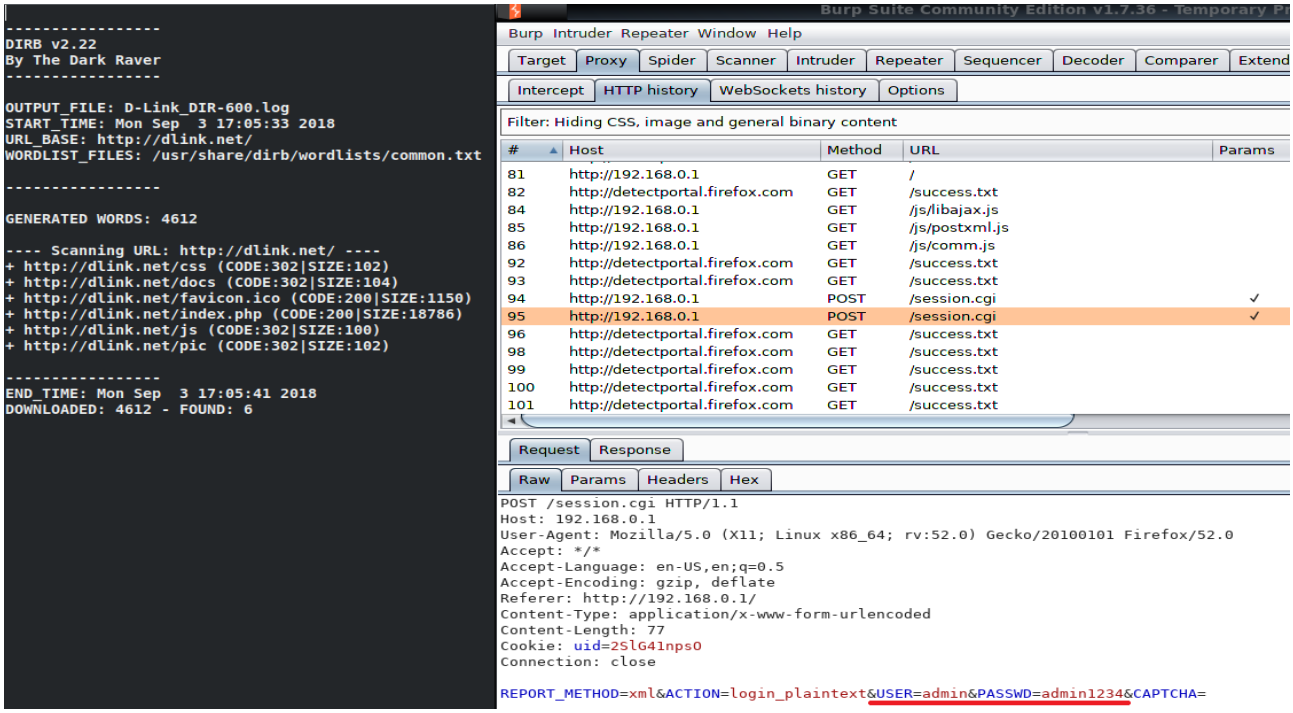
Port		State (toggle closed [0] | filtered [1])	Service	Reason	Product	Version
53	tcp	open	domain	syn-ack	dnsmasq	2.45
	dns-nsid	bind.version: dnsmasq-2.45				
80	tcp	open	http	syn-ack	D-Link DIR-600 WAP http config	2.14
	http-favicon	Unknown favicon MD5: 107579220745D3B21461C23024D6C4A3				
	http-methods	Supported Methods: GET HEAD POST				
	http-server-header	Linux, HTTP/1.1, DIR-600 Ver 2.14				
	http-title	D-LINK SYSTEMS, INC. | WIRELESS ROUTER | HOME				
49152	tcp	open	upnp	syn-ack	D-Link DIR-600 WAP UPnP	2.14

Remote Operating System Detection

- Used port: **53/tcp (open)**
- Used port: **3/tcp (closed)**
- Used port: **36993/udp (closed)**
- OS match: **D-Link DIR-600 or DIR-645 WAP (Linux 2.6.33) (100%)**

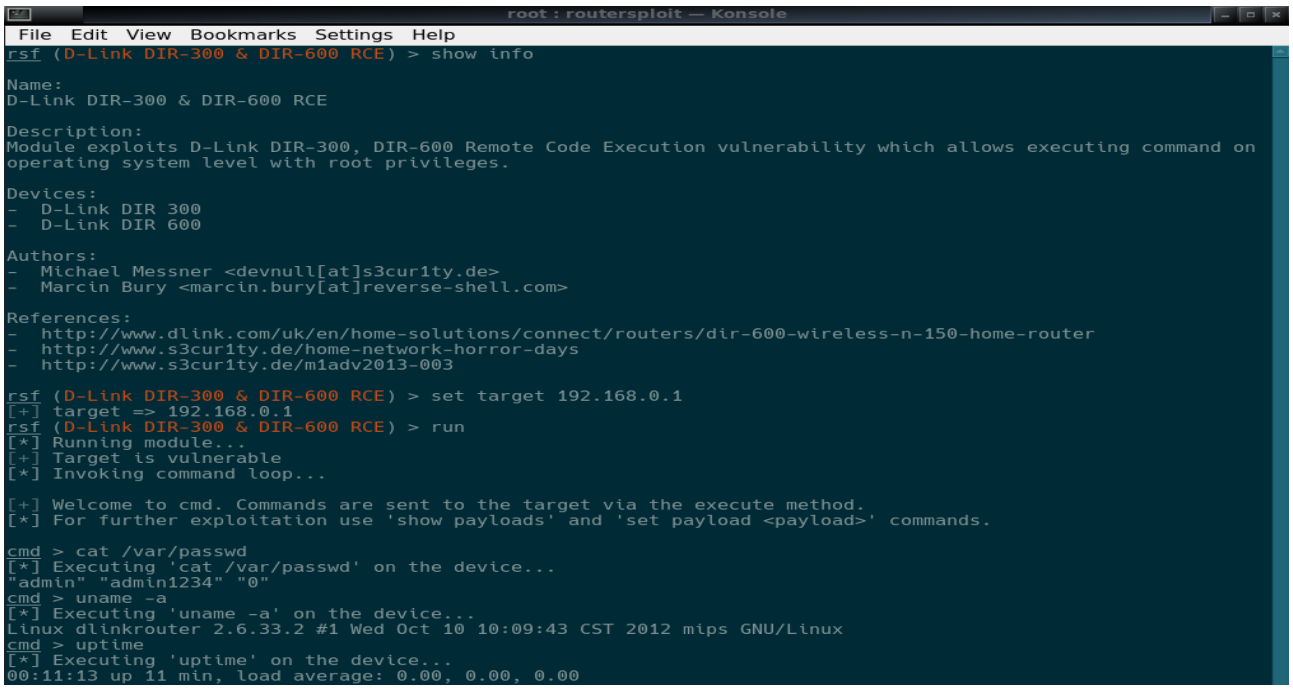
Slika 13. Rezultati skeniranja programskim alatom *Nmap* na mrežnom usmjerniku D-Link DIR-600

Programski alat *DirBuster* nije bio u mogućnosti ispisati datoteke i mape na mrežnom sučelju D-Link mrežnog usmjernika, zato je korišten veoma sličan programski alat *dirb* koji ima samo tekstualno sučelje, ali je bio u mogućnosti ispisati četiri mape i dvije datoteke čiji su rezultati vidljivi na slici 14. Na istoj slici su prikazani rezultati presretanja komunikacije alatom *Burp Proxy*. Web sučelje ne podržava kriptiranu verziju HTTP protokola, HTTPS, i za razliku od Asus usmjernika korisničko ime i lozinku šalje u čitljivom tekstu bez kodiranja što se može očitati iz HTTP poruke. Uz to je vidljiv i kolačić koji će poslužiti za spremanje sesije korisnika na web sučelje.



Slika 14. Lijevo: prikaz rezultata programskog alata *dirb*. Desno: prikaz HTTP poruka dohvaćene MITM napadom koristeći *Burp Proxy*

Programski alat *Routersploit* je pokazao izvrsne rezultate na mrežnom usmjerniku od D-Linka. Iskorištena je ranjivost EDB-ID:24453 usmjernika serije DIR-600 koji omogućuje napadaču koji je spojen na lokalnu mrežu izvršavanje naredbi na samom usmjerniku bez administratorskih ovlasti. Na slici 15 je prikazan postupak unutar samog alata. Nakon što se učita modul koji će iskoristiti ranjivost, upiše se odredišna adresa i pokrene se modul. Odmah se dobije terminalno sučelje u koje se mogu unositi naredbe, [32].



Slika 15. Iskorištavanje ranjivosti EDB-ID: 24453 na D-Link Dir-600 mrežnom usmjerniku pomoću programskog alata *Routersploit*

Kao što je vidljivo na slici administratorska lozinka i korisničko ime su spremljeni u običnom tekstualnom formatu i napadač ih je u stanju pročitati bez posebnih alata. Također se može doći do informacije o verziji Linux kernela, koja prema slici se minimalno razlikuje u verziji od verzije dobivene *Nmap* programskim alatom.

Pristup UART sklopovlju na tiskanoj pločici nije davao nikakve rezultate bez obzira na podešenu brzinu bauda serijske komunikacije. Iz toga se sigurno može zaključiti kako je osim maknutih pinova serijsko sučelje isključeno u proizvodnom procesu.

4.1.3. TP-Link WR741ND

Iz analize *Nmap* programskim alatom vidljivo je na slici 16 kako TP-Link mrežni usmjernik ima otvorene samo portove 80 i 1900. Na portu 1900 je pokrenut UPnP, i nije vidljiv nikakav DNS koji bi služio za prevođenje adresa. Detektirana verzija Linux kernela je 2.6.23 do 2.6.38 sa 100% točnošću. Time bi od sva tri mrežna usmjernika verzija kernela bila najstarija ako je *Nmap* skeniranje točno.

192.168.0.1

Address

- 192.168.0.1 (ipv4)
- F8:D1:11:2C:86:74 - Tp-link Technologies (mac)

Ports

The 998 ports scanned but not shown below are in state: **closed**

- 998 ports replied with: **resets**

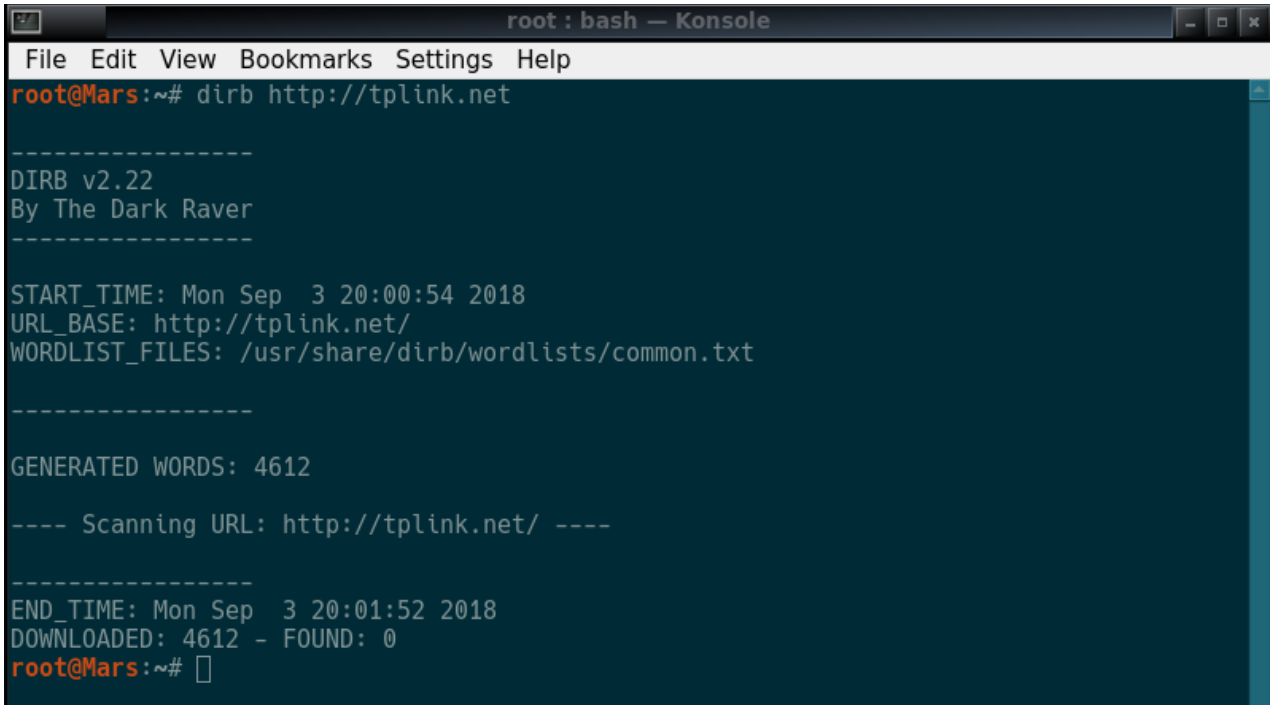
Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product	Version	Extra info
80	tcp	open	http	syn-ack	TP-LINK WR741N WAP http config		
	http-auth	HTTP/1.1 401 N/A\x0D Basic realm=TP-LINK Wireless Lite N Router WR741N					
	http-title	Login Incorrect					
1900	tcp	open	upnp	syn-ack	ipOS upnpd		TP-LINK TL-WR741N WAP 4.0; UPnP 1.0

Remote Operating System Detection

- Used port: **80/tcp (open)**
- Used port: **1/tcp (closed)**
- Used port: **42818/udp (closed)**
- OS match: **Linux 2.6.23 - 2.6.38 (100%)**

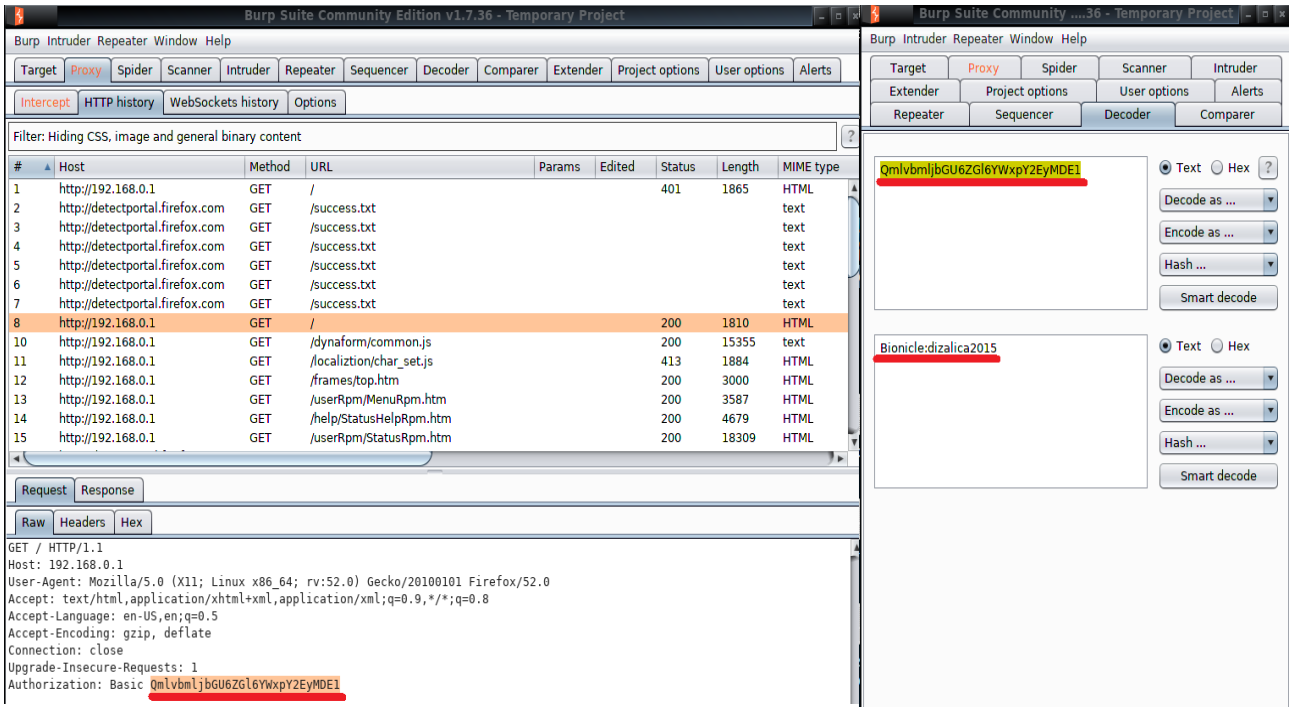
Slika 16. Rezultati skeniranja programskim alatom *Nmap*

Niti programski alat *DirBuster* niti programski alata *dirb* nisu bili u mogućnosti ispisati mape i datoteke na web sučelju što je vidljivo na slici 17. Od 4612 generiranih riječi koje se najčešće koriste kao imena datoteka i mapa na web sučeljima na nijedan zahtjev nije odgovoreno s HTTP statusom 200.



Slika 17. Rezultati programskog alata *dirb* na mrežnom usmjerniku TP-Link WR741ND

Korištenjem programskog alata *Burp Proxy* uspješno je napravljen MITM napad i očitani su korisničko ime i lozinka što se vidi na slici 18. Na lijevoj strani slike je HTTP paket koji nosi autorizacijsku poruku od strane korisnika koji se prijavljuje u web administrativno sučelje. Na desnoj strani slike je dekodirana poruka u formatu koji koristi bazu 64. Na temelju toga napadaču je u mogućnosti se prijaviti u web sučelje mrežnog usmjernika s administratorskim ovlastima.



Slika 18. Lijevo: HTTP paket koji nosi autorizacijsku poruku. Desno: dekodirana poruka iz koje se može očitati korisničko ime i lozinka

Programski alat *Routersploit* je uspješno iskoristio ranjivost koja mu omogućuje čitanje datoteka s mrežnog usmjernika bez prijave u web sučelje. Na temelju tih datoteka automatski je preuzeo datoteku koja sadrži kriptirane lozinke, što je vidljivo na slici 19. Lozinke u takvom obliku napadač je u mogućnosti dekriptirati koristeći programske alate za dekriptiranje lozinki, kao što je programski alat *john*. Rezultati dekriptiranja lozinke su prikazani na gornjem dijelu slike 19, lozinka za glavni *root* korisnički račun glasi 5up, [33], [34].

Slika 19. Gore: prikaz rezultata dekriptiranja administratorske lozinke u programskom alatu *John*. Dolje: prikaz načina pristupa na UART sučelje usmjernika

Spajanjem na UART pinove na način prikazan na donjoj strani slike 19 nije omogućilo povezivanje na Linux terminal od mrežnog usmjernika. Dodatnom provjerom voltmetrom od strane autora utvrđeno je kako su pinovi za napon Vcc i uzemljenje Gnd aktivni, ali na pinovima Rx i Tx ne postoji signal. Nakon ove provjere sigurno se može zaključiti kako je UART sučelje onemogućeno u *firmware*-u mrežnog usmjernika.

4.2. Komparativna analiza rezultata

S obzirom na provedenu sigurnosnu analizu i traženje ranjivosti u prošlom poglavlju, mrežni usmjernici Asus RT-N12E, D-Link DIR-600 i TP-Link WR741ND se mogu objektivno usporediti po pitanju razine njihove sigurnosti. Razina sigurnosti mrežnog usmjernika u IoT okruženju odgovara razini sigurnosti cijelog okruženja ako nije provedena obrana u dubinu, odnosno nakon ugroze mrežnog usmjernika ne postoje dodatni mehanizmi zaštite koji mogu jamčiti sigurnost mrežnog prometa ili detektirati narušavanje sigurnosti. Crvenom bojom su označeni parametri koji narušavaju sigurnost dok su zelenom bojom označeni parametri koji povećavaju sigurnost mrežnog usmjernika.

Tablica 4. Komparativna analiza ranjivosti mrežnih usmjernika Asus RT-N12E, D-Link DIR-600 i TP-Link WR741ND

	TIP MREŽNOG USMJERNIKA		
Sigurnosna značajka	**Asus RT-N12E**	**D-Link DIR-600**	**TP-Link WR741ND**
Moguća detekcija operativnog sustava na otvorenim portovima	**DA**	**DA**	**DA**
Moguća detekcija aplikacija na otvorenim portovima	**DA**	**DA**	**DA**
Moguće je doći do imena datoteka i mapa bez prijave u web sučelje	**NE**	**DA**	**DA, CVE-2015-3035**
Moguće pristupiti datotekama i mapama bez prijave u web sučelje	**DA, CVE-2017-5892**	**DA**	**DA**
DoS napad bez uporabe velike količine prometa	**DA**	**NE**	**DA, EDB-ID: 38483**
MITM presretanje administratorske lozinke web sučelja	**DA**	**DA**	**DA**
Udaljeno izvršavanje koda bez administratorskih ovlasti	**NE**	**DA, EDB-ID: 24453**	**DA, CVE-2017-14250**
Curenje informacija o lokalnoj mreži trećim stranama izvan lokalne mreže	**DA**	**NE**	**NE**
UART sučelje aktivno na mrežnom usmjerniku	**DA**	**NE**	**NE**
UART sučelje omogućuje automatsku prijavu u uređaj s administracijskim ovlastima	**DA**	**NE**	**NE**

Iz tablice 4 se može uvidjeti kako niti jedan od tri mrežna usmjernika ne uspijeva zaštititi informaciju o verziji operativnog sustava uređaja od ostalih sudionika na mreži. Programski alat *Nmap* je pomoću otvorenih portova mrežnih usmjernika u svakom slučaju

uspio utvrditi verziju operativnog sustava. Osim operativnih sustava *Nmap* je u mogućnosti bio i detektirati verziju aplikacija koje su bile pokrenute na otvorenim portovima.

Od sva tri uređaja samo je Asus RT-N12E uspješno sakrio svoje mape i datoteke od skeniranja tako što je vraćao lažno pozitivne rezultate. Unatoč tome zbog poznate ranjivosti CVE-2017-5892 moguće je bilo doći do unutarnjih datoteka koje otkrivaju strukturu lokalne mreže. Usmjernik D-Link DIR-600 je otkrivao unutarnju strukturu web sučelja bez poteškoća, dok je na TP-Link WR741ND uređaju bilo potrebno izvršiti CVE-2015-3035 metodu za iskorištavanje ranjivosti. Samo na DIR-600 uređaju nije bilo moguće napraviti DoS napad na aplikacijskoj razini, usmjernik Asus RT-N12E je moguće onesposobiti s većom količinom HTTP zahtjeva dok je TP-Link WR741ND uređaj ranjiv na EDB-ID: 38483, [35].

Kako niti jedan mrežni usmjernik nije podržavao web sučelje koje koristi enkriptirani HTTPS tako je na svim usmjernicima bilo moguće izvršiti MITM napad s lokalne mreže i presresti autorizacijske oznake za prijavu s administratorskim ovlastima. Samo su Asus RT-N12E i TP-Link WR741ND kodirali lozinku i korisničko ime u bazi 64 dok je D-Link model oznake za prijavu prenosio kao čitljivi tekst u originalnom obliku.

Dok Asus-ov model nije sadržavao ranjivosti za udaljeno neautorizirano izvršavanje naredbi, na D-Link-ovom i TP-Link-ovom modelu je bilo moguće neautorizirano udaljeno izvršiti naredbe zbog načina za iskorištavanja ranjivosti EDB-ID:24453 i CVE-2017-14250, ali je Asus-ov model otkrivao informacije o konfiguraciji lokalne mreže trećim stranama izvan mreže dok ostala dva modela nisu otkrivala takve informacije, [32], [36].

Što se tiče fizičkog sučelja, samo je Asus-ov model imao aktivirano UART sučelje preko kojega je bilo moguće doći do administratorskog terminala i na temelju toga napraviti daljnje modifikacije *firmware*-a uređaja, dok je UART sučelje bilo onesposobljeno na D-Link-ovom i TP-Link-ovom modelu.

Iz ove komparativne analize je vidljivo kako niti jedan od tri uspoređena mrežna usmjernika nije u mogućnosti pružiti dubinsku obranu lokalne mreže od napadača. Svaki implementira zaštitu na određenoj razini, dok ostale razine ostavlja nezaštićenima. Tako primjerice Asus RT-N12 usmjernik se štiti od uvida u datoteke i mape preko mrežnog sučelja, ali sadrži ranjivost koja preko podešenih HTTP zahtjeva može otkriti konfiguraciju čitave mreže. U IoT okruženju, u kojemu je veći broj IoT uređaja spojen na ove usmjernike, zbog njihove loše konfiguracije i ranjivosti napadač bi bio u mogućnosti izvršiti DoS napad na IoT okruženje ili preko administratorskih ovlasti promijeniti DNS postavke na usmjerniku čime bi IoT okruženje nenamjerno moglo vršiti DoS napad na treću lokaciju. U tablici 5 su prikazani rezultati skeniranja Interneta u potrazi za navedenim mrežnim usmjernicima.

Tablica 5. Rezultati skeniranja Internet adresa web portalom Shodan u potrazi za mrežnim usmjernicima iz ovog poglavlja

	TIP MREŽNOG USMJERNIKA		
NAZIV REZULTATA	**Asus RT-N12E**	**D-Link DIR-600**	**TP-Link WR741ND**
Ukupan broj uređaja u top 10 zemalja gdje su detektirani	1207	5698	38472

Ukupan broj uređaja u top 10 organizacija gdje su detektirani	431	2562	21497
Broj uređaja s otvorenim HTTP portovima	712	5036	10090
Domena s najvećim brojem detektiranih uređaja	rdsnet.ro	debacom.pl	worldcall.net.pk

Podaci iz tablice su dobiveni koristeći se web portalom *Shodan*. Skeniranje Internet adresnog prostora se vrši na vanjskom mrežnom sučelju uređaja. Iz toga se može zaključiti kako je veliki broj mrežnih usmjernika koji odgovaraju trima nad kojima je provedena analiza u ovom poglavlju dostupni iz vanjske mreže čime navedene ranjivosti nisu više samo ograničene na napad iz lokalne mreže. TP-Link WR741ND je najrasprostranjeniji unatoč tome što je uređaj najstariji od tri dok je Asus-ov model najmanje zastupljen. Iz toga se može izvesti zaključak kako su najstariji uređaji najrasprostranjeniji. U slučaju da svaki od tih mrežnih usmjernika postane dio IoT okruženja rizik od DoS napada koje takvi IoT uređaji mogu prouzrokovati je puno veći od situaciju u kojoj je samo nekoliko korisnika ugroženo iza ranjivih mrežnih usmjernika, kao što je u tradicionalnim rezidencijalnim mrežama. [37], [38], [39].

5. PRIJEDLOG NAČIN ZAŠTITE MREŽNIH USMJERNIKA U IoT OKRUŽENJU

U ovom poglavlju će biti napravljen osvrt na dosadašnje prijedloge i postojeća rješenja za zaštitu mrežnih usmjernika koja bi pri primjeni na IoT okruženje povećala sigurnost takvog okruženja. Nakon osvrta će biti pružen prijedlog zaštite mrežnih usmjernika u IoT okruženju koji će se temeljiti na konceptu obrane u dubinu. Pri tome treba uzeti u obzir kako veliki broj IoT uređaja namijenjen rezidencijalnim korisnicima još nije ostvario projekciju prema *Gartner*-u koja iznosi preko 20 milijardi uređaja u 2020. godini. Na temelju toga se može zaključiti kako niti jedan od prijedloga nije bio testiran u okruženju gdje rezidencijalni korisnici imaju po više desetaka IoT uređaja koji su povezani na Internet pomoću komercijalnih mrežnih usmjernika koji ne pružaju razinu sigurnosti kao i poslovni ili mrežni usmjernici za industrijsku uporabu, [28].

5.1. Dosadašnja istraživanja ranjivosti mrežnih usmjernika

Asimetrična digitalna pretplatnička linija (*Asymmetric digital subscriber line* – ADSL) označuje zadnji dio pristupne mreže koji dolazi do krajnjeg korisnika. ADSL linija na korisničkoj strani terminira s ADSL mrežnim usmjernikom koji je pružen od strane davatelja usluga. U [40] je napravljena sigurnosna analiza i potraga za ranjivostima ADSL mrežnog usmjernika. Nađene su dvije ozbiljne sigurnosne ranjivosti u web sučelju usmjernika. Navedene ranjivosti su nađene ručnim testiranjem, spomenuto je kako automatizirani alati za pronalaženje ranjivosti nisu uspjeli detektirati ranjivosti. Kod pronalaženja ranjivosti na određenom mrežnom usmjerniku od određenog davatelja usluga rizik od štete tim je veći što je moguće skenirati sve IP adrese koje su dodijeljene tom davatelju usluga u potrazi za svim uređajima kojima je moguće pristupiti iz vanjske mreže.

Istraživanje za sigurnosne mjere predlaže korištenje HTTPS protokola umjesto HTTP, validaciju korisničkog unosa u web sučelje kako bi se zaštitilo od ubacivanja malicioznog koda, enkripciju osjetljivih podataka pri pohrani na mrežni usmjernik i redovite sigurnosne provjere mrežnih usmjernika pri proizvodnji na aplikacijskoj i *firmware* razini. Također je navedeno kako korisnici moraju redovito ažurirati *firmware* mrežnog usmjernika, brisati kolačiće web preglednika nakon što su gotovi u radu web sučelja usmjernika i korisnici ne smiju posjećivati sumnjive poveznice koje su dobili u elektroničkoj pošti. Ove predložene mjere sigurnosti se oslanjaju na rad korisnika i njegovo znanje i ne mogu biti pouzdane mjere u okolini jer za pružanje usluga davatelji usluga ne testiraju tehničko znanje korisnika.

Uz to u istraživanju nije provedena analiza UART sučelja na mrežnom usmjerniku i time nije dobiven uvid u unutarnju programsku strukturu i rad ADSL usmjernika. Osim vanjskih prijetnji i krajnji korisnik može biti maliciozan i potrebno je zaštititi usmjernik od njegove analize ranjivosti onesposobljavanjem UART sučelja. Ažuriranje *firmware*-a te uporaba i rukovanje kolačićima web sučelja treba biti odrađena automatizirano od strane programa u mrežnom usmjerniku kako se krajnji korisnik ne bi opterećivao dodatnim radnjama.

U istraživanju [41] analiziran je Cisco mrežni usmjernik na ranjivosti i mogući način iskorištavanja istih. Za analizu je korišten alat koji koristi *fuzzing* metodu temeljenu na polu-validnom *fuzzing* generatoru testnih rješenja (*Semi-valid Fuzzing Test Case Generator* – SFTCG) modelu, metoda koja koristi automatsko generiranje poruka protokola za kontrolu internet poruka (*Internet Control Messsage Protocol* - ICMP). U istraživanju su uspješno

otkrivene ranjivosti na Cisco mrežnim usmjernicima i predloženo je proširenje SFTCG modela na Cisco mrežne preklopnike. Otkriveno je da pri većem broju ICMP poruka Cisco mrežni usmjernik prestane odgovarati na nove zahtjeve jer svi resursi na mrežnom usmjerniku postanu zauzeti obrađivanjem malicioznih ICMP zahtjeva.

Nedostatak ovog istraživanja jest što nije analizirano web sučelje mrežnog usmjernika već samo jedna vrsta protokola. Također nije provedena analiza ostalim programskim alatima već je samo korištena *fuzzing* tehnika. Mrežni usmjernik također nije analiziran koristeći njegovo fizičko sučelje na samom sklopovlju, niti je utvrđena vrsta fizičkog sučelja ako ga usmjernik sadržava. Potrebno je analizirati više od jednog protokola kako bi se dobio detaljan uvid u sve moguće ranjivosti koje mogu biti iskorištene od strane napadača.

U [42] je napravljena analiza korištenja UPnP tehnologije na mrežnim usmjernicima. Analiziran je sigurnosni aspekt UPnP tehnologije na mrežnim usmjernicima koji su korišteni u rezidencijalnim lokalnim mrežama. U analizi je korišten programski alat za detekciju UPnP ranjivosti na mrežnim usmjernicima. Alat je automatiziran i namijenjen je korištenje od strane krajnjeg korisnika. Na 6 mrežnih usmjernika alat je pokušao dodati nove parove UPnP portova i izbrisati postojeće. Jedan od testiranih mrežnih usmjernika je bio i DIR-600 nad kojim je provedena i analiza u ovom radu.

Predloženo rješenje istraživanja je korištenje navedenog alata od strane korisnika kako bi korisnici utvrdili jesu li njihovi uređaji ranjivi na određene UPnP napade. Za implementaciju većeg rješenja također je predložen razvoj platforme koja će prikupljati rezultate skeniranja od individualnih korisnika. Nedostatak ovakvog rješenja jest što se od krajnjeg korisnika traže dodatne radnje kako bi se utvrdila ranjivost sustava. Također nije utvrđena volja korisnika za promjenu ranjive opreme u slučaju u kojemu su ranjivosti otkrivene. Još jedan nedostatak jest što se samo analizom UPnP tehnologije na mrežnim usmjernicima ne mogu utvrditi sve ranjivosti. Primjerice u istraživanju je otkrivena UPnP ranjivost na DIR-600 modelu. Čak i ako ta ranjivost bude maknuta programskom zakrpom od strane proizvođača na navedenom modelu je moguće iskoristiti druge ranjivosti koje se ne temelje na UPnP kao što je demonstrirano u četvrtom poglavlju.

Kako bi se odvojio legitiman mrežni promet od nelegitimnog koji je potencijalan DDoS napad na mrežu, u [43] je predložena arhitektura mrežnog usmjernika koja koristi izolaciju resursa između različitih vrsta mrežnog prometa. Predložena arhitektura koristi oznaku kvalitete usluge koja služi za razlikovanje prometa. Kako su resursi odvojeni pri DDoS napadu neće doći do zauzeća svih resursa i mrežni usmjernik će i dalje biti u mogućnosti obavljati usmjeravanje mrežnog prometa.

Nedostatak prijedloga ovog istraživanja jest to što su mrežni usmjernici ranjivi na razne vrste napada, osim DDoS-a neki od mogućih napada su udaljeno izvršavanje koda, neautorizirano preusmjeravanje mrežnog prometa i neovlašten pristup web sučelju mrežnog usmjernika. IoT okruženje s ranjivim mrežnim usmjernikom za napadača predstavlja resurs koji je dalje moguće koristiti u maliciozne svrhe dok DDoS napadom na mrežni usmjernik napadač gubi takav resurs. Uz DDoS napade mrežne usmjernike je potrebno zaštiti od ostalih vrsta napada, pogotovo u IoT okruženju.

U istraživanje [44] je napravljena analiza xDSL mrežnog usmjernika na otpornost DoS napada. U istraživanju su korišteni TCP paketi različitih veličina i na testnom usmjerniku je otkriveno kako dolazi do DoS ako je veličina TCP paketa manja od 60 bajta. Predloženo rješenje uključuje filtraciju paketa na razini jezgrene mreže operatera kako bi se izbjegao DoS napad na krajnje korisnike.

Nedostatak ovakvog rješenja jest što zahtijeva dodatna ulaganja od strane operatera mreže bez vidljivog povećanja kvalitete kod krajnjeg korisnika. Uz to osim DoS napada mrežni usmjernici mogu imati ranjivosti u njihovoj konfiguraciji ili *firmware*-u što je demonstrirano u četvrtom poglavlju. Nije provedena analiza ostalih ranjivosti što znači da čak i u slučaju gdje je nadograđena jezgrena mreža xDSL mrežni usmjernici krajnjih korisnika i dalje mogu biti ranjivi na ostale neotkrivene ranjivosti.

U [45] je provedena analiza sigurnosti mrežnih usmjernika u malim rezidencijalnim i malim poslovnim mrežama. Testirana je ranjivost mrežnih usmjernika na preusmjeravanje DNS zahtjeva na maliciozno odredište. U istraživanju je zaključeno kako postoje sigurnosni propusti na razini proizvođača i na razini davatelja usluga. Prijedlog rješenja uključuje dostatnu zaštitu za udaljeni pristup, redovito ažuriranje *firmware*-a i instalacija sigurnosnih zakrpi, generiranje nasumičnih lozinki za pristup mrežnom usmjerniku umjesto iste tvorničke lozinke za sve usmjernike te edukacija korisnika o sigurnosnim rizicima na mreži.

Nedostatak prijedloga rješenja jest što ne spominje redovnu sigurnosnu provjeru od strane proizvođača kako bi se ranjivosti utvrdile prije nego postanu javne. Čak i u slučaju redovne instalacije sigurnosnih zakrpi ako postoji ranjivost koja još nije otkrivena od strane proizvođača neće postojati niti sigurnosna zakrpa za nju. Sa strane davatelja usluga edukacija korisnika o sigurnosnim rizicima predstavlja dodatni trošak bez vidljivog povećanja kvalitete usluge sa strane korisnika čime postaje nepraktično educirati korisnika o takvim prijetnjama. Sigurnosni mehanizmi provedeni unutar usmjernika na razini *firmware*-a moraju biti izgrađeni na pretpostavci nesigurnih korisničkih radnji kako bi se razina zaštite dovela na najveću moguću razinu.

5.2. Postojeća rješenja i prijedlozi zaštite mrežnih usmjernika

Kako bi se ubrzala konfiguracija i uspostavljanje mreže unutar IoT okruženja moguće je postaviti mrežne usmjernike koji već imaju u sebi ugrađene povećane mjere sigurnosti i zaštite. Primjerice Cisco mrežni usmjernici tipa Cisco IPsec VPN podržavaju automatske testove za provjeru krivih konfiguracija, provjeru verzija *firmware*-a i traženje nekih vrsta ranjivosti, pomoću protokola za automatizaciju sigurnosnog sadržaja (*Security Content Automation Protocol* – SCAP). Na temelju ovakvog testa moguće je u kratkom vremenskom periodu provjeriti veći broj mrežnih usmjernika i time održavati veću razinu sigurnosti unutar IoT okruženja, [46].

Nedostatak ovakvog rješenja jest što većina rezidencijalnih korisnika i mala poduzeća nemaju dovoljno sredstava za ovakva rješenja i uz to nemaju potrebno znanje za rukovanjem ovakvim uređajima čime je ovakvo rješenje nepraktično. Veliki industrijski i poslovni korisnici pri implementaciji IoT rješenja u svoje proizvodne sustave bi s ovakvim sigurnosnim rješenjem uspostavili samo jednu razinu zaštite, zaštitu konfiguracije i verzije

firmware-a jer bi u slučaju komprimiranja mrežnog usmjernika neotkrivenom ranjivošću ostatak IoT okruženja također bio komprimiran.

Postavljanjem mamaca u IoT okruženje moguće je odvratiti napadača od dijela mreže kojeg je potrebno zaštiti. Prema predloženom rješenju u [47] mrežni usmjernik koji bi pri detekciji malicioznog mrežnog prometa usmjeravao takav promet na mamce u lokalnoj mreži bi upravo takvom metodom štitio glavni dio mreže. Mamci bi među sobom dijelili mrežno opterećenje kako ne bi došlo do pojedinačnog opterećenja. U prijedlogu zaštite lokalne mreže ovakav mrežni usmjernik bi bio implementiran softverski na zasebnom poslužitelju koji bi se nalazio neposredno poslije ADSL mrežnog usmjernika.

Nedostatak ovakvog rješenja jest što pretpostavlja sigurnost ADSL mrežnog usmjernika i u slučaju njegove ugroze mrežni promet koji generira mreža može biti preusmjeren od strane napadača koji je preuzeo kontrolu nad mrežnim usmjernikom. K tome ovakvo rješenje nije praktično za komercijalne korisnike koji će prema predviđanjima posjedovati najveći udio IoT uređaja 2020. godine. U IoT okruženju ovakvo rješenje bi uvelo dodatnu konfiguraciju, ali bez podizanja razine sigurnosti u slučaju ugroze mrežnog usmjernika.

Jedno od predloženih rješenja nastoji detektirati i spriječiti napade na rezidencijalne mrežne usmjernike praćenjem potrošnje električne energije. Prijedlog u [48] detektira napade na mrežne usmjernike ako je potrošnja električne energije usmjernika izvan modela potrošnje tijekom normalnog rada mrežnog usmjernika. Ova metoda zaštite uzima u obzir kako pri dekriptiranju lozinki na web sučelju dolazi do slanja velike količine zahtjeva prema mrežnog usmjerniku i time do povećane potrošnje energije. Za praćenje potrošnje električne energije u prijedlogu se koriste odvojeni moduli jer mrežni usmjernici za rezidencijalne korisnike na web sučelju nemaju prikaz vlastite potrošnje.

Nedostatak ovakvog rješenja jest u tome što podrazumijeva povećanu količinu prometa pri napadu. Iako točno za DoS napad i ako je u tijeku udaljeno dekriptiranje lozinki s vanjske mreže u slučaju u kojemu se koriste ranjivosti samog *firmware*-a ili loše konfiguracije neće doći do povećane količine prometa i time se napad neće moći detektirati povećanom potrošnjom energije. Kao što je demonstrirano u prethodnom poglavlju moguće je preko fizičkog UART sučelja doći do informacija o unutarnjoj konfiguraciji mrežnog usmjernika čak i ako programski alati daju negativne rezultate. Unutar IoT okruženja bi bilo potrebno redovito izrađivati nove modele potrošnje koji bi se koristili za usporedbu. Pri proširenju mreže s novim IoT uređajima koji generiraju novi promet i kako postojeći mijenjaju ponašanje na mreži zbog programske nadogradnje, model potrošnje električne energije je potrebno konstantno nadograđivati što nije praktično rješenje za rezidencijalnog korisnika.

Kako bi se mrežni usmjernik zaštitio od novih i promjenjivih prijetnji njegov sigurnosni mehanizam mora biti prilagodljiv. Upravo se na tome temelji prijedlog u [49]. Kako bi se mrežni usmjernik zaštitio od napada na uređaju je instaliran sustav za praćenje stanja mrežnog usmjernika koji koristi validaciju rada usmjernika. U slučaju u kojemu je detektirano abnormalno ponašanje i otkriven napad na mrežni usmjernik pokreće se preusmjeravanje mrežnih funkcionalnosti usmjernika na drugu verziju mrežnog protokola od onog na kojemu je detektiran napad. Predlaže se instalacija različitih verzija protokola na usmjernike i u slučaju ranjivosti na jednoj verziji sustav za praćenje stanja usmjernika automatski u

uporabu stavlja stariju verziju protokola koji nema iste ranjivosti. Ovime bi se izgubile funkcionalnosti koje donose novije verzije protokola, ali bi se povećala razina sigurnosti.

Nedostatak ovakve zaštite mrežnog usmjernika koji se nalazi u IoT okruženju jest to što mrežna oprema, a time u usmjernici, koja omogućuje povezivanje IoT uređaja mora biti prilagodljiva IoT uređajima. Različiti IoT uređaji funkcioniraju na različitim protokolima, jer IoT kao pojam ne definira točan način komunikacije i protokole koji se koriste. Na taj način proizvođači imaju potpunu slobodu proizvoditi IoT uređaje ovisno o potrebama tržišta, ali dolazi do problema interoperabilnosti između različitih verzija istih IoT uređaja. U slučaju u kojemu su mrežni usmjernici prilagodljivi na temelju protokola po pitanju sigurnosti i zaštite mreže može doći do prekida rada određenih ili svih IoT uređaja ako se promijeni mrežni protokol na verziju koja ne sadržava funkcionalnost koju oni koriste.

Niti jedan od navedenih prijedloga ne koristi metodu sigurnosti i zaštite u dubinu, gdje će u slučaju narušavanja sigurnosti jednog sloja ostali slojevi i dalje pružati dostatnu razinu zaštite IoT okruženju gdje IoT uređajima neće biti prekinuta dostupnost ili iskorišteni za DoS napad na treće strane. U svakom prijedlogu kod narušavanja ili zaobilaženja predloženog načina zaštite ostatak lokalne mreže ostaje zaštićen samo onim metodama zaštite koje su već implementirane u mrežni usmjernik, a koje nisu dostatne što je demonstrirano u prošlom poglavlju.

5.3. Prijedlog zaštite usmjernika u IoT okruženju

U analizi u četvrtom poglavlju svi napadi i analiza ranjivosti na mrežnim usmjernicima su bili provedeni na lokalnoj mreži. Iako mrežni usmjernici moraju biti u mogućnosti usmjeravati sav mrežni promet prema odredištu također moraju imati implementiranu mogućnost filtracije paketa s ciljem povećanja razine sigurnosti ako je sam mrežni usmjernik odredište. Mrežni usmjernik mora odbacivati pakete ako odgovor na njih može otkriti verziju operativnih sustava uređaja ili verziju aplikacije koja je pokrenuta na usmjerniku. Time mrežni usmjernik treba onemogućiti prikupljanje informacija o unutarnjem radu uređaja bez obzira dolaze li paketi s lokalne ili vanjske mreže.

Niti jedan od tri uređaja, Asus RT-N12E, D-Link DIR-600 i TP-Link WR741ND nemaju implementiran HTTPS protokol za pristup web administrativnom sučelju. Kako nije implementiran HTTPS napadač s lokalne mreže je u stanju presresti komunikaciju i dohvatiti korisničko ime i lozinku za prijavu u web sučelje. Nakon presretanja korisničkog imena i lozinke administratora napadač će biti u stanju promijeniti sve postavke usmjernika, od konfiguracije mreže, DNS postavki do promjene *firmware*-a uređaja. Implementacijom HTTPS protokola u web sučelje mrežnog usmjernika MITM napad s lokalne mreže postaje otežan za napadača u usporedbi s HTTP protokolom. U prilagodljivom IoT okruženju, koje svakodnevno mijenja broj i vrstu IoT uređaja te ponašanje, mrežni usmjernik će te IoT uređaje morati smatrati potencijalnim prijetnjama jer maliciozni IoT uređaji mogu biti instalirani od strane napadača u IoT okruženje.

Sva tri uređaja iz četvrtog poglavlja nisu podržavala automatsku nadogradnju vlastitog *firmware*-a. Za nadogradnju *firmware*-a svaki uređaj ima opciju u web sučelju koja pokreće nadogradnju, ali prije toga se *firmware* mora ručno preuzeti na uređaj kojemu se pristupa web sučelju kako bi se na mrežni usmjernik ta verzija mogla učitati. Pri ovom postupku sam *firmware* nije zaštićen ključem i također web stranice proizvođača s kojih se

preuzima nemaju mogućnost verifikacije preuzete datoteke *firmware*-a. Tako pri preuzimanju web sučelja napadač je u stanju učitati prilagođeni *firmware* na mrežni usmjernik. Implementacijom kriptografski potpisanih datoteka koje je mrežni usmjernik u stanju automatski preuzeti s web stranica proizvođača se ova ranjivost može zaobići. Krajnjem korisniku se i dalje može pružiti opcija da ručno učita *firmware*, ali datoteka u kojoj se nalazi mora biti kriptografski zaštićena čime čak i pri preuzimanju kontrole od strane napadača napadač neće biti u mogućnosti učitati svoj prilagođeni *firmware.* Automatskom nadogradnjom *firmware*-a se izbjegava zastarjelost i uklanjanje ranjivosti uređaja bez interakcije s korisnikom.

Najnovija verzija Linux kernela koja je pronađena na usmjernicima u četvrtom poglavlju je bila 2.6.36. koja je prema službenoj e-mail listi Linux programera puštena u uporabu za široku javnost u veljači 2011. godine. Mrežni smjernici s tvorničkim postavkama koriste zastarjele verzije Linux kernele, same jezgre operativnog sustava. Zastarjele verzije svih operativnih sustava postanu ranjive jer se ranjivosti uklanjaju programskim kodom koji dolazi s idućom verzijom. Navedena verzija Linux kernela sadrži preko 50 otkrivenih ranjivosti od kojih najmanje 10 kritičnih. Osim *firmware*-a mrežni usmjernici moraju imati i mogućnost nadogradnje verzije Linux kernela s najmanjom opcijom instalacije koja uključuje samo sigurnosne zakrpe. Ako jezgra operativnog sustava na kojoj se pokreću aplikacije nije sigurna onda se niti jedna aplikacija ne može smatrati sigurnom, [50], [51].

Nakon proizvodnog procesa mrežnog usmjernika UART sučelje na tiskanoj pločici uređaja mora biti onesposobljeno kako bi se onemogućila analiza unutarnje programske strukture usmjernika. Takve informacije napadaču povećavaju površinu za napad jer mu pomažu naći veći broj ranjivosti koje se možda nalaze unutar mrežnog usmjernika. Osim toga moguće je pomoću UART sučelja vršiti direktnu kontrolu nad mrežnim usmjernikom. Napadač je u mogućnosti na taj način instalirati stalne promjene koje bi komprimirale IoT okruženje čak i u slučaju povratka na tvorničke postavke.

Osim zaštite samo mrežnog usmjernika unutar IoT okruženja je potrebno uspostaviti zaštitu s više slojeva koja će u slučaju probijanja zaštite jednog sloja i dalje biti u mogućnosti održavati sigurnost na istoj razini. U slučaju preuzimanja kontrole nad mrežnim usmjernikom od strane napadača s lokalne mreže IoT okruženje mora biti u stanju i dalje koristiti sigurnu komunikaciju s odredištem bez obzira na to što se sama komunikacija vrši preko malicioznog usmjernika. To se može postići implementacijom sigurne komunikacije potpisane kriptografskim ključem koja će biti zaštićena od kraja do kraja. Na taj način maliciozni mrežni usmjernik neće biti u mogućnosti izmjenjivati komunikacijske poruke na uspješan način. Osim toga sam mrežni usmjernik se ne smije koristiti kao DNS poslužitelj, već unutar IoT okruženja IoT uređaji moraju imati unaprijed podešene adrese javnih DNS poslužitelja koje će koristiti, a koji se ne nalaze na lokalnoj mreži. Time će se izbjeći preusmjeravanje na krivi DNS poslužitelj od strane napadača čime se promet iz IoT okruženja može koristiti za DoS napada na treću lokaciju.

Zaštita *firmware*-a mora pretpostavljati korisnika koji na nesiguran način koristi mrežni usmjernik. Oko te pretpostavke moraju biti podignute zaštite na samom usmjerniku i napravljena procjena rizika. Ako se mrežni usmjernici zaštite oko pretpostavke da korisnik neće poduzeti nikakve štetne radnje, namjerno ili nenamjerno, sigurnost mrežnog usmjernika, a time i mreže koju poslužuje postaje ugrožena otvaranjem maliciozne

poveznice od strane korisnika. Ovakav način zaštite, koji podrazumijeva najgore scenarije, također ne zahtijeva dodatna ulaganja u edukaciju korisnika o sigurnosti korištenja mrežne

Sve većim korištenjem IoT uređaja u svakodnevnom životu i očekivanim porastom IoT uređaja u uporabi od strane rezidencijalnih korisnika kućanstva se postepeno pretvaraju u IoT okruženja. Rezidencijalni korisnici nisu si u mogućnosti priuštiti naprednu mrežnu opremu koja ima veliku razinu zaštite. S porastom broja IoT uređaja u lokalnoj mreži takvi korisnici, ali i mali poslovni korisnici će imati potrebu za većim brojem mrežnih usmjernika. Prilikom širenja mreže IoT uređajima mrežni usmjernici tipa kao mrežni usmjernici testirani u četvrtom poglavlju će im zadovoljavati sve potrebe za njihov rad. Kako bi se spriječilo stvaranje IoT okruženja koja su pod kontrolom malicioznih čimbenika potrebno je dodatno povećati razinu zaštite takvih okruženja mjerama koja su navedena u ovom potpoglavlju.

6. ZAKLJUČAK

S velikim porastom broja IoT uređaja koji se očekuje u narednih par godina veliki broj IoT uređaja se očekuje kod rezidencijalnih korisnika. S takvom promjenom lokalne mreže komercijalnih korisnika postaju IoT okruženja. Novi uređaji unutar lokalne mreže komercijalnog korisnika neće promijeniti njegove sigurnosne prakse i razina sigurnosti takvih IoT okruženja će biti na razini rezidencijalne lokalne mreže. Takva IoT okruženja će postati potencijalni resurs za napadače koji će htjeti IoT uređaje staviti pod svoju kontrolu kako bih ih mogli koristiti za daljnje napada na treće lokacije ili kao resurs s računalnom snagom.

Porastom broja IoT uređaja u lokalnoj mreži pojaviti će se potreba komercijalnih korisnika za većim brojem mrežnih usmjernika koji će povezati IoT uređaje koristeći Wi-Fi mreže. Ti mrežni usmjernici će se zbog svoje uloge umrežavanja IoT uređaja postati meta napada jer stavljanjem mrežnog usmjernika pod svoju kontrolu napadač neće morati tražiti pojedinačne ranjivosti u različitim IoT uređajima koji čine lokalnu mrežu. S obzirom na mogućnosti rezidencijalnog korisnika većina mrežnih usmjernika koji će biti u rezidencijalnoj lokalnoj mreži će biti za komercijalnu širu uporabu i potencijalni napadači će moći analizirati ranjivosti koje će oni sadržavati pomoću fizičkog sučelja mrežnog usmjernika.

U četvrtom poglavlju ovoga rada su tri mrežna usmjernika, Asus RT-N12E, D-Link DIR-600 i TP-Link WR741ND, bila analizirana u potrazi za ranjivostima. Sva tri usmjernika nisu uspjeli pružiti adekvatnu zaštitu lokalne mreže na kojoj su se nalazili. Kod sva tri usmjernika u slučaju proboja jedne vrste zaštite usmjernik je odmah pao pod kontrolu napadača. U IoT okruženju kontrola usmjernika jamči napadaču kontrolu prometa lokalne mrežom i time generiranog prometa svih IoT uređaja u toj mreži.

Kako bi se izbjegao scenarij gdje lokalne mreže rezidencijalnih korisnika sa svojim IoT uređajima postaju resurs u rukama raznih malicioznih čimbenika potrebno je osim pojedinačne zaštite IoT uređaja zaštiti mrežne usmjernike koji će se nalaziti u rezidencijalnim mrežama. Potrebno je uvesti HTTPS na web sučelju, ne otkrivati informacije o radu mrežnog usmjernika na njegovim portovima te je potrebno uvesti automatske nadogradnje *firmware*-a koje moraju biti potpisane kriptografskim ključem kako bi se izbjeglo njihovo krivotvorenje. Uz sve te mjere potrebno je onemogućiti pristup serijskim ulazima na tiskanoj pločici mrežnog usmjernika jer napadač preko takvih ulaza može dobiti bolji uvid u rad samog usmjernika i time može pronaći potencijalne ranjivosti koje bi inače ostale neotkrivene.

Uz navedene mjere pri porastu IoT uređaja u svakodnevnom životu lokalne mreže rezidencijalnih korisnika će imati povećanu razinu zaštite od one koje je sada na mrežnim usmjernicima aktivna. Time će preuzimanje kontrole nad prometom takvog IoT okruženja zahtijevati povećani napor od strane malicioznih čimbenika i u najboljem slučaju ih može odvratiti od takvog postupka te ograničiti prouzrokovanu štetu uspješnim preuzimanjem kontrole usmjernika. Kako se prema predviđanjima najveći porast IoT uređaja očekuje poslije 2020. godine tada se može očekivati najveći broj pojava IoT okruženja u lokalnim mrežama rezidencijalnih korisnika gdje će onda mjere zaštite mrežnih usmjernika biti testirane u stvarnom IoT okruženju.

LITERATURA

[1] Bruno Dorsemaine, Jean-Philippe Gaulier, Jean-Philippe Wary, Nizar Kheir, Pascal Urien, "A New Threat Assessment Method for Integrating an IoT Infrastructure in an Information System", *Distributed Computing Systems Workshops (ICDCSW) 2017 IEEE 37th International Conference on*, pp. 105-112, 2017

[2] https://www.statista.com/topics/2286/cisco/ (Pristupljeno: kolovoz 2018)

[3] C. Kolias, G. Kambourakis, A. Stavrou and J. Voas, "DDoS in the IoT: Mirai and Other Botnets," in *Computer*, vol. 50, no. 7, pp. 80-84, 2017

[4] https://www.gartner.com/newsroom/id/3869181 (Pristupljeno: kolovoz 2018)

[5]https://www.signify.com/global/about/news/press-release-archive/2018/20180319-philips-lighting-underlines-leadership-in-lighting-for-the-internet-of-things-with-new-iot-platform (Pristupljeno: kolovoz 2018)

[6] https://www.agilealliance.org/agile101/ (Pristupljeno: kolovoz 2018)

[7] Spyridon Samonas, David Coss, „The CIA Strikes Back: Redefining Confidentiality, Integrity and Availability in Security“, *Journal of Information System Security Volume 10, Number 3 (2014), pp. 21–45*, ISSN 1551-0123

[8] *ISACA (2006). CISA Review Manual 2006. Information Systems Audit and Control Association. p. 85. ISBN 1-933284-15-3*

[9] ISO/IEC, „Information technology - Security techniques - Information security management systems - Overview and vocabulary“ ISO/IEC 27000:2018

[10] ISO/IEC, „Information technology - Security techniques - Information security risk management“ ISO/IEC 27005:2018

[11] Andress, J. (2014). *The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice*. Syngress. Chapter I

[12] *Kakareka, A. (2013). "Chapter 31: What is Vulnerability Assessment?", In Vacca, J.R. Computer and Information Security Handbook (2nd ed.), Elsevier. pp. 541–552. ISBN 9780123946126*

[13] *Bayuk, J. (2009). "Chapter 4: Information Classification". In Axelrod, C.W.; Bayuk, J.L.; Schutzer, D. Enterprise Information Security and Privacy. Artech House. pp. 59–70. ISBN 9781596931916*

[14]https://www.businessinsider.com/internet-of-things-survey-and-statistics-2015-1 (Pristupljeno: kolovoz 2018)

[15] https://www.iotsecurityfoundation.org/about-us/ (Pristupljeno: kolovoz 2018)

[16]https://www.iotsecurityfoundation.org/wp-content/uploads/2017/12/IoT-Security-Compliance-Framework_WG1_2017.pdf (Pristupljeno: kolovoz 2018)

[17] K. Ghirardello, C. Maple, D. Ng and P. Kearney, "Cyber security of smart homes: Development of a reference architecture for attack surface analysis," *Living in the Internet of Things: Cybersecurity of the IoT - 2018*, London, 2018, pp. 1-10

[18] https://blog.cloudflare.com/iot-security-anti-patterns/ (Pristupljeno: kolovoz 2018)

[19] C. Sha and Z. Lin, "Design Optimization and Implementation of Bootloader in Embedded System Development," *2015 International Conference on Computer Science and Applications (CSA)*, Wuhan, 2015, pp. 151-156

[20] https://tools.kali.org/exploitation-tools/routersploit (Pristupljeno: kolovoz 2018)

[21] U. Nanda and S. K. Pattnaik, "Universal Asynchronous Receiver and Transmitter (UART)," *2016 3rd International Conference on Advanced Computing and Communication Systems (ICACCS)*, Coimbatore, 2016, pp. 1-5

[22] https://tools.kali.org/web-applications/dirbuster (Pristupljeno: kolovoz 2018)

[23] https://httpstatuses.com/ (Pristupljeno: kolovoz 2018)

[24] https://tools.kali.org/information-gathering/nmap (Pristupljeno: kolovoz 2018)

[25] https://tools.kali.org/web-applications/burpsuite(Pristupljeno: kolovoz 2018)

[26] IEEE Standard Test Access Port and Boundary - Scan Architecture," *in IEEE Std 1149.1-1990* , vol., no., pp.0_1-, 1990

[27] C. Anley, J. Heasman, F. Linder, G. Richarte: *The Shellcoder's Handbook, Second Edition: Discovering and Exploiting Security Holes*, Wiley Publishing, Inc., 2007., Part I-Chapter 3

[28] https://www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016 (Pristupljeno: kolovoz 2018)

[29] http://www.oissg.org/files/issaf0.2.1.pdf (Pristupljeno: kolovoz 2018)

[30]https://www.asus.com/Networking/RT-N12E-C1/HelpDesk_BIOS/ (Pristupljeno: kolovoz 2018)

[31] https://nvd.nist.gov/vuln/detail/CVE-2017-5892 (Pristupljeno: kolovoz 2018)

[32] https://www.exploit-db.com/exploits/24453/ (Pristupljeno: kolovoz 2018)

[33]https://websec.ca/publication/advisories/path-traversal-vulnerability-tplink-wdr740 (Pristupljeno: kolovoz 2018)

[34] https://tools.kali.org/password-attacks/john (Pristupljeno: kolovoz 2018)

[35] https://www.exploit-db.com/exploits/38483/ (Pristupljeno: kolovoz 2018)

[36] https://www.cvedetails.com/cve/CVE-2017-14250/ (Pristupljeno: rujan 2018)

[37] https://www.shodan.io/report/6Zm1wzVm (Pristupljeno: rujan 2018)

[38] https://www.shodan.io/report/OeE2cPN3 (Pristupljeno: rujan 2018)

[39] https://www.shodan.io/report/pEcZHM0U (Pristupljeno: rujan 2018)

[40] A. Stasinopoulos, C. Ntantogian and C. Xenakis, "The weakest link on the network: Exploiting ADSL routers to perform cyber-attacks," *IEEE International Symposium on Signal Processing and Information Technology*, Athens, 2013, pp. 000135-000139.

[41] F. Li, L. Zhang and D. Chen, "Vulnerability mining of Cisco router based on fuzzing," *The 2014 2nd International Conference on Systems and Informatics (ICSAI 2014)*, Shanghai, 2014, pp. 649-653.

[42] S. Esnaashari, I. Welch and P. Komisarczuk, "Determining Home Users' Vulnerability to Universal Plug and Play (UPnP) Attacks," *2013 27th International Conference on Advanced Information Networking and Applications Workshops*, Barcelona, 2013, pp. 725-729.

[43] Haining Wang and K. G. Shin, "Transport-aware IP routers: a built-in protection mechanism to counter DDoS attacks," *in IEEE Transactions on Parallel and Distributed Systems*, vol. 14, no. 9, pp. 873-884, Sept. 2003.

[44] M. Polivka, V. Oujezsky and V. Skorpil, "Modem network vulnerabilities and security testing - Actual threats," *2015 38th International Conference on Telecommunications and Signal Processing (TSP)*, Prague, 2015, pp. 33-36.

[45] P. Poornachandran, R. Sreeram, M. R. Krishnan, S. Pal, A. U. P. Sankar and A. Ashok, "Internet of Vulnerable Things (IoVT): Detecting Vulnerable SOHO Routers," *2015 International Conference on Information Technology (ICIT)*, Bhubaneswar, 2015, pp. 119-123.

[46] G. B. Peterside, P. Zavarsky and S. Butakov, "Automated security configuration checklist for a cisco IPsec VPN router using SCAP 1.2," *2015 10th International Conference for Internet Technology and Secured Transactions (ICITST)*, London, 2015, pp. 355-360.

[47] A. More and S. Tapaswi, "A software router based predictive honeypot roaming scheme for network security and attack analysis," *2013 9th International Conference on Innovations in Information Technology (IIT)*, Abu Dhabi, 2013, pp. 221-226.

[48] B. Silverajan, M. Vajaranta and A. Kolehmainen, "Home Network Security: Modelling Power Consumption to Detect and Prevent Attacks on Homenet Routers," *2016 11th Asia Joint Conference on Information Security (AsiaJCIS)*, Fukuoka, 2016, pp. 9-16.

[49] C. Mansour, Y. E. H. Shehadeh and D. Chasaki, "Design of an adaptive security mechanism for modern routers," *2015 IEEE International Conference on Consumer Electronics (ICCE)*, Las Vegas, NV, 2015, pp. 241-244.

[50] http://lkml.iu.edu/hypermail/linux/kernel/1102.2/01003.html (Pristupljeno: Pristupljeno: rujan 2018)

[51] https://www.cvedetails.com/vulnerability-list/vendor_id-33/product_id-47/version_id-123837/Linux-Linux-Kernel-2.6.36.html (Pristupljeno: Pristupljeno: rujan 2018)

POPIS KRATICA

IoT (Internet of Things) Internet stvari

SaaS (Software as a Service) *softver* kao usluga

DDoS (Distributed Denial of Service) distribuirani prekid usluge

IK informacijsko-komunikacijski sustav

UART (Universal Asynchronous Receiver-Transmitter) univerzalni asinkroni prijamnik-predajnik

HTTP (Hyper Text Transport Protocol) hiper-tekstualni transportni protokol

URL (Uniform Resuorce Locator) uniformni lokator resursa

TCP (Transmission Control Protocol) protokola za kontrolu transmisije

UDP (User Datagram Protocol) protokola korisničkih datagrama

JTAG (Joint Test Action Group) zajednička grupa za testiranje

ISSAF (Information Systems Security Assessment Framework) okvir za sigurnosnu procjenu informacijskih sustava

MITM (Man In The Middle attack) napad s napadačem u sredini komunikacije

DNS (Domain Name System) sustav za imenovanje domena

UPnP (Universal Plug & Play) univerzalni uključi i pokreni protokol

ADSL (Asymmetric digital subscriber line) asimetrična digitalna pretplatnička linija

SFTCG (Semi-valid Fuzzing Test Case Generator) *fuzzing* generator polu-validnih testnih slučajeva

ICMP (Internet Control Messsage Protocol) Internet protokol za kontrolu poruka

SCAP (Security Content Automation Protocol) protokol za automatizaciju sigurnosnog sadržaja

POPIS SLIKA

POPIS TABLICA

Sveučilište u Zagrebu
Fakultet prometnih znanosti
10000 Zagreb
Vukelićeva 4

IZJAVA O AKADEMSKOJ ČESTITOSTI I SUGLASNOST

Izjavljujem i svojim potpisom potvrđujem kako je ovaj diplomski rad isključivo rezultat mog vlastitog rada koji se temelji na mojim istraživanjima i oslanja se na objavljenu literaturu što pokazuju korištene bilješke i bibliografija.

Izjavljujem kako nijedan dio rada nije napisan na nedozvoljen način, niti je prepisan iz necitiranog rada, te nijedan dio rada ne krši bilo čija autorska prava.

Izjavljujem također, kako nijedan dio rada nije iskorišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

Svojim potpisom potvrđujem i dajem suglasnost za javnu objavu diplomskog rada pod naslovom **ANALIZA RANJIVOSTI MREŽNIH USMJERNIKA U IoT OKRUŽENJU**

na internetskim stranicama i repozitoriju Fakulteta prometnih znanosti, Digitalnom akademskom repozitoriju (DAR) pri Nacionalnoj i sveučilišnoj knjižnici u Zagrebu.

U Zagrebu, 14.9.2018

Student/ica:
Luka Brletić
(potpis)